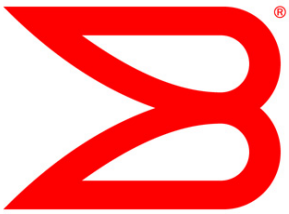

STORAGE AREA NETWORK

SafeNet KeySecure k460 with Brocade Encryption Solutions

KeySecure k460, the SafeNet Enterprise Key Management solution is a purpose-built key management appliance that succeeds the NetApp Lifetime Key Management Appliance. KeySecure is an enterprise-class, centralized key management solution that integrates with Brocade encryption solutions, as well as various KMIP-compliant solutions. The combined solution enables visibility, control, and reliable access to encrypted data while maintaining the highest level of security for your encryption keys.

BROCADE

CONTENTS

INTRODUCTION

Brocade®, NetApp®, and SafeNet® have combined forces to provide a robust and scalable encryption solution with an enterprise-class key management solution—SafeNet KeySecure™. KeySecure offers a hardened OS, a tamper-resistant chassis, multifactor authentication, and dual-person control of critical operations to ensure complete security of encryption keys. This paper explores how the Brocade encryption solutions leverage many of the features of KeySecure to deliver the most secure Fibre Channel (FC) encryption solution on the market.

NOTE: The term "Brocade encryption solution" is used in this paper to refer to both the Brocade Encryption Switch and the Brocade FS8-18 Encryption Blade.

A unique aspect of the Brocade-NetApp-SafeNet data-at-rest encryption solution is the centralized key lifecycle management and key sharing capabilities of KeySecure. For regulatory compliance and confidential data sharing, encrypted data and data encryption keys are often required to be transported between sites. The trusted relationship between Brocade encryption solutions and SafeNet KeySecure enable simple-yet-secure key lifecycle management between multiple geographically dispersed sites. KeySecure and its trusted relationship with Brocade encryption solutions enables secure and automated key sharing and consistent policy enforcement between multiple sites, providing transparent access to encrypted data at all times by authorized users.

This paper focuses on key management with SafeNet KeySecure and assumes a basic understanding of the Brocade data-at-rest encryption solutions. White papers that discuss the basics of encryption and Brocade encryption solutions can be found at www.brocade.com.

OVERVIEW

A quick overview of the equipment provided in the solution is helpful in understanding the context of this discussion. Brocade recommends deploying encryption with redundant encryption devices and redundant SafeNet KeySecure appliances. As shown in Figure 1, the components of this scenario include the following:

- An initiator to read and write the data
- A target to store the data
- An FC fabric, which in this example consists of two Brocade Encryption Switches
- Encryption devices to encrypt and decrypt the data
- Redundant KeySecure appliances to centrally manage and share the Data Encryption Keys (DEKs) from Brocade and other heterogeneous encryption devices, including Key Management Interoperability Protocol (KMIP)-compliant devices.
- Brocade Network Advisor to manage the fabric and encryption
- A management Local Area Network (LAN) to link the management station and fabric devices (including the encryption devices and other equipment)
- A separate cluster LAN of Gigabit Ethernet (GbE) links between the encryption devices for exchanging DEKs (not shown in Figure 1)

KeySecure securely connects and communicates with Brocade encryption solutions, NetApp DataFort appliances, NetApp LKM appliances, and NetApp NSE (NetApp Storage Encryption) appliances, as well as heterogeneous encryption devices. KeySecure manages storage security device keys and settings, including exchanging DEKs between SafeNet KeySecure, Brocade encryption solutions, and other third-party encryption platforms. The Brocade encryption solution generates the DEKs and wraps (encrypts) them before sending them to KeySecure within a Transport Layer Security (TLS) session. The SafeNet KeySecure appliance automatically backs up and synchronizes key lifecycle, policy, and configuration information between clustered KeySecure appliances. KeySecure manages the DEKs and performs other tasks, which are discussed in the next section.

Figure 1 shows how the DEKs are exchanged between devices in the encryption solution. The DEK is first generated by the encryption device and can be sent to the primary KeySecure appliance. The encryption device then synchronizes DEKs with the other encryption devices in the fabric through the Cluster LAN. The KeySecure

appliances also synchronize keys and policies between clustered appliances to ensure access to keys if one appliance is unavailable. These redundant key exchanges are crucial to ensuring that the data can be encrypted or decrypted without creating a single point of failure.

