AT-A-GLANCE

Brocade Comprehensive Network Encryption

HIGHLIGHTS

- This comprehensive solution supports end-to-end use cases for secure data center interconnect, secure multisite campus, and virtual private cloud
- Support for industry-standard IP security (IPsec) ensures information privacy and integrity when transiting a non-customer-owned infrastructure and MAC security (MACsec) for data privacy with support for flexible policy application on a customer-owned network
- Hardware-based in-line encryption ensures data privacy without performance compromise or complex deployment
- Standards-based Suite-B algorithms with 256-bit IP-layer encryption provides the modern strong encryption that is required by public sector and commercial customers
- Hardware-based in-line IPsec at wire-speed, as well as deep buffers and jumbo frame support, deliver industry-first terabit-per-second (Tbps) IPsec throughput in a single router

Multi-Site Campus, Data Center Interconnect, and Virtual Private Cloud

Ensuring End-to-end Data Privacy

For organizations and businesses of all types, ensuring data privacy and controlling the digital footprint is at the forefront of current concerns. Almost daily, the news reports a new data breach, with cases appearing in organizations of all types: the public sector, small business, large enterprises, and service providers.

As enterprises continue to move to the cloud, the volume and variety of data that exists in digital form has exploded, so much so that—in aggregate—the digital footprint increasingly provides a comprehensive view into the mission of an organization or the life of an individual. And this trend is not slowing down, given the expectation that just about any information desired will eventually be available in digital form. This explosion of data offers a tempting opportunity to unscrupulous individuals who are willing to abuse the data they obtain—underscoring the current intense interest in ensuring that private data remains private.

Data risks are widespread—from retailers breached for credit card theft, compliance requirements—such as in healthcare and financial sectors—and the need to protect constituents in the public sector. This is why ensuring data privacy at all parts of the network has become critical to support business operations and enable increased growth, productivity, and profitability. For example, in the public sector, the National Association of State Chief Information Officers (NASCIO) in the U.S. recently identified data privacy as the top state CIO priority for 2014, highlighting the need to protect the personally identifiable information of constituents. In the cloud, security consistently ranks as a top concern of C-level executives,

underscoring the need to better ensure data security and privacy for both the enterprise and the service provider. For enterprises, compliance requirements and costs (both financial and reputational) to identify and remedy data breaches is a top concern that impacts business success. With customers demanding more assurance that their data-in-flight is secure from prying eyes, service providers are looking for ways to meet this demand and differentiate their service offerings.

Table 1: Brocade IP Products for the Data Privacy Solution.

Product	Place in Network	Encryption Supported	Models
Brocade ICX® Switch	Campus Access/ Aggregation	MACsec	Brocade ICX 6610 Switches
Brocade MLX® Series Core Routers	Data Center Core/Border/ Interconnect	MACsec	Brocade MLX-10Gx20-M
	Campus Core/Border Provider Core	IPsec	Brocade MLX-10Gx4-IPSEC-M
Brocade vRouter	Network Function Virtualization (NFV) router for Cloud environments	IPsec	Brocade Vyatta 5400

Data Privacy Cannot be Assumed

Individuals and organizations have always needed to keep certain digital information private. It has often been assumed that attacks are primarily of criminal origin and are targeted in nature, and that they require advanced expertise and resources, such as when tens of millions of credit card records are breached from a major retailer. To protect against such breaches of data, encryption of data-at-rest and data-in-flight is the gold standard.

Yet, while encryption provides significant data protection, it traditionally has not been seamless to deploy, and it came with a high cost and reduced performance. With end-customer service level expectations, enterprise IT and service providers cannot afford to have encryption degrade network performance. As such, encryption has typically been applied only where there was no dedicated physical network link—such as when data left the private network and transited public IP networks, or in wireless networks. At the same time, private (leased or owned) fiber links and private Wide-Area Network (WAN) services (such as Multiprotocol Label Switching Virtual Private Networking [MPLS VPN]) from service providers were assumed to be secure and private, with encryption of these links being the rarity rather than the norm.

Recent events have shown that it is not just criminals out for financial gain or hackers out for a thrill who compromise data privacy. It is now recognized that the majority of data breaches, criminal or otherwise, are opportunistic, indiscriminate, and not targeted. Furthermore, almost two-thirds of data breaches go unnoticed for months, as reported in the "Data Breach Investigations Report 2013" by Verizon. And even those breaches are for data-at-rest, where logging and other forensics provide an audit trail of intruder activity. Compromised network links where data is in flight often go unnoticed, especially if they are not under the physical control of the end user, as is the case with the WAN.

