Spitfire StoreSafe Benchmarks

May 2005

Bloombase
Least Invasive Security

Bloombase
Least Invasive Security

AMD

Tests in this report are carried out with support and sponsor of Advanced Micro Device Inc.

Document No.

Contents

Executive Summary

Spitfire StoreSafe is an all-in-one storage protection product to protect corporate and user data at persistence yet at the same time has least invasive effects to existing user workflow and application processes. Persistent data protection used to be a difficult subject in enterprise. 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. Existing enterprise systems can hardly be torn-down and redeveloped using encryption utilities. First concern is cost-risk while second being most enterprise systems operate non-stop at 7x24. How to secure a corporate storage without invading existing infrastructure is what Spitfire StoreSafe is strong at.

Spitfire StoreSafe sits half-way between enterprise application servers and storage network. By writing data through StoreSafe to the storage network, Spitfire encryption engine changes plain text data into ciphered data which appear like garbage. Trusted applications withdrawing data from storage through StoreSafe gets decrypted immediately. Thus Spitfire StoreSafe acts as a middleman virtualizing the encrypted data storage AS IF in plain to applications and end users.

Spitfire StoreSafe possesses a highly capable encryption/decryption engine to encrypt/decrypt network data on-the-fly. StoreSafe offers ciphers including AES, DES, 3DES, RC4, etc for data encryption. StoreSafe also adds access control flavor to the storage network by allowing/disallowing user access of data in user-configurable time-window, finer-grain file and directory access control, obfuscation or data shuffling for less sensitive data as well as file sharing. Spitfire StoreSafe works with all hardware and operating systems and supports storage protocols including NAS, SAN, tape and legacy storage. It also has rich auditing, web-based management console, redundancy support and integrating with key storage appliances.

Spitfire StoreSafe, to quote a few examples, can be applied on the following enterprise systems

Enterprise Systems	**Applications**
Transparent database encryption	ERP, finance, customer data, etc
Email repository encryption	top management emails, etc
Intellectual property protection	design files, source code, etc

Secure data backup and archival	tape, cartridges, etc

Spitfire StoreSafe is a family of storage encryption and access control hardening products for

Storage System	**Protocols**
Direct attached storage (DAS)	SCSI
Network attached storage (NAS)	NFS, CIFS, FTP, HTTP
Storage area network (SAN)	Fiber channel, i-SCSI

This document serves as a report of benchmarking tests of Spitfire StoreSafe appliances on different aspects of applications including

- Simple file read/write/append/rewrite
- Large file read/write
- Block-based file read/write
- Database access – inquire, update, delete, insert
    - Online transaction processing (OLTP)
    - Data mining/warehousing
- Backup and archive

Important: The tests were carried out on well-tuned and well-patched systems. Tests were designed and system parameters made constant during the course of regression to produce the fairest results as possible. The performance figures are for reference only and may differ per hardware, operating systems, applications, system parameters and probes. The performance benchmarks MAY OR MAY NOT be reproduced and more capable and efficient hardware and software applications MAY OR MAY NOT produce better results.

Customers are strongly advised to design and run their own tests to obtain the best sizing predictions for their future systems before procurement. Bloombase Technologies makes no assumption the products MUST fit in customers' requirements.

Overview

Why Benchmarking

Spitfire StoreSafe enterprise network storage protection appliances secure storage data at the core by centralized access control and cryptography.

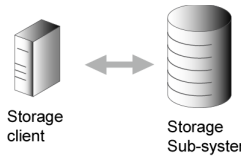

Figure – A typical enterprise system showing a storage client accessing a network storage sub-system

Access Control

Due to the requirements of remote network access and identity management governed by network attached storage (NAS) protocols including network file system (NFS), common interface file system (CIFS), file transfer protocol (FTP/SFTP), and hypertext transfer protocol (HTTP/HTTPS), extra time is required to establish user sessions for network storage secured by Spitfire StoreSafe for NAS appliances. As such authentication process is session-based and is only carried out once at the start of the session before actual storage packets traverse, storage client will experience a single latency while negotiating a session, however, no latency will be introduced to actual storage data communications.

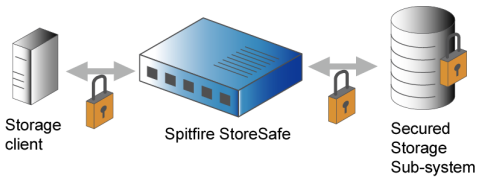

Figure – A visual showing Spitfire StoreSafe appliance acting as a proxy to storage sub-system virtualizing and securing data read from and written to the network storage. Spitfire StoreSafe might introduce slight latency of data transmission due to extra access control and cryptographic operations.

Small computer system interface (SCSI) protocol utilized in direct attached storage (DAS) and storage area network (SAN), regardless it is Internet Protocol-SAN (IP-SAN) or Fiber-channel SAN (FC-SAN) are block-based storage protocols which are over-abstractive without knowledge of user identity, host and filesystem. Thus access control is not required on these cases and no latency will be added by introducing Spitfire StoreSafe to the storage sub-system.

Cryptography

Cryptography is commonly perceived as shuffling and coding of data which is wrong. Data shuffling refers to the process of altering the order of sequence of data in a systematic way. By reversing the disordering process, one regains the original contents. Obfuscation is a coding process of data against a pre-defined look-up table. Again, obfuscation can be undone if one gets hold of the contents of the look-up table.

Cryptography is comparatively much complicated than both data shuffle and obfuscation described above. Cryptography originates from the good old idea of key-and-lock to secure precious objects inside a compartment. Similarly, cryptography requires a pre-generated key which is a series of random data resembling ridges of a physical key while the mathematical operation – the cipher, resembling mechanics of a physical lock, a transfer function of both key and data-to-be-secured which turns confidential data (precious objects) into a meaningless vault (secured compartment).

Numerous ciphers have been invented, a few examples are Blowfish, RC2, DES, 3DES and AES, etc. They differ in the algorithmic process, key length requirement, strength, complexity, ease of hardware implementation, resource requirement, ability to work with streamed data, performance and efficiency. Regardless of level of cipher efficiency and cryptographic processing engine performance, cryptographic operations – encryption and decryption, must add a relatively amount of time in the course of storage network data communications.

