NETAPP SALES FAQ

Brocade Encryption Switch and Brocade FS8-18 Encryption Blade—Frequently Asked Questions

April 2011 | TR-3722

FAQ OVERVIEW

This FAQ discusses encryption in general, including why to encrypt and what data to encrypt, as well as the Brocade encryption solutions and their particular advantages.

1 SECURITY AND ENCRYPTION OVERVIEW

WHAT IS ENCRYPTION?

Encryption is the process of obscuring information to make it unreadable without special knowledge. Modern encryption methods use a cipher, a method of encrypting data that uses a standard algorithm to perform encryption and decryption processes.

WHY DO MY CUSTOMERS NEED TO ENCRYPT DATA AT REST?

Network-accessible data is increasingly vulnerable, and the rate of identity theft (stemming from the unlawful use of nonpublic personal information) is skyrocketing. The combination has resulted in an emerging market for security products that distinctly address the need to protect your customers' stored data, or "data at rest." If your customers experience a loss of personal data, they are likely to incur enormous costs—in terms of penalties, notification costs, damage to reputation, and lost customers—that average in the multiple millions of dollars. Moreover, the theft of intellectual property can be devastating to your customers' ability to compete.

WHY HASN'T EVERY IT ORGANIZATION DEPLOYED ENCRYPTION?

Many IT professionals have traditionally believed that the application of strong encryption comes with a severe system performance penalty due to the additional layer of processor-intensive computation required. This perception remains to some extent despite the development of more efficient encryption algorithms, such as the Advanced Encryption Standard (AES), and the use of dedicated hardware-based processing, which together negate the impact on system performance. Another source of concern and reluctance to use encryption has been the management of the digital keys required to encipher and recover encrypted information.

WHAT TYPE OF DATA NEEDS TO BE ENCRYPTED?

Many companies undertake a data classification project to identify their most sensitive data, which require the additional layer of security provided by encryption. This often involves regulated data such as personal information, financial documentation, entrusted partner information, intellectual property, vendor data, customer lists, and personnel data. An increasing number of companies are electing to encrypt *all* sensitive company information, particularly if they expect it to leave the control of their facilities.

HOW IS STORAGE SECURITY ENCRYPTION DIFFERENT FROM VPNS OR PKI?

Storage security encryption is significantly different from both VPN and PKI. VPNs use a combination of authentication, asymmetric encryption, and hashing to protect the confidentiality and integrity of data in flight, usually across the public network, as opposed to data at rest. PKI uses certificate policies and asymmetric encryption key pairs to enforce secure communication between users in a closed group. By contrast, Brocade® fabric-based encryption uses symmetric encryption with a single, shared secret key to apply encryption to designated target storage that contains sensitive information.

HOW CAN MY CUSTOMERS MEASURE THE RETURN ON INVESTMENT FROM STORAGE SECURITY?

Storage security protects against asset losses in the event of a security breach. So to measure the ROI, you estimate the potential loss and multiply it by the probability of the loss happening. However, other tangible financial benefits can be more easily identified, such as:

- Increased business gained (or lost business avoided) by providing your customers with data security assurance
- Enhanced ability to demonstrate compliance with confidentiality regulations
- Avoidance of penalties assessed for failure to comply with regulations and industry standards for personal data protection

WHAT INDUSTRY MANDATES AND REGULATIONS ARE RELEVANT TO DATA ENCRYPTION?

Encryption is increasingly becoming part of best-practice strategies and frameworks for compliance with numerous regulations and standards, including these:

• Nevada Senate Bill 227, in effect since January 1, 2010, addresses certain provisions concerning identity theft. The bill relates to the security of personal information, requiring the use of encryption by data collectors when transferring personal information.

• The Health Information Technology for Economic and Clinical Health Act of 2009 extends the privacy and security provisions of the Health Insurance Portability and Accountability Act to business associates of covered entities, including civil and criminal penalties for noncompliance. It also imposes new notification requirements for breach of Personal Health Records and imposes penalties for noncompliance.

• California SB1386 and other security breach disclosure legislation provide an exception for data that was obtained while in “ciphertext” form. The California Office of Privacy Protection recommends in its "Recommended Practices on Notification of Security Breach Involving Personal Information″ the use of data encryption, wherever feasible, to protect higher-risk personal information.

• California AB 1950 specifies that holders of personal information about a California resident implement and maintain reasonable security procedures and practices to prevent unauthorized access, destruction, use, modification, or disclosure when held in unencrypted form.

• Massachusetts General Law Chapter 93H requires any firm conducting business with state residents to deploy encryption on portable devices, including tape media and disks in transport, to protect personal, private information. Data that must be encrypted includes the person’s name along with the social security number, bank account, or credit card number stored on portable devices or transmitted wirelessly on public networks.

• The Gramm-Leach-Bliley Act (GBLA) of 1999 requires financial institutions to have a security plan to protect the confidentiality and integrity of Non-Public Personal Information (NPI). The "Interagency Guidelines Establishing Standards for Safeguarding Customer Information" published by GLBA’s enforcing government agencies provides guidelines and standards for safeguarding customer information. Under the section “Manage and Control Risk,” recommended procedures include “encryption of electronic customer/member information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access.”

