Spitfire StoreSafe Cookbook

Bloombase
Least Invasive Security

Bloombase
Least Invasive Security

Document No.

Contents

Introduction

Digital assets including financial reports, legal documents, private human resources information, confidential contracts and sensitive user data are invaluable properties of a corporation. A business cannot risk losing these information, both confidentiality and non-repudiation. Nevertheless, the Internet has becoming more pervasive, security attacks have grown. News and reports have revealed millions of dollars of loss in various enterprises and organizations due to security breaches.

Data protection at the persistence layer used to be an uncommon subject in information technology industry. Persistence data, in the old days, are assumed safely kept and stored in highly secure data centers with effective physical access control and close surveillance. However, trends in the industry in backup, archive and high availability with an aim to safeguard data from the worst attack and be responsive to rescues, keeping the enterprise core system running non-stop, have opened up chances confidential data get disclosed and tampered by unauthorized parties.

Numerous security compliance and standards including Sarbanes Oxley, Gramm-Leach-Bliley Act and Personal Data Privacy Ordinance have raised enterprises' awareness of securing their core business and customer data. However, persistence data protection is technically a difficult subject. One has to prepare for additional system complexity, loss of performance, at the same time, maintaining the same level of stability and scalability, and most important of all, be highly secure, hacker-proof rather than exposing more security loopholes.

Core business data of an enterprise constitutes a major segment of assets that a corporation possesses. Customer data, marketing strategies, intellectual properties in form of source codes and business logic, sales history and prediction figures, and other decision support numerical analysis as result of data-mining may often bury forward looking intelligence that in some sense have very high future value when put into good use.

A number of factors put persistence data at risk

- Office automation
- Company insider
- Information lifecycle management (ILM) and backup/restore (BURA)

- Disaster recovery (DR) and high availability (HA)
- Growth of storage data
- Storage consolidation
- Inter-corporate application integration
- Storage device
- System backdoors
- Viruses, worms and spyware
- Remote accessibility
- Hardware disposal handling
- Outsourcing
- Effective perimeter protection

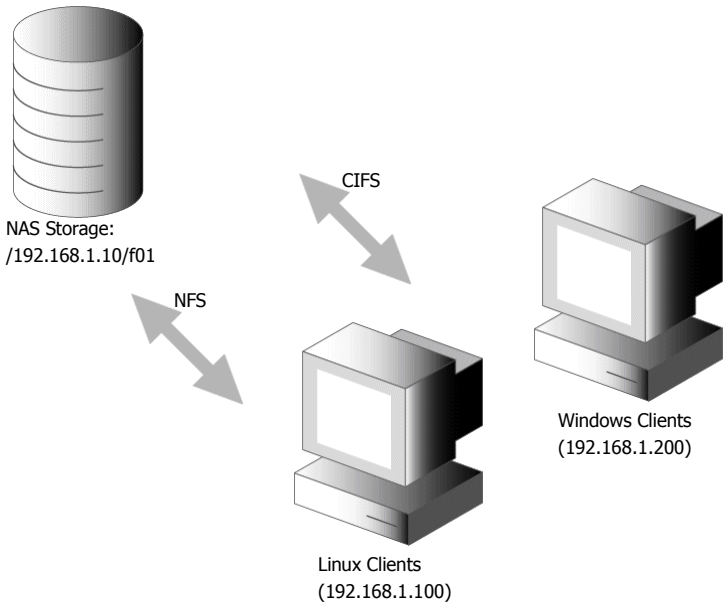
This paper studies how Spitfire StoreSafe enterprise storage security server helps to fill in the missing puzzle of enterprise data threats and serves as a cookbook for a number of typical applications in today's enterprise computing environment.

Intellectual Property Protection

Problem

A Japan based video production and broadcasting company requires their multimedia data files be secured by their homeland information security standards.

The company's production artists use Adobe Premiere to edit and retouch video files which are stored centrally in their EMC network attached storage (NAS) sub-system. Their 3-D animation designers/engineers use their proprietary graphics software on Linux platform to render artificial graphics.



Challenges

Video data in form of files have to be encrypted by Japan's Camellia cipher, co-developed by both NTT and Mitsubishi, with at least 128-bit key length. Storage encryption products of vendors from the United States only support AES but not Camellia.