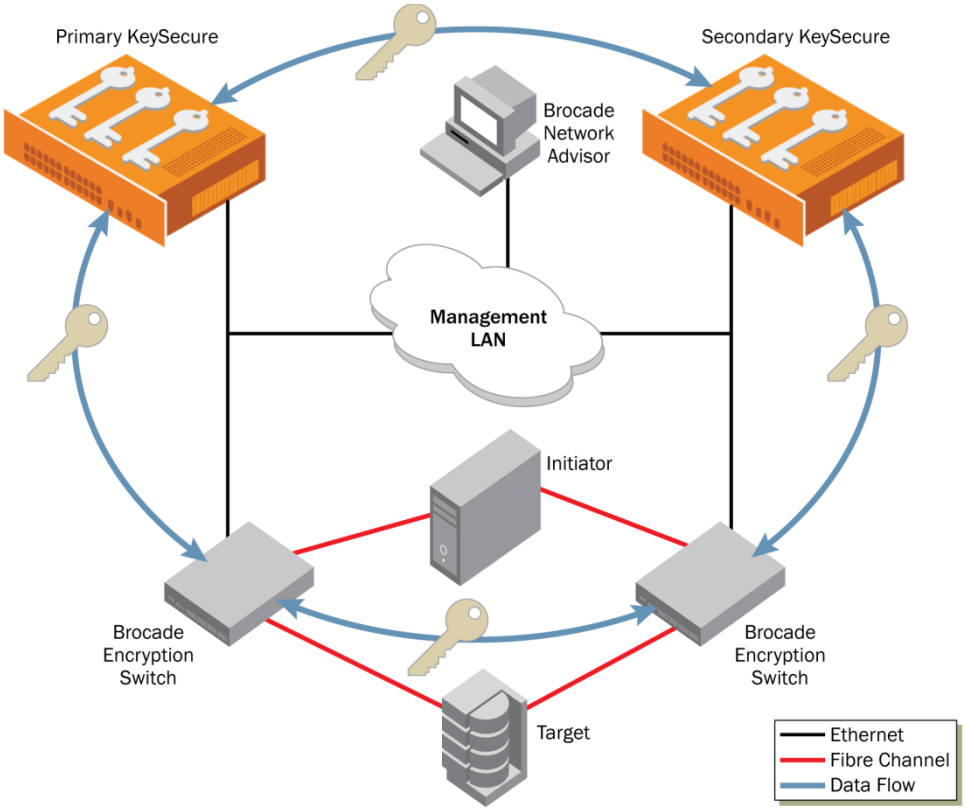

Figure 1. Components of the Brocade-SafeNet solution

KEYS AND KEY MANAGEMENT

One of the strengths of the solution is that data encryption keys are secured on a Federal Information Processing Standard (FIPS) 140-2 Level 3 hardware security module within KeySecure. KeySecure uses a SafeNet Luna PCI-e Cryptographic Module to secure all encryption keys. All transportation of the keys between clients and SafeNet KeySecure occurs on a secure channel. To ensure security of the keys during movement, a hierarchical key model with crypto trusted links is used. Hierarchical key sharing groups enables clients to belong to more than one group. Through this hierarchy of keys, higher-level keys are always used to wrap lower-level keys before leaving the FIPS security boundary.

As mentioned earlier, the unique trust relationship between SafeNet and Brocade allows establishment of a symmetric 256-bit strength link key to facilitate movement of all encryption keys. In order to maintain the key strength in the entire system, whenever the key is in transit, it is protected using this 256-bit strength link key. The decision to use symmetric keys for this solution was important to ensure consistent key strength throughout the solution. Use of a different key protection mechanism, such as asymmetric keys, could significantly lower the overall key strength of the system. Asymmetric keys must be significantly larger in order to achieve the same bit strength. Table 1 compares the relative key strength of symmetric and asymmetric keys.

Table 1. Comparative Key Strengths of Symmetric vs. Asymmetric Keys

Symmetric Key Size (bits)	Asymmetric Key Size (bits)
80	1024
112	2048
128	3072
192	7680
256	15360

KeySecure and the Brocade encryption solution establish a 256-bit strength link key after digital certificates are verified. The link key is used to encrypt DEKs before they are transported. To be compliant with FIPS 140-2 Level 3, both the Brocade encryption device and SafeNet KeySecure have a security boundary that defines where DEKs are encrypted and stored. Before being transported outside the encryption boundary, DEKs are always encrypted, or wrapped, with the link key.

