Technical Report

Encrypting Snapshot Copies with SafeNet

Neil Shah, Clay Ryder; NetApp
July 2013 | TR-4209

A Complete Data at Rest Solution

This solution applies 256-bit AES encryption to NetApp® Snapshot™ copies and SnapVault® data without modifying or encrypting primary data. The solution is implemented through standard off-the-shelf offerings from NetApp and SafeNet to deliver highly effective encryption of backups and protect against unauthorized data access.

TABLE OF CONTENTS

LIST OF FIGURES

1 Introduction

This solution applies 256-bit AES encryption to NetApp Snapshot copies and SnapVault data without modifying or encrypting primary data. The solution is implemented through standard off-the-shelf offerings from NetApp and SafeNet, which are discussed in subsequent sections.

Data backups are created through Snapshot copies, which leverage the block-level incremental replication provided by SnapVault in conjunction with SafeNet StorageSecure and SafeNet KeySecure to deliver a disk-to-disk backup solution that is protected by 256-bit AES encryption.

This solution is compatible with clustered Data ONTAP®, which means it can be deployed to support primary data no matter where it resides on the NetApp infrastructure in clustered environments.

1.1 Solution Benefits

This encryption solution does not affect primary data operations. This is an important consideration for organizations that have deemed encrypting primary data as undesirable for either performance or architectural reasons.

The following are the key benefits of this solution:

- **No impact on primary data performance.** Organizations can achieve encrypted backups without any impact on operations. This solution does not disturb or modify primary data; this data remains in the clear and incurs no performance impact.
- **Secure use of commercial cloud-based storage.** Since the Snapshot copies (backups) are encrypted at rest, organizations can use commercial cloud storage to store sensitive data without risk of its contents being disclosed to unauthorized users.
- **Flexible access.** Access to encrypted backup data is readily available from multiple or replacement sources so long as the proper encryption keys are provided.
- **Scalability and flexibility.** As workloads respond to changes in the business environment, the scalable and flexible nature of this solution readily adapts to meet changing capacity and performance requirements.

2 Solution Overview

The Snapshot and SnapVault encryption solution is straightforward and easily implemented using the standard TCP/IP NFS, SMB (CIFS), and iSCSI protocols with few additional components. The solution utilizes a Linux® 5 or 6 data transfer server (DTS) to mount two NetApp volumes. The unencrypted primary Snapshot data volume will be mirrored to a secondary volume through the SafeNet StorageSecure appliance utilizing the NFS, SMB (CIFS), or iSCSI protocol. The secondary storage volume provides for a second backup of the encrypted data, which can also be mirrored to a third remote/off-site storage facility by NetApp SnapMirror® software.

