White Paper
Enova® Technology SecureNAS

Table of Content

Abstract

The ***Enova Technology SecureNAS*** **(the picture on the first page shows model T1)** is a real-time encrypted networked storage server that equips with proven data-at-rest security, advanced security architecture, secure authentication, and access control. It integrates Enova Technology's latest ***X-Wall MX***®[1] on the backplane of a high performance hardware RAID 5 storage sub-system while the KEYS and CERTIFICATES are delivered securely via a remote Key Server which runs under Windows XP Pro, Windows Vista, and/or Windows Server 2003. As simple as a notebook computer running XP Pro can act as the Key Server which provides enterprise-class key management system. The entire high performance hardware RAID 5 and/or RAID 6 storage sub-system is secured by ***X-Wall MX*** **real time full disk encryption** processor thus the overall disk IO throughput is unaffected. Each of the SATA disk drive that connects to the high performance hardware RAID 5 and/or RAID 6 storage sub-system is real-time encrypted with NIST (USA) and CSE (Canada) certified AES 256-bit cryptographic processor with ECB (Electronic Code Book) or CBC (Cipher Block Chaining) mode of operation. As the keys that operate each individual SATA disk drive are not stored permanently inside the system, attempts to remove each individual drive to get to the sensitive data will be proven futile. Furthermore, stolen of the entire ***SecureNAS T1*** presents absolutely no harm to the data stored inside the disk drives as the KEYS and CERTIFICATES will need to be delivered via a remote Key Server upon power on authentication for which a proven Public Key Infrastructure (PKI) architecture has been deployed.

SecureNAS T1 Addresses Requirements of Regulatory Compliance

Regulatory compliant requirements are increasing in both laws established and enforced world-wide in light of numerous high-profile data security and privacy breaches as well as corporate scandals. Compliance to those laws and regulations is no longer an option to corporate IT management but implementing such compliance solution isn't a simple task, which often places corporate executives and IT managers into a dilemma: divert insufficient IT resources to manage ever broaden access, storage, and security requirements or simply accept whatever consequences that may be enforced by regulatory enforcement due to none-compliance. The later is obviously not an option as fines and penalty may potentially

[1] *X-Wall MX* comes with SATA interface and AES ECB or CBC 256-bit strength. Reference to Enova Technology web link http://www.enovatech.net/support/download/X-Wall%20MX_FAQ_v4.pdf for details.

put your company out of business, regardless damages to the company reputation due to data breaches and time spent to try to recover customer trusted relationship.

The goal for the IT professionals must then be to minimize the cost while eliminate the threats and exposures to possible litigation, none-compliance fines, and reputation damage. There are three objectives while IT professionals deal with regulatory compliance: 1) data security, 2) data retention, and 3) data auditability. This white paper primarily deals with number 1 and 2 and with a lesser degree, the number 3.

Data storage system plays an essential role in those three objectives as each one of those three objectives involves with data written and retrieval from the storage device. Sensitive data such as patient digital records, medical examination images (where HIPPA enacts), personal information (where CA 1386 enacts), personal financial records (where GLBA enacts), and employees privacy (where EU Data Protection Act enacts) are all required for authentication and encryption down to the storage level, and *SecureNAS T1* adequately help accomplish your goals with significantly reduced cost.

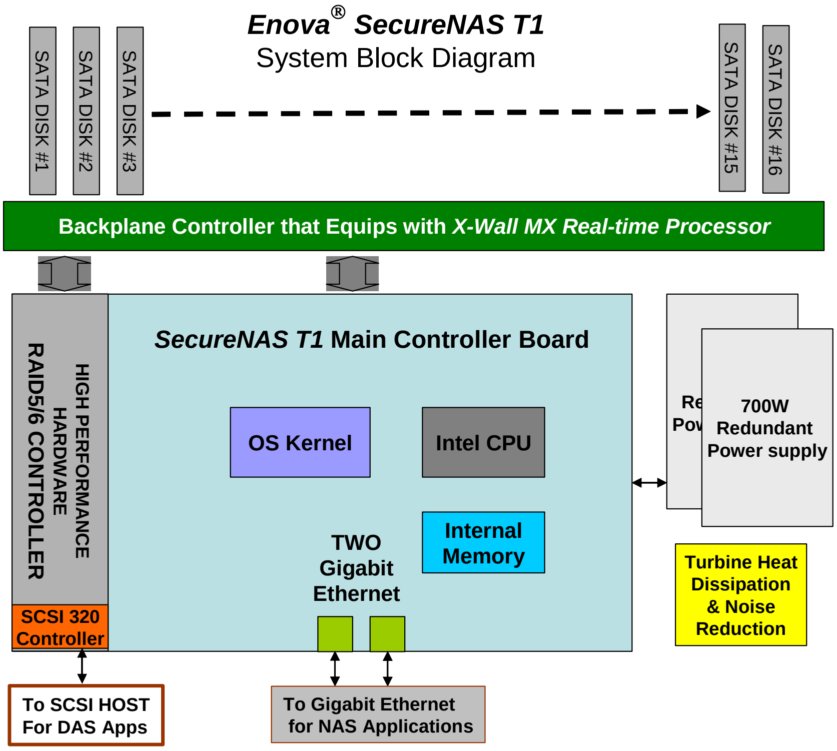
SecureNAS T1 supports native CIFS, NFS, and AppleTalk file protocols thus it merges nicely into your existing Gigabit Ethernet network. Applications running over CIFS and NFS can be easily migrated into the *SecureNAS T1* without modifications; Authentication service such as Active Directory Service (ADS) and LDAP can be integrated nicely with the *SecureNAS T1* as the cryptographic operations are done on the data read/write commands over SATA interface and are not on the Packet level thus compliance to the ADS and LDAP is automatic and transparent; Encryption is done real-time with the dedicated NIST and CES certified hardware AES 256-bit cryptographic processor with ECB or CBC mode of operation to ensure that all Data-At-Rest (DAR) are properly secured with US and Canada government certified AES hardware; No performance degradation over disk IO operations due to heavy cryptographic operations; And enterprise key management system is provided for authentication and key management to each network connected *SecureNAS T1* through a working Key Server.

