BROCADE

AT-A-GLANCE

Secure Data Communications for Enterprise Networks

HIGHLIGHTS

- The comprehensive solution enables cost-effective pervasive network encryption to secure sensitive traffic between campus, data center, and hybrid cloud environments.
- Hardware-based inline encryption ensures data confidentiality without performance compromise or complex deployment.
- Connecting workloads within the network simply and securely at wire speed eliminates the need for—and costs of—dedicated appliances.
- Support for industry-standard IP security (IPsec) Suite B end-to-end helps ensure regulatory compliance and protects data in transit.
- Industry-standard MAC security (MACsec) ensures data confidentiality and provides flexible policy application on a private network.

Pervasive Data Security Between Sites

For enterprises sending business-critical data between sites, ensuring data security is at the forefront of concerns and needs. Organizations are challenged to implement security policies and controls necessary to mitigate the legal, regulatory, and financial risks associated with data theft. Loss of organization or customer data can potentially affect 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, which must be guarded against.

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 and confidentiality for all types of data.

A New Kind of Network Encryption is Required

As the cloud becomes the new LAN, and with networks an integral enabler of the cloud, the network increasingly needs to know about—and ensure the integrity of—the data that traverses it. To protect against data breaches, encryption of data-at-rest and data-in-flight is the gold standard and should be deployed as complements of one another. Network-based encryption

is an increasingly important means of ensuring data privacy, obscuring the underlying individual application and user flows (which may themselves be encrypted as well). Data privacy 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 traditionally has not proved 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 a constant requirement to increase data volume, encryption scale is critical. As such, encryption has typically been applied only when absolutely required or where performance was not a priority. New solutions are needed that 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 Privacy and Network Performance are Not Mutually Exclusive

With an increasing focus around data security and integrity, the ability to encrypt more traffic across the network and in the cloud becomes a priority. However, a new model is needed, one that supports scale-out site-to-site encryption for larger locations that require high-performance, hardware-based encryption, as well as for smaller sites that need a robust, low-cost, flexible solution to support Virtual Private Network (VPN) connection over the Internet.

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 standards-based strong encryption that is built into physical or virtual networking hardware. Brocade solutions provide both hardware-based, site-to-site encryption (using IPsec)[2] and hop-by-hop encryption (using MACsec[3]).

The Brocade solution is comprised of multiple products with applications in:

- Workloads deployed in the cloud or remote offices
- The data center border
- The campus access or aggregation and backbone

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 confidentiality 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 solution extends traditional site-to-site IPsec encryption to encryption from the wiring closet, enabling end-to-end network encryption across premises.

MACsec, on the other hand, proves to be ideal for fast, low-latency, easy-to-deploy encryption within the campus where the physical network is owned. MACsec provides the additional benefit of enabling policy application to network traffic at the switch or router as it traverses the campus network.

Key Benefits and Differentiation

The Brocade solution is unique, because applying encryption within the router and the switch no longer results in a performance "tax." Inline hardware-based encryption in physical platforms ensures data confidentiality without performance compromise or complex deployment.

This comprehensive solution provides encryption from the wiring closet in the campus, to data centers and cloud deployments, delivering up to four times the performance of existing solutions, without the need for additional licenses or offloading to expensive security or encryption appliances.

The IPsec module for Brocade MLXe Series Core Routers is ideal for off-net traffic between central sites and data centers, as well as on-net traffic within the campus. The module leverages the Brocade VersaScale™ processor—the innovative programmable architecture of the Brocade MLXe routers—to extend traditional Layer 2 (L2) and Layer 3 (L3) routing 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 1 Tbps of IPsec traffic at wire speed—an industry

[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.

first. This capability is ideal to ensure that service levels are not impacted in even the largest data center and cloud networks, while increasing operational efficiencies and maximizing investment protection for the core or border router. Brocade MLXe routers also support Software-Defined Networking (SDN) with OpenFlow 1.3 in Brocade Hybrid Port Mode,[4] enabling a smooth transition to programmatic control of the network for advanced secure traffic engineering.

Key Use Cases

Enterprise Security via IPsec and MACsec

For organizations with strict compliance and regulatory requirements, ensuring data privacy is paramount. The IPsec module with MACsec for Brocade MLXe routers enables data privacy at Layer 2 and Layer 3. MACsec and IPsec integration with Brocade Ethernet switches—the Brocade ICX® 6610 Switch and the Brocade ICX 7450 Switch—enables security of data down to the desktop or server without testing, installation, or management of encryption software on desktop or server operating systems. This simplifies data security and eliminates evasive measures by users, as data encryption does not impede performance.

Secure Data Center Interconnect

Many organizations have built out multiple data centers 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. Brocade MLXe routers with IPsec encryption enable Layer 2 and Layer 3 traffic transmission to be unimpeded between data centers, to mitigate the risk of data theft.

Virtual Private Cloud

With many organizations adopting a hybrid cloud strategy to enable faster and more flexible deployment of applications, ensuring security of data-in-flight between virtual infrastructure on-premise and off-premise is difficult. The IPsec module for Brocade MLXe routers not only enables Layer 2 and Layer 3 traffic transmission unimpeded between on-premise data centers—it also protects data in off-premise virtual data centers by integrating with the Brocade vRouter IPsec VPN solution.

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, data center, and hybrid cloud environments, but it does so at a fraction of the cost of traditional IPsec router service blades and dedicated encryption appliances. 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 when transiting on a publicly owned infrastructure. MACsec encryption and visibility on a customer-owned network 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 on Brocade MLXe routers and the Brocade ICX 7450 supports 256-bit AES encryption, it can easily be applied on-net (on customer-owned network links) for environments requiring encryption stronger than the 128-bit encryption provided by MACsec. Encrypting and decrypting with wire-speed performance allows for zero impact to the user's experience and mitigates the need for additional network devices.

IPsec encryption on the Brocade ICX 7450 with service module ensures high-performance end-to-end encryption from the wiring closet to the data center and cloud deployments. By combining the performance and flexibility of network switching with the advantages of site-to-site IPsec VPN, the Brocade ICX 7450 helps organizations better meet compliance and protect their data. Organizations have the ability to direct traffic into an IPsec tunnel using static routes or with multi-VRF or ACL selection using policy-based routing. With support for Suite B algorithms and 128/256-bit AES, and with 10 Gbps throughput per service module, a single Brocade ICX 7450 Switch or stack helps ensure that end-user service levels are not affected as compliance requirements and security needs across the enterprise increase.

[4] Hybrid Port Mode: A Brocade MLXe router can support OpenFlow and standard protocols simultaneously on a per-interface basis.

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

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.