DECRU®
A NetApp Company

Secure Backup and Recovery Whitepaper

Securing Data in Backup and Disaster Recovery Sites with Decru DataFort™ Appliances

September 2005

Secure Backup and Disaster Recovery

Secure Backup and Disaster Recovery

Introduction

As organizations seek to manage and store burgeoning volumes of data, storage networks continue to increase in size and complexity. IT teams are tasked with the growing challenge of ensuring this mass of data is available -- they must back it up, restore it as needed, and ensure it is protected in the event of a disaster. Today's backup technologies go a long way toward addressing these requirements. However, they do not take into account the security and privacy of the data itself.

By nature, backup procedures introduce additional threats to stored data: with each additional distributed copy of cleartext data, organizations increase the risk of unauthorized access. Most disaster recovery plans place data offsite in a remote or outsourced facility, most likely with less stringent security. Further, information density continues to increase. When hundreds of gigabytes of data are easily stored on a single backup tape, the stakes go up significantly if that tape goes missing.

Decru provides solutions that dramatically simplify data security in these scenarios. By encrypting data before it is ever written to disk or tape, Decru DataFort ensures that only authorized people are able to read data, and fully protects data against unauthorized access if a disk or tape is lost or stolen.

This paper provides recommendations for deploying Decru DataFort storage security appliances to lock down data in a variety of backup and disaster recovery environments.

Decru DataFort™ Storage Security Appliances

Decru DataFort™ storage security appliances use wire-speed encryption, authentication, and access controls to secure stored data. Decru appliances can be deployed transparently in SAN, NAS, DAS and Tape environments, with no changes to servers, desktops, applications, or user workflow. By locking down stored data with strong encryption, and routing all access through secure hardware, DataFort radically simplifies the security model for networked storage.

There are three models of Decru DataFort appliances. DataFort E-Series supports Gigabit Ethernet for NAS environments. DataFort FC-Series appliances support 1 and 2-Gig Fibre Channel networks, and can support both disk and tape encryption. DataFort i-Series appliances are designed to secure data in iSCSI storage networks.

Decru DataFort appliances are engineered with key objectives in mind, including:

- **Security** – All encryption and key management are handled in secure hardware, ensuring maximum security with minimum complexity for end users and administrators. Decru DataFort's encryption engine, the Storage Encryption Processor (SEP) has been certified by NIST for compliance with FIPS 140-2, level 3.
- **Interoperability** –DataFort is fully compatible with existing backup configurations and mechanisms, as well as third-party backup software such as VERITAS and Legato.
- **Transparency** – DataFort can be deployed transparently into the existing infrastructure, without requiring changes to clients, servers or backup processes.
- **Performance** – The overall performance of the backup/restore environment must be maintained.

Secure Backup and Disaster Recovery

DataFort Deployment in Primary Storage

To best understand DataFort functionality in backup environments, it is helpful to understand a typical DataFort deployment within primary storage, such as NAS or SAN.

Network Attached Storage (NAS)

DataFort appliances can be deployed to solve a range of security concerns. To protect data in primary storage, DataFort E-Series appliances can be deployed between clients and the storage array, ensuring that sensitive data is written to disk in a secure, encrypted format. DataFort essentially functions as a storage proxy: Application servers and other storage clients see it as another storage server, while storage servers view it as a client. Clients write data to DataFort using CIFS or NFS, encapsulating the data in IPSec (if configured) for maximum protection. DataFort encrypts the data at wire-speed in a manner optimized for static data, then writes the encrypted data to the storage server, into a DataFort-encrypted share or volume – a Cryptainer™. Data flows through the same process in reverse for data read from storage by an authorized user.