1. The following numbered items correspond to the circled numbers in Figure 2, which shows the process of exchanging keys.
2. A trusted relationship is created through a secure exchange between the Brocade encryption solution and SafeNet KeySecure. The trusted link generates a symmetric link key (shown in orange), which is stored in each device and is used to wrap the DEK for secure transport.
3. The Brocade encryption device creates a new DEK in cleartext (shown in red) within its security boundary.
4. The DEK is encrypted (wrapped) with the link key to create a wrapped DEK (shown in blue) before it leaves the encryption boundary.
5. The wrapped key is sent to SafeNet KeySecure in the Secure Sockets Layer (SSL) session with a key strength of 256 bits. (Note that the DEK was already wrapped with the 256-bit strength key, so the SSL session key does not weaken the key strength of the system.)
6. After the wrapped key arrives inside the security boundary of KeySecure, KeySecure uses its symmetric link key to unwrap the DEK to discover DEK in cleartext.
7. KeySecure then uses the KeySecure domain key (shown in gray) to encrypt the DEK for storage outside the security boundary in its redundant disk drives.

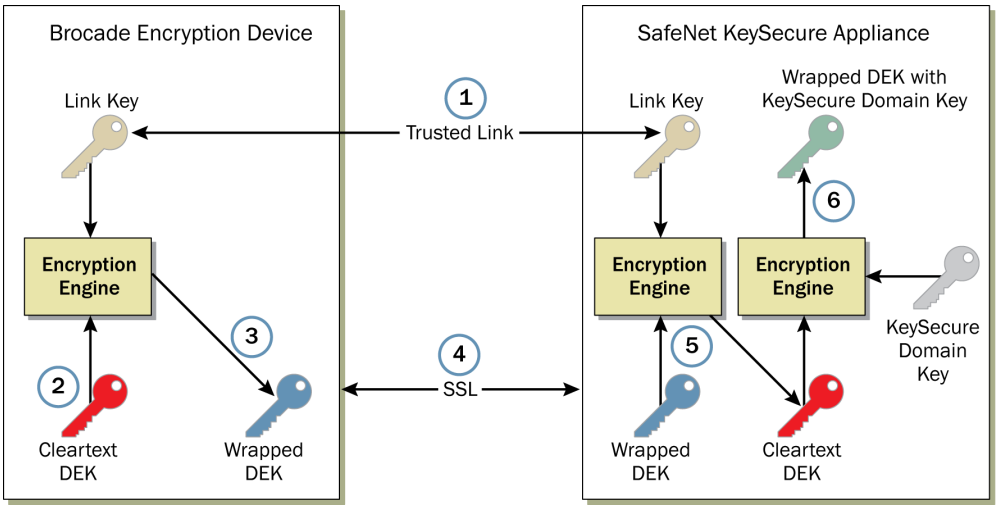

Figure 2. Key exchange between a Brocade encryption device and SafeNet KeySecure

One of the principal benefits of the trusted relationship between SafeNet KeySecure and the Brocade encryption solution is the ability to share keys within Key Sharing Groups (KSGs). The ability to create a trusted relationship with another appliance is the foundation of the KSG feature. KSGs are key movement policies that govern which encryption device can gain access to which keys. The KSG rules are simple, but the implementation enables sophisticated deployments.

The three rules of Key Sharing Groups are as follows:

1. Encryption devices within the same KSG can share keys.
2. Encryption devices in a parent KSG can access keys in their child KSG.
3. Encryption devices in a child KSG cannot access keys from their parent KSG.

Consider the example deployment shown in Figure 3. Each device represents a Key Sharing Group to which an encryption device could belong. All devices in the U.S. KSG can access keys from devices in the U.S., New York, or San Francisco (SF). However, New York and SF devices can access only keys in their respective KSGs. In this way, a customer could compartmentalize groups of encrypting devices and restrict their key access depending on which KSG they are assigned to.