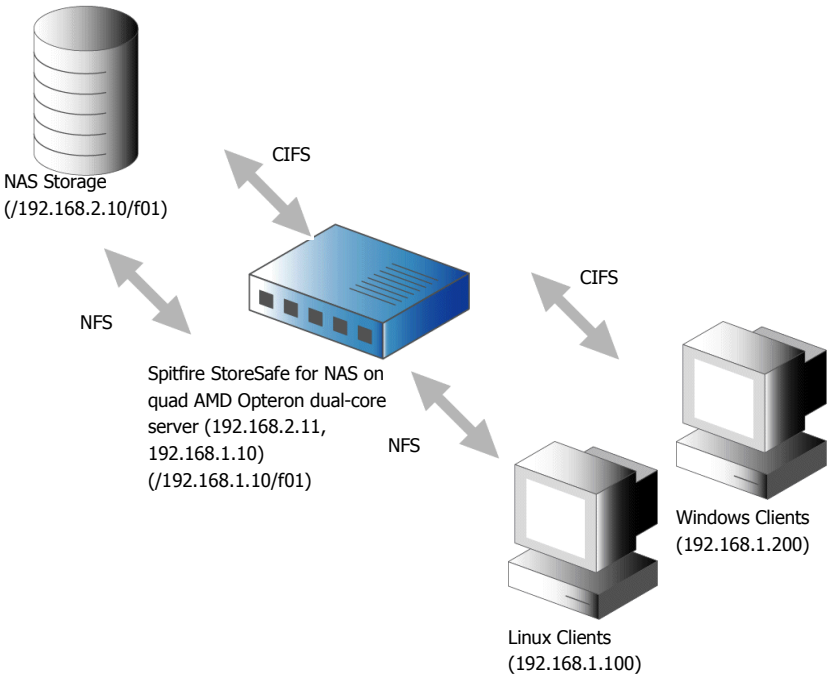
Video editors and animation designers should have no change in their daily workflow after implementation of data encryption.

Encryption should take place when media files are written to storage sub-system by Adobe Premiere and their proprietary graphics rendering software while decryption takes place when files are read. However, Adobe has no plan to add cryptography into their file handlers and their software engineers are not well equipped in cryptographic programming, second development of the render software would be highly risky and not cost-effective.

Digital video files are normally huge files. Video editing is a trial-and-error process with a lot of random file access. Data encryption engine has to be performance capable and supports random access of file contents such that file cryptographic processes can be carried out on the fly.

Solution

Spitfire StoreSafe for NAS enterprise storage security server is installed on a dedicated quad AMD Opteron dual-core with dual gigabit network interface rack-dense server to deliver wirespeed storage cryptography of digital intellectual property.



Spitfire StoreSafe acts as a bridge between the storage and host network as well as a storage cryptographic processor to encrypt and decrypt network storage data on-the-fly. To enable transparent deployment of Spitfire StoreSafe, one of its network interfaces has to take over NAS storage's IP address. The NAS storage server assumes a new IP from the administration network of subnet 192.168.2.0/255.255.255.0.

Configurations

Firstly, backup all data under f01 at the NAS storage and purge all data under f01 upon completion. The backup image will be used for data migration to the end of configurations. Release NAS storage's original IP address and rebind as 192.168.2.10.

Configure Spitfire StoreSafe appliance network interfaces by using serial console. Bind first network interface to NAS' original IP address 192.168.1.10

```
<Update IP Address>

Select Network Interface :
1) eth0
2) eth1
Select : 1
Configure IP address of <eth0>
Input new IP address [192.168.1.107]: 192.168.1.10
Input new netmask [255.255.255.0]:
IP address updated successfully
Press [enter] to continue
```

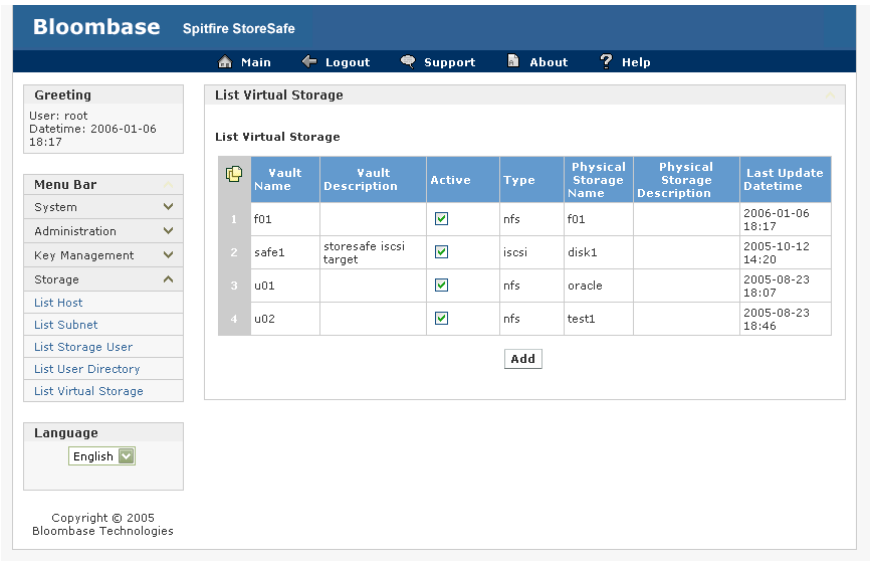
Then, bridge the host network with storage network at IP 192.168.2.11

```
<Update IP Address>

Select Network Interface :
1) eth0
2) eth1
Select : 2
Configure IP address of <eth0>
Input new IP address [192.168.1.108]: 192.168.2.11
Input new netmask [255.255.255.0]:
IP address updated successfully
Press [enter] to continue
```