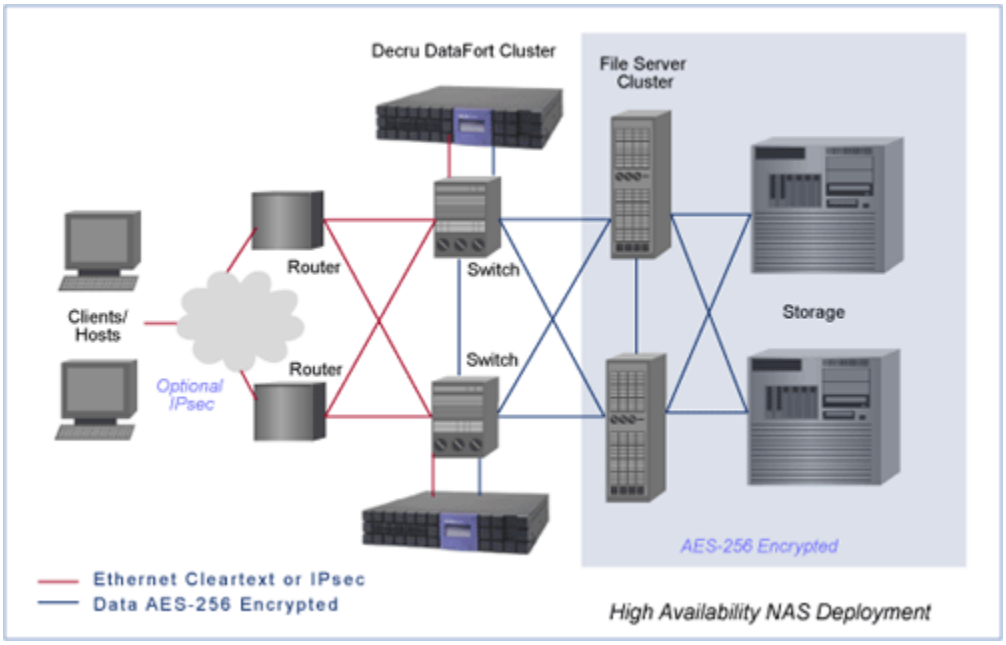

Figure 1: Clustered DataFort E-Series Deployment in a NAS environment

Because it is a proxy, DataFort does not need to be placed *physically* within the network path -- it only handles those requests that are directed to it by clients. Storage requests that do not require the security of encrypted storage, or that have not yet been migrated into secure storage, continue to function exactly as they do without DataFort.

Storage Area Networks (SAN)

DataFort FC-Series appliances can be added to existing SAN infrastructure without impacting network functions or data availability. As with NAS, DataFort effectively separates the network into two parts: a cleartext (unencrypted data) portion and a ciphertext (encrypted data) portion. In SANs, hosts (rather than users) are connected to the cleartext side, and the storage devices are connected to the ciphertext side. Two separate HBAs are available to make these connections.

Secure Backup and Disaster Recovery

Basic installation places the DataFort in the SAN environment so that data passes from network hosts through the DataFort for encryption and on to storage targets. When data is read from storage, the process occurs in reverse, with the DataFort decrypting the data before it reaches the host. This encryption and decryption procedure occurs at line speed, and is invisible to the host.

Clustering
Multiple DataFort appliances on a single network provide failover protection and increased performance, as SAN DataFort appliances can operate in Active/Active mode. A recommended installation includes two DataFort devices per network segment, though the number of devices that should be installed within the network depends on total data throughput.

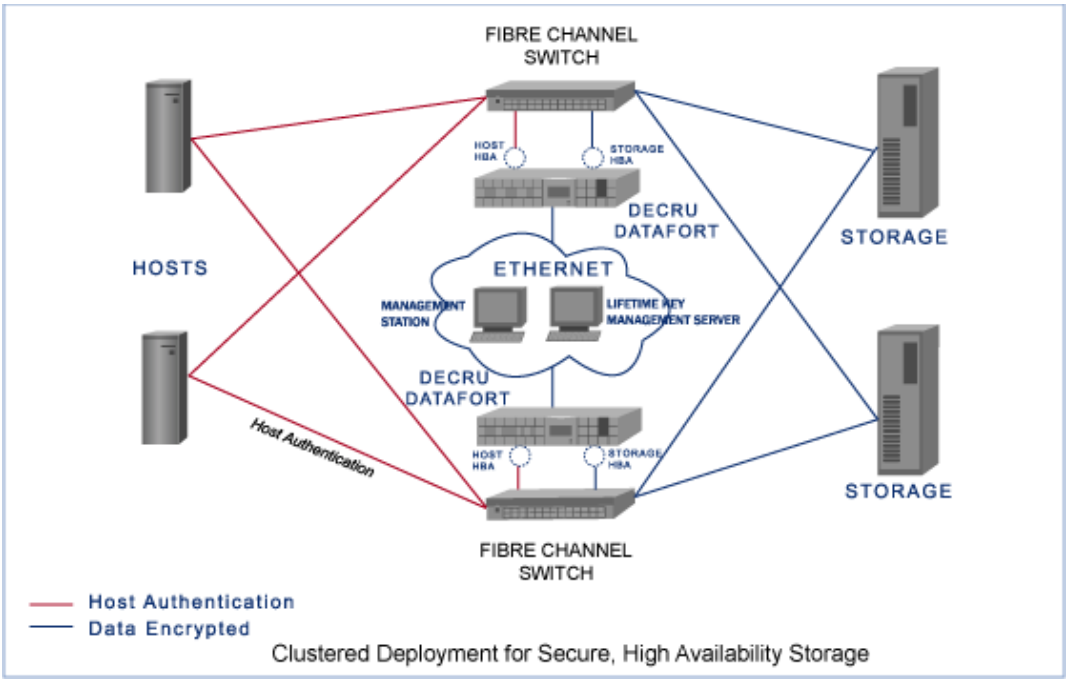

Figure 2: Clustered DataFort FC-Series deployment in a SAN environment

Components of a Simple Backup System

Defining a "typical" backup system can be as difficult as defining a typical network topology, as there are so many variations between organizations. Further, different vendors frequently refer to each component with slightly different terminology. However, in *most* environments, there are **data servers** that need to be backed up, **tape libraries** to receive the data, and a **backup client** to configure and potentially perform the backup. In many cases, there is also a **data mover** that performs the "heavy lifting" of backing up the data from the server to the tape, or vice versa in a restore operation.