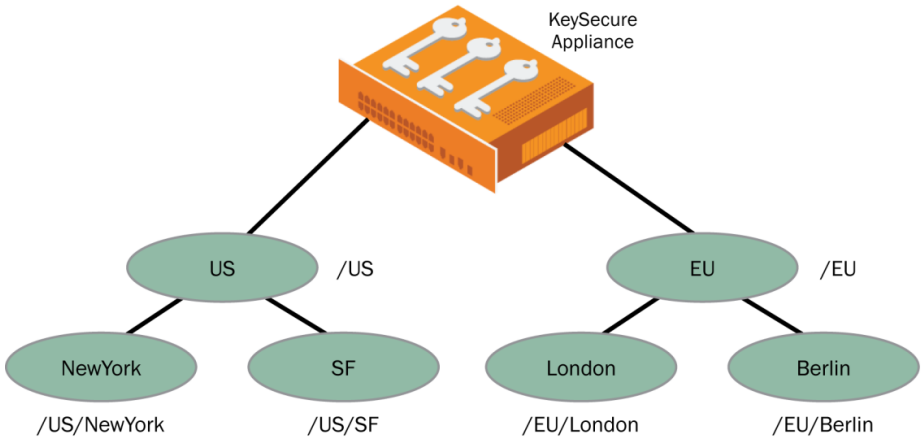

Figure 3. Key Sharing Group example

Assignment to a particular KSG is not a permanent state. The KeySecure Administrator can move both keys and encryption devices from one KSG to another to facilitate access. Table 2 illustrates results from a typical query for keys in the KeySecure appliance. A single key or group of keys can be easily identified by many parameters, including their KSG membership or tape label. In this example, encrypted tape A0004 was written from an encryption device in /US/NewYork. If the tape needs to be restored in London, there are two ways to give the devices in /EU/London access to the encryption key:

- First, an encryption device can be moved from the existing /EU/London KSG into the /US/NewYork KSG. This enables the London encryption device to access all keys in the /US/NewYork KSG.
- Second, the administrator can simply select the individual encryption key—identified by the tape label A0004—and move that key into the /EU/London KSG. This limits access to only the key that is needed.

Table 2. Sample Output Table from SafeNet KeySecure, Showing Encryption Key IDs and KSGs

Key ID	Key Sharing Group	Pool Label	Tape Label
1c2709e09c3dbec63a0ca2737ea4b66e	/US/NewYork	Full	A0001
2c7c217a53dcc470b7c0b97b05b65c81	/US/NewYork	Incremental	A0004

NOTE: The Key IDs shown are simply pointers, and not the actual encryption keys.

The previous example illustrates how simple but powerful the concept of Key Sharing Groups is, to allow easy, yet secure movement of encryption keys across geographic boundaries. Keys can be moved in bulk by putting encryption devices in the same KSG, but KeySecure also permits granular key movement—down to the level of individual encrypted tape.

SafeNet KeySecure provides not only enterprise-level key distribution, but it also ensures availability of the keys with multiple layers of redundancy. KeySecure has two hot-swappable power supplies, as well as two hot-swappable Small Computer Systems Interface (SCSI) disks configured in RAID1. Even if a single disk drive fails, access is still enabled to all encryption keys from the local KeySecure appliance.

Availability across systems is possible through trustee links with up to 16 other SafeNet KeySecure appliances. By forming trustee relationships with other KeySecure appliances, encryption keys are automatically synchronized between all peers; thus, they are made available in case of the failure of an entire appliance. Furthermore, configuration databases (configdbs) from each SafeNet KeySecure appliance are backed up to other KeySecure appliances to facilitate recovery of any failed appliance.

Each Brocade encryption solution has the capability to send and request encryption keys to and from multiple KeySecure appliances. Newly generated encryption keys are automatically sent to all registered KeySecure appliances to ensure availability of the keys. The administrator can also manually initiate a backup of the keys and their configuration database. In the event of a failure on the Brocade encryption solution, keys can be quickly and easily recovered by recreating the trustee relationships between a replacement Brocade encryption solution and any SafeNet KeySecure appliance on the network.