Spitfire StoreSafe operates on the network storage communications channel. When a storage client (e.g. database server, application server, messaging server, etc) sends a file or portion of file or segment of storage space to the storage subsystem, Spitfire StoreSafe encrypts the plain data on-the-fly before they are committed into the actual storage media. When a storage read process is triggered, as encrypted data flows through Spitfire StoreSafe, Spitfire StoreSafe readily decrypts the data and reveals the true contents to trusted storage clients. Comparing to the unsecured scenario where storage client directly accesses storage subsystem, to secure storage data by Spitfire StoreSafe, one pays extra latency of storage data access in exchange of data privacy, confidentiality and integrity.

Actual storage data seek time is the ensemble of physical storage media access and data cryptographic times which accounts for the extra latency by introducing Spitfire StoreSafe to secure an enterprise storage subsystem. However, such latency, or in storage client's perspective, data seek penalty, has no direct relation to the overall throughput of a storage system by considering Spitfire StoreSafe and actual storage system as a single component of an enterprise system. Enterprise applications including web, email and database are highly multi-threaded while Spitfire StoreSafe's core encryption engine is built to be multi-threaded and multi-tasked for storage clients' concurrent multiple access. Spitfire StoreSafe appliances are highly scalable and can be configured to work as a cluster for parallel cryptographic processing. For multi-threaded applications, storage access will be deserialized and streamlined without propagating the latency penalty. Thus, latency penalty effect becomes diminished and overall storage throughput gets less deteriorated and remains relatively the same as if without encryption present.

This document quantifies and summarizes the change of storage network throughput per introduction of Spitfire StoreSafe into storage subsystem and serves as a reference for sizing and performance tuning by use of mathematical interpolation.

How Tests Were Done

The tests described in this document aim on the followings

- To quantify maximum throughput of the Spitfire StoreSafe Core Encryption Engine which is the core building block of the entire Spitfire security appliance platform
- To quantify maximum throughputs of individual Spitfire StoreSafe model for specific application
- To observe and measure degradation of throughputs of individual Spitfire StoreSafe

StoreSafe Family

Spitfire StoreSafe family is composed of the following models which are included into the tests

StoreSafe Model	Specifications
Spitfire StoreSafe for DAS SF-SC110	For direct attached storage use, supports Ultra 160 SCSI low voltage differential (LVD)
Spitfire StoreSafe for NAS SF-C110	For network attached storage use, supports NFS v2/v3 over TCP/UTP, Microsoft Windows CIFS, FTP and HTTP
Spitfire StoreSafe for SAN SF-FC110	For storage area network, supports SCSI over fiber channel/IP

Setup

Benchmark tests for different Spitfire StoreSafe model, use and application require specific setup and component all the way from storage clients/hosts to the actual storage subsystem.

The following diagram shows an over-simplified and abstract architecture for tests carried out which consists of components

- Storage client cluster – group of hosts to create storage access load
- Transmission wire - interconnects
- Switch – for storage access multiplexing
- Spitfire StoreSafe – storage data cryptographic engine
- Secured storage sub-system – storage system with physical media

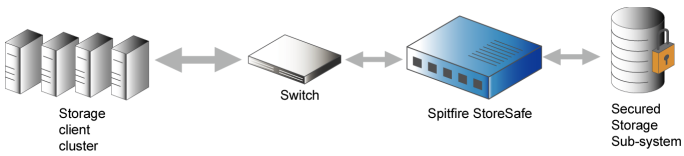

Figure – An abstract benchmark setup for testing of individual Spitfire StoreSafe model for specific application

The following matrix describes candidates of above abstract components in specific storage subsystems and protocols

Storage Type	Protocol	Client	Host Bus Adapter	Inter-connect	Switch	Spitfire StoreSafe	Storage Sub-system
DAS	SCSI	Intel-based Linux or Windows, RISC-based UNIX	SCSI interface card	Copper SCSI cable	N/A	Spitfire StoreSafe for DAS	SCSI disk array

NAS	NFS, CIFS, FTP, HTTP	Intel-based Linux or Windows, RISC-based UNIX	LAN card with TCP/IP offload engine (TOE)	LAN cable	IP switch	Spitfire StoreSafe for NAS	NAS server: NFS daemon, Windows SMB/CIFS, SAMBA, FTP daemon, HTTP daemon
SAN	SCSI	Intel-based Linux or Windows, RISC-based UNIX	Host bus adapter (HBA) card with TOE or native iSCSI	Fiber-channel cable	SAN switch	Spitfire StoreSafe for SAN	SAN and IP-SAN storage array

Connectivity

To eliminate the performance degradation factors contributed by the interconnects, the following hardware are used in the tests

Media	Connectivity
Copper	• AMP Netconnect Category 6 patch cables each of lengths below 4 feet
	• 3COM Gigabit 16-port Baseline Switch 2816-SFP Plus
Fiber channel	• Stock LSI Logic SFP fiber optics cables
	• Brocade Silkworm 3850 running at 2G bps

Storage Subsystems

The following storage hardware are used in the tests

Storage Type	Hardware
DAS	Dell PowerVault 220 SCSI Storage with 10,000rpm 1" LVD Ultra 160 and Ultra3 SCSI drives
NAS	Dell PowerVault 745N Network Attached Storage Server
SAN	Dell EMC Fiber Channel AX100 and iSCSI AX100i Storage Array

Storage Clients

To create enough loading simulating comparable storage throughput in typical enterprise use, 4 Intel-based boxes are used

Detailed configurations are as follows

Client	Dell PowerEdge 2850 Rackmount Server
Processor	Intel 64-bit Xeon 3 GHz single processor with 1 MB L2 cache
Main Memory	1 GB
Operating System	Windows XP, Redhat Linux kernel 2.6
Ethernet Adapter	Integrated dual gigabit
Host Bus Adapter	LSI Logic LSI7102XP-1 2-Gbps FC cards
SCSI Interface	ADAPTEC 2906 SCSI Card

Stress Tester

Apache JMeter of project Jakarta is a 100% native Java application used to generate loading to the storage sub-system which supports virtually all platforms.