As these components are all logical entities, it is possible that the components would physically co-exist on the same system in some cases. For example, in direct attached storage, the data server, tape library, and data mover could all be the same machine.

Secure Backup and Disaster Recovery

Securing Backups in Network Attached Storage

Integrating Decru DataFort appliances into file server (NAS) environments is typically seamless, both for CIFS and NFS implementations. Because DataFort sits *in front* of the backup and restore system components, the data behind it is always encrypted, and therefore secure. In other words, the main data path between the **data server, data mover, and tape library** does not pass through the DataFort (as they are behind the DataFort). This is done for several reasons:

- The data is encrypted once to primary disk.
- The bulk backup/restore traffic does not have to flow through the DataFort.
- Data to be backed up from the servers is already encrypted, allowing for completely secure backups and restores.

Because metadata is left in cleartext, backup software accesses files normally, so backup operations do not need to be changed.

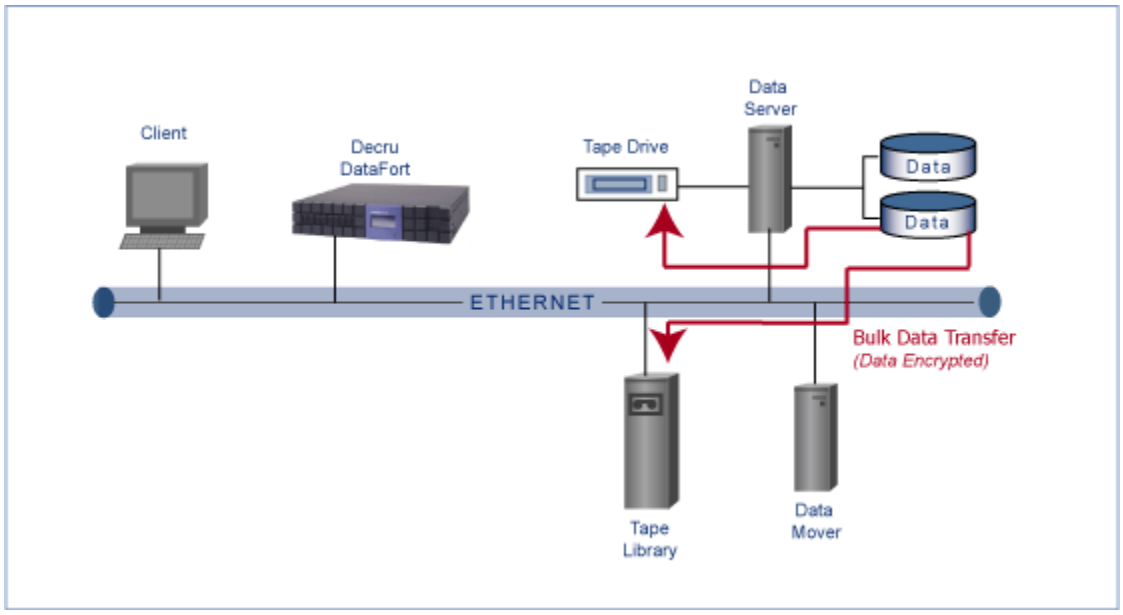

Figure 3: A typical DataFort implementation for Direct Attached or NAS storage

File Name Encryption

There is one optional security feature available in E-Series DataFort appliances that has implications for backup operations. DataFort supports two options for File Name Encryption: **Off** or **On**. As the name implies, File Name Encryption not only encrypts the contents of the file, but also encrypts the file name itself.

With File Name encryption turned off (the default setting), the filename is unencrypted and can be saved in backup indexes for single-file or bulk restore operations. However, for organizations with more stringent security policies, Decru DataFort E-Series appliances can be configured with File Name Encryption **On**. This does have an impact on granularity for backups and restores, as only complete restores (non-indexed) are possible.