ENTERPRISE SECURITY FEATURES

To complement the enterprise level security, key movement, and availability, KeySecure also offers features necessary for a device of its class, as described in this section:

- Granular role-based access control
- Auditing, logging, and alerting
- Verification of key integrity

Role-Based Access Control

Customers who choose encryption as their solution to protecting data-at-rest are also often looking for features that allow them to compartmentalize administration functions to ensure role separation. With SafeNet KeySecure, granular role-based access controls are a critical step in the right direction. KeySecure supports multiple roles for administrators, such as Full Admin, Account Admin, Key Admin, Security Admin, Backup Admin, Machine Admin, and Read-Only Admin. Each administrator role is allowed to perform only a subset of duties, to distribute responsibility across multiple individuals. For example, the Key Admin can assign appliances to Key Sharing Groups and move keys between KSGs, while the Account Admin can only create, manage, and delete administrator accounts. KeySecure is also flexible enough to create custom administrator roles by combining multiple roles into an administrator role that suits a company's needs.

Auditing, Logging, and Alerting

Auditing and compliance are essential considerations to ensuring security of data-at-rest. SafeNet KeySecure provides cryptographic assurances that the log messages are authentic. All keys are securely managed, key ownership is clearly defined, and key lifecycle management and modifications are recorded and securely stored, providing a non-repudiative audit trail of key state changes. Administrators and security personnel are informed if attempts to breach protected keys occur.

Verification of Key Integrity

As discussed earlier, the SafeNet KeySecure appliance provides a hardened cryptographic boundary to ensure that encryption keys are always physically secure. KeySecure also wraps DEKs during transport, using the same bit

strength (256-bit) as the DEK itself, to ensure security of the key as it moves through the network. KeySecure provides a further check on all DEKs by digitally signing each DEK as it is stored. KeySecure accomplishes this by using a unique signing key and applying the HMAC-SHA-256 function on each key to create a unique key signature for each DEK. When an encrypting device requests a DEK from KeySecure, this key signature is verified for integrity before the key is made available for encryption or decryption services, as shown in Figure 4. This additional safeguard on the key ensures that the key has not been tampered with, which has the potential to weaken the strength of the data the key was designed to protect.

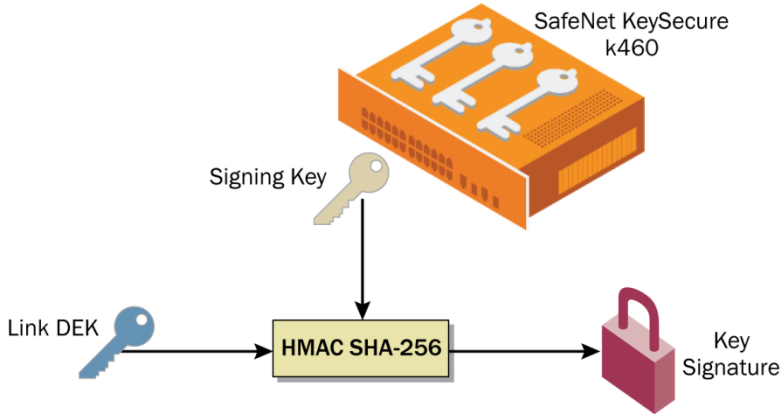

Figure 4. Key signing for integrity

INTEGRATION SCENARIOS

SafeNet key management solutions have provided robust encryption and key management for years, and the Brocade encryption solutions are designed as an upgrade path to increase port density and ease scaling to higher throughputs. Three scenarios are described in this section:

- Mirrored data facilities
- Remote tape
- NetApp DataFort upgrade

Mirrored Data Facilities

Figure 5 investigates disk mirroring using NetApp SnapMirrror® technology between sites. Site 1 is the primary site, where the data and DEK are generated and mirrored to Site 2. The Brocade encryption solutions synchronize DEKs over the cluster LAN, while SafeNet KeySecure synchronizes key replication and movement over a separate IP network that may be on a different virtual LAN (VLAN). Hosts at either site must be configured for encryption to access the storage. The DEK exchange between SafeNet KeySecure Appliance 4 and Brocade Encryption Device 2 is not used, unless the cluster LAN is down and new DEKs are created at Site 1. With multiple access routes to the DEKs, the Brocade encryption solutions ensure that the data is highly available.