JMeter is a general-purpose, highly-customizable and pluggable stress creator and performance probe. Actual stress is created by individual JMeter plug-in's which are developed by stress testing designers. Stress test designers pre-design test vectors to cater different levels of load and stress types. Operators are required to load these test vectors into JMeter as testing parameters before every run of

Bloombase Technologies created a number of stress tester plug-in's for JMeter's use

Plug-in	Purpose
HammerFS	Read, write, append and truncate files
HammerFTP	Upload and download files
HammerOra	Oracle TPC-C test with query, insert, update, delete

Apart from creating stress, JMeter is capable of measuring and timing stress tasks.

Probing and Performance Measurement

Probing of actual storage network communications utilization is done by examining throughput data retrieved from network and SAN switches.

Overall performance of stress tests created by client cluster is calculated by simply ensembling effective throughput of individual stress client which is trivial and requires no dedicated tools.

Users of Spitfire StoreSafe are interested in two sets of figures in view of benchmarking

- Latency
- Throughput degradation

Latency refers to the additional time it takes to process a storage command on introduction of encryption in the storage channel. Latency is measured in absolute value of seconds (s) while change is in percentage.

Throughput degradation, on the other hand, describes the drop of maximum storage data transfer rate of the storage network on introduction of encryption. Throughput is measured in gigabits per second (Gbps) while degradation is in percentage.

Spitfire Core Cryptographic Engine

Introduction

Before tests are carried out on complete applications constructed with storage subsystems and Spitfire StoreSafe appliances where thousands of factors might contribute to the overall system throughput, a critical aspect one may query – is the encryption engine capable enough to process storage data at wire-speed at gigabit per second order of magnitude?

This section of test aims to examine the maximum processing capacity of Spitfire Core Cryptographic Engine which is the main building block of entire Spitfire Security Platform. Spitfire Core Encryption Engine is a well-tuned and highly-optimized cryptographic software core which executes on Spitfire StoreSafe's multi-cryptographic processor grid.

Spitfire StoreSafe is built on a highly scalable platform where multiple Spitfire Core Cryptographic Engine modules can be installed to boost processing power, therefore, cryptographic throughput.

Engine Throughput Test

To eliminate network and input/output (I/O) wait times and communications latency, a manufacturer's engine throughput test is carried out on Spitfire Core Cryptographic Engine loaded onto a dual-AMD Opteron dual-core processor grid to obtain the maximum cryptographic processing power of the unit.

Regardless of application, storage devices, protocol, transmission media and transmission interfaces, multiple endless streams of random data are generated and fed into a Spitfire Core Cryptographic Engine for encryption and decryption using Advanced Encryption Standard (AES) cryptographic cipher by randomly generated 256-bit symmetric key.

Setup

The following diagram shows the setup of this test. A Spitfire Core Encryption Engine is installed onto a system running on Spitfire OS which is a hardened and customized Linux of kernel version 2.6.11. Multiple plain random data streams are fed into for processing.

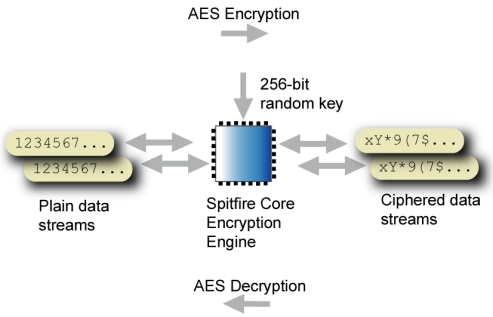

Figure – Setup of cryptographic processing performance tests on Spitfire Core Cryptographic Engine

The following table summarizes the hardware configuration of Spitfire StoreSafe appliance

Processing Unit	Dual AMD Opteron dual-core 265 with true 64-bit support
Main Memory	2 GB
Persistence Storage	4 GB Flash
Operating System	Spitfire OS – Hardened and customized OS based on embeded Linux of kernel version 2.6.11

Security specific setup is as follows

Spitfire Core Cryptographic Engine	Version 1.0.8
Encryption Algorithm	Advanced Encryption Standard (AES) Cipher Block Chaining (CBC)
Encryption Key	Software only
Key Length	256-bit
Number of Random Data Streams	4
Cryptographic Tasks	• encryption • decryption

Spitfire Core Encryption Engine actively pulls in random data from input stream which is a random number generator. Ciphered data are outputted and encryption throughput is measured simply as the ensemble of ciphered data output rates.

Decryption performance tests, on the other hand, require more sophisticated technique because input data are supposedly ciphered data which cannot be randomly generated, or decryption will fail immediately due to unexpected runtime errors. To enable data be decrypted without error, ciphered data previously outputted as results of encryption are temporarily stored on memory. Decryption process intakes ciphered input from memory and again, decrypted output data rate measured and summed yielding overall decryption throughput rate.

Results

10 rounds of encryption and decryption tests are carried out successfully without error and throughput measured and averaged.

Results are summarized in below table

Encryption (Gbps)	Decryption (Gbps)
1.8119	1.7213

Results are plotted as follows

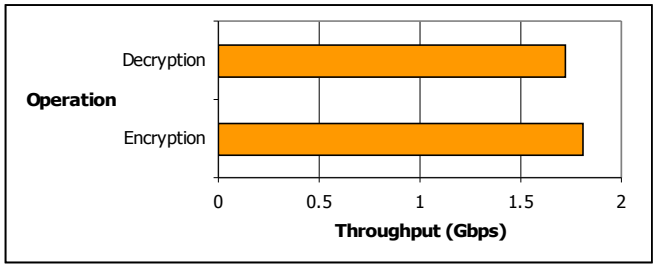

Figure – Spitfire Core Cryptographic Engine Net Processing Throughput

Encryption and decryption both run at gigabit speed

Encryption performs a little better (approximately 5%) than decryption

Conclusion

- Spitfire Cryptographic Encryption Engine running on dual AMD-Opteron module can encrypt and decrypt at rates of the same order of magnitude as current storage network communications speeds (1 Gbps and 2 Gbps). For applications running on 2 Gbps storage systems at full speed, ideally, the engine may barely become the bottleneck

- Even though later application tests are built on storage network hardware operating at maximum 2 Gbps, there is slim chance an application can fully utilize the entire bandwidth in actual use. As Spitfire Core Encryption Engine's maximum throughput is still close to this speed, one can still claim such bottleneck effect should not be dominant in the tests follow

- To cater for next generation storage network which operates at 4 Gbps and above, one might need to increase the processing power of the appliance by installing more processors to raise the overall cryptographic capability and further relieve the encryption bottleneck

Spitfire StoreSafe for DAS - SF-SC110

Introduction

Storage problems of departmental and workgroup applications are best solved by Direct Attached Storage (DAS). It is a cost-effective and scalable enterprise storage solution for environments where sizing and scalability are not major concerns.