The solution matrix below exhibits what those laws and regulations are and how the *SecureNAS T1* adequately answers those calls:

Laws or Regulations	**Administrator or Agency**	**Requirements**	**Who are impacted?**	**Enova Technology Solutions**
California Senate Bill	State of	To protect	Financial	SecureNAS T1

1386 (or SB1386)	California, USA	consumer privacy	services that do business in the State	-- All Data-At-Rest are AES 256-bit encrypted which can only be accessed through the Directory Service
DoD 5015.2-STD	US Department of Defense	Strong authentication and encryption	US Military	SecureNAS T1 -- all DAR are hardware AES 256-bit real-time encrypted in either ECB or CBC mode; Authentication is secure through the built-in SAC;
Gramm-Leach-Bliley Act (or GLBA)	Federal Trade Commission (FTC)	Encryption, Secure Backup, Data destruction	Financial Services	SecureNAS T1 -- All DAR are AES 256-bit secure; Hardware RAID 5 or 6 ensure data integrity and backup; data destruction is as simple as removing the AES key;
Health Insurance Portability and Accountability Act (or HIPPA)	US Health and Human Services	Privacy, security, long data retention	Health Insurance and healthcare providers	SecureNAS T1 -- Hardware RAID 5 or 6 ensure data integrity and longevity; Hardware AES 256-bit secures all DAR; Authentication is transparent with all known directory services such as ADS;
Sarbanes-Oxley (or SOx)	Security Exchange Commission (SEC)	Reliability, protection, data retention, and protect against alternation or destruction	Public companies and accounting firms	SecureNAS T1 -- RAID 5 or 6 ensures data reliability; Hardware AES 256-bit ensures DAR protection with consideration of data alteration and destruction;
Data Protection Act	EU, UK Data Commissioner	Employees privacy	EU operations and global firms	SecureNAS T1 -- Hardware AES 256-bit ensures DAR protection; Authentication is transparent through known directory services such as ADS

SecureNAS T1 Architecture


Enova® SecureNAS T1
System Block Diagram
SATA DISK #1
SATA DISK #2
SATA DISK #3
SATA DISK #15
SATA DISK #16
Backplane Controller that Equips with *X-Wall MX Real-time Processor*
HIGH PERFORMANCE HARDWARE RAID5/6 CONTROLLER
SCSI 320 Controller
SecureNAS T1 Main Controller Board
OS Kernel
Intel CPU
Internal Memory
TWO Gigabit Ethernet
700W Redundant Power supply
Turbine Heat Dissipation & Noise Reduction
To SCSI HOST For DAS Apps
To Gigabit Ethernet for NAS Applications

Please reference above ***Enova Technology SecureNAS T1*** hardware architecture for which ***X-Wall MX*** sits at the backplane of the high performance hardware RAID 5 and/or RAID 6 storage sub-system and the keys that operate each individually connected SATA disk drive are securely delivered via the Gigabit LAN port through a remote Key Server. Each one of the connected SATA disk drive is controlled by an *X-Wall MX* real-time cryptographic processor, ensuring absolute security over all written data.

The ***SecureNAS T1*** boasts a 16TB[2] capacity and can extend more with upcoming models. The high performance hardware RAID configuration is set at either RAID 5 or RAID 6. Two or more full duplex Gigabit Ethernet ports, which can be trunked together through software settings that offers multiplied bandwidth a standard Gigabit Ethernet could offer, are provided for TCP/IP connection.

SecureNAS Secures Your Networked Storage, Guaranteed.

