interopLab

Bloombase StoreSafe Security Server NAS Benchmarking

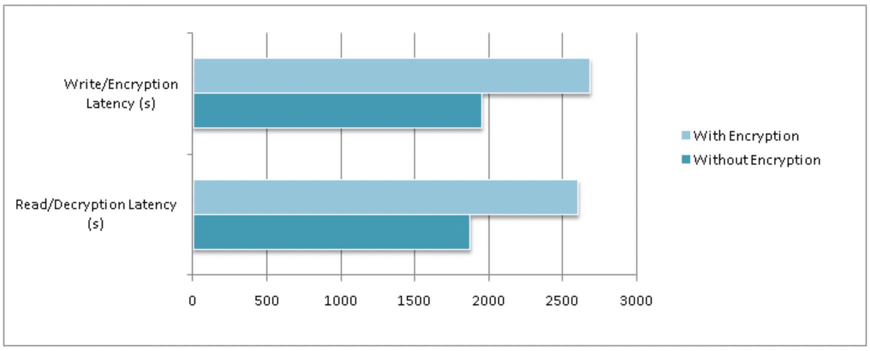
BLOOMBASE®

AMD

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

Document No.

Contents


Write/Encryption Latency (s)
Read/Decryption Latency (s)
0
500
1000
1500
2000
2500
3000
With Encryption
Without Encryption

Executive Summary

Bloombase Spitfire StoreSafe Security Server 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 Bloombase Spitfire StoreSafe Security Server is strong at.

Bloombase Spitfire StoreSafe Security Server 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 Bloombase Spitfire StoreSafe Security Server acts as a middleman virtualizing the encrypted data storage AS IF in plain to applications and end users.

Bloombase Spitfire StoreSafe Security Server 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. Bloombase Spitfire StoreSafe Security Server 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.

Bloombase Spitfire StoreSafe Security Server, 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

Bloombase Spitfire StoreSafe Security Server 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 (FC), FCoE, i-SCSI

This document serves as a report of benchmarking tests of Bloombase Spitfire StoreSafe Security Server 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

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

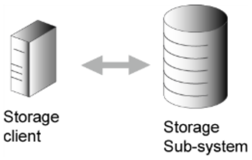


Figure – A typical enterprise system showing a storage client accessing a network storage sub-system

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 Bloombase Spitfire StoreSafe Security Server 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.

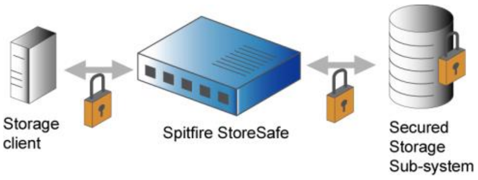


Figure – A visual showing Bloombase Spitfire StoreSafe Security Server appliance acting as a proxy to storage sub-system virtualizing and securing data read from and written to the network storage. Bloombase Spitfire StoreSafe Security Server might introduce slight latency of data transmission due to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

Bloombase Spitfire StoreSafe Security Server 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, Bloombase Spitfire StoreSafe Security Server 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 Bloombase Spitfire StoreSafe Security Server, Bloombase Spitfire StoreSafe Security Server 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 Bloombase Spitfire StoreSafe Security Server, 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 Bloombase Spitfire StoreSafe Security Server 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 Bloombase Spitfire StoreSafe Security Server and actual storage system as a single component of an enterprise system. Enterprise applications including web, email and database are highly multi-threaded while Bloombase Spitfire StoreSafe Security Server's core encryption engine is built to be multi-threaded and multi-tasked for storage clients' concurrent multiple access. Bloombase Spitfire StoreSafe Security Server 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 Bloombase Spitfire StoreSafe Security Server 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 Bloombase Spitfire StoreSafe Security Server Core Encryption Engine which is the core building block of the entire Spitfire security appliance platform
- To quantify maximum throughputs of individual Bloombase Spitfire StoreSafe Security Server model for specific application
- To observe and measure degradation of throughputs of individual Bloombase Spitfire StoreSafe Security Server

Bloombase Spitfire StoreSafe Security Server Family

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

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

Setup

Benchmark tests for different Bloombase Spitfire StoreSafe Security Server 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
- Bloombase Spitfire StoreSafe Security Server – storage data cryptographic engine
- Secured storage sub-system – storage system with physical media

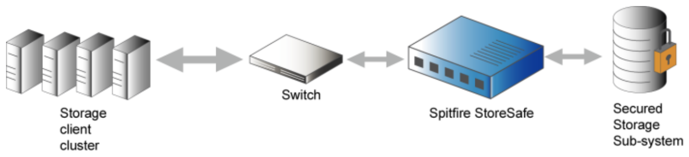


Figure – An abstract benchmark setup for testing of individual Bloombase Spitfire StoreSafe Security Server model for specific application