Restart Spitfire StoreSafe appliance for it to pick up the new network settings

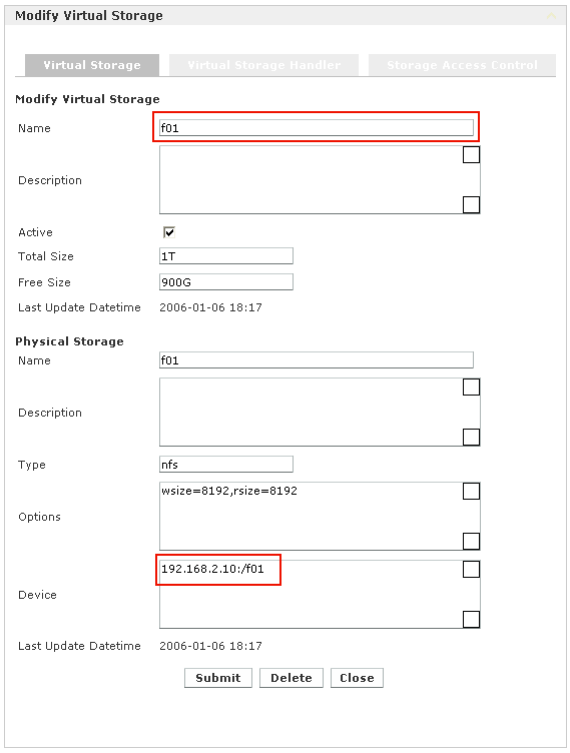
```
<Restart / Shutdown>

1) Restart
2) Shutdown

b) Back to Main Menu

Select : 1_
```

Open web browser (e.g. Internet Explorer, Firefox, Mozilla, etc) and point to https://192.168.1.10



Create virtual plain view of encrypted storage by clicking Add button, fill in details as follows. Virtualize NAS storage by Spitfire StoreSafe by naming it 'f01'

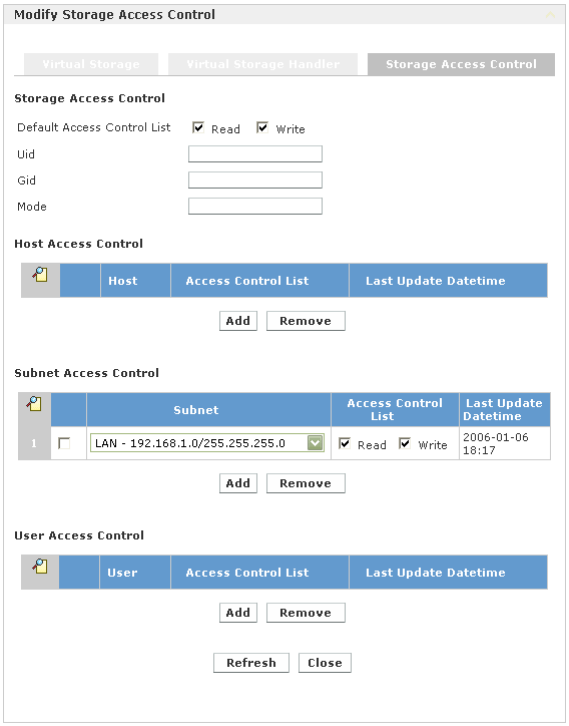
Field	Value
Virtual storage name	f01
Device	192.168.2.10:/f01



Turn to Virtual Storage Handler tab and input the followings. Camellia is Japan's official strongest cipher, thus, we take Camellia with 128-bit key strength for this setup

Field	Value
Key	Demo Valid 1
Encryption algorithm	Camellia 128-bit

Lastly the access control, as the virtual storage is supposedly only accessible by host network, simply add 192.168.1.0/255.255.255.0 to Subnet access control.



Commit the changes, a virtual plain network storage will be created on Spitfire StoreSafe delegating read/write and cryptographic operations between hosts and storage sub-system.

Data Migration

Backup archive is then restored at one of the host workstations to the NAS storage via Spitfire StoreSafe at /192.168.1.10/f01.

Benefits

As soon as data restore is done, users can work on the protected media files with no change in their desktop settings at no noticeable degradation in speed.

System administrators work on administration network at 192.168.2.0/255.255.255.0 while users work on host network at 192.168.1.0/255.255.255.0 providing basic network access control to the storage infrastructure.

Spitfire StoreSafe for NAS provides rich connectivity protocols including NFS, CIFS, FTP, HTTP for hosts of different platforms to consume data at the storage end.

Invaluable digital intellectual properties are stored in their encrypted form on physical hard drives, even if the hard drives are stolen, there is no way one can obtain the secret information inside without knowing the key.