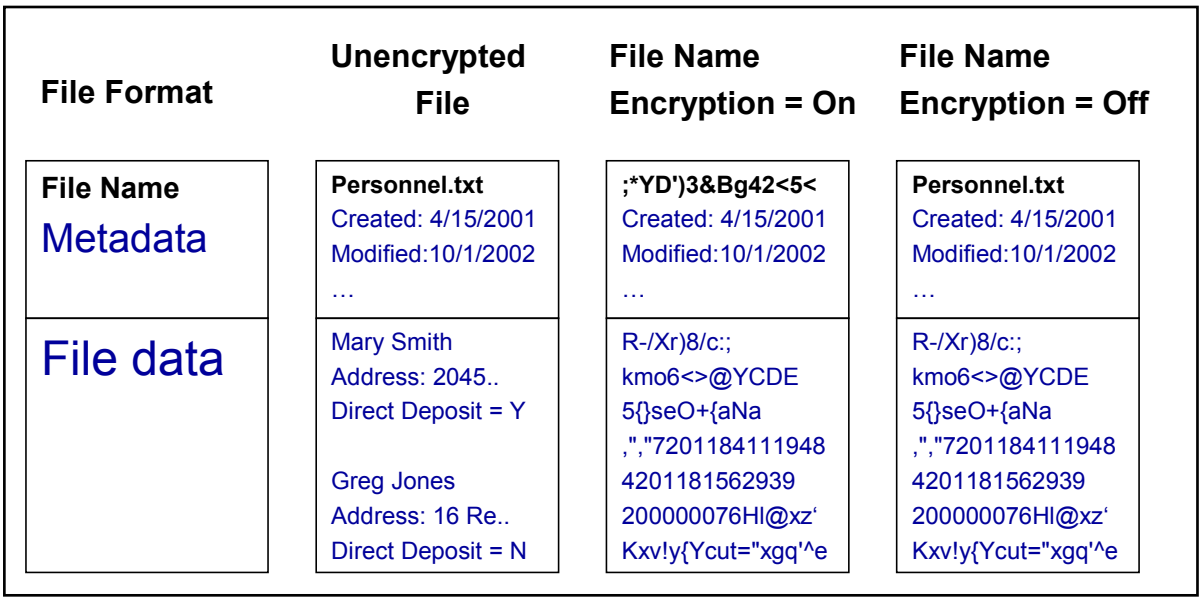

Figure 4: File Name Encryption

Data Restores

When restores are made to the same Cryptainer (a DataFort-encrypted volume or share) where the data was backed up, no changes are required to the normal restore procedures, and the restore operation is completely transparent to both the administrator and the end user. Administrators may decide to use a specific directory per volume for restores, or simply restore to the original directory. It is possible to restore data to another location using the secure procedures defined by Decru's Lifetime Key Management System. For more information about Lifetime Key Management, additional whitepapers are available.

Snapshots

Snapshots are commonly used within backup operations for NAS environments. Snapshots create a virtual copy of a filesystem, usually on the same disk. Some of the features of snapshots include: providing a view of the filesystem at the exact moment the snapshot was taken, the ability to maintain several snapshots per filesystem, and the ability to create the virtual copy in mere seconds, versus the time it would take to perform a full copy or backup. Other technologies used for disaster recovery operations, such as SnapMirror technology from Network Appliance, are discussed in the next section.

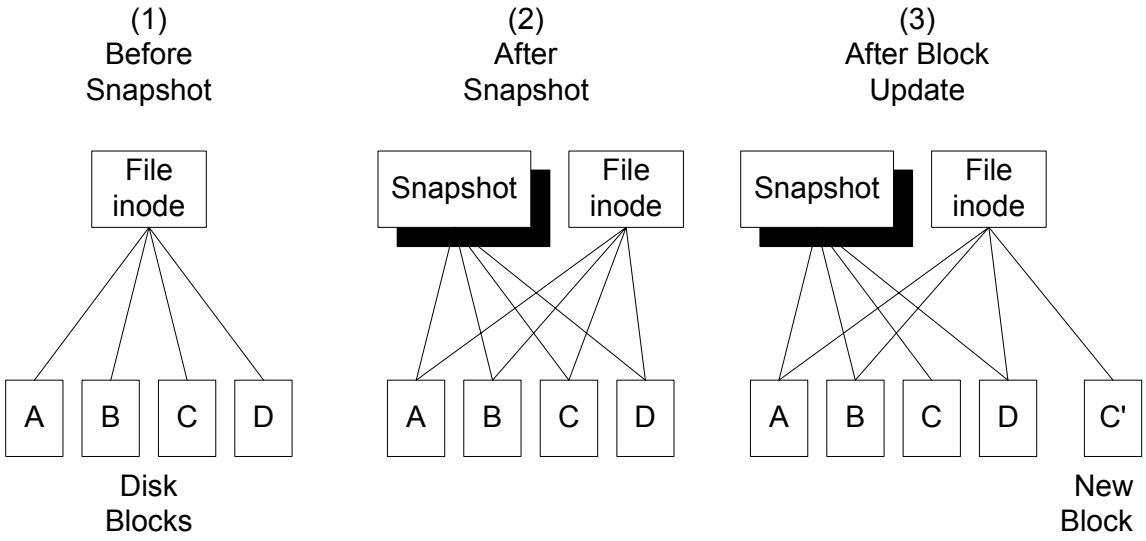

Figure 5: Virtual copies of data using snapshot technology

DataFort works seamlessly in snapshot environments where the virtual copy of the filesystem is made to the same disks, or in this case, the same Cryptainer. In cases where the snapshot is not on the same physical set of disks, the user or administrator has several options. With the NAS 2.0 firmware release, which began shipping in April, 2004, DataFort supports the creation of "Cryptainer aliases" – Cryptainer vaults that span several disparate locations. This way, an administrator can define a specific location as a target for all snapshots of a given Cryptainer. If Cryptainer aliases are not defined, recovery is still quite easy, but it requires the administrator to copy the data to the original Cryptainer before users can access the file in non-encrypted form.

It is important to note that a snapshot should not span several Cryptainer vaults, or include both cleartext and encrypted data.

SnapMirror

As snapshots do not protect against physical problems such as blocks going bad or disk failure, administrators may choose to copy file systems to another disk or location. For example, SnapMirror™ is a Network Appliance-specific technology that allows for mirroring of snapshot data to a remote filer. Other storage vendors have similar proprietary features. The remote filer can be located anywhere across a LAN or WAN.