In addition, compliance requirements and associated penalties and costs to mitigate a data breach are on the rise, while the barriers to attack are low: over three-quarters of all attacks require little to no special skill, and the amount and value of data that must be kept private is increasing. Clearly, it is not enough to rely on existing levels of assurance.

Network Encryption is the New Norm

Given the current risks to security, organizations are increasingly concerned about their data and show a heightened interest in encrypting more data, especially as it moves across the network. With the cloud becoming the new computer—and networks as an integral enabler of the cloud—the network increasingly needs to know about and help ensure privacy of the data that traverses it. Encryption is becoming an increasingly important means of ensuring data privacy. You can no longer take data privacy for granted, even on private network links. With the massive increase in digital data, encryption can no longer be a luxury reserved for only a few links, applications, or flows. There is a pervasive need for increased encryption network-wide. However, the current infrastructure does not provide the ability to support this at scale. New solutions are required that help organizations better encrypt their data in the network without impacting the performance, cost, and operational ease needed for widespread deployment.

Data Privacy and Network Performance are not Mutually Exclusive

With the increasing focus around data security and privacy, the need to encrypt more traffic across the network and in the cloud becomes a priority. However, what is needed is a new model that supports scale-out site-to-site encryption for larger locations that require high-performance hardware-based encryption and for smaller sites that need a robust, low-cost, flexible solution to support VPN over the Internet.

The Brocade® data privacy solution provides just such a model, challenging the commonly held belief that ensuring data privacy in the network is costly and complex, and that it compromises network performance. Customers can now more easily deploy an end-to end encryption solution using standards-based strong encryption that is built into the physical or virtual switch and router. Brocade solutions provide both site-to-site (using IPsec) and hop-by-hop (MACsec) encryption supported in hardware. They also deliver wire-speed encrypted performance up to 1 Tbps in a single device, ensuring privacy for all data on all links, with no performance loss.

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

- The enterprise and public sector campus access or aggregation and backbone
- The enterprise, public sector and service provider data center border
- Workloads deployed in the cloud or remote offices

These applications support industry-standard IPsec and MACsec encryption and integrate with existing standard key management and distribution configurations, enabling end-to-end deployments that support a variety of data security and privacy needs. IPsec provides a cost-effective, scalable solution for the 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. MACsec, on the other hand, proves 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 to be applied to network traffic at the switch or router as it traverses the campus network.

Key Benefits and Differentiation

The Brocade solution is unique in that no longer does applying encryption at the switch or router to ensure data privacy result in a performance "tax." In-line hardware-based encryption in physical platforms ensures data privacy without performance compromise or complex deployment.

This comprehensive solution provides encryption from the campus across the WAN and into or between data centers, delivering 2 to 17 times the performance of existing solutions—without the need for separate service modules, additional licenses, or offloading to expensive security or encryption appliances.

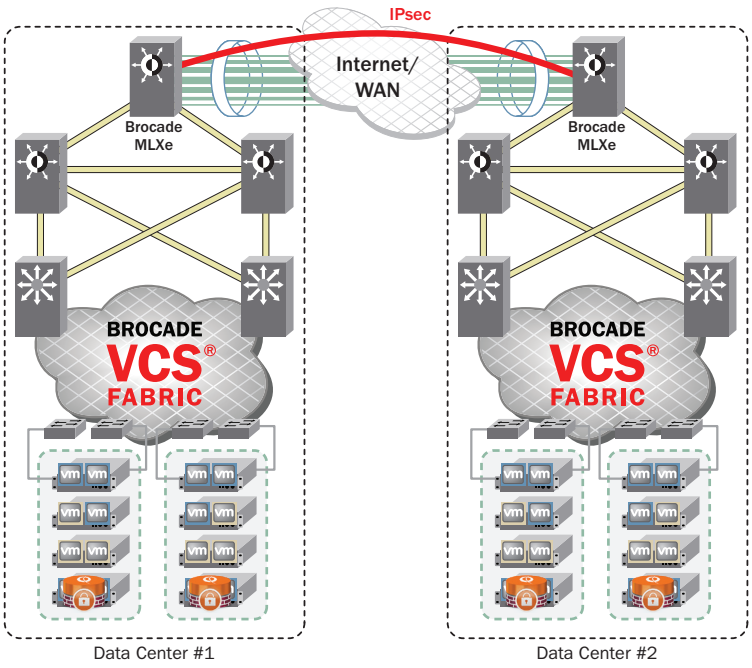

Figure 1: Key Use Case: Secure Data Center Interconnect.
Secure Data Center Interconnect with the Brocade MLXe router and in-line wire-speed IPsec encryption, ensuring the integrity and privacy of all data across uncontrolled network links between data centers.