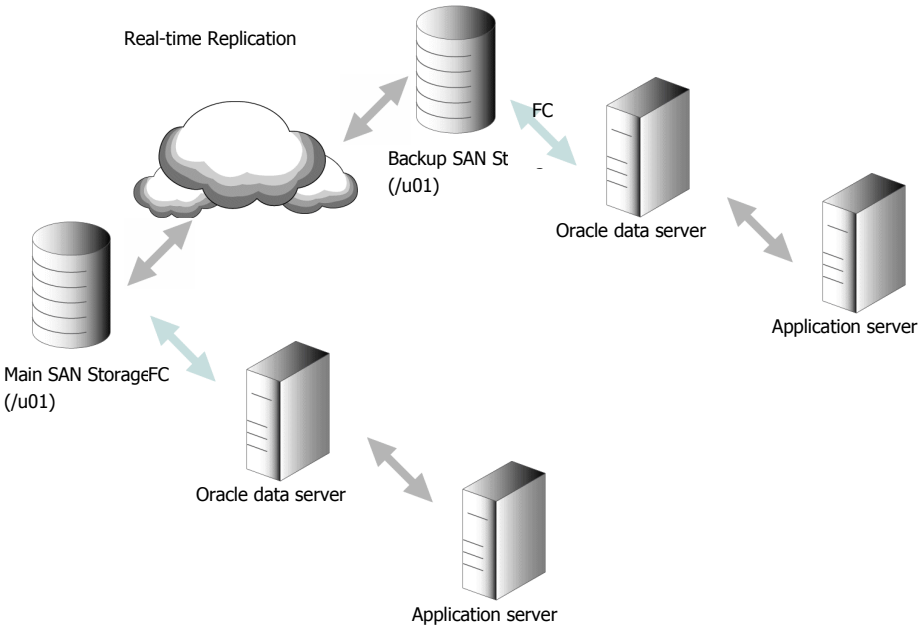
Backup and restore remain the same as before. Only difference is that it operates on the administration network, thus, backup archives are in their original encrypted form increasing data privacy for backup and offsite data.

Database and Real-time Replication Protection

Problem

A government security bureau processes large volume of trade declarations which needs to be secured as they are persisted into Oracle databases. As their system has been on production for years, it is required that data security has to be introduced without requiring application changes. Again, the system cannot tolerate throughput degradation by more than 30%.

Apart from the production system, they have another backup system which receives delta changes of the master database timely. At any one time the production system goes down, this resilience system will be switched over as the master system and resumes service.



Their system runs on a high-end enterprise class Sun Microsystems Sun Fire E6900 which is highly scalable and supports virtual containers. Their storage sub-system is a SAN from Sun Microsystems OEM'ed by Hitachi Data Systems.

They also mandate encryption keys to be safe-guarded at least at FIPS-140-1 level 2.

Challenges

Securing Oracle data files is not an easy task as data files are dynamic, they keep updated at all times which means static way of data encryption offered by encryption utilities are not going to fit the bill.

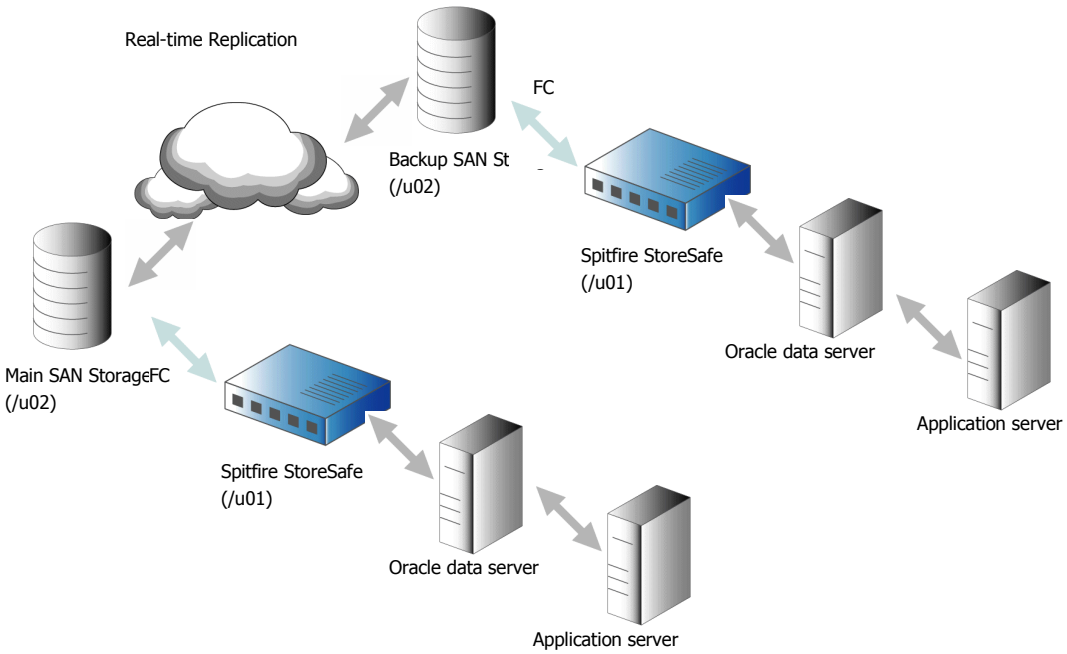
Sensitive data committed to Oracle data files will also be written to database redo logs, archive logs and flash recovery logs. Thus, to secure the system as a whole, all data files, redo, archive and flash recovery logs have to be encrypted.

The Oracle data server runs on a high end system with a very capable SAN storage sub-system, introducing encryption (AES 256-bit as suggested for government use) to the storage path at the same time achieving throughput degradation no more than 30%. It requires a highly multi-threaded, adaptive and scalable encryption solution which can hardly be entertained by ordinary encryption products.

It has to support both the active and standby systems, and guarantees smooth switch-over in worst case scenario.