In a typical environment, the same DataFort (or DataFort cluster) will be accessing both primary and mirrored data. The administrator will configure a Cryptainer Alias for the SnapMirror target, so the mirrored data will be recognized by DataFort.

In the event that a primary filer fails, Decru DataFort appliances will use the remote filer in a transparent fashion. After failure of a primary filer, the clients accessing that filer will switch to the mirror image, as exported by DataFort. Since DataFort maintains all the encryption keys for the cluster, users may continue to access data without interruption.

In the event that a separate DataFort cluster is serving the mirrored data, Decru's Lifetime Key Management System (LKM) can be used to replicate the Cryptainer key from the primary to the remote DataFort cluster. A Cryptainer Alias is not needed in this case.

Secure Backup and Disaster Recovery

NDMP

Network Data Management Protocol (NDMP) is an open standard for centralized control of enterprise-wide data management. NDMP was originally developed by Network Appliance and PDC (since acquired by Legato), and the standard is now administered by SNIA. Although the details of the protocol are complex, the central idea of NDMP is the separation of data control from data transfer.

As with other backup/restore methodologies, the Decru DataFort works transparently with NDMP when the network is configured such that the DataFort is in front of the backup/restore components. All NDMP devices are able to function as necessary behind the DataFort, as illustrated in the figure below.

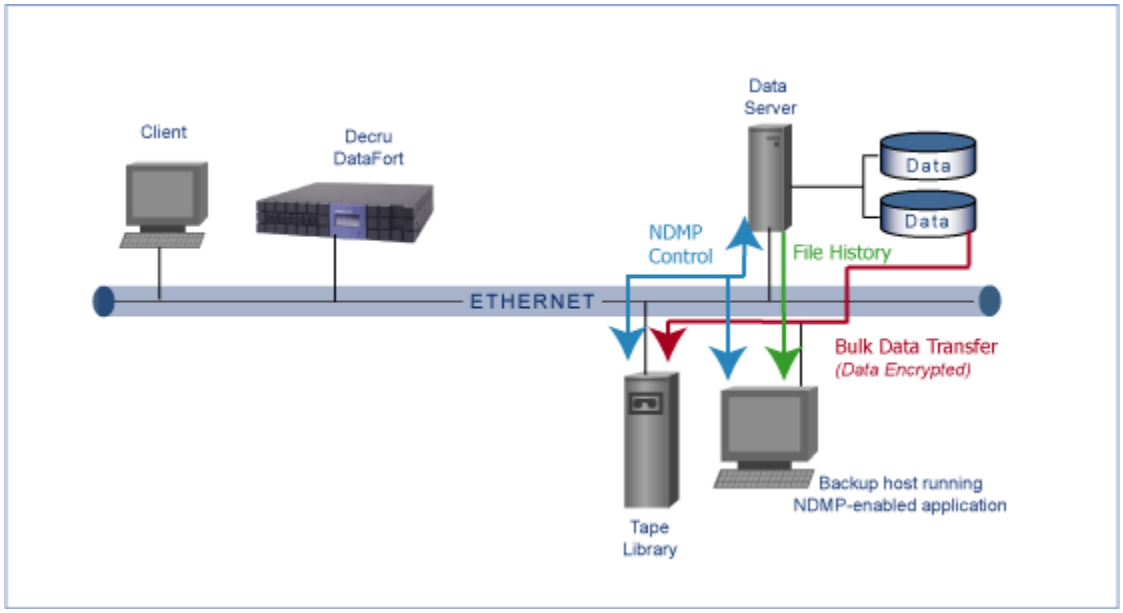

Figure 6: NDMP data flow, independent of the DataFort

Securing Backups in Storage Area Networks

Although there are many cooperative technologies and similarities between NAS and SAN backup environments, SAN backup/recovery is usually described using different terminology. The three main SAN backup topologies are LAN-free, Client-free, and Server-free.

The quick definitions are as follows:

- **LAN-free** – The bulk data flow occurs between the backup client (application server) and the tape library, with the backup client CPU performing the backup, thereby using CPU cycles of the client but without loading the LAN.
- **Client-free** – The bulk data flow is between the back-end disk array through the backup server and to the tape library. In this case the client (data server) is freed from performing the backup.

- **Server-free** – The bulk data flow goes directly from the disk array to the tape library. This topology is supported through the use of the SCSI *extended copy* command, or in some cases vendor proprietary features.

As Server-free is the newest technology, it is currently not as widely deployed. Both LAN-free and Client-free are in extensive use today. Decru DataFort easily supports both LAN-Free and Client-free topologies, and the most common deployment options are explained in more detail in the following paragraphs.

LAN-free

LAN-free backup was one of the first backup methods used in SAN environments. As SANs have continued to grow in size and usage, some shortfalls in LAN-free backups have led to development of other backup methods. Common difficulties associated with LAN-free backups include high CPU, backplane, and memory usage on the data server, as well as application interruption during backups and restores.