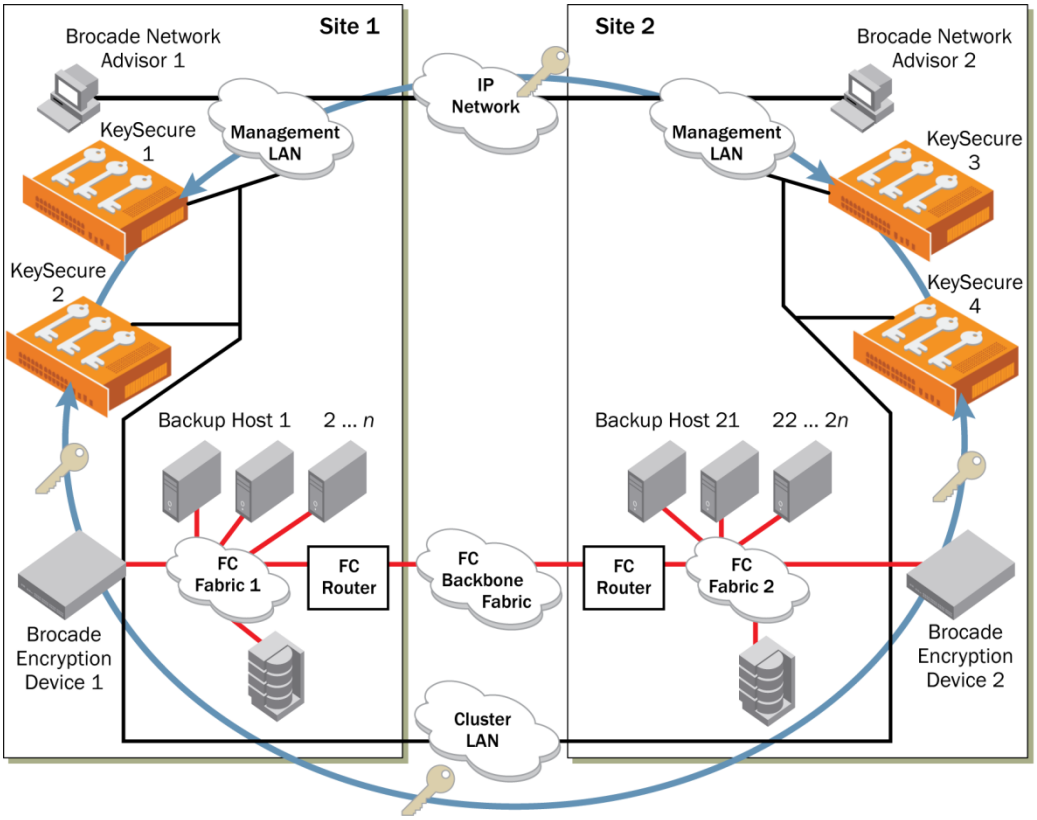

Figure 5. Data mirroring, encryption, and key management spanning two sites

Remote Tape

Another example of the tight integration between Brocade, NetApp, and SafeNet shows how keys are interoperable in tape environments. In this scenario, a company has been backing up tapes at multiple remote sites and shipping the tapes back to headquarters. To decrypt the tapes at headquarters, keys are transparently and securely exchanged between the SafeNet KeySecure appliances. In the scenario, the most difficult part of the restore is transporting the encrypted tapes between the data centers in a delivery truck. Since the tapes are encrypted, the company can feel secure in sending them via any overnight carrier.