Solution

To cope with the demanding speed and throughput, Spitfire StoreSafe is installed on the same physical Oracle data server rather than on separate dedicated server. The Oracle data server is scaled up by adding more processors and memory modules to provide enough processing power for both Oracle data server and Spitfire StoreSafe to run without being hunger for system resources.



Configurations

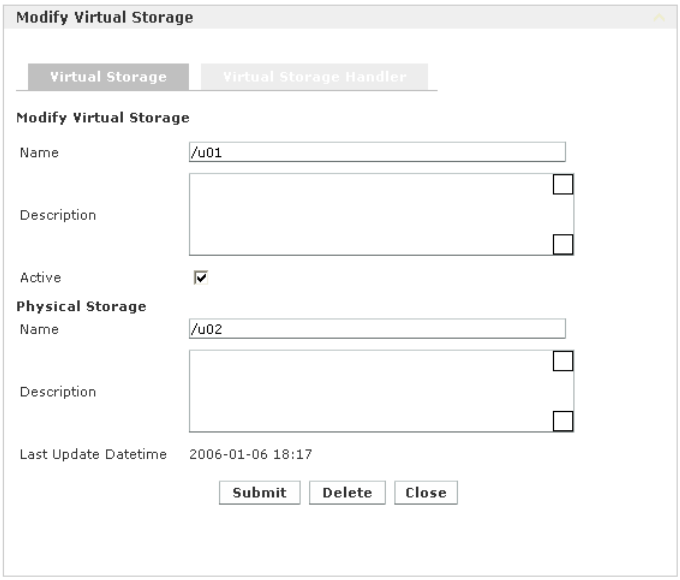
Shutdown Oracle data server.

Assuming Oracle data, redo, archive and flash recovery log files are all located at mount point /u01 of the data server to which the SAN fabric is attached. Backup all files under /u01 follow by clearing all contents. The mount point is detached and remounted as /u02.

Install Spitfire StoreSafe on Solaris platform, and point web browser to https://localhost at data server's GUI console.

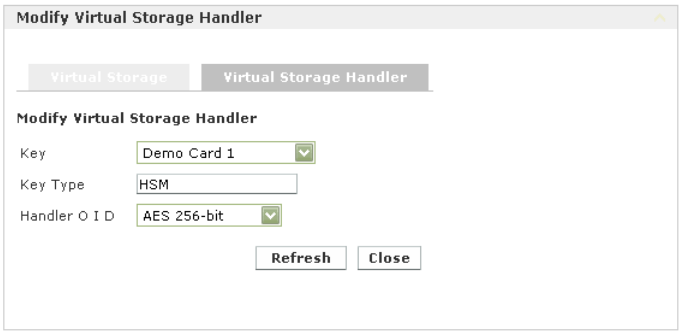
Create new virtual storage as follows

Field	Value
Virtual storage name	/u01
Physical storage	/u02



Turn to Virtual Storage Handler tab, choose Key as 'Demo Card 1' and Encryption algorithm as AES 256-bit

Field	Value
Key	Demo Card 1
Encryption Algorithm	AES 256-bit



Commit and save this new virtual storage configuration. The configurations are backup and restored at the backup site.

Data Migration

Restore backup archive to /u01 at data server. Plain data and log files will get encrypted automatically on-the-fly by Spitfire StoreSafe before they are written to the actual SAN storage at /u02.

Data synchronization mechanism will be able to pick up the changes in form of encrypted data and replicated to the remote site in a timely manner, thus backup replica will assume the same image as soon as data migration is done.

Oracle data server instance is started and application runs seamlessly as before.

Benefits

Data files together with all log files are secured by the same solution. And indeed, Spitfire StoreSafe can be applied on all databases in addition to Oracle.

Migration of database data does not require knowledge of database schemas. For databases with large amount of data at limited cutover time window, one can break down migration into smaller time window and conquer one by one without affecting data integrity and service continuity.

By operating Spitfire StoreSafe with database server, it eliminates performance bottleneck which exists at the connectivity between Spitfire StoreSafe appliance and host servers in standalone deployment scenario. As Spitfire StoreSafe runs on the host which attaches to the storage network directly, it guarantees to be compatible to the storage infrastructure that is hardly attained by other hardware-based solutions.

Spitfire StoreSafe scales with the data server. One can easily cope with increase in throughput demand by adding more processors and main memory.

As encrypted data are written to the storage sub-system, delta changes of files are replicated and sent over the data synchronization network in their encrypted form – additional data security.

Backup and restore operate as before with benefit that backup archives are encrypted by nature.

File Server Protection

Problem

An international bank generates daily transaction settlement reports to their individual financial partners for pick-up via file transfer protocol (FTP). In return, individual partners submit acknowledgement reports to the bank by the same channel. According to local financial and monetary regulatory standards, the reports in form of files, which contain confidential information, have to be secured by encryption no matter they are on transmission or at-rest.

Challenges

Transmission encryption on FTP can easily be implemented using secure socket layer (SSL) over FTP. However, to protect persistence data on storage sub-system, they have no idea where to start with. The bank's FTP system runs on IBM AIX platform. Their corporate IT strategy has strong initiatives to migrate their subsidiary platform to Linux in 2 years' time. The entire solution has to support both AIX and future platforms.

