BROCADE

AT-A-GLANCE

# Secure Data Communications Between Enterprise Data Centers

## HIGHLIGHTS

- Enables cost-effective pervasive network encryption for sensitive traffic within the campus and data centers
- Provides hardware-based inline encryption that ensures wire-speed data security without compromising performance or complicating deployment
- Eliminates the need for—and costs of—dedicated appliances by simply and securely connecting workloads within the network
- Provides support for industry-standard IP security (IPsec) Suite B end-to-end that ensures regulatory compliance and protects data in transit
- Offers industry-standard MAC security (MACsec) support that ensures data security and provides flexible policy application on a private network

## Pervasive Data Security for Data Centers

For enterprises looking to create truly secure campus and data center networks, ensuring data security is at the forefront of their priorities. Organizations are challenged to implement the security policies and controls necessary to mitigate the legal, regulatory, and financial risks associated with data theft. Loss of organization or customer data brings potential impact to customer retention and corporate reputation. In fact, of the organizations that have experienced a security breach, 74 percent reported a loss of customers, 59 percent faced potential litigation, and 32 percent experienced a decline in share value.[1] With the explosion of volume and variety of data in digital form, enterprise networks are, more than ever, the target of unscrupulous individuals and groups.

In order to protect data from theft, networks must meet security requirements, compliance standards, and the expectations of partners and customers who share sensitive information. As organizations increasingly move data to the cloud, new challenges arise when ensuring data security for all types of data.

### Scalable Network Encryption Is Required

As the number of devices connecting to the networks proliferates, the network natively needs to ensure the security of the data that traverses it. To protect against espionage or data theft, encryption of data-at-rest and data-in-flight should be deployed as complements of one another. Network-based encryption is an important method of obscuring the underlying individual application and user flows (which may be encrypted themselves as well). Data security cannot be taken for granted, even on private networks. With the massive increase in digital data, encryption is no longer a luxury that can be reserved for only a few links, applications, or flows. There is a pervasive need for increased encryption services network-wide.

[1] Survey, Scott & Scott, 2014.

Yet, while encryption provides significant data protection, deploying encryption on the network has not traditionally proven to be a straightforward process. Added complexity, high CapEx and OpEx costs, and reduced performance are a few of the resultant concerns. The current market is fragmented with solution infrastructures that do not provide the ability to support a high level of encryption at scale. With server application and end-user service-level expectations, enterprises cannot afford to have encryption degrade network performance. With the constant requirement of increasing data volume, encryption scale is critical. Because of this, encryption has typically been applied only when absolutely required or where performance was not a priority. New solutions are needed to help organizations better encrypt their data as part of a larger security strategy, without impacting the performance, and that provide operational ease along with the cost profile needed for widespread deployment.

## Data Security and Network Performance Are Not Mutually Exclusive

With an increasing focus around data security, the ability to encrypt more traffic across campus and data center networks is becoming a higher priority. However, legacy solutions cannot support today's business demands. A new model is needed, one that supports scale-out, hardware-based encryption for campus and data center networks that need a robust, low-cost, and flexible solution to support Virtual Private Network (VPN) connections.

The Brocade® data security solution provides such a model, challenging the commonly held beliefs that ensuring data security in the network is costly and complex, network performance must be compromised, and deployment can occur only on a limited scale. Enterprises can now more easily deploy an end-to-end encryption solution using a robust, standards-based encryption that is built into physical or virtual networking hardware. Brocade solutions provide both hardware-based IPsec[2] and MACsec[3]. These in-flight solutions deliver wire-speed encrypted performance up to 800 Gbps in a single device, ensuring security for all data on all links.

The Brocade solution is a combination of the Brocade MLXe Enterprise Switch with the Brocade ICX® Switch for applications in both campus networks and data centers. These applications support industry-standard IPsec and MACsec encryption and integrate with existing key management and Certificate Authority (CA) configurations, enabling end-to-end deployments that support a variety of data security and security needs. IPsec provides a cost-effective, scalable solution for environments that need a secure, economical, and proven way to connect data centers, remote sites, employees, and business partners to networked systems and applications across any IP network where the physical network is not under their control.

The Brocade ICX 7450 Switch with service module for IPsec extends traditional site-to-site IPsec encryption to encryption from the wiring closet, enabling data security within the campus and end-to-end network encryption across premises. MACsec, on the other hand, proves to be ideal for fast, low-latency, and easy-to-deploy encryption within the campus where the physical network resides. IPsec provides an additional benefit to the campus by enabling policy application to network traffic as it traverses the campus network.

## Key Benefits and Differentiation

The Brocade solution is unique in its ability to apply encryption within the switch without incurring a performance "tax." Inline hardware-based encryption in physical platforms ensures data security without compromising performance or complicating deployment.

This comprehensive solution delivers up to five times the performance of existing solutions, without the need for additional licenses, or offloading to expensive security or encryption appliances.

