BROCADE

SOLUTION BRIEF

Brocade Pervasive Data Security

HIGHLIGHTS

- Industry-first end-to-end secure network access from the wiring closet to the data center, and the hybrid cloud
- Unprecedented control and protection of data within the enterprise network, extending to business ecosystems
- Significant capital expenditure savings by reducing layers of dedicated encryption devices and simplifying the security infrastructure
- Flexibility to add IP security (IPsec) Virtual Private Networking (VPN) service where needed and align with the business
- High-performance encryption solution that ensures data security and meets compliance requirements without performance compromise and deployment complexity

Delivering End-to-End Data Confidentiality

Various organizations—including hospitals, banks, and government agencies—often deploy the newest and most sophisticated network security capabilities at headquarters but provide only minimal protection at branch offices. As businesses move to a hybrid architecture and enable access to business partners that are geographically dispersed, they create more exposure to vulnerabilities. The combination of distributed business ecosystems of onsite employees and contractors, partners, and the cloud creates new demand on networks and new challenges for IT professionals who are responsible for ensuring data security and compliance with regulators and enterprise policies while supporting an agile business.

Network connectivity is the foundation for the extended enterprise, linking together company sites, partner businesses, and data centers, as well as the hybrid cloud. The goal of the extended enterprise is to extend collaboration and productivity beyond the physical office, enabling organizations to transition smoothly to a world where information and applications reside anywhere. The key technologies that enable the extended enterprise are VPNs.

Two types of VPNs are essential building blocks for securing the delivery and consumption of business applications across the extended enterprise—site-to-site VPN and remote access VPN.

IPsec VPN is the standard deployment for site-to-site connections. IPsec VPN uses encrypted tunnels across the public Internet for connectivity and protection of the data that traverses it. As organizations build out their business ecosystems and move to the cloud, ensuring pervasive data security at all links of the network becomes more critical when supporting business operations and increasing growth, productivity, and profitability.

For example, in the public sector, the National Association of State Chief Information Officers (NASCIO) in the U.S. identified data security as the top CIO priority highlighting the need to protect personal information. In the

cloud, security consistently ranks as a top concern of C-level executives, underscoring the need to better ensure data security and integrity for both the enterprise and the service provider. For enterprises, the compliance requirements and costs (both financial and reputational) that are associated with identifying and resolving data breaches can impact business success. To protect against data breaches, encryption of data at rest and data in motion is a best practice.

Ensuring Enough Encryption

VPNs that are based on the IPsec protocol suite offer a cost-effective, scalable solution for enterprises seeking to securely connect remote sites, employees, contractors, and partners to the business ecosystem. IPsec provides robust security and encryption functionalities to protect critical data across any IP network. While encryption provides a valuable extra layer of protection against cybercriminals, it traditionally has been difficult to deploy due to interoperability issues, and it comes with high costs and degraded performance. Thus, encryption has typically been applied only when absolutely required or where performance was not a priority.

Given the current risks to security, organizations are showing a heightened interest in securing more data, especially as it moves across the network. The shift to cloud creates challenges for network and IT managers who must facilitate secured delivery of applications to and from the extended edge of corporate networks. Encryption is becoming an increasingly important means of ensuring pervasive data security. However, current infrastructures do not provide the flexibility to support this security strategy at scale. Organizations are seeking to better secure data in their extended enterprise without affecting performance, cost, or operations.

Simplifying the Security Infrastructure

The increasingly distributed nature of today's environment and the pervasiveness of "anytime, anywhere" ways of working are the realities that companies of all sizes face. The growing complexity of extended enterprise operations requires a holistic strategy to provide the network performance, resiliency, and security needed to drive end-user productivity, achieve operational efficiency, and guarantee overall investment protection.