Direct attached storage (DAS) is the simplest and least cost storage architecture that are commonly used in applications demanding less scalability, e.g. directory servers, name servers, and as local system storage, etc.

Spitfire StoreSafe for DAS SF-SC110 is a cost effective storage protection solution for direct attached SCSI devices including SCSI disks, tape drives and dedicated SCSI storage appliances. Spitfire StoreSafe for DAS directly attaches to the protected SCSI storage, while host system connects to Spitfire StoreSafe for DAS as a SCSI loop.

File Access

To study the effect of Spitfire StoreSafe on file encryption and decryption of DAS storage data, one would be interested in the followings

- File access latencies
- Overall storage network throughput degradation

File access latencies, as described in earlier texts, account for the time taken to encrypt or decrypt file data in addition to

- physical I/O seek/access
- data transmission
- and error correction times

For DAS, both data transmission and error correction times should be negligible, as SCSI commands are directly sent to device to data access.

Storage communications throughput refers to how much data at maximum can be sent or received over time. As encryption is introduced in the storage channel which might introduce an unknown amount of latency in file access, ideally, concurrent file access tasks will become congested and might affect effective throughput of the storage network. The tests will examine the amount of throughput loss with assumption that such loss is not the result of performance bottleneck caused by the cryptographic unit.

Setup

Tests are carried out on identical storage hosts and storage sub-system with and without Spitfire StoreSafe for DAS.

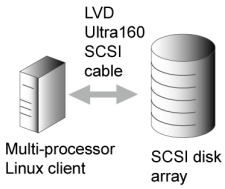

Figure – DAS test setup without Spitfire StoreSafe protection

Detailed hardware/software setup is as follows

Storage Type	DAS
Storage Communications Protocol	Ultra160 LVD SCSI
Test Client	1 dual-processor rackmount server • Intel 64-bit Xeon 3 GHz processor with 1 MB L2 cache • 1 GB main memory • Redhat Linux 9 • ADAPTEC 2906 SCSI card • Sun JRE 1.5.0_04 • JMeter 2.0.2
Interconnects	Stock SCSI cable
Storage	Dell PowerVault 220 SCSI Storage with 10,000rpm 1" LVD Ultra 160 and Ultra3 SCSI drives
Spitfire StoreSafe	Spitfire StoreSafe for DAS – SF-SC110 with Spitfire Core Cryptographic Engine version 1.0.8 • Dual AMD-Opteron dual-core 265 • 2 GB main memory

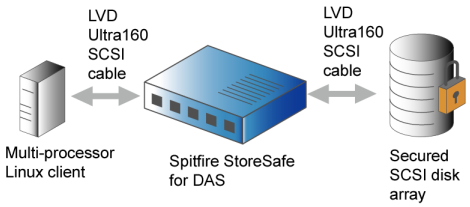

Figure – DAS test setup with Spitfire StoreSafe protection

Security specific setup is as follows

Encryption Algorithm	Advanced Encryption Standard (AES) Cipher Feedback (CFB)
Key Length	256-bit
Encryption Key	Spitfire KeyCastle PKCS#11 hardware security module (HSM)
Cryptographic Tasks	• encryption • decryption

Results

4 storage hosts each of 10 concurrent threads reading/writing random files each of 10MB

	Without Encryption	With Encryption	Change
Read/Decryption Throughput (Gbps)	0.171	0.136	-20.5%
Write/Encryption Throughput (Gbps)	0.132	0.103	-21.9%

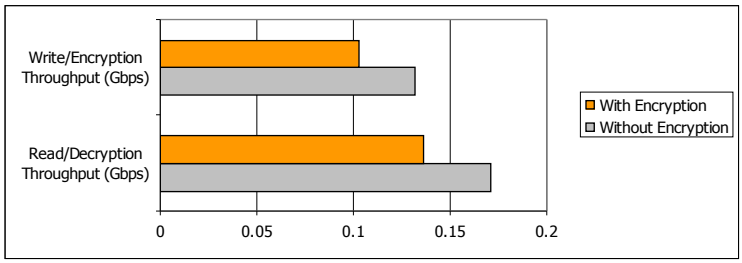

Figure – DAS throughput test results

1 storage host with 1 thread reading/writing 600 files each of 100MB

	Without Encryption	With Encryption	Change
Read/Decryption Latency (s)	7989	10326	+29.25 %
Write/Encryption Latency (s)	9686	12346	+27.46 %

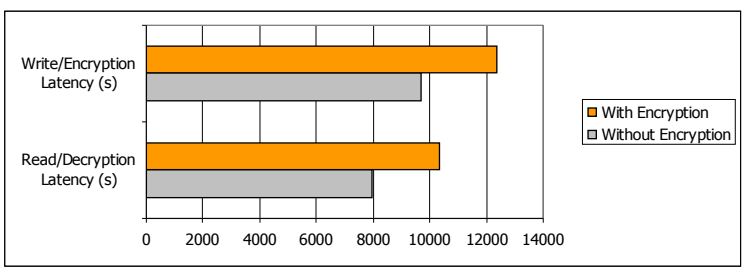

Figure – DAS latency test results

Conclusion

- Introduction of Spitfire StoreSafe for DAS lowers overall throughput of storage read/write by around 20%
- In single-threaded environment where encryption/decryption can only process sequentially, Spitfire StoreSafe increases read/write latency by close to 30%

Spitfire StoreSafe for NAS – SF-C110

Introduction

Network attached storage (NAS) is the only type of storage that allows data and corporate resource sharing by connecting host and server systems. It is by far the most mature networked storage solution in the industry.

NAS originally is developed and deployed for enterprises in data sharing environment as a low-cost solution, together with performance and most important of all, scalability, extensibility, heterogeneity and availability.

NAS can easily be deployed in enterprise computing environment and virtually works with all server and client hardware and operating systems. NAS enables quick and no down-time deployment. Any clients connect to the same networked environment with authenticated user credentials can readily access the remote data.