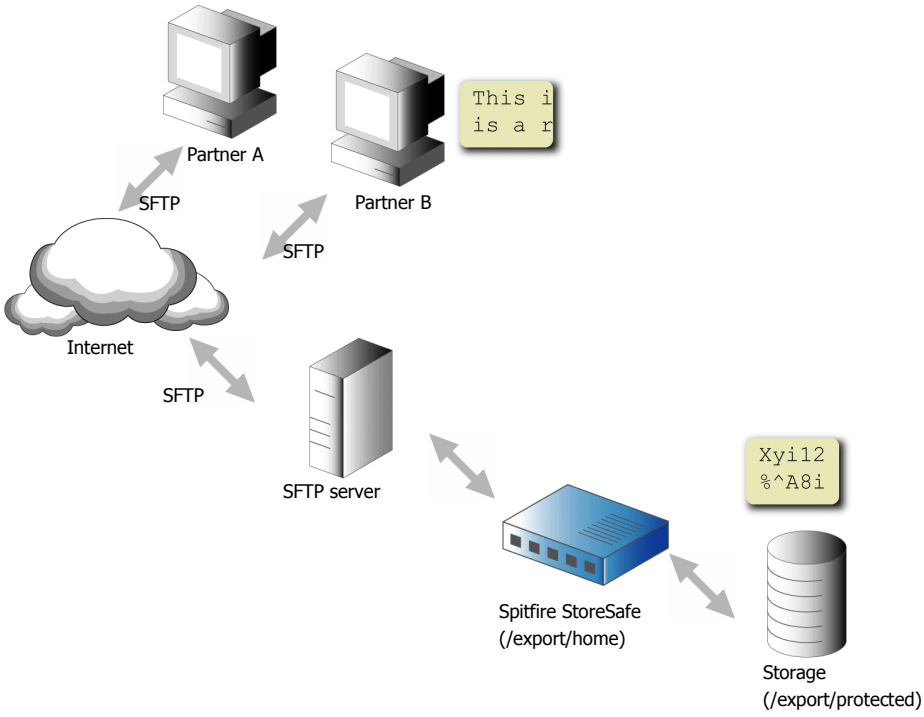
As far as they know, AIX does not have any solution on filesystem protection. They are planning to develop their own file protection programs. As in most enterprises, the IT security team does not have adequate hands-on knowledge on developing codes with encryption. They will have to either outsource the work to third-party system integrators or train their own staff. Both options mean for high total cost of ownership (TCO) which are not cost effective and yet highly risky.

Their high level design plan suggests on generation of reports, an encryption routine is invoked to cipher the plain data before they are written to the file repository. While on consumption of incoming reports, a decryption routine is invoked to decipher the data file stored on file repository. Thus proposed, it requires their partner systems to equip with the same encryption and decryption capabilities to be able to interoperable one another. This increases difficulty and risk of implementation. For sure alteration of partner systems are not welcomed and should be avoided at all times. The need for transparent operation at partner sites is a must and cannot be sacrificed.

Solution

SFTP server is installed replacing original FTP server which has no data protection on transmission channels.

Spitfire StoreSafe is installed on the SFTP server to virtualize ciphered transaction settlement report files persisted on storage sub-system.

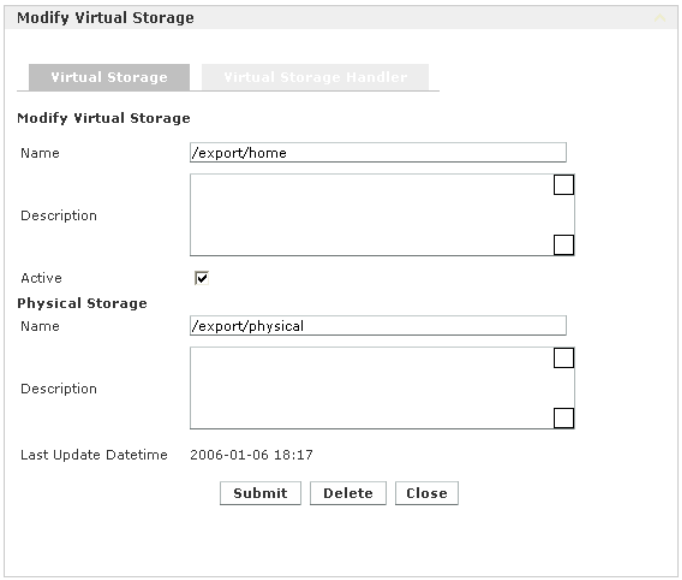


Configurations

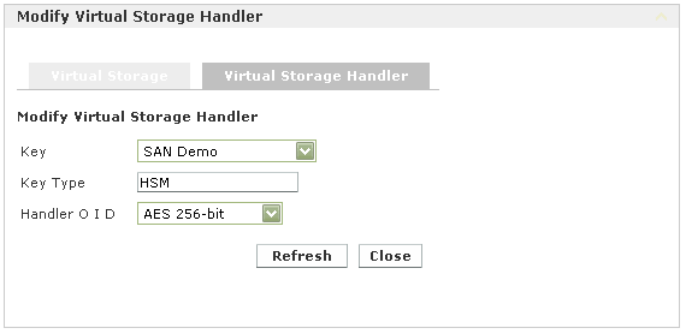
Business partners used to sign on FTP server and upload/download files in their home directory, e.g. partner A signs on with user ID 'partnera' and works on home directory located at '/export/home/partnera'.