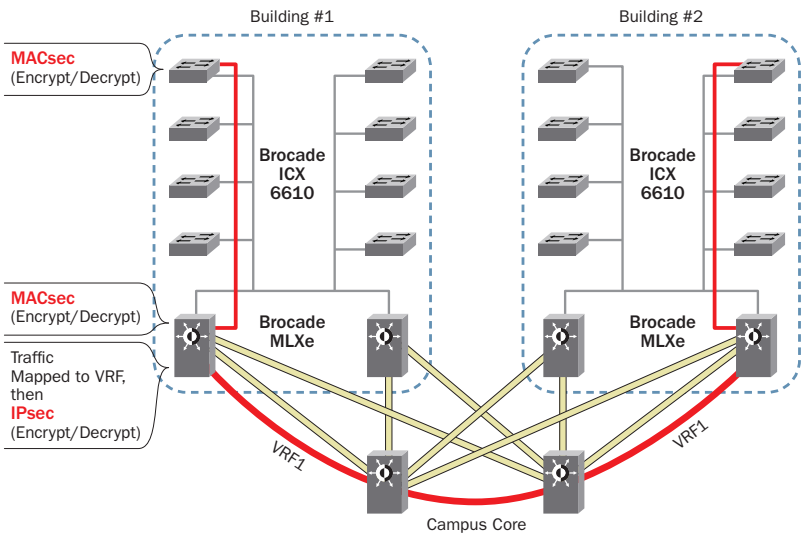

Figure 2: Key Use Case: Multisite Secure Communities of Interest.
Multisite secure communities of interest with the Brocade MLXe router and Brocade ICX switch and MACsec and IPsec encryption ensures secure segmentation of traffic across the campus and WAN for diverse groups sharing the same network.

The hardware IPsec module is ideal for off-net traffic between central sites and data centers, as well as on-net traffic within the campus that requires encryption stronger than the 128-bit AES provided by MACsec. The module leverages the programmable architecture of Brocade MLX routers, extending traditional Layer 2 (L2) and Layer 3 (L3) routing capabilities to include encryption with Suite-B algorithms and support for 256-bit AES keys. 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 first. This capability is ideal to ensure that service levels are not impacted in even the largest data center and cloud networks while increasing Return on Investment (ROI) and maximizing investment protection for the core or border router.

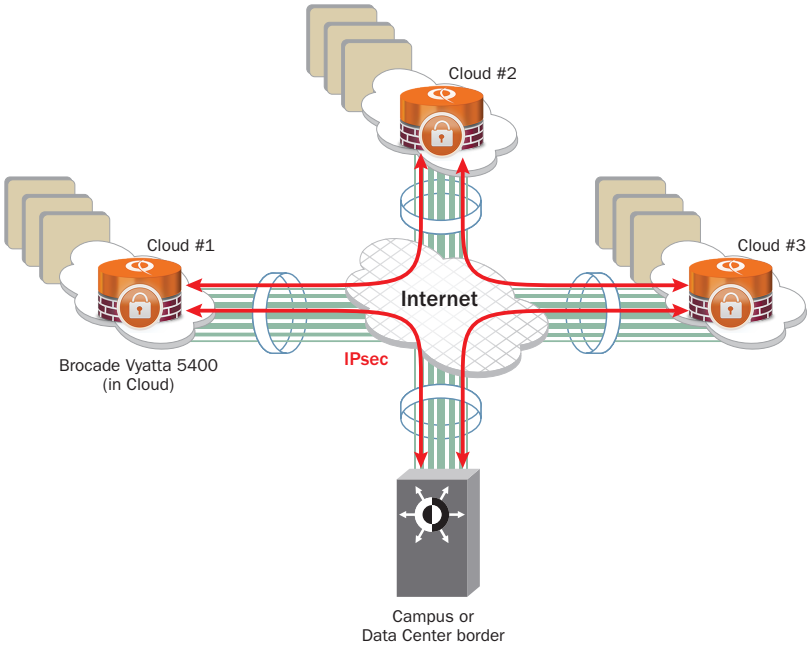

Figure 3: Key Use Case: Virtual Private Cloud.
Virtual private cloud with the Brocade 5400 vRouter and IPsec VPN ensures workloads in the cloud have the same data privacy as in the campus or data center.

Conclusion

The combination of IPsec and MACsec offers an ideal solution. IPsec provides encryption for data cloaking on networks that are vulnerable to snooping, ensuring information integrity when transiting on a non-customer-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 is integrated in the interface module and 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 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.

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

BROCADE