2.1 Solution Components

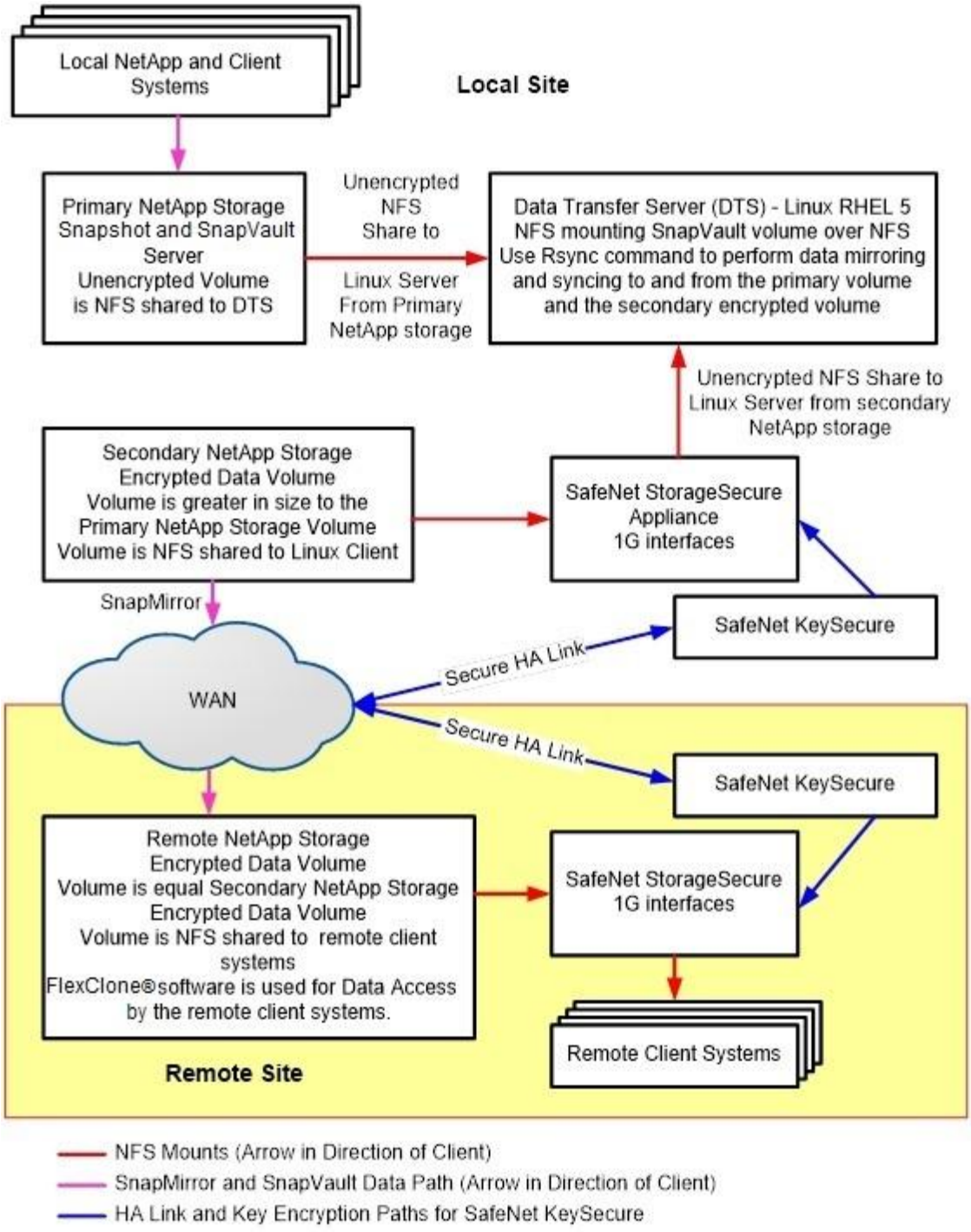
The encrypted Snapshot and SnapVault backup solution is composed of the following components:

- **Primary NetApp storage.** This is the existing NetApp storage implementation supporting NFS, SMB (CIFS), and iSCSI protocols that is hosting the primary data.
- **Data transfer server (DTS).** This is a Red Hat Enterprise Linux 5 or 6 system that includes the rsync command; it can be a standalone system or part of a VMware® deployment. The DTS mounts the Snapshot volume from the primary storage and the SafeNet StorageSecure appliance. The rsync command mirrors the data from the primary storage to the SafeNet mount point.
- **SafeNet StorageSecure appliance.** This provides the 256-bit AES encryption and decryption to and from the NetApp data volumes at the local and remote sites. Two appliances are recommended at each site to provide redundancy and maintain availability.
- **SafeNet KeySecure appliance.** This stores the encryption keys for the StorageSecure appliances. It is recommended that two KeySecure devices be deployed in a high-availability configuration with one at the local site and the other at the remote site.
- **Secondary NetApp storage.** This volume stores the encrypted Snapshot data and can be located on the primary storage or another NetApp system. The storage volume needs to be larger than the unencrypted primary storage because each encrypted file is 512 bytes larger than the original. The additional capacity required for this volume is determined by the number of files within the primary storage. The secondary storage requires SnapMirror software and the NFS protocol to be enabled.
- **Remote NetApp storage.** This NetApp system mirrors the encrypted Snapshot data from the secondary storage at the local site. The remote storage volume needs to be the same size as the secondary storage. The remote storage requires SnapMirror software and the NFS protocol to be enabled. The SnapMirror destination volume is NFS exported to the StorageSecure appliance.

2.2 Encryption Process Flow

The DTS mounts the primary data volume and utilizes the rsync command to mirror the data to a secondary NFS share. The secondary NFS volume data path passes through the SafeNet StorageSecure encryption appliance. This volume can be located on the NetApp system hosting the primary storage volume or on another NetApp system, as illustrated in Figure 1. The secondary volume (with the encrypted data) can be replicated by SnapMirror to a remote site or commercial cloud-based storage.