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	Bloombase Spitfire StoreSafe Security Server	Storage Sub-system
DAS	SCSI	Intel-based Linux or Windows, RISC-based UNIX	SCSI interface card	Copper SCSI cable	N/A	Bloombase Spitfire StoreSafe Security Server 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	Bloombase Spitfire StoreSafe Security Server 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	Bloombase Spitfire StoreSafe Security Server 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 (Microsoft® Windows® Powered OS based on Windows Storage Server 2003)
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 Bloombase Spitfire StoreSafe Security Server 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.

Bloombase Spitfire StoreSafe Security Server on NAS

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.

Bloombase Spitfire StoreSafe Security Server protects enterprise persistence data with wire-speed strong encryption and transparent operation least affecting existing corporate computing infrastructure. Bloombase Spitfire StoreSafe Security Server 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

Network File System (NFS)

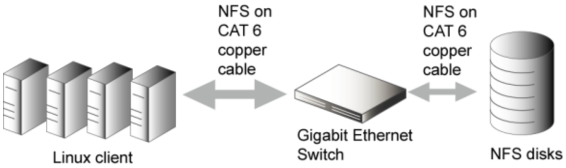


Figure – NAS NFS test without protection

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

Bloombase Spitfire StoreSafe Security Server	Bloombase Spitfire StoreSafe Security Server for DAS – SF-C110 with Spitfire Core Cryptographic Engine version 2.0 • Dual AMD-Opteron dual-core 265 • 2 GB main memory

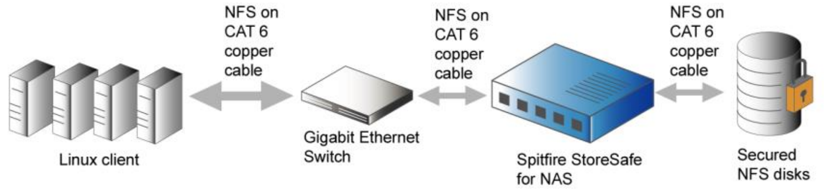

NFS on CAT 6 copper cable
NFS on CAT 6 copper cable
NFS on CAT 6 copper cable
Linux client
Gigabit Ethernet Switch
Spitfire StoreSafe for NAS
Secured NFS disks

Figure – NAS NFS test with Bloombase Spitfire StoreSafe Security Server for NAS protection

Security specific setup is as follows

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

Common Internet File System (CIFS)

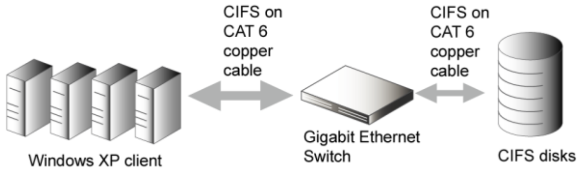


Figure – NAS CIFS test without protection

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)
Bloombase Spitfire StoreSafe Security Server	Bloombase Spitfire StoreSafe Security Server for DAS – SF-C110 with Spitfire Core Cryptographic Engine version 2.0 • Dual AMD-Opteron dual-core 265 • 2 GB main memory

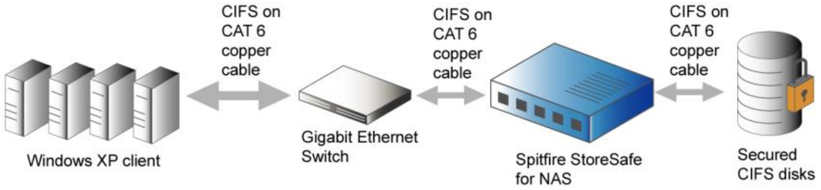

CIFS on CAT 6 copper cable
CIFS on CAT 6 copper cable
CIFS on CAT 6 copper cable
Windows XP client
Gigabit Ethernet Switch
Spitfire StoreSafe for NAS
Secured CIFS disks

Figure – NAS CIFS test with Bloombase Spitfire StoreSafe Security Server 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

Network File System (NFS)

1 storage host each of 1 concurrent thread reading/writing random files each of 10MB

	Without Encryption	With Encryption	Change
Read/Decryption Throughput (Gbps)	0.2641	0.1799	-31.9%
Write/Encryption Throughput (Gbps)	0.2776	0.1851	-33.3%