As users enjoy convenience of data access, it opens up a huge security vulnerability to NAS storage contents - data can be duplicated and NAS hardware can easily be detached. Sensitive and confidential corporate data can readily come to the hands of unauthorized trespassers or business competitors.

Spitfire StoreSafe protects enterprise persistence data with wire-speed strong encryption and transparent operation least affecting existing corporate computing infrastructure. Spitfire StoreSafe for NAS is a self-contained network appliance that encrypts and decrypts storage data on-the-fly with high-availability capabilities for mission critical environments.

File Access

Setup

NFS

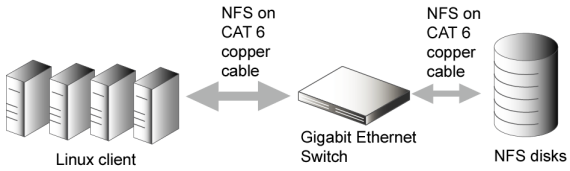

Figure – NAS NFS test without protection

Detailed hardware/software setup is as follows

Storage Type	NAS
Storage Communications Protocol	NFS v2/v3
Test Client	4 single-processor rackmount server • Intel 64-bit Xeon 3 GHz processor with 1 MB L2 cache • 1 GB main memory • Redhat Linux 9 • Integrated dual gigabit Ethernet network interface • Sun JRE 1.5.0_04 • JMeter 2.0.2
Interconnects	AMP Netconnect CAT 6 gigabit patch cables
Switch	3COM Gigabit 16-port Baseline Switch 2816-SFP Plus
Storage	Dell PowerVault 745N Network Attached Storage Server
Spitfire StoreSafe	Spitfire StoreSafe for DAS – SF-C110 with Spitfire Core Cryptographic Engine version 1.0.8 • Dual AMD-Opteron dual-core 265 • 2 GB main memory

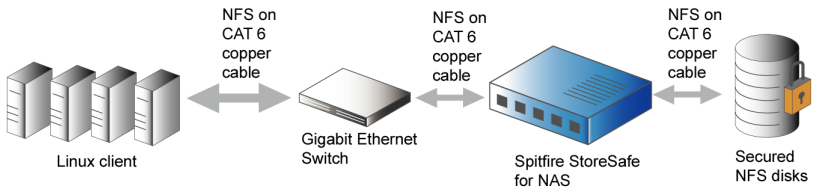

Figure – NAS NFS test with Spitfire StoreSafe for NAS protection

Security specific setup is as follows

Encryption Algorithm	Advanced Encryption Standard (AES)
Key Length	256-bit
Encryption Key	Spitfire KeyCastle PKCS#11 hardware security module (HSM)
Cryptographic Tasks	• encryption • decryption

CIFS

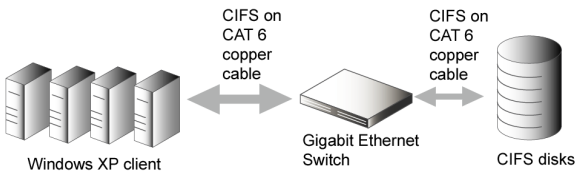

Figure – NAS CIFS test without protection

Detailed hardware/software setup is as follows

Storage Type	NAS
Storage Communications Protocol	Microsoft Windows CIFS
Test Client	4 single-processor rackmount server • Intel 64-bit Xeon 3 GHz processor with 1 MB L2 cache • 1 GB main memory • Windows XP • Integrated dual gigabit Ethernet network interface • Sun JRE 1.5.0_04 • JMeter 2.0.2
Interconnects	AMP Netconnect CAT 6 gigabit patch cables
Switch	3COM Gigabit 16-port Baseline Switch 2816-SFP Plus
Storage	Dell PowerVault 745N Network Attached Storage Server with 1" Serial ATA (SATA) hard disk drives (7,500 rpm)
Spitfire StoreSafe	Spitfire StoreSafe for DAS – SF-C110 with Spitfire Core Cryptographic Engine version 1.0.8 • Dual AMD-Opteron dual-core 265 • 2 GB main memory

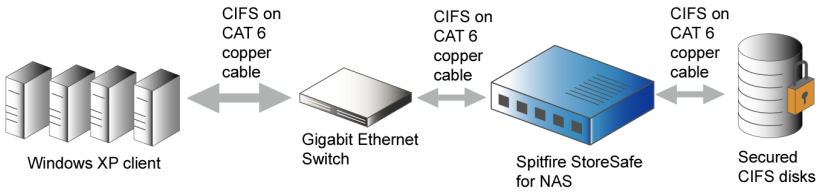

Figure – NAS CIFS test with Spitfire StoreSafe for NAS protection

Security specific setup is as follows

Encryption Algorithm	Advanced Encryption Standard (AES)
Key Length	256-bit
Encryption Key	Spitfire KeyCastle PKCS#11 hardware security module (HSM)
Cryptographic Tasks	• encryption • decryption

Latency and throughput tests are carried out on read/write operations of files of the following sizes

- 10 MB
- 100 MB

Results

NFS

4 storage hosts each of 10 concurrent threads reading/writing random files each of 10MB

	Without Encryption	With Encryption	Change
Read/Decryption Throughput (Gbps)	0.0419	0.0293	-30.1%
Write/Encryption Throughput (Gbps)	0.0376	0.0251	-33.2%

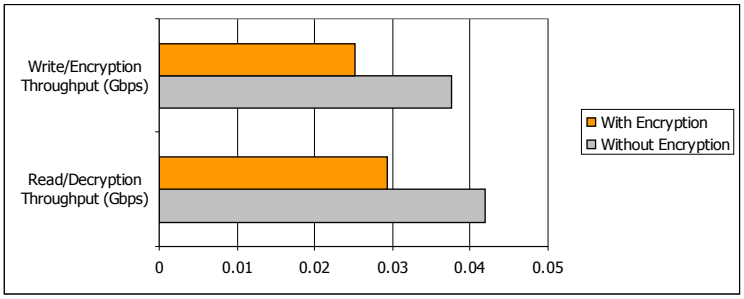

Figure – NFS throughput test results

1 storage host with 1 thread reading/writing 600 files each of 100 MB

	Without Encryption	With Encryption	Change
Read/Decryption Latency (s)	9873	13726	+39.0%
Write/Encryption Latency (s)	11353	15610	+37.5%