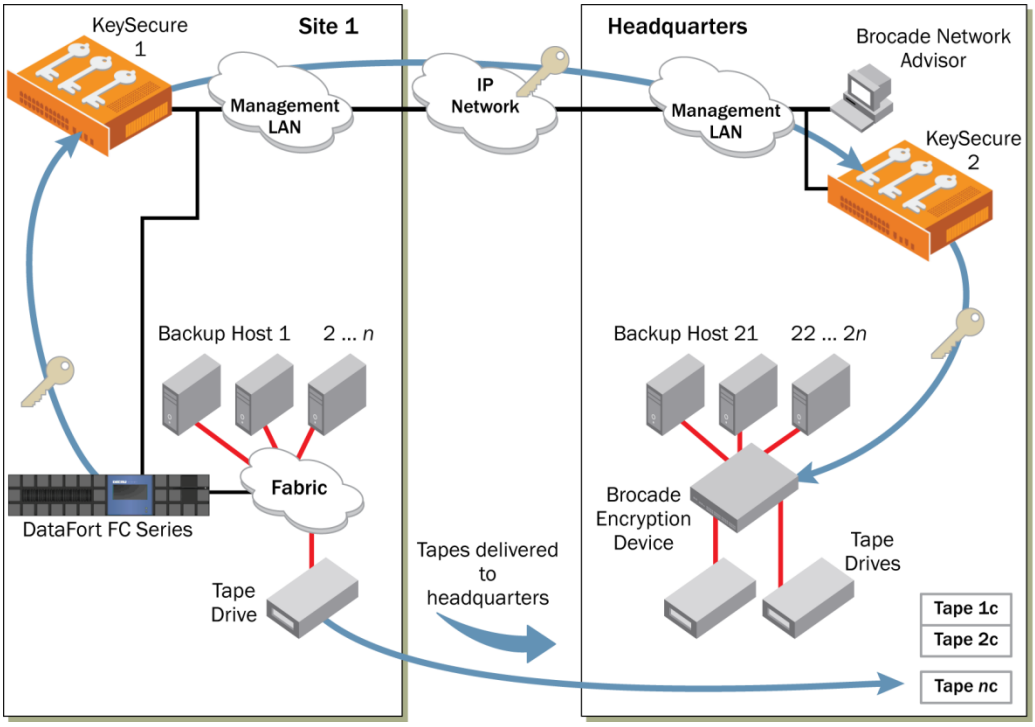

Figure 6. Key exchange between remote sites

After mergers and acquisitions, large enterprises often have a variety of systems that need to be integrated. This scenario shows how keys can be exchanged for a variety of applications. A user needs only an Internet connection to exchange the keys, so that the tapes can then be delivered to a central location for decoding. If a company needs to provide records stored on tape to auditors, the tape and keys can be provided to the auditor for decryption.

NetApp DataFort Upgrade

This final scenario shows an initial deployment with a pair of NetApp DataFort FC-Series encryption appliances attached to the fabric and a 4-port storage array. The customer has gone through significant expansion of data and is upgrading its storage with a 32-port storage array.

Figure 8 shows how the same key management infrastructure can be used with Brocade encryption solutions and NetApp DataFort appliances, which initially encrypt eight of the array ports. The SafeNet KeySecure appliance provides a key management infrastructure that allows integration of both vendor products to provide encryption services for an expanding storage environment. In addition, the upgrade path is backward and forward compatible, to provide a continued Return on Investment (ROI).