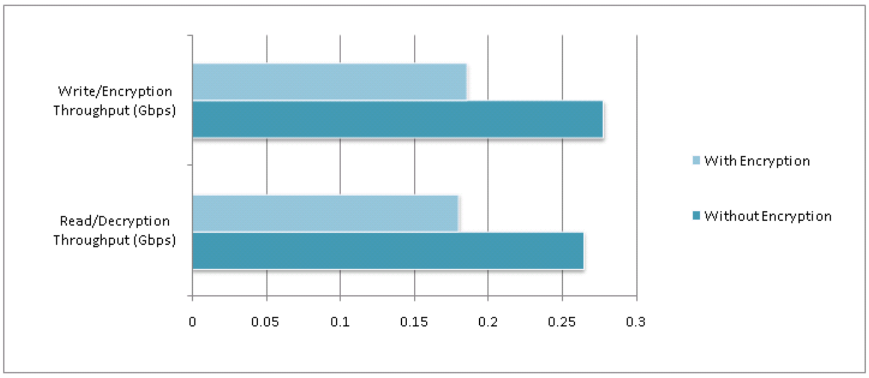


Figure – NFS throughput test results

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

	Without Encryption	With Encryption	Change
Read/Decryption Latency (s)	1873	2604	+39.0%
Write/Encryption Latency (s)	1953	2685	+37.5%

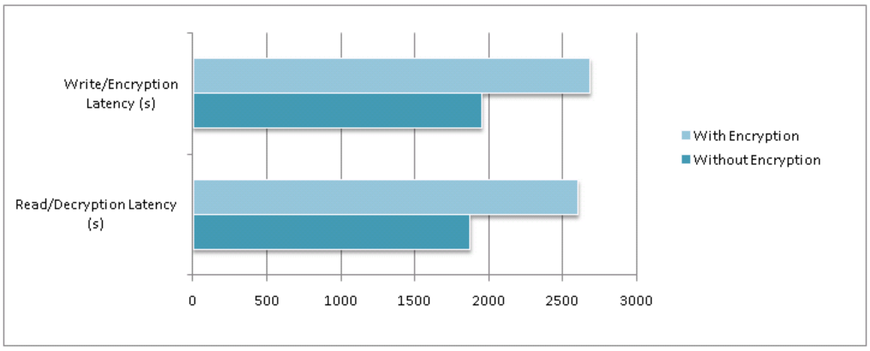


Figure – NFS latency test results

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

	Without Encryption	With Encryption	Change
Read/Decryption Throughput (Gbps)	0.9244	0.6697	-27.6%
Write/Encryption Throughput (Gbps)	0.9716	0.6879	-29.2%

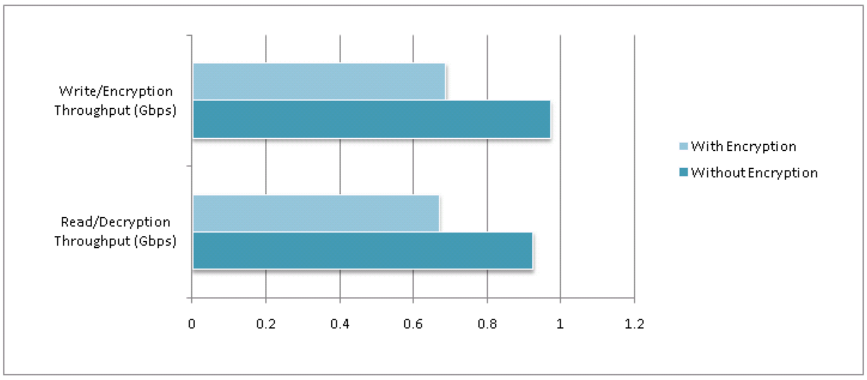


Figure – NFS throughput test results

Common Internet File System (CIFS)

1 storage host each of 1 concurrent thread reading/writing random files each of 10 MB

	Without Encryption	With Encryption	Change
Read/Decryption Throughput (Gbps)	0.2058	0.1222	-40.6%
Write/Encryption Throughput (Gbps)	0.2179	0.1346	-38.2%