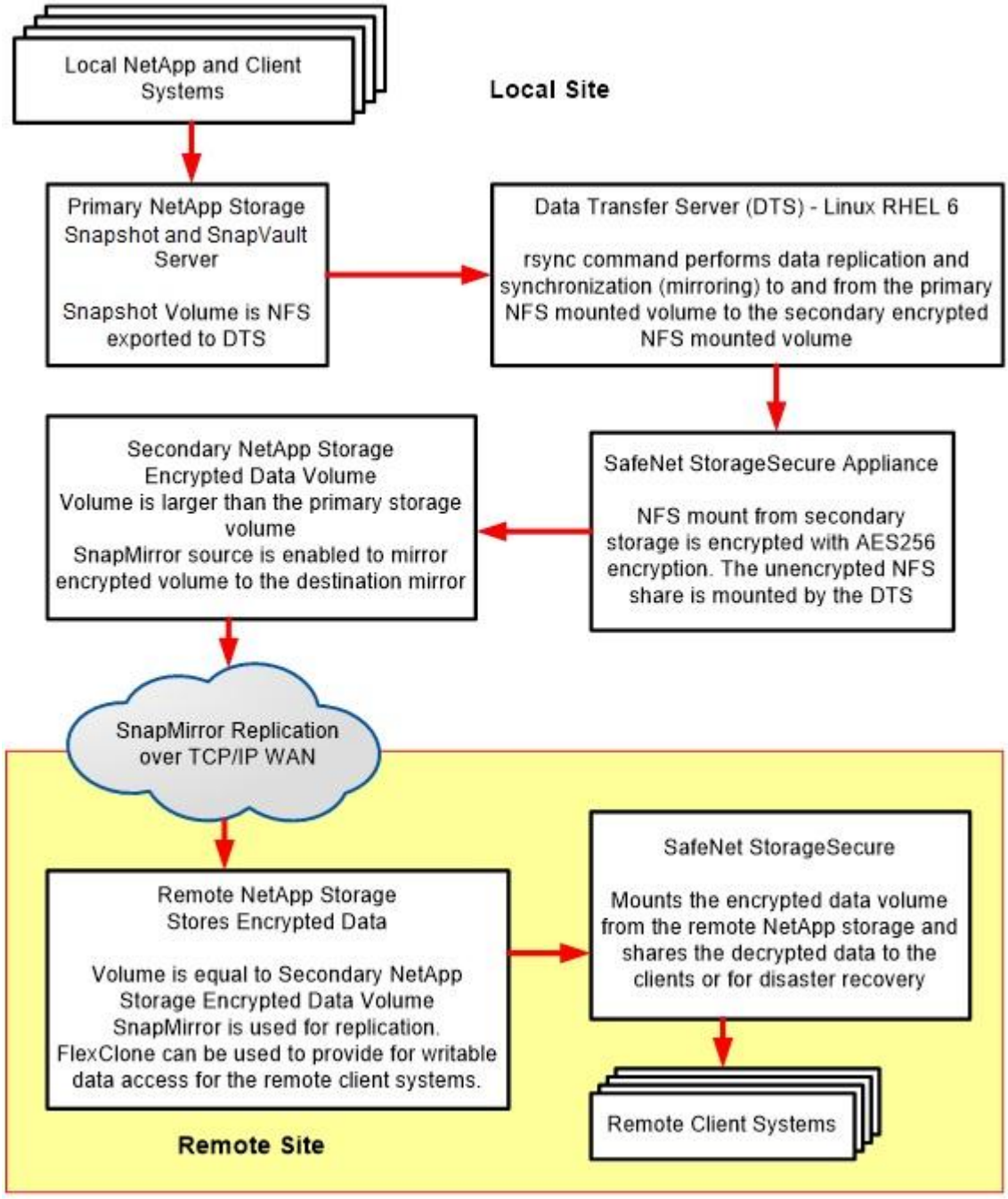
Figure 1) Encryption block diagram.



2.3 Data Flow Process

Proper data flow timing is essential for the solution. The DTS system should perform the rsync mirror update after the Snapshot and SnapVault operations are finished on the primary storage volume. If the remote data storage is implemented, then the SnapMirror operation between the secondary and remote NetApp systems should be performed after the DTS rsync command has completed. The data flow for this solution is referenced in Figure 2.

Figure 2) Data flow diagram.