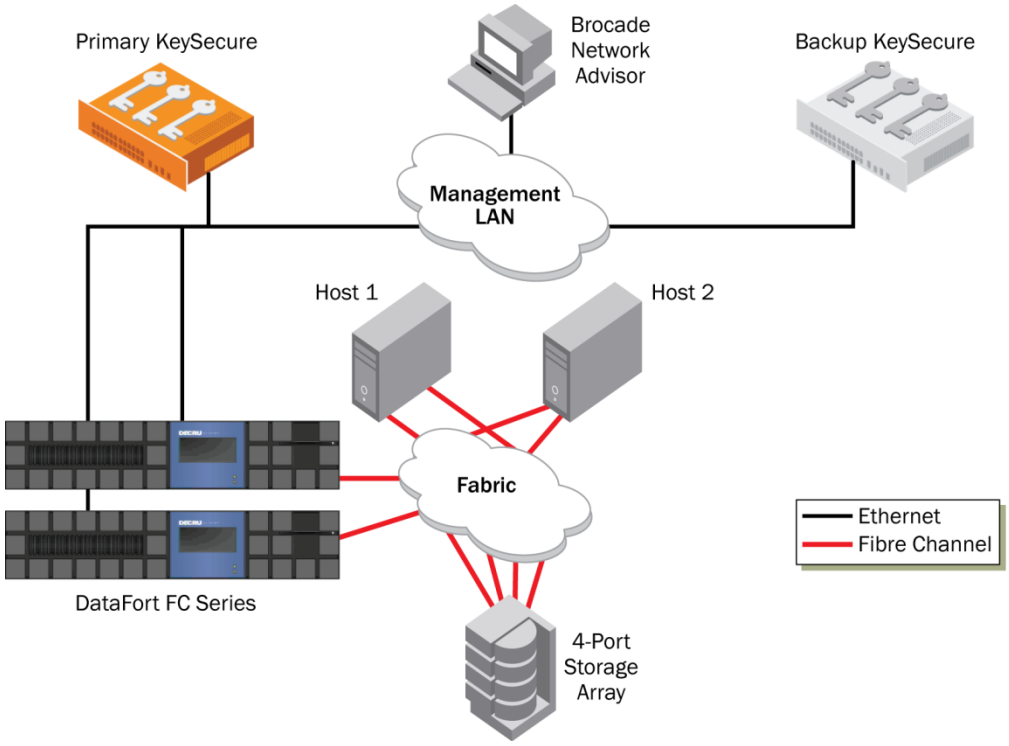

Figure 7. Initial deployment

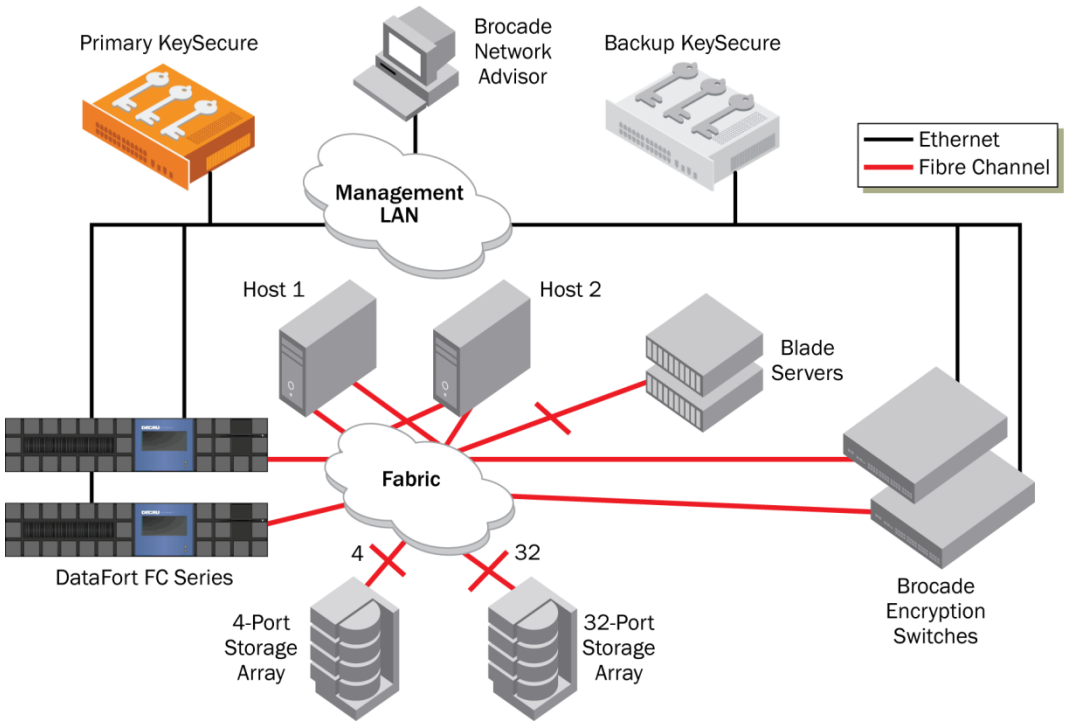

Figure 8. Upgraded deployment

SUMMARY

The scenarios in this paper illustrate how the Brocade encryption solutions and SafeNet KeySecure work together to provide reliable and trusted encryption and key management solutions. The basic configuration with redundant SafeNet KeySecure appliances and Brocade encryption solutions shows how the joint solution ensures high availability to encrypted data, while securing, sharing, and centralizing all of the encryption keys into a hardened hardware appliance. Brocade, NetApp, and SafeNet have also designed solutions so that existing systems can easily be upgraded to achieve high port density. While using the same SafeNet KeySecure appliances, an administrator can use the latest hardware running at 8 Gbps per port and encryption processing power that starts at 48 Gbps and scales to 96 Gbps on the Brocade encryption solutions. Combining power and ease of use, these encryption solutions also deliver compliance to the most stringent regulations.

Together, NetApp, SafeNet, and Brocade have combined their expertise in security and storage networks, respectively, to provide the leading Fibre Channel data-at-rest encryption solution. With FIPS 140-2 Level 3 validation, customers are assured the highest level of security. NetApp, SafeNet, and Brocade also provide consulting services to make it easier to plan and deploy the solution. Given the years of experience in storage networking and encryption from NetApp, SafeNet, and Brocade, customers have peace of mind knowing that their data is secure and protected with the latest encryption technology.