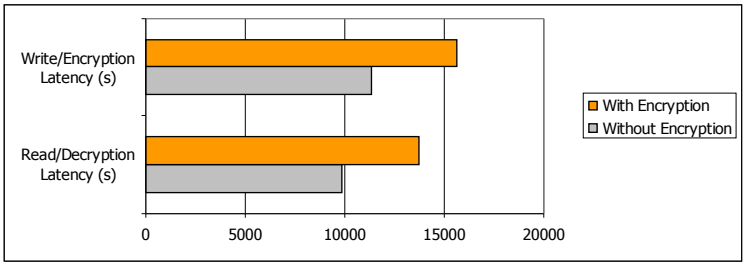

Figure – NFS latency test results

CIFS

4 storage hosts each of 10 concurrent threads reading/writing random files each of 10 MB

	Without Encryption	With Encryption	Change
Read/Decryption Throughput (Gbps)	0.0379	0.0246	-35.1%
Write/Encryption Throughput (Gbps)	0.0358	0.0222	-38.0%

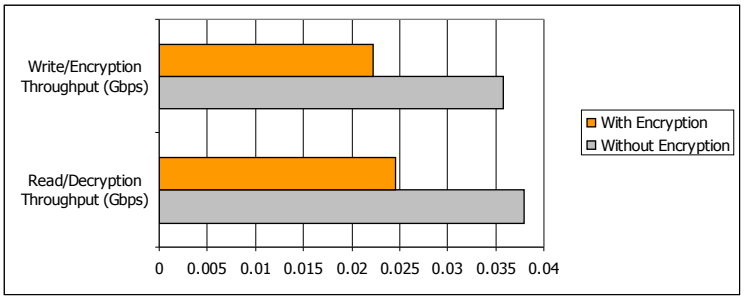

Figure – CIFS throughput test results

1 storage host with 1 thread reading/writing 600 files each of 100 MB

	Without Encryption	**With Encryption**	**Change**
Read/Decryption Latency (s)	12679	17877	+40.0%
Write/Encryption Latency (s)	13786	20127	+46.0%

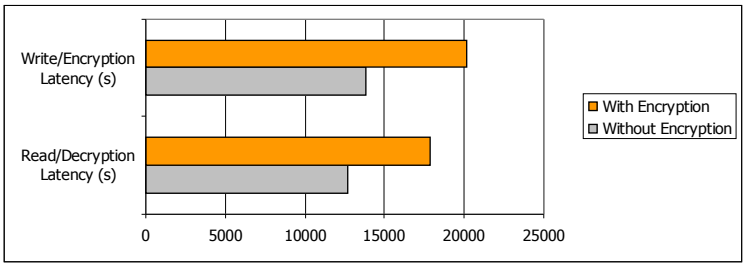

Figure – CIFS latency test results

Conclusion

- Introducing Spitfire StoreSafe for NAS to NFS and CIFS storage reduces data throughput by 30% to 40%
- Spitfire StoreSafe increases read/write turn around times for 40% to 45%
- NFS and CIFS rely heavily on TCP/IP data packets to transmit storage data, though are cost-safe, they suffer from less optimized communications protocols, thus relatively greater overhead when working with Spitfire StoreSafe on data encryption. Spitfire StoreSafe for NAS introduces the greatest drop of throughputs and longest latencies amongst the Spitfire StoreSafe family
- NFS is comparatively more efficient and optimized than CIFS. NFS beats CIFS on absolute throughputs and latencies as well as the change of throughputs and latencies per introduction of Spitfire StoreSafe

Spitfire StoreSafe for SAN – SF-FC110

Introduction

Storage Area Network (SAN) is a high-end storage topology for enterprises having highly scalable and sizable storage requirements at the same time cannot risk losing performance. SAN is supported by various major hardware vendor and enterprise grade operating systems.

Full redundancy, high performance and improved storage utilization are some of the key major benefits of SAN. SAN is a purpose-built architecture for mission critical enterprise core storage systems. Most if not all business data rest in SAN are confidential and requiring very high level of integrity.

As SAN data are mostly vital, enterprises opt for replication, staging and backup as disaster recovery measures to keep enterprise systems at high availability. Replication and backup data in storage media other than production system opens up another risk area that sensitive corporate data will easily be disclosed and made known to public and unauthorized parties.

To protect SAN data without sacrificing performance and high availability is a major challenge in most corporations and organizations.

Spitfire StoreSafe SAN are a family of high-speed network storage cryptographic engines to virtualize core business SAN storage. It can be directly applied to enterprise core databases and backup systems to gain always-available data and have business owners' mind at rest in data security.

File Access

Setup

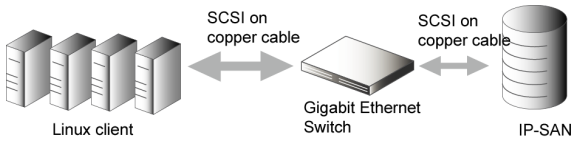

Figure – IP-SAN/i-SCSI test without protection

Detailed hardware/software setup is as follows

Storage Type	SAN
Storage Communications Protocol	SCSI
Test Client	4 single-processor rackmount servers • Intel 64-bit Xeon 3 GHz processor with 1 MB L2 cache • 1 GB main memory • Redhat 9.0 • Integrated dual gigabit Ethernet network interface • Sun JRE 1.5.0_04 • JMeter 2.0.2
Interconnects	AMP Netconnect CAT 6 gigabit patch cables
Switch	3COM Gigabit 16-port Baseline Switch 2816-SFP Plus
Storage	Dell EMC Fiber Channel AX100 and iSCSI AX100i Storage Array at RAID-5 with 10,000rpm 1" LVD Ultra 160 and Ultra3 SCSI drives
Spitfire StoreSafe	Spitfire StoreSafe for DAS – SF-FC110 with Spitfire Core Cryptographic Engine version 1.0.8 • Dual AMD-Opteron dual-core 265 • 2 GB main memory