To maintain application transparency at user end, a virtual storage /export/home is created on SFTP server which virtualizes encrypted storage physically located at /export/protected.

Field	Value
Virtual storage	/export/home
Physical storage	/export/protected



Local financial storage data security regulatory mandates confidential information to be secured by at least AES 256-bit length. The encryption specification for the virtual storage at /export/home is configured accordingly as follows



Original FTP user credentials are migrated to the new SFTP server without alterations. Once SFTP server and Spitfire StoreSafe are properly configured, they can be started and users be able to upload/download secured report files as if they are in plain.

Data Migration

All directories and plain report files originally mounted under /export/home are archived to backup media before configurations start.

After Spitfire StoreSafe virtual plain storage at /export/home is created, the archive is restored and the files will be automatically encrypted when they are physically persisted at /export/physical.

Benefits

Immediately meet information security regulatory standard with just a few mouse clicks on configurations and least alteration of system. No impact or change of workflow to end-users.

No change to data backup configurations but additional benefit that backup archives become encrypted in their natural form.

By configuring user home directory Spitfire StoreSafe virtual storage individually, one can easily achieve user-based file protection, e.g. files located under /export/home/partnera are encrypted by partner A's key while files located under /export/home/partnerb are encrypted by partner B's key.

Email Repository and Backup Archive Protection

Problem

A semi-government financial and monetary regulatory organization develops a portal for banks and financial institutions to exchange data and messages online using web-based electronic mail.

Some of these email contents contain highly confidential business secrets that need to be protected and not to be disclosed to backup operators.

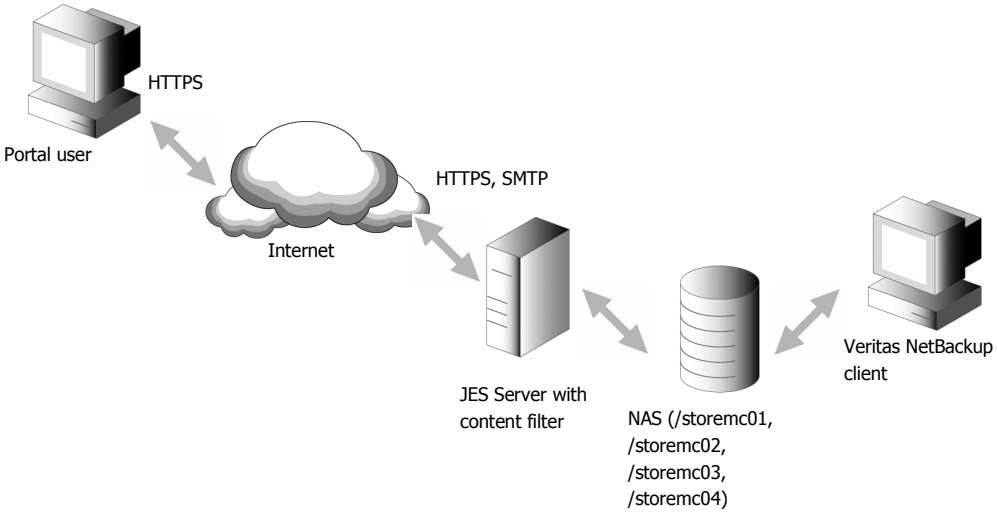
Challenges

To secure email messages, one might opt for secure MIME (SMIME) which protects email contents by encrypting using recipients' public keys. As portal users are mostly from top management who do not want to adopt new workflow in sending or reading email messages, SMIME protection can hardly be considered.

Web-mail function of the portal is supported by Sun Microsystems' Java Enterprise Server (JES) which stores individual email message as discrete plain file on filesystem. Without protection, anyone who can get access to the email repository no matter on physical disks or backup media, gets access to the secret information inside email messages. Encrypting the email repository without affecting JES' infrastructure and integrity is the real challenge to the development of the portal.

The organization uses Veritas NetBackup on Solaris 9 operating system as the standard backup and restore software. It also manages tape catalog and indexes. The encryption solution has to guarantee interoperability on Veritas NetBackup and ensure operators transparent operation on both backup and restore processes with only difference in inability in perception of the true contents inside emails.

While backup and restore process data on the encrypted view, the portal's content filter is required to work on the plain view to block viral and malicious contents as well as SPAM. The encryption solution needs to provide a transparent plain view to the encrypted email message files for portal's content filter to scan with.