Regardless of the potential drawbacks, Decru DataFort appliances easily support LAN-free configurations. There are several possible configurations, depending on whether DataFort has been deployed to secure data in primary storage. If an organization wants only to encrypt data going to tape, DataFort is placed between the Backup Client and the tape library, and it will encrypt data as it flows to tape. (See figure 7). If data in primary storage is encrypted, a DataFort FC-Series appliance or cluster of appliances can be used. In this scenario, DataFort will encrypt data stored on the primary disk. When a backup is initiated, DataFort will decrypt the data as it is copied to the Backup Client, and then re-encrypt the data as it is moved to the tape library. Because DataFort is designed for wire-speed encryption, performance degradation will not be a problem.

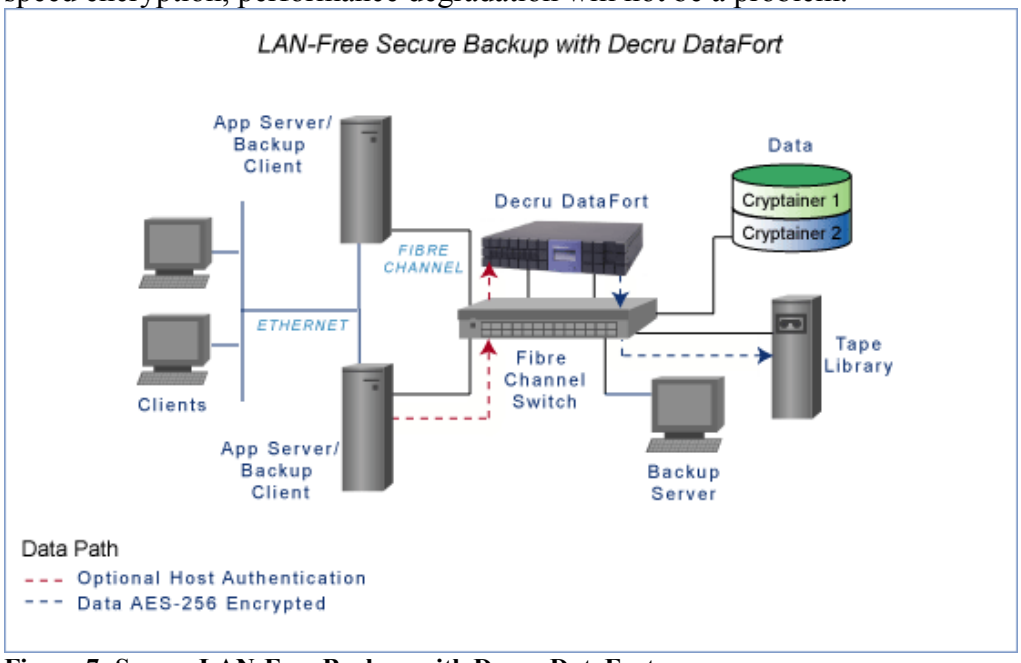

Figure 7: Secure LAN-Free Backup with Decru DataFort

Secure Backup and Disaster Recovery

Client-free

Decru DataFort also supports Client-free backup. Client-free environments allow for highly-secure backups and restores, while allowing flexibility in backup operations. There are several DataFort deployment options for Client-free backups, depending on the desired outcome.

Securing Data in Both Primary and Secondary Storage: To achieve the highest level of security for Client-free backups, it is important to design the topology such that the Decru DataFort is *in front* of the backup server, storage, and tape libraries. This way, the data to be backed up from the servers is already encrypted by the DataFort, allowing for completely secure backups and restores. (See Figure 8).

Securing Only Secondary Storage: If an organization wishes to encrypt only backup tapes, DataFort FC-Series appliances can be deployed between the backup server and the tape library.

Because the DataFort FC-Series encrypts data in blocks rather than files, all the blocks seen by the backup server are encrypted, so backup/restore operations must be at the block level. Methods for encrypted Client-free backup and restores must be either full backup/restores at a device or logical volume level, or incremental backup/restores at a block level.

> NOTE: If file-level backup is desired in a SAN environment, we recommend using the NAS DataFort E-Series appliances for data encryption. The storage arrays are attached to the filers via Fibre Channel, and everything else remains the same as in a file-based NAS environment.

