File Server Protection by Spitfire StoreSafe

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.

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.

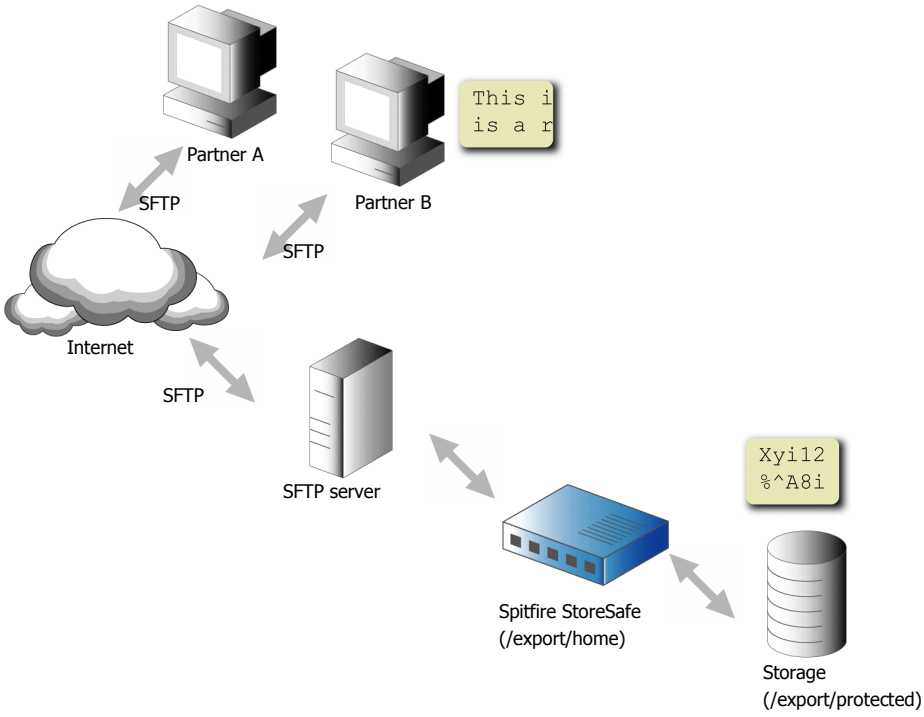
As far as they know, AIX does not have any solution on filesystem protection. They are planning to develop their own file protection programs. As in most enterprises, the IT security team does not have adequate hands-on knowledge on developing codes with encryption. They will have to either outsource 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.

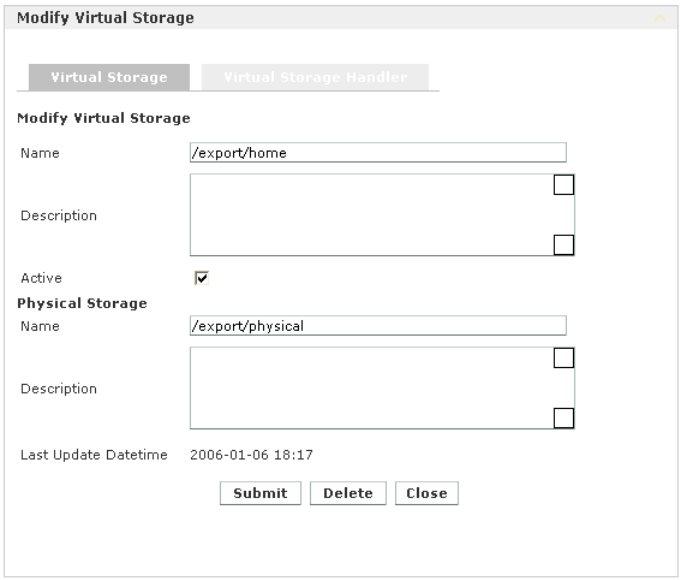


Configurations

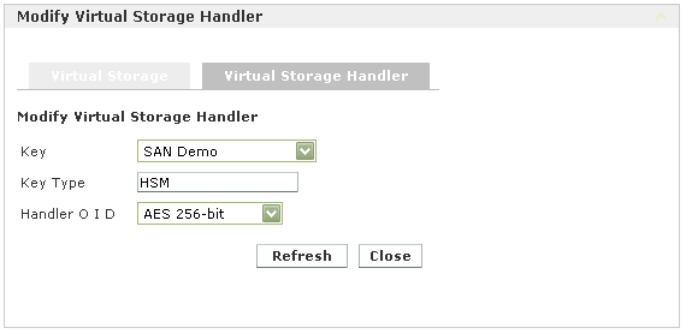
Business partners used to sign on FTP server and upload/download files in their home directory, e.g. partner A signs on with user ID 'partnera' and works on home directory located at '/export/home/partnera'.

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.