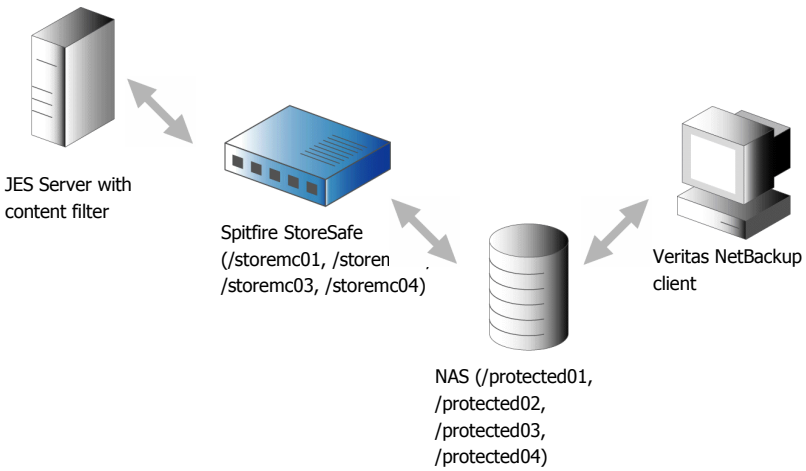
Solution

Configurations

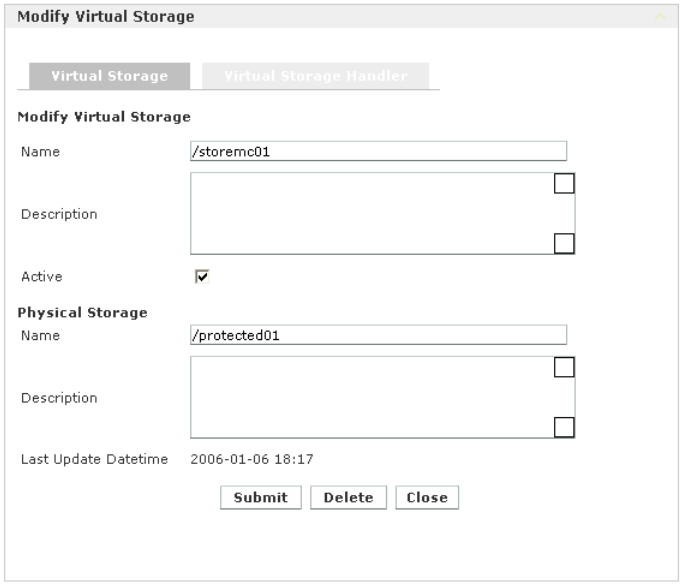
JES server instance is shutdown.

Four physical storages are created on NAS server with names protected01, protected02, protected 03 and protected04 accessible by both JES server and Veritas NetBackup client.

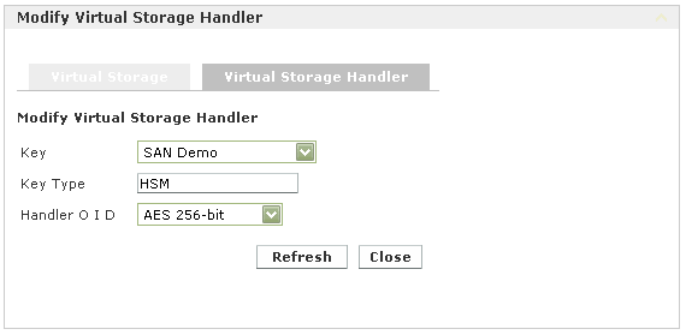
Spitfire StoreSafe is installed on the same server where JES server runs. 4 virtual storages are created on Spitfire StoreSafe management console secured by the same encryption key at AES 256-bit encryption strength.



Field	01	02	03	04
Virtual storage	/storemc01	/storemc02	/storemc03	/storemc04
Physical storage	/protected01	/protected02	/protected03	/protected04



All four virtual storages should be secured by the same encryption key with same encryption strength.



JES server and content filter should be configured to work on the virtual plain view of the email repository which are logically located at /storemc01 to /storemc04.

But for Veritas NetBackup client, as it is required to work on the encrypted version, it should be configured to mount directly to the NAS server at /protected01 to /protected04 so that backup and restore are carried out at the natural encrypted form forbidding backup operators' prying eyes to the sensitive email contents. While sensitive contents inside email message files are protected by strong encryption, they assume the same integrity in form of discrete files which Veritas NetBackup are able to work on. Without limiting NetBackup's capabilities, backup operators can choose individual email files for selective backup or restore. Thus, no change of workflow is required for operators.

Data Migration

Files and directories originally under /storemc01 to /storemc04 are archived before Spitfire StoreSafe implementation.

The archives are then restored via Spitfire StoreSafe at /storemc01 to /storemc04, which will automatically get encrypted and persisted at /protected01 to /protected04.

Benefits

Email repository encryption at storage side secures sensitive email persistent contents without having to change application logic or end users' workflow.

Spitfire StoreSafe secures email contents by strong encryption from operators' prying eyes. Direct intrusion on persistence storage sub-system including hard-drive theft or electronic theft can only obtain the ciphered contents which appear like garbage.

Backup media contains only the encrypted version of confidential data. In worst case scenario where backup media is lost into the hands of criminals, secret contents remain safe as there is technically no way of revealing the true information from ciphered contents without knowledge of encryption key.