• The Payment Card Industry Data Security Standard (PCI DSS) adopted by leading credit and debit card vendors requires under Section 3.4 that merchants store account numbers (in databases, logs, files, and backup media) securely by means of encryption or truncation. Large merchants must additionally submit to an annual on-site PCI data security assessment that is validated by a “Qualified Data Security Company” or internal audit if signed by an officer of the company.

WHAT IS THE DIFFERENCE BETWEEN THE VARIOUS ENCRYPTION ALGORITHMS?

Encryption algorithms are not generally considered to be well vetted until the security community has had several years to test them and discover any hidden vulnerabilities. For this reason, new and proprietary algorithms are generally not accepted for critical applications. Algorithms that have been extensively tested and that utilize long key lengths (suggested as greater than 128 bits for symmetric keys) are considered “strong” and trusted for use.

The AES describes the algorithm approved by the Federal Information Processing Standard (FIPS) for use by U.S. government organizations to protect sensitive, unclassified information. The AES is available in 128-, 192-, and 256-bit key lengths. Assuming that one could build a machine that could recover a DES key in a second (for example, attempt 255 keys per second), it would take that machine approximately 149 trillion years to crack a 128-bit AES key.

2 BROCADE ENCRYPTION PRODUCT INFORMATION

WHAT ARE THE KEY HARDWARE CHARACTERISTICS OF THE BROCADE ENCRYPTION SWITCH?

The Brocade Encryption Switch is a full-featured 32-port 8Gb Fibre Channel switch that supports up to 96Gbps of encryption and up to 48Gbps of compression processing.

WHAT ARE THE KEY HARDWARE CHARACTERISTICS OF THE BROCADE FS8-18 ENCRYPTION BLADE?

The Brocade FS8-18 Encryption Blade for the Brocade DCX® Backbone family provides 16-port 8Gbps Fibre Channel connectivity with a maximum 96Gbps of encryption processing and 48Gbps of compression processing.

WHAT SECURITY FEATURES ARE AVAILABLE ON THE BROCADE ENCRYPTION PRODUCTS?

In addition to enabling you to encrypt data at line speed, the Brocade encryption products provide storage access controls, data integrity checking for tape, and administrative audit logging. In addition, the systems provide secure management connections and Smart Card support for system card and quorum-based recovery of system master keys. Both Brocade encryption products (switch and blade) are FIPS 140-2 Level 3 validated.

CAN THE BROCADE ENCRYPTION PRODUCTS BE CLUSTERED AND, IF SO, HOW?

Brocade encryption products can be clustered into pairs. Two redundant Gigabit Ethernet ports enable clustering and synchronization of I/O activity during rekeying operations for data integrity and recoverability.

HOW MANY BROCADE ENCRYPTION PRODUCTS CAN BE CONFIGURED IN A SINGLE FABRIC? IN A DUAL FABRIC?

Up to four encryption devices (switches or blades) can be configured in a single fabric; two clusters can be configured in a dual fabric.

HOW DO KEYS GET ARCHIVED AND SYNCHRONIZED?

Following their creation, keys are archived and synchronized to the designated key management system. Best practices dictate the use of two or more clustered key management devices for synchronization.

WHAT BROCADE FABRIC OS RELEASE IS REQUIRED TO RUN THE ENCRYPTION PRODUCTS?

Brocade Fabric OS® (FOS) 6.1.1_enc or later is required to run on the Brocade Encryption Switch or on the Brocade DCX Backbone family with the Brocade FS8-18 for disk encryption. Brocade FOS 6.2 is required to support tape encryption or the Brocade FS8-18 in the Brocade DCX-4S Backbone.

IS A SPECIAL LICENSE KEY REQUIRED TO UPGRADE THE PERFORMANCE OF BOTH PRODUCTS?

The base Brocade Encryption Switch and Brocade FS8-18 Encryption Blade provide 48Gbps of encryption hardware processing and can be upgraded to a maximum of 96Gbps for disk encryption with the purchase of a disk performance upgrade license key.

ARE DISK AND TAPE ENCRYPTION SUPPORTED CONCURRENTLY ON A SINGLE DEVICE?

Yes, the Brocade FOS 6.4 release allows encryption to be configured for both disk and tape on a single Brocade Encryption Switch or Brocade FS8-18 Encryption Blade.

3 KEY MANAGEMENT INTEGRATION

WHAT IS KEY MANAGEMENT?

In cryptography, digital “keys” (pieces of information that control the operation of a cryptographic algorithm) are required for the encryption and decryption of secured data. Key management describes the process of creating, distributing, authenticating, and storing encryption keys to optimize proper use. Because these procedures provide no security when the keys are handled incorrectly, the ability to obtain keys without permission must be considered the equivalent to obtaining “cleartext” data. The Brocade encryption solutions are integrated with NetApp® Lifetime Key Management™, which restricts key creation to authenticated security administrators, provides secure key distribution among clustered Brocade switches or blades, and exports keys only in ciphertext form without compromising the strength of the key.

