Email Repository 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.

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.

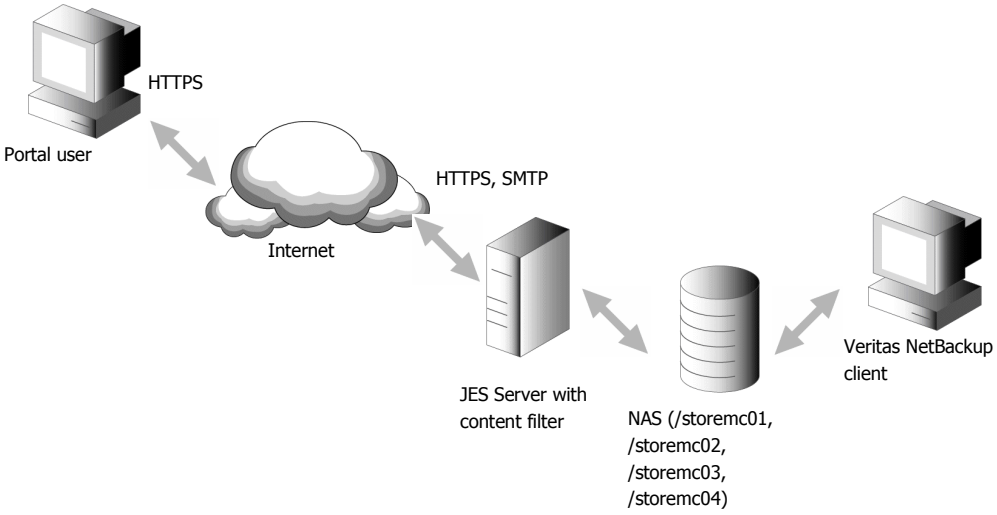
Challenges

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.



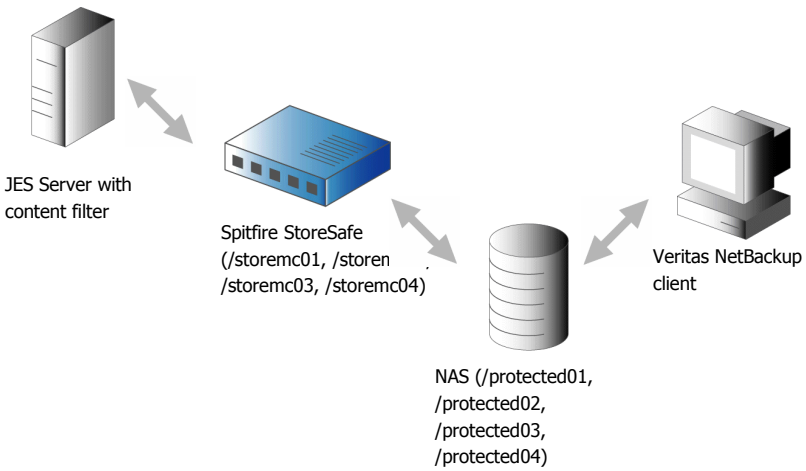
Solution

Configurations

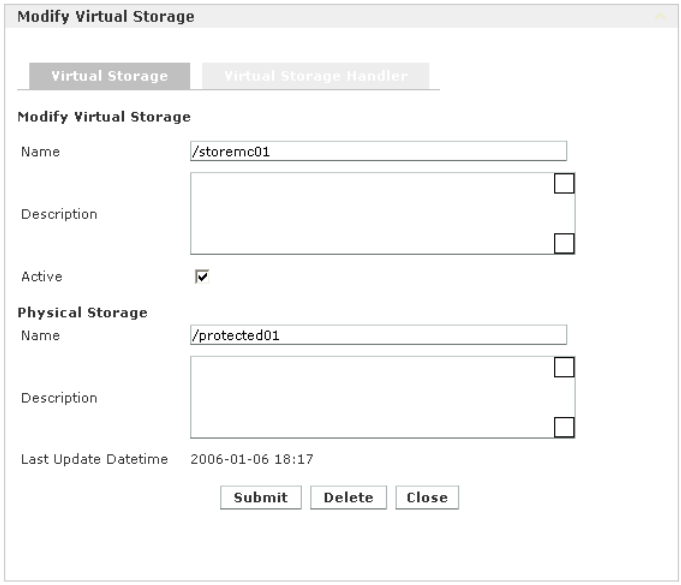
JES server instance is shutdown.

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.

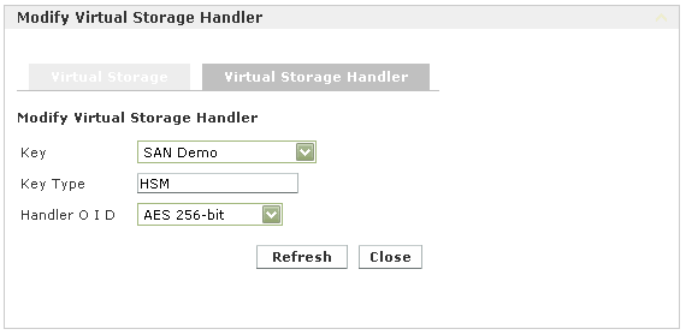
Spitfire StoreSafe is installed on the same server where JES server runs. 4 virtual storages are created on Spitfire StoreSafe management console secured by the same encryption key at AES 256-bit encryption strength.



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.