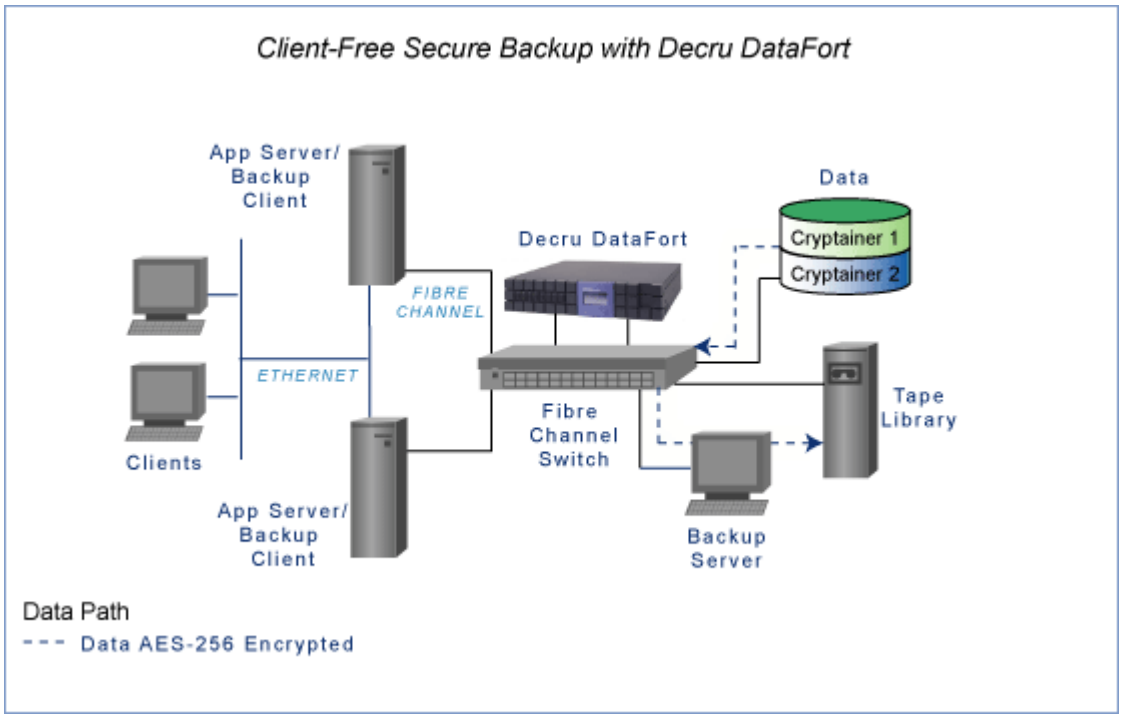

Figure 8: Secure Client-Free Backup with Decru DataFort

Secure Backup and Disaster Recovery

Server-free

As described earlier, Server-free technology is a relatively new addition to backup and restore methods for SANs. This topology is supported through the use of the SCSI *extended copy* (xcopy) command, or similar vendor proprietary features.

Currently the Decru DataFort FC-series appliances do not support the xcopy SCSI command for Server-free environments. However, a backup server operating *behind* the DataFort can use xcopy to copy encrypted data from disk to tape. This operation works seamlessly as data is copied directly from the storage array to the tape library. In this case too, the backup/restore operations are done at the block level.

Securing Mainframe Tape Backups

Decru has partnered with several technology leaders to enable high-performance encryption for data written to backup tapes from mainframe systems. Decru has tested interoperability with Luminex, NearTek, and Fujitsu Siemens, providing a range of options for companies with mainframe, as well as open systems storage.

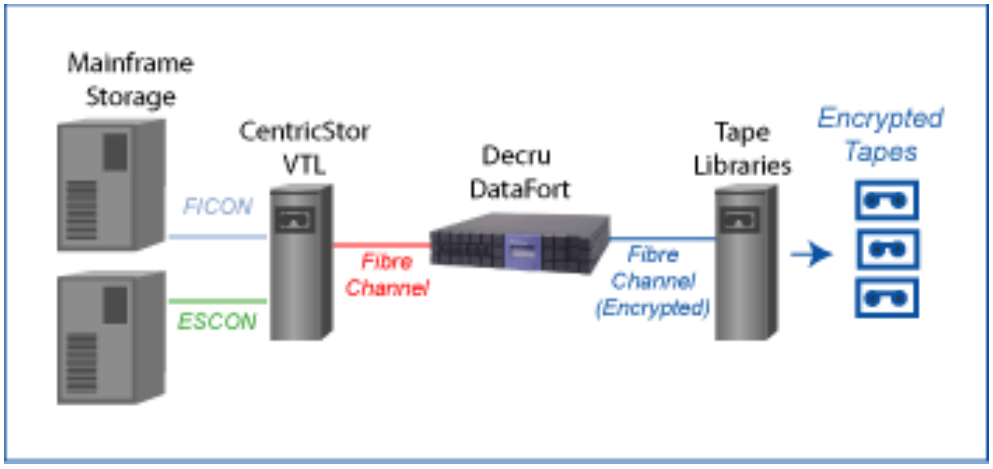

Figure 9: Example: Secure Mainframe Tape Backup with Decru DataFort and CentricStor

Disaster Recovery: SAN Mirroring

Both local and remote SAN Mirroring are useful tools in SAN backup and recovery. The backup procedure usually involves:

- Shutting down the application or placing it in backup mode, and flushing the cache
- Establishing a mirror
- Splitting the mirror
- Mounting the mirror on the backup server and writing to tape

Decru DataFort can operate in mirrored environments. As the data is already encrypted on the storage arrays, the mirrored data is also encrypted – ensuring that it secure both in flight and at rest. Similar to a NAS deployment, this mirrored copy can then be

Secure Backup and Disaster Recovery

transferred to tape, or in the event of a system failure, can be configured as the primary storage array. If the DataFort appliances in the local and remote sites are configured as a cluster, they will automatically and securely share encryption keys between them. If the primary array is unavailable, the remote DataFort-Storage deployment can be utilized immediately.