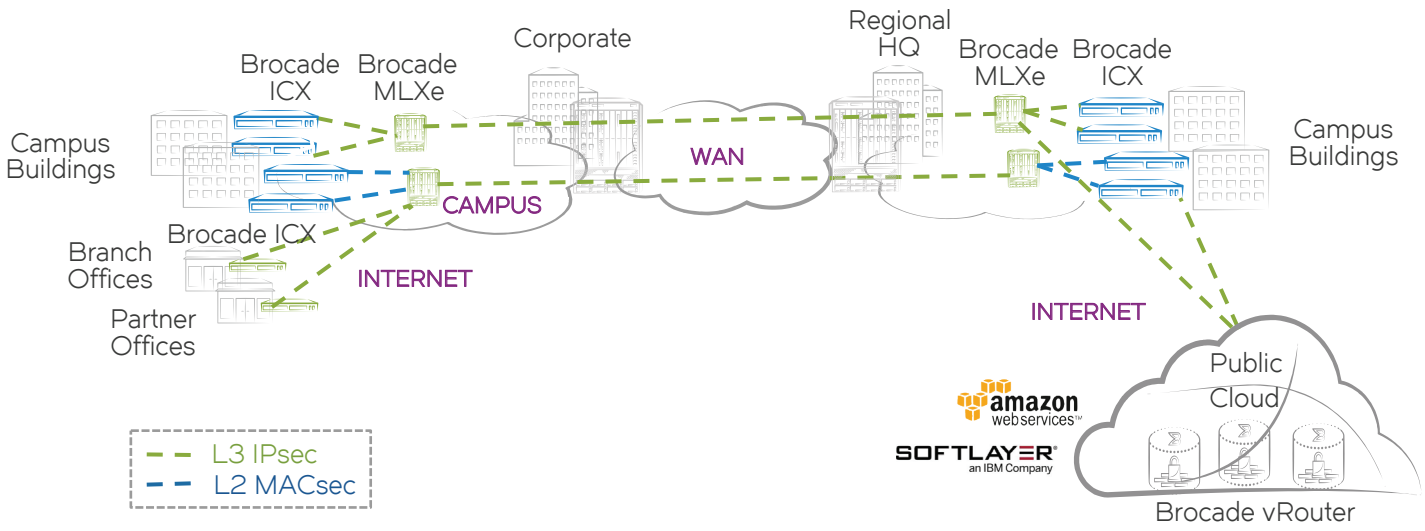

Figure 1: Brocade end-to-end network encryption for data security.

Brocade® pervasive data security solutions challenge the common belief that ensuring data security in the extended enterprise is costly and complex and compromises network performance. Customers can now more easily deploy an end-to-end network encryption solution that is embedded in the physical or virtual switch and router. Using standards-based strong encryption technology, Brocade solutions provide site-to-site encryption (using IPsec), hop-by-hop encryption (using Media Access Control security, or MACsec), and remote access encryption (using SSL) that ensures fast and secure delivery of data on all links.

The Brocade solutions are comprised of multiple products: the Brocade ICX® 7450 Switch, the Brocade MLXe Series Routers, and the Brocade vRouter. The IPsec security capabilities and interoperability of these products offer a wide variety of ways to leverage end-to-end consolidated network and encryption to achieve business outcomes. (See Table 1.)

Data Security within the Campus

The Brocade ICX 7450 with the service module extends traditional site-to-site IPsec VPN encryption to encryption from the wiring closet. This solution consolidates network switching and encryption to provide a cost-effective, scalable way to secure network data as it traverses the enterprise network or the Internet. By initiating an IPsec tunnel from the switch for transporting selected traffic, this solution enables organizations to save time and lower costs, as compared to installing and managing encryption software on individual computers or deploying purpose-built encryption appliances. This provides a valuable extra layer of protection for security-conscious organizations that need the flexibility to deploy VPN more closely aligned with how their business works.

For example, for customers that employ contractors on-site, this solution enables them to provide contractors with secure access to their respective corporate networks without installation or management of encryption software on the contractors' devices. Furthermore, customers have the flexibility to tunnel all traffic from specific ports on the switch to provide path isolation for traffic traversing the same physical network.

In healthcare, the explosion of volume and variety of data in digital form and the constant pressure to comply with regulations and data security policies are creating a pervasive need for increased encryption services network-wide. The

Table 1: Brocade pervasive data security solutions.

Product	Models	Encryption Supported	Models
Brocade ICX Switches	Campus access/aggregation	MACsec	Brocade ICX 6610 Switch Brocade ICX7400-4X10GF
		IPsec	Brocade ICX 7450 Brocade ICX7400-SERVICE-MOD
Brocade MLXe Series Routers	Data center core/border/interconnect	MACsec	Brocade MLXe Series Routers Brocade MLX-10Gx20-M Brocade MLX-10Gx4-IPSEC-M
	Border provider core	IPsec/MACsec	Brocade MLXe Series Routers Brocade MLX-10Gx4-IPSEC-M
Brocade vRouter	Network Function Virtualization (NFV) router for cloud environments	IPsec	Brocade 5600 vRouter

modular design of the Brocade ICX 7450 allows easy deployment of additional ports and services for high-performance security, enabling organizations to scale and deliver data security services faster and more efficiently.

The service module provides hardware-based acceleration for IPsec VPNs, using the Advanced Encryption Standard (AES). The service module leverages programmable hardware technology to future-proof data security, enabling more features to be added to IPsec VPN deployments as business needs evolve. The service module accelerates IPsec traffic performance by offloading the CPU-intensive part of the overall process—while relying on the switch processor to identify traffic for encryption, negotiate the security associations, and forward encrypted traffic. Thus, the Brocade processor extends traditional Layer 3 routing capabilities to include encryption with Suite B algorithms and support for 128-bit and 256-bit AES. With 10 Gigabits per second (Gbps) throughput per service module and multi-VRF and jumbo frames support, a single Brocade ICX 7450 or stack helps ensure that service levels are not affected as compliance requirements and security needs increase.