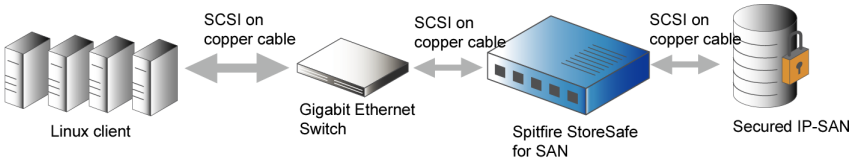

Figure – IP-SAN/i-SCSI test with Spitfire StoreSafe for SAN protection

Security specific setup is as follows

Encryption Algorithm	Advanced Encryption Standard (AES) Electronic Code Book (ECB)
Key Length	256-bit
Encryption Key	Spitfire KeyCastle PKCS#11 hardware security module (HSM)
Cryptographic Tasks	• encryption • decryption

Results

4 storage hosts each of 10 concurrent threads reading/writing random files each of 10 MB

	Without Encryption	With Encryption	Change
Read/Decryption Throughput (Gbps)	0.386	0.343	-11.2%
Write/Encryption Throughput (Gbps)	0.379	0.330	-12.9%

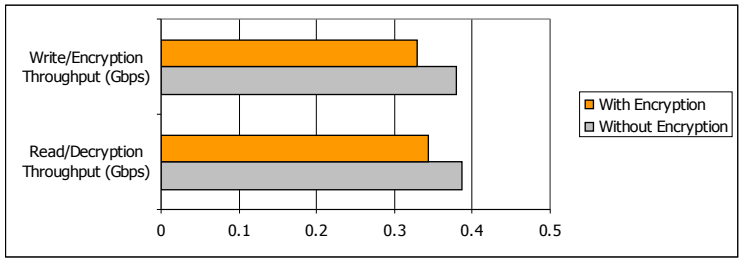

Figure – SAN throughput test results

1 storage host with 1 thread reading/writing 600 files each of 100 MB

	Without Encryption	With Encryption	Change
Read/Decryption Latency (s)	3857.3	4879.3	+26.5%
Write/Encryption Latency (s)	4628.7	5904.1	+27.5%

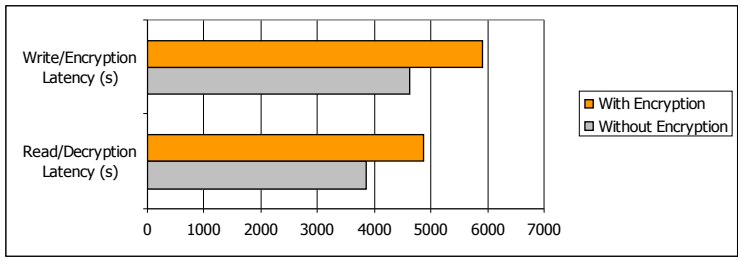

Figure – SAN latency test results

Conclusion

- SCSI proves to be a much more optimized storage protocol than NFS and CIFS, it allows storage network to run at much higher bandwidth in the order of 300 Mbps
- Spitfire StoreSafe for SAN introduces approximately 10% degradation in performance throughput
- For single-threaded processes where read/write operations are serialized with cryptographic overhead, Spitfire StoreSafe for SAN adds more than 25% of time to the entire read/write cycle

Database Access

Transaction Processing Performance Council (TPC) [] defines TPC-C [] benchmark as a standard for online transaction processing (OLTP) applications which are assumed multi-threaded and multi-tasked. As an OLTP system benchmark, TPC-C simulates a complete environment where a population of terminal operators executes transactions against a database. The benchmark is centered around the principle activities (transactions) of an order-entry environment. These transactions include entering and delivering orders, recording payments, checking the status of orders, and monitoring the level of stock at the warehouses. However, it should be stressed that it is not the intent of TPC-C to specify how to best implement an Order-

Entry system. While the benchmark portrays the activity of a wholesale supplier, TPC-C is not limited to the activity of any particular business segment, but, rather, represents any industry that must manage, sell, or distribute a product or service.

In the TPC-C business model, a wholesale parts supplier (called the Company below) operates out of a number of warehouses and their associated sales districts. The TPC benchmark is designed to scale just as the Company expands and new warehouses are created. However, certain consistent requirements must be maintained as the benchmark is scaled. Each warehouse in the TPC- C model must supply ten sales districts, and each district serves three thousand customers. An operator from a sales district can select, at any time, one of the five operations or transactions offered by the Company's order-entry system. Like the transactions themselves, the frequency of the individual transactions are modeled after realistic scenarios.

The most frequent transaction consists of entering a new order which, on average, is comprised of ten different items. Each warehouse tries to maintain stock for the 100,000 items in the Company's catalog and fill orders from that stock. However, in reality, one warehouse will probably not have all the parts required to fill every order. Therefore, TPC-C requires that close to ten percent of all orders must be supplied by another warehouse of the Company. Another frequent transaction consists in recording a payment received from a customer. Less frequently, operators will request the status of a previously placed order, process a batch of ten orders for delivery, or query the system for potential supply shortages by examining the level of stock at the local warehouse. A total of five types of transactions, then, are used to model this business activity. The performance metric reported by TPC-C measures the number of orders that can be fully processed per minute and is expressed in tpm-C.

Setup

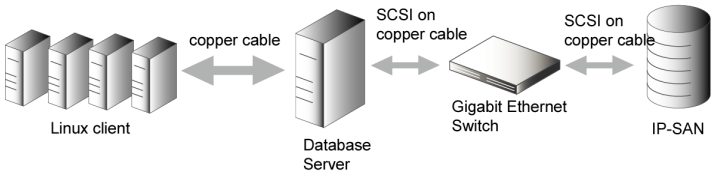

Figure – TPC-C test without protection

Detailed hardware/software setup is as follows

Storage Type	SAN
Storage Communications Protocol	SCSI
Test Client	4 single-processor rack-mount servers • Intel 64-bit Xeon 3 GHz processor with 1 MB L2 cache • 1 GB main memory • Redhat 9.0 • Integrated dual gigabit Ethernet network interface • Sun JRE 1.5.0_04 • JMeter 2.0.2
Interconnects	AMP Netconnect CAT 6 gigabit patch cables
Switch	3COM Gigabit 16-port Baseline Switch 2816-SFP Plus

