# Corporate Digital Asset Protection by Spitfire StoreSafe

Bloombase
Least Invasive Security

Bloombase
Least Invasive Security

Sun Partner Advantage
ASSOCIATE PARTNER

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

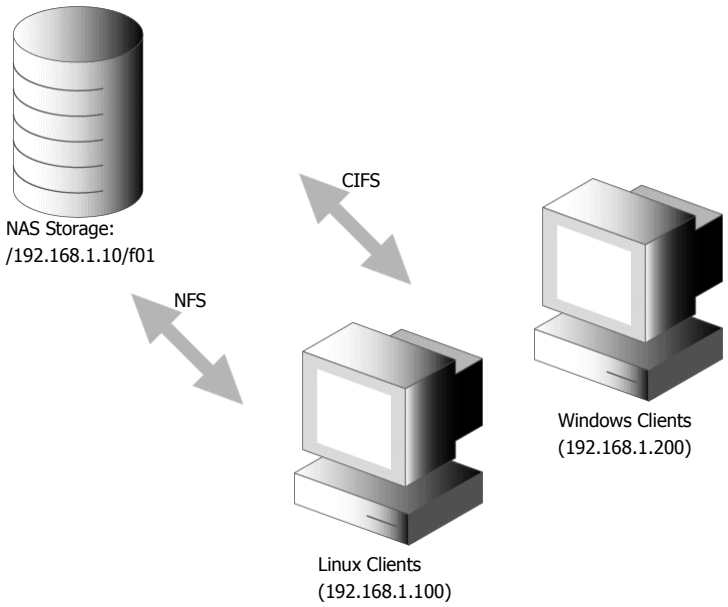
This paper studies how Spitfire StoreSafe enterprise storage security server helps to fill in the missing puzzle of enterprise data threats and serves as a cookbook for a number of typical applications in today's enterprise computing environment.

# Intellectual Property Protection

## Problem

A 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.

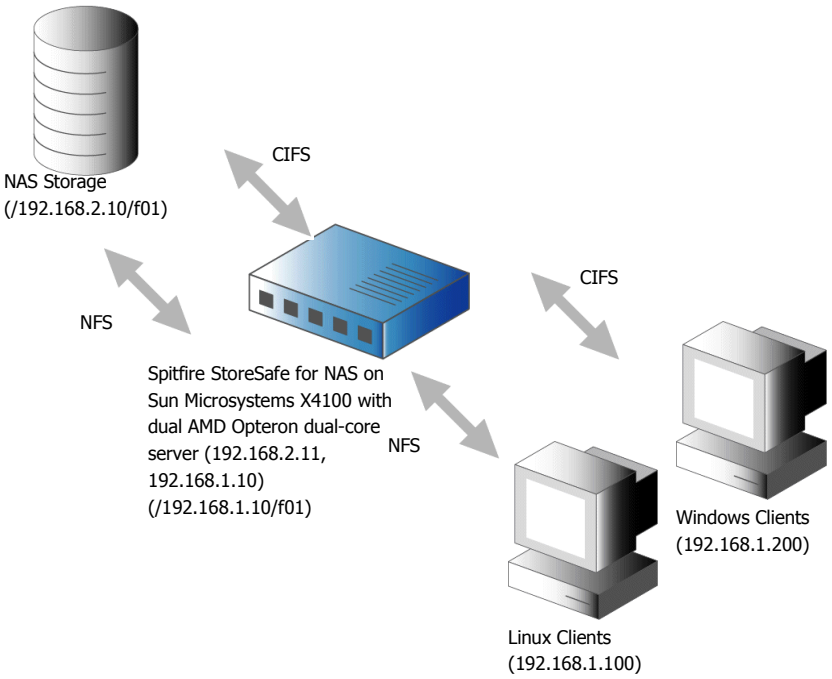
Video editors and animation designers should have no change in their daily workflow after implementation of data encryption.