Data Security across the WAN

The unique value of the Brocade solution is its end-to-end encryption, which is built into high-performance physical and virtual networking switches and routers. From the wiring closet within the campus to data centers across the Wide-Area Network (WAN), the Brocade solution supports a variety of data security and integrity needs without additional licenses or expensive purpose-built encryption appliances. This comprehensive solution is powered by the IPsec and MACsec encryption capabilities of the Brocade ICX 7450 and the Brocade MLXe Series Router.

The ability to encrypt data at Layer 2 using MACsec or at Layer 3 using IPsec—and to integrate with existing key management and distribution configurations—strengthens data security while maximizing investment protection for the switch and router. IPsec provides a cost-effective, scalable solution for environments that need a secure, economical, and proven way to connect remote sites and employees, business partners, and data centers across any IP network. Along with MACsec, the Brocade solution provides great flexibility and the additional benefit of enabling fast, low-latency, easy-to-deploy encryption within the campus or data center. Organizations that embrace these technologies fully will be best positioned to achieve end-user productivity and cost and operational efficiency.

Data Security into the Hybrid Cloud

Enterprise data centers are no longer the only source for business applications and content, and corporate WANs are no longer the sole on-ramp to these resources. Businesses are shifting spending to hosted private cloud infrastructures to take advantage of the cost and agility benefits of the cloud. As organizations move to hybrid cloud solutions or enable direct Internet access from the branch offices, every user's connection needs to be encrypted for security.

The Brocade vRouter virtualizes network services such as IPsec VPN to provide services faster and more efficiently. For site-to-site connections, the Brocade ICX 7450 with the service module, the Brocade vRouter, and the Brocade MLXe Series Router can be used to create an end-to-end network encryption solution between the on-premises network and the virtual network. This enables users to securely access resources and applications that reside in on-premises data centers or off-premises virtual data centers. In addition, this solution secures and encrypts data moving between on-premises data centers and virtual data centers. Within the hybrid cloud, a new VPN virtual machine can be started in minutes, using a small fraction of an existing server. Maintaining content and applications on-site and in the cloud requires integrated, secure network access to ensure consistent availability and performance for end users.

Data Security Between Data Centers

Brocade MLXe Series Routers provide data center connectivity and aggregate traffic from all the elements in the data center and between data centers. With the IPsec encryption module, these routers not only enable Layer 2 and Layer 3 traffic transmission unimpeded between on-premises data centers, they also help protect data in off-premises virtual data centers.

The IPsec module for the Brocade MLXe Series Routers leverages Brocade programmable hardware technology to extend traditional Layer 2 and Layer 3 routing capabilities to include Suite B algorithms and support 128-bit and 256-bit AES. With 44 Gbps throughput per module, a single Brocade MLXe platform can support over 1 Terabit per second (Tbps) of traffic per chassis at wire speed—another industry first. Other advantages of the Brocade MLXe IPsec module include multi-VRF support, load distribution, and jumbo frames

(9,000 bytes) support for dynamic traffic patterns caused by applications in cloud, mobile, and Big Data. This capability helps ensure that service levels are not affected in even the largest data center and cloud networks.

For example, many healthcare organizations are adopting a hybrid cloud strategy to enable faster and more flexible application deployment. These organizations are also mandated to comply with the regulatory requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Payment Card Industry Data Security Standard (PCI DSS). The Brocade pervasive data security solution helps ensure compliance for organizations with high security needs and sensitive data. This solution interconnects multiple data centers across premises by using high-performance routing and advanced encryption technology, enabling removal of dedicated encryption appliances or off-loading of encryption processing from firewalls.

Conclusion

Today, many enterprises use a variety of sites, such as mobile workers, partner businesses, large data centers, and campus environments—all of which need to connect to the same corporate network with secure, predictable network performance. Brocade delivers a comprehensive solution to enable cost-effective pervasive network encryption across today's extended enterprise. The Brocade ICX 7450 switching solution, used in conjunction with the Brocade MLXe routing and Brocade vRouter network virtualization solutions, provide organizations end-to-end VPN connectivity for accessing business applications from anywhere, anytime. The Brocade solutions give organizations the flexibility to connect their applications between offices or users, which includes access to private cloud services using a variety of encryption technologies and methods.

The combination of IPsec, MACsec, and SSL encryption technologies supported within the Brocade switching and routing solutions offers various solutions to achieve business compliance and strengthen data security. These solutions not only secure traffic within the campus and between campus, data center, and hybrid cloud environments, but it does this without affecting performance. With increasingly complex multisite environments extending to the hybrid cloud, end-to-end high-performance data security is an important component of enterprise security that provides a better user experience.

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. 03/16 GA-SB-5377-00

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.

BROCADE