If the remote location is a dark or semi-dark site used entirely for disaster recovery, additional options are available to ensure data can be decrypted via the remote location.

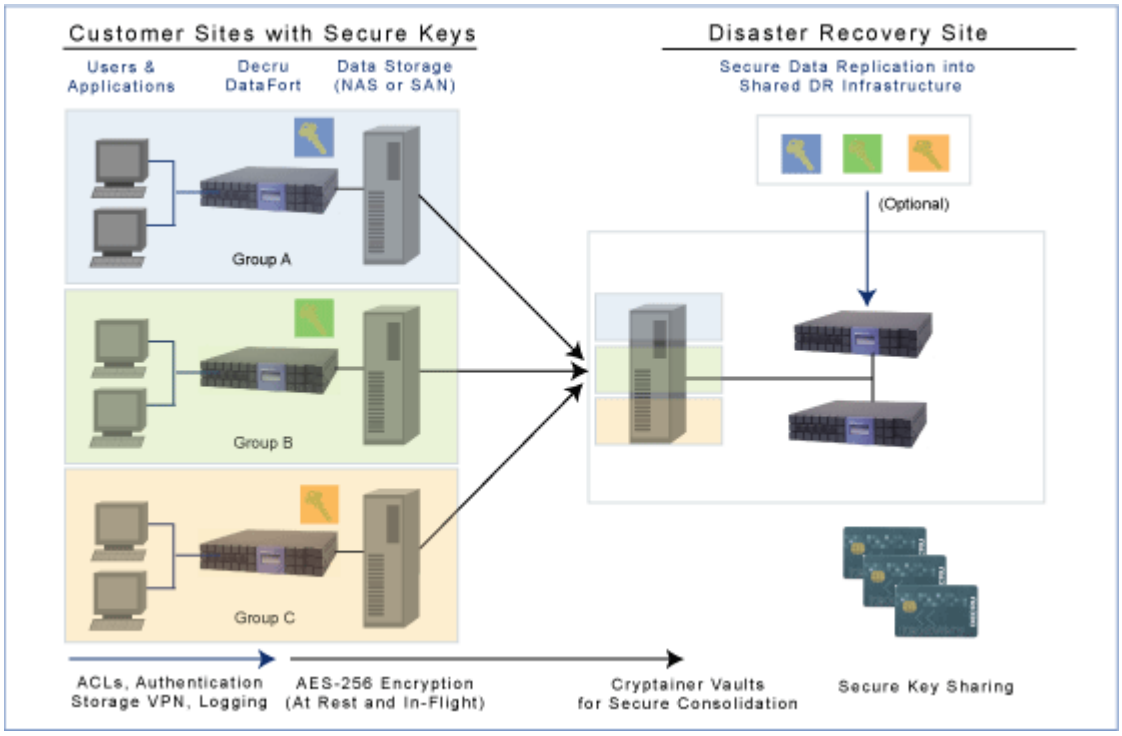

Figure 10: Secure Disaster Recovery with DataFort

Lifetime Key Management™ System

Decru's Lifetime Key Management™ System is a software utility that automates the secure backup and archiving of encryption keys from all DataFort appliances within an enterprise. This powerful software also enables administrators to quickly "clone" a new DataFort by pulling a configuration database from LKM, and presenting it with a quorum of Decru Recovery Cards to a new DataFort.

In a disaster recovery scenario, an organization can maintain a hot or cold standby DataFort at the mirrored location. Data will be stored in a secure, encrypted format until it is needed. When access to data in that site is required, DataFort can be quickly updated with the latest configuration database, and data will be accessible in less than an hour. For more information on LKM, visit Decru's website at http://www.decru.com/products/ltkm.htm.

Secure Backup and Disaster Recovery

Software Recovery Tool

The Software Recovery Tool (SRT) is a version of DataFort decryption that can be run on a standard server. It can be used for secure information sharing, as well as for disaster recovery scenarios.

Many organizations use backup tapes to share data with customers or partners, but are concerned about the repercussions if those tapes fall into the wrong hands. DataFort supports the ability to generate encryption keys for specific tapes, or for specific customers or partners. The data on the tape is encrypted at the primary location, and then sent in secure format to the customer or partner. The key is sent separately, via email or another format. The recipient then uses the Software Recovery Tool to decrypt the data on the tape. While the SRT will decrypt significantly slower than a DataFort appliance, it is perfectly adequate for smaller amounts of data.

For additional protection in Disaster Recovery environments, or in extreme cases where a DataFort may not be available on the network, Software Recovery Tool can be used to ensure data can be decrypted. The SRT can be used in conjunction with DataFort Recovery Cards to decrypt DataFort-encrypted data using Windows, Linux and/or Solaris servers. This ensures that data will always be recoverable, even in the event that DataFort hardware is rendered inoperable.

Conclusion

In summary, Decru DataFort storage security appliances offer critical security for sensitive data both inside and outside the datacenter. Decru DataFort has been tested and certified for interoperability with a broad range of storage and backup vendors, and is the only transparent security appliance that supports all storage infrastructures.