3 Configuration and Setup

The volume configuration on the NetApp systems and the security configuration on the SafeNet appliances follow standard configuration practices. The solution does require some additional configuration steps for proper operation. Configuration and setup for each respective subsystem component of the solution are detailed in the following sections. NFS is the preferred protocol.

3.1 General

Make sure that the all of the systems can be reached and are known within the naming services.

3.2 Primary NetApp Storage

Export the Snapshot and SnapVault directory to the DTS system.

3.3 Secondary NetApp Storage

1. Create the secondary storage volume that will store the encrypted Snapshot copies according to these specifications:
   - This volume must not have Snapshot enabled.
   - The volume must be larger than the primary source volume to accommodate the additional 512 bytes of data added to each encrypted file for the hash string.
   - By default, set maxfiles to 1 inode per 32KB of volume size.

   When a volume grows, the inode count is increased automatically to MAXIMUM of (1 inode per 32KB of volume size, 33 million). This can be further increased to 1 inode per 4KB of volume size up to an enforced maximum of 2 billion inodes using the maxfiles (7-Mode) or the vol modify –files (clustered Data ONTAP) command.

   The secondary volume must also account for the full size of the primary volume without dedupe savings. The rsync program mirrors the NFS file system from the client level and does not recognize dedupe efficiency savings that were performed on the primary storage.
2. Make sure that the exported volume going to SafeNet StorageSecure has the same share and volume name as the volume connecting to SafeNet StorageSecure on the secondary SnapMirror storage.

   Note: This is required for the correct decryption to occur with the common keys between the StorageSecure high-availability pair.
3. Make sure that Snapshot has been disabled:

   ```
   vol options <Volume Name> nosnap on

   vol options <Volume Name> nosnapdir on
   ```
4. License and enable the SnapMirror software for the source SnapMirror operations:

   ```
   license add <SnapMirror license>

   options snapmirror.enable on
   ```
5. Export the SnapMirror primary volume to SafeNet StorageSecure.

3.4 SafeNet StorageSecure Appliance

1. Mount up the encrypted volume from the secondary storage.
2. Export a volume to the DTS system.

3.5 SafeNet KeySecure Appliance

1. Create necessary keys for the encrypted volume mounts.
2. Set up as a high-availability configuration if more than one KeySecure appliance is deployed.

3.6 Data Transfer Server

1. Make directory mount points for the primary and secondary storage:

```
mkdir /mnt/primary /mnt/secondary
```

2. Mount the primary storage:

```
mount <NetApp server>:<Snapshot Volume> /mnt/primary
```

3. Mount the StorageSecure mount. Use the -sync option; otherwise, the initial burst of data from the rsync command can lock up the appliance, and the error “Reached maximum entries in large packet pool on SafeNet” is triggered.

```
mount <NetApp server>:<Snapshot Volume> /mnt/secondary -o sync
```

4. Create the .decru file within the secondary storage if not already present.
5. Test the rsync command to make sure that the source data from the primary storage can be read and the destination mount from the secondary system can be written:

```
rsync –aHAXEv –delete –exclude '.decru' /<source mount point>
/<destination mount point>
```

3.7 Remote NetApp Storage

Note: The Data ONTAP version must be the same as the SnapMirror primary (secondary NetApp storage).

1. Create an aggregate to store the SnapMirror volumes.
2. Create the remote storage volume (SnapMirror secondary) that will store the encrypted Snapshot copies with the SnapMirror configuration tool according to these specifications:
   - This volume must not have Snapshot enabled.
   - The volume must be slightly larger than the SnapMirror primary source volume.

   Note: The initialize flag must be used for the first SnapMirror sync. The update option will be used for subsequent updates of the mirror.
3. Using NFS, export the SnapMirror secondary volume to the SafeNet StorageSecure appliance.
4. Make sure that the exported volume going to SafeNet StorageSecure has the same share and volume names as the volume connecting to SafeNet StorageSecure on the secondary SnapMirror storage.

   Note: This is required for the correct decryption to occur with the common keys between the StorageSecure high-availability pair.

Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

NetApp provides no representations or warranties regarding the accuracy, reliability, or serviceability of any information or recommendations provided in this publication, or with respect to any results that may be obtained by the use of the information or observance of any recommendations provided herein. The information in this document is distributed AS IS, and the use of this information or the implementation of any recommendations or techniques herein is a customer's responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. This document and the information contained herein may be used solely in connection with the NetApp products discussed in this document.

Go further, faster®

www.netapp.com