Database Server	Single-processor rackmount server • Intel 64-bit Xeon 3 GHz processor with 1 MB L2 cache • 2 GB main memory • Redhat 9.0 • Integrated dual gigabit Ethernet network interface Oracle 10g database server • TPC-C database with 10 warehouses total size 1 GB • 3 x 30 MB redo log • archive log on
Storage	Dell EMC Fiber Channel AX100 and iSCSI AX100i Storage Array at RAID-5 with 10,000rpm 1" LVD Ultra 160 and Ultra3 SCSI drives
Spitfire StoreSafe	Spitfire StoreSafe for DAS – SF-FC110 with Spitfire Core Cryptographic Engine version 1.0.8 • Dual AMD-Opteron dual-core 265 • 2 GB main memory

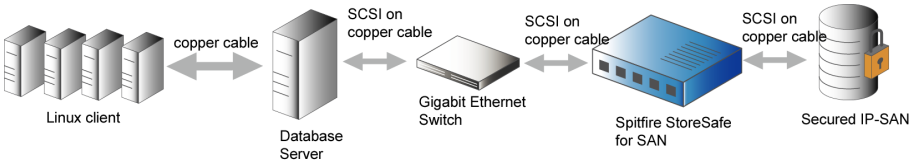

Figure – TPC-C test with Spitfire StoreSafe for SAN protection

Security specific setup is as follows

Encryption Algorithm	Advanced Encryption Standard (AES) Electronic Code Book (ECB)
Key Length	256-bit
Encryption Key	Spitfire KeyCastle PKCS#11 hardware security module (HSM)
Cryptographic Tasks	• encryption • decryption

TPC-C tests are carried out on plain and encrypted data. Tests carried out with Spitfire StoreSafe have the followings files encrypted

- Oracle control files
- Oracle data and index files
- Redo logs
- Archive logs

Results

4 storage hosts each of 10 concurrent threads creating random OLTP stress

	Without Encryption	**With Encryption**	**Change**

Query Intensive (R/W = 4/1) Throughput (tpm-C)	3695.5	3446.0	-6.8%
Update Intensive (R/W = 1/10) Throughput (tpm-C)	4433.0	3465.5	-21.8%

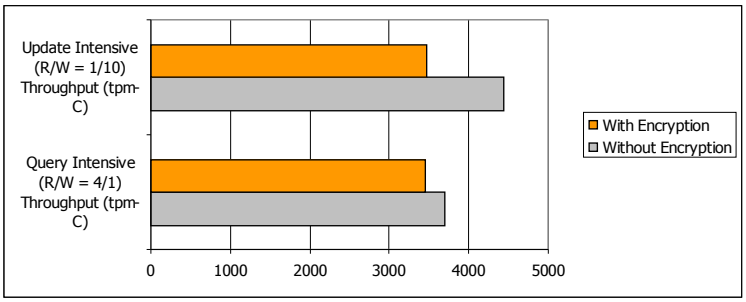

Figure – TPC-C throughput test results

Conclusion

- Spitfire StoreSafe for SAN introduces approximately 10% - 20% degradation in performance throughput on TPC-C tests
- Read-intensive tests tend to have less effect on performance degradation due to encryption which can be explained by presence of Oracle data cache – system global area (SGA) that reduces number of actual disk read
- Write-intensive tests result in a more significant drop of performance compared with file access test in earlier section. As redo and archive logging are turned on and they are encrypted by Spitfire StoreSafe, update of a single record at database triggers encryption of record at data file, encryption of delta update log at redo log file, and if chances that archival of redo log is required, encryption has to be applied on archive log as well. A transaction can be completed only if both data and redo log files are updated, transaction turn-around time is increased and thus lowers transaction throughput

Conclusion

The benchmark tests are completed successfully without error. We declare the test results are valid.

Due to the intrinsic properties and characteristics of the storage network protocol, hardware configuration, cipher efficiency, storage network parameters and environment, specific Spitfire StoreSafe models result in slightly different absolute throughput and latency results. Nevertheless, they follow relatively similar order of magnitude in change of throughput and latency. In general, introduction of Spitfire StoreSafe into the storage network

- lowers overall throughput by 10% to 25% and
- increases read/write latency by 25% to 45%

Therefore, for multi-threaded applications such as database and web applications, the effect of Spitfire StoreSafe should be limited to under 25%. For single-threaded applications such as backup and archival, one should expect the same operation will take up to 45% more time to complete. However, such estimation applies to the following conditions only

- storage read/write operations are synchronous, i.e. requests wait till data are completely committed before they are returned, and
- all data to be processed are required to be encrypted

Real-life systems normally do not require all data to be protected. Customers are advised to rank their data into levels of security while different level of data should be protected by different strategy. For example, public data require no protection, less sensitive data are stored in protected storage requiring special authentication and access control, most sensitive data are protected by Spitfire StoreSafe.

Assuming sensitive data constitutes only 10% of the entire data volume, actual effect of Spitfire StoreSafe to such a system might reduce to 10% of above reference figures, i.e. less than 2.5% for throughput and less than 4% for latency. However, such interpolation may not be too accurate, customers are suggested to evaluate Spitfire StoreSafe on their testing environment and obtain better estimation of performance impact.

Spitfire StoreSafe for SAN produces the best results by demonstrating least performance impact to storage network throughput and latency, Spitfire StoreSafe for DAS ranks the second, NFS in Spitfire StoreSafe for NAS ranks the third and CIFS in Spitfire StoreSafe for NAS ranks the fourth.

Storage network protocol has the dominant effect which accounts for the difference in the effect of Spitfire StoreSafe to storage data communications. More efficient and scalable protocols on error-free media couple with StoreSafe better, introducing comparatively less overhead, thus having least invasive effect to storage security.

References

1. Spitfire StoreSafe, http://bloombase.com/products/spitfire/storesafe/index.html
2. Apache JMeter, http://jakarta.apache.org/jmeter/
3. NIST FIPS-197 AES, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
4. NIST FIPS-140-1, http://csrc.nist.gov/publications/fips/fips140-1/fips1401.pdf
5. NIST FIPS-140-2, http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
6. NIST FIPS-46-3 DES, http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf
7. AMD Opteron, http://www.amd.com/us-en/Processors/ProductInformation/0,,30_118_8796,00.html
8. TPC, http://www.tpc.org
9. TPC-C, http://www.tpc.org/tpcc/detail.asp