The MACsec encryption within the 20×10 GbE module for the Brocade MLXe Enterprise Switch is ideal for traffic between campus networks. The module leverages the Brocade VersaScale™ processor—the innovative programmable architecture of the Brocade MLXe Enterprise Switches—to extend traditional Layer 2 switching capabilities to include 128-bit AES encryption provided by MACsec. With 200 gigabits per second (Gbps) throughput per module, a single Brocade MLXe chassis can support over 1.6 Tbps of MACsec traffic at wire speed—an industry first. This capability is ideal to ensure that service levels are not impacted in even the largest campus networks while increasing operational efficiencies and maximizing investment protection.

The IPsec module for the Brocade MLXe Enterprise Switches is ideal for traffic between data centers and within campus networks. The module leverages the Brocade VersaScale™ processor—the innovative programmable architecture of the Brocade MLXe Enterprise Switches—

[2] The IPsec Suite B profile is based on RFC 6380 with a cryptographic suite based on RFC 6379.

[3] MACsec support is based on the IEEE 802.1ae 2011 revision.

to extend traditional Layer 2 switching capabilities to include encryption with Suite B algorithms and support for 256-bit Advanced Encryption Standard (AES) keys provided by IPsec or for 128-bit AES provided by MACsec. With 44 Gigabits per second (Gbps) throughput per module, a single Brocade MLXe chassis can support over 352 Gbps of IPsec traffic at wire speed—an industry first. This capability ensures that service levels are not impacted in even the largest data center while increasing operational efficiencies and maximizing investment protection.

The Brocade MLXe Enterprise Switch also supports Software-Defined Networking (SDN) with OpenFlow 1.3 in Brocade Hybrid Port Mode, enabling programmatic control of the network for advanced secure traffic engineering.

## Key Use Cases

### Campus Security through IPsec and MACsec

For organizations with strict compliance and regulatory requirements, ensuring data security is paramount. The IPsec and MACsec modules for the Brocade MLXe Enterprise Switches enable the industry's highest data security at Layer 2. MACsec and IPsec integration with Brocade Ethernet switches—the Brocade ICX 6610 Switch and the Brocade ICX 7450 Switch—enables end-to-end security of data down to the desktop or server without testing, installation, or management of encryption software on desktop or server operating systems.

The Brocade ICX 7450 Switch with the integrated IPsec VPN service module consolidates network switching and encryption to provide VPN deployment flexibility and cost savings within the campus and across premises. By initiating an IPsec tunnel from the Brocade ICX 7450 for transporting selected traffic, organizations save the time and reduce the costs from having to install and manage encryption software on individual computers or deploy purpose-built encryption appliances. This simplifies data security and eliminates evasive measures by users.

### Data Center Applications through IPsec

Many organizations have built out a multitude of data center applications to meet the needs of greater automation and the explosive growth of mobility and social media. At the same time, many IT organizations have added separate data centers to meet computing demand and ensure reliability. While the interconnect is provided by a trusted partner, data is traveling over a shared infrastructure and is therefore potentially susceptible to theft. The Brocade MLXe Series of Enterprise Switches with IPsec encryption enables Layer 2 traffic transmission to be unimpeded between data centers, to mitigate the risk of data theft.

## Conclusion

Brocade delivers a comprehensive solution to enable cost-effective pervasive network encryption at wire speed. The solution not only secures sensitive traffic between campus and data center environments, but it does so at a fraction of the cost of traditional switch security service modules. With the highest encryption standards available natively in the network to protect internal and customer data at scale, Brocade supports compliance initiatives and strengthens data security without degrading the performance of the network or the user experience.

The combination of IPsec and MACsec offers an ideal solution for enterprises challenged to support compliance initiatives and strengthen data security, without impacting the network performance. IPsec provides encryption for data cloaking on networks that are vulnerable to snooping, ensuring information integrity and protection. MACsec and IPsec encryption and visibility on campus networks provides great flexibility, securing against denial-of-service attacks, identifying malevolent users within the network, and applying policy for specific application needs. Additionally, because IPsec integration on the Brocade MLXe Enterprise Switch and the Brocade ICX 7450 Switch supports 256-bit AES encryption, it can easily be applied within environments requiring encryption stronger than the 128-bit encryption provided by MACsec Encrypting and decrypting with wirespeed performance allows for zero impact to the user's experience and mitigates the need for additional encryption appliances.

## About Brocade

Brocade networking solutions help organizations achieve their critical business initiatives as they transition to a world where applications and information reside anywhere. Today, Brocade is extending its proven data center expertise across the entire network with open, virtual, and efficient solutions built for consolidation, virtualization, and cloud computing. Learn more at www.brocade.com.

**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

© 2016 Brocade Communications Systems, Inc. All Rights Reserved. 05/16 GA-AG-513-01

Brocade, Brocade Assurance, the B-wing symbol, ClearLink, DCX, Fabric OS, HyperEdge, ICX, MLX, MyBrocade, OpenScript, VCS, VDX, Vplane, and Vyatta are registered trademarks, and Fabric Vision is a trademark of Brocade Communications Systems, Inc., in the United States and/or in other countries. Other brands, products, or service names mentioned may be trademarks of others.

Notice: This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered or to be offered by Brocade. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use. This informational document describes features that may not be currently available. Contact a Brocade sales office for information on feature and product availability. Export of technical data contained in this document may require an export license from the United States government.