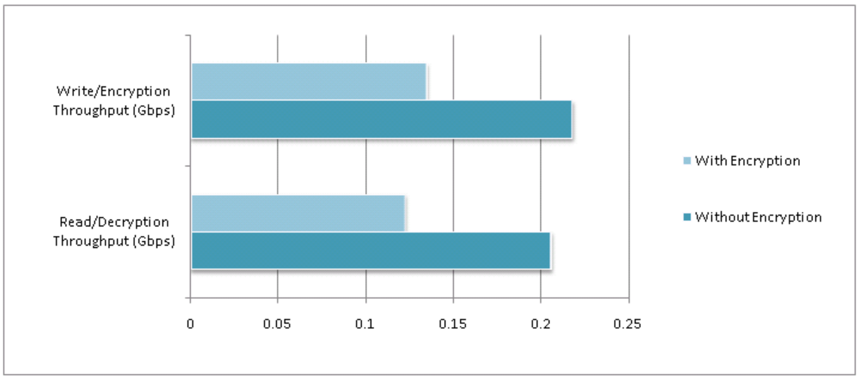


Figure – CIFS throughput test results

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

	Without Encryption	With Encryption	Change
Read/Decryption Latency (s)	2216	3235	+46.0 %
Write/Encryption Latency (s)	2202	3083	+40.0 %

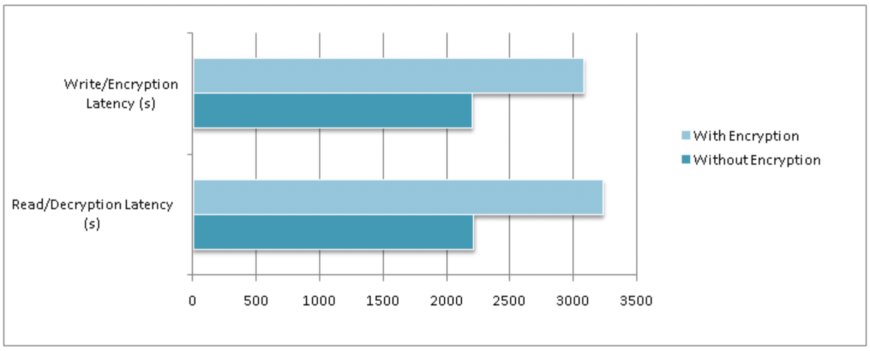


Figure – CIFS latency test results

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)	0.7409	0.4579	-38.2%
Write/Encryption Throughput (Gbps)	0.7812	0.5140	-34.2%

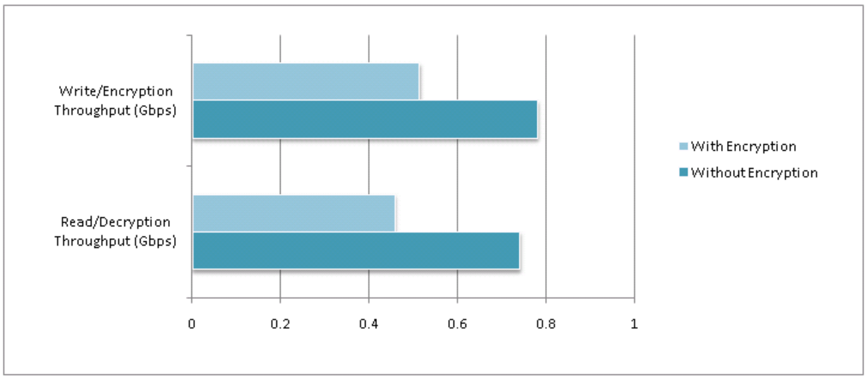


Figure – CIFS throughput test results

Conclusion

- Introducing Bloombase Spitfire StoreSafe Security Server for NAS to NFS and CIFS storage reduces data throughput by 20% to 40%

- Bloombase Spitfire StoreSafe Security Server increases read/write turn around times for 30% to 40%

- 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 Bloombase Spitfire StoreSafe Security Server on data encryption. Bloombase Spitfire StoreSafe Security Server for NAS introduces the greatest drop of throughputs and longest latencies amongst the Bloombase Spitfire StoreSafe Security Server 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 Bloombase Spitfire StoreSafe Security Server

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 Bloombase Spitfire StoreSafe Security Server 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 Bloombase Spitfire StoreSafe Security Server into the storage network

- lowers overall throughput by 20% to 40% and
- increases read/write latency by 30% to 40%

Therefore, for multi-threaded applications such as database and web applications, the effect of Bloombase Spitfire StoreSafe Security Server 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 Bloombase Spitfire StoreSafe Security Server.

Assuming sensitive data constitutes only 10% of the entire data volume, actual effect of Bloombase Spitfire StoreSafe Security Server 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 Bloombase Spitfire StoreSafe Security Server on their testing environment and obtain better estimation of performance impact.

Storage network protocol has the dominant effect which accounts for the difference in the effect of Bloombase Spitfire StoreSafe Security Server 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. Bloombase Spitfire StoreSafe Security Server, 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