WHAT KEY MANAGEMENT SYSTEM DO YOU USE?

The Brocade Encryption Switch and Blade both support NetApp’s industry-leading, enterprise-class Lifetime Key Management KM500 (4.0 or later), which simplifies key management, maximizes key security, and simultaneously lowers total cost of ownership.

4 BROCADE ENCRYPTION ADVANTAGES

WHY SHOULD I DEPLOY FABRIC-BASED ENCRYPTION?

There are many advantages to fabric-based encryption, the biggest of which is that encryption is nondisruptive to both your host servers and your storage arrays. Another advantage is that you don't need to perform a forklift upgrade of your storage, a process that requires mass data migration, entailing months of work. With the Brocade encryption switch or blade, you can install and be up in a matter of days. Finally, setting up encryption in the fabric allows you to separate the roles of storage and security, building in administrative controls and reducing the risk of internal threats that can occur if the storage administrator also holds all the keys.

WHAT ADVANTAGES DO THE BROCADE ENCRYPTION APPLIANCES OFFER COMPARED TO OTHER IN-LINE ENCRYPTION APPLIANCES?

Brocade encryption products provide multiple advantages over other in-line encryption appliances:

- The high-performance, low-latency encryption solutions provide from 48 to 96Gbit/sec of encryption processing power, allowing you to take advantage of encryption without affecting your network performance.
- Brocade cryptographic functions run on multiple dedicated hardware engines, providing you with a level of performance as much as 50 times that of other in-line encryption appliances.
- By integrating into a scalable encryption module-based platform, Brocade products enable performance scaling in a modular chassis with the simple addition of blades.
- Brocade encryption products provide a central point of management that simplifies deployment and configuration changes.
- Brocade supports seamless deployment using Frame Redirection technology.
- The multipurpose switching functionality provides flexible deployment options, allowing the installation of 32 ports, universal (F/FL/E/EX/M) auto-sensing, and programmable 1, 2, 4, and 8Gbit/sec speeds.
- Brocade encryption products provide the lowest total cost of ownership of any currently available enterprise-class solution based on initial investment, deployment costs, management costs, environmental costs, and the opportunity to support additional storage services and applications.
- The high port count and bandwidth of the Brocade encryption solutions give you a solution for encrypting mass amounts of data on storage arrays with high port counts.

WHAT IF I ALREADY HAVE NETAPP DATAFORT IN MY STORAGE NETWORK?

Brocade's encryption solutions can operate in NetApp DataFort™ compatibility mode. This license-enabled mode allows you to protect your investments in any NetApp security offerings. You can read/write in NetApp DataFort compatibility mode, meaning that anything encrypted with NetApp FC series DataFort appliances can be decrypted by the Brocade encryption products, and vice versa. You can purchase NetApp DataFort compatibility mode only from NetApp and its partners.

HOW DOES NETAPP DATAFORT COMPATIBILITY MODE WORK IN THE BROCADE ENCRYPTION SOLUTIONS?

When operated in this mode, the Brocade solution enables you to decrypt (disk or tape) data that was previously encrypted by NetApp DataFort 1.x and 2.x formats. Also, data (disk or tape) encrypted by Brocade can be decrypted by FC series NetApp DataFort appliances. This tight integration of technology enables you to scale your existing NetApp DataFort deployments by adding a Brocade solution to your security infrastructure without having to worry about format compatibility. You can continue to use your existing FC series NetApp DataFort appliances alongside the new Brocade solution or redeploy those appliances for other applications while maintaining data workflow.

WHAT KIND OF MEDIA DOES BROCADE SUPPORT?

You can configure the Brocade encryption products to support either disk, tape, or concurrent disk and tape encryption using a switch or blade configuration.

HOW DO BROCADE ENCRYPTION PRODUCTS AFFECT SYSTEM PERFORMANCE?

Because Brocade encryption products are based on dedicated high-speed, hardware-based processing, the impact on system performance for most applications is imperceptible.

WHAT KIND OF ATTACKS DO BROCADE PRODUCTS PROTECT AGAINST?

By encrypting sensitive data at rest, Brocade products protect you against:

- Threats to in-transit media outside the data center
- Theft of removable media from third-party storage facilities
- Theft of data by physical removal of hardware or storage media
- Unauthorized viewing of replicated data at remote sites
- Inadvertent exposure of data on media returned to external facilities for repair or replacement

WILL THE BROCADE PRODUCTS HAVE ANY GOVERNMENT CERTIFICATIONS?

The Brocade Encryption Switch and Brocade FS8-18 Encryption Blade are validated to meet or exceed the requirements of FIPS 140-2, Level 3. Please refer to the online list of FIPS-validated products at http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2009.htm.

The products have also been submitted for Common Criteria validation at EAL-4. Please refer to the Common Criteria page at http://www.niap-ccevs.org/cc-scheme/in_evaluation/ for the current status.

www.netapp.com

www.netapp.com