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 Sun Microsystems X4100 with dual AMD Opteron dual-core with quad 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
```

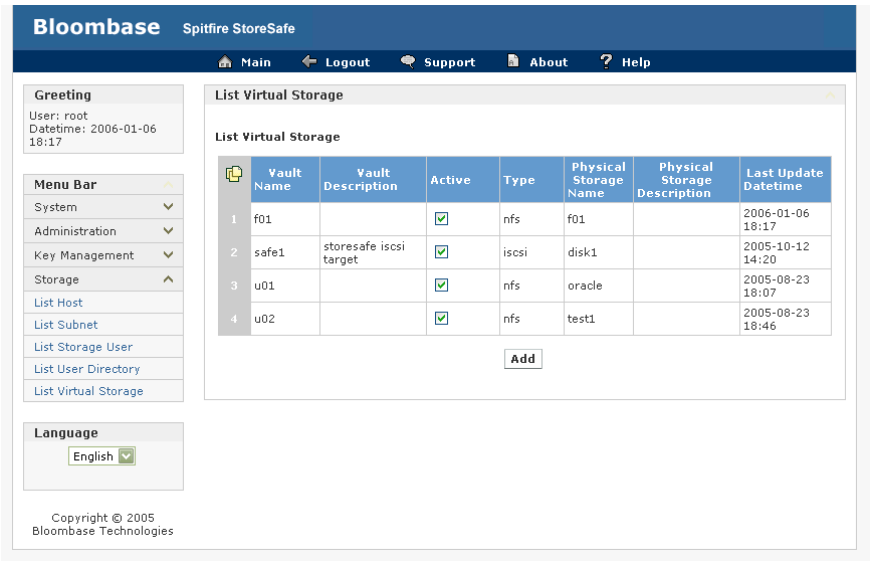
Then, bridge the host network with storage network at IP 192.168.2.11

```
<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

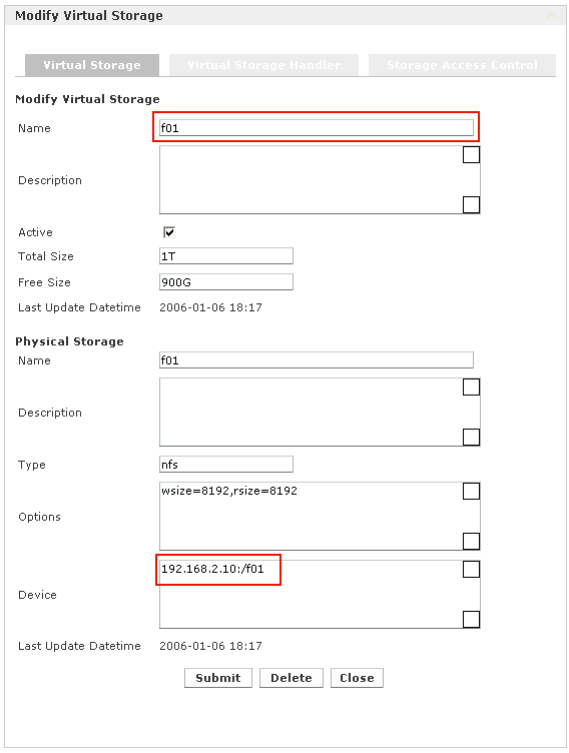
```
<Restart / Shutdown>

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 |

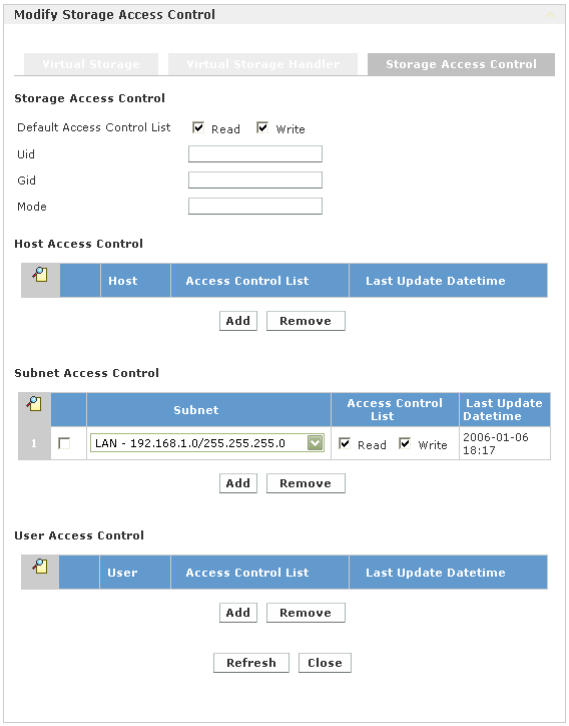



Turn to Virtual Storage Handler tab and input the followings. Camellia is Japan's official strongest cipher, thus, we take Camellia with 128-bit key strength for this setup

| 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.