[2] Disk drives are not included in the ***SecureNAS T1 System***

SecureNAS T1 Features

Bullet Proved Data-At-Rest (DAR) Security

The ***SecureNAS T1*** equips with the high performance hardware RAID 5 or RAID 6 storage sub-system that is real-time encrypted by the ***Enova Technology X-Wall MX*** with NIST and CSE certified 100% hardware AES 256-bit strength with ECB or CBC mode of operation[3][4]. It combines secure authentication, real-time full disk encryption to each individually connected SATA disk drive, and secure logging to provide unprecedented protection for sensitive data-at-rest. All addressable data blocks of a SATA disk drive are encrypted without exception. The **KEY and CERTIFICATE**[5] that operate the SATA disk drives of a hardware RAID 5 or RAID 6 storage sub-system are securely delivered via a remote secure Key Server upon booting and upon secure authentication. The KEY and CERTIFICATE are **NEVER** stored inside the *SecureNAS T1* system after the power is been removed, which guarantees absolutely harmless situation should an ***Enova Technology SecureNAS T1*** ever get stolen. In the case of installing a new Key Server to authenticate the stolen *SecureNAS T1*, the prior registered profile over the true Key Server can successfully prevent the authentication. Furthermore, attempts to remove a number of disk drives to get to the sensitive data stored are proven futile as each connected SATA disk drive is real-time encrypted whereas KEY and relevant CERTIFICATE are only available through secure authentication from a true Key Server.

Complete Advanced Security Architecture

The security system consists of five primary security sub-systems:

1. **The *SecureNAS T1*.** It consists of a Secure Authentication Channel (SAC) that is responsible for the Key and relevant CERTIFICATE delivery and a License evaluation module that is responsible for evaluating available license rights;
2. **The Key Server.**A Key Server operating over Microsoft Windows platform including XP Pro, Vista, and Server 2003, whose purpose is to manage the Keys and license information to the ***SecureNAS T1***; As simple as an administrator's notebook PC can

[3] For complete Enova *X-Wall MX* real-time cryptographic processor information, please review below web link: http://www.enovatech.net/products/mx_info.htm for more information.

[4] To review Enova's AES CBC NIST/CSE certificates, please review below web link: http://www.enovatech.net/resources/aes_no250.htm#a for more information.

[5] KEY refers to the AES 256-bit key that operates the RAID 5 and/or RAID 6 storage sub-system with each connected SATA disk drive owns one AES 256-bit key. CERTIFICATE, generated by a remote License Server, refers to the X.509 certificate that defines features and functions of each Key Server and *SecureNAS T1*.

properly execute all the Key Server functions;

3. **<u>The Backup Key Server.</u>** An optional Backup Key Server operating over Microsoft Windows platform, including XP Pro, Vista, and Server 2003, whose purpose is to substitute/perform the functions of the Key Server in the event of Key Server failure;

4. **<u>The License Server.</u>** This is separated from the Key Server. A License Server operating remotely, whose purpose is to create licenses files for each connected ***SecureNAS T1*** and Key Server such that only pre-defines functions and features can be properly executed; and

5. **<u>An Administrator PC.</u>** An Administrator PC or laptop that runs Windows and can manage the ***SecureNAS T1*** as well as the Key Server over the network;

No Performance Degradation

The ***Enova Technology X-Wall MX*** transparently and automatically encrypts each individually connected SATA disk drive of a high performance hardware RAID 5 and/or RAID 6 storage sub-system, offering each SATA channel a ***sustained*** 1.2Gbit/sec throughput of AES ECB or CBC 256-bit cryptographic strength, which is more than adequate that a modern SATA disk drive is capable of producing. **<u>As a matter of fact, the designer can use a Port Multiplier or 1 SATA to 4 SATA controller to obtain the same disk IO performance using single *X-Wall MX.*</u>** As the entire cryptographic operations are performed real-time at the backplane controller, disk IO performance is not impacted and frequently, it is enhanced[6]. The transfer rate to the client computers is limited to the two Gigabit LAN connections, which can also be trunked together to enhance performance further. As a result, there is absolutely no performance degradation due to heavy AES 256-bit cryptographic operations.

Enterprise Class Key Management System

The ***SecureNAS T1*** contains a set of patented ***X-Wall MX*** real-time full disk cryptographic processors sitting at the backplane controller of the high performance hardware RAID 5 and/or RAID 6 storage sub-system. The cryptographic key (AES 256-bit length) used by the ***X-Wall MX*** parts is generated and stored securely on the remote Key Server, which is the only place that stores the secret AES KEY and related CERTIFICATE. During the ***SecureNAS T1*** power-on-reset (POR) process, these AES KEY and CERTIFICATE are delivered via a secure authenticated channel (SAC) to the ***SecureNAS T1***. Within the

[6] RAID 5 and RAID 6 storage sub-system test data with and without *X-Wall MX are* available. Make request to your sales representative.

SecureNAS T1, the AES KEY and CERTIFICATE are decrypted and delivered across the backplane controller of a RAID 5 and/or RAID 6 storage sub-system. In order to establish the secure tunneling, the ***SecureNAS T1*** and Key Server must be able to authenticate one another. This process is facilitated by a one-time setup operation initiated by the system administrator during which time the ***SecureNAS T1*** and Key Server exchange their respective CERTIFICATES. System administrator can monitor and administrate the working conditions of each connected ***SecureNAS T1*** and Key Server and export their work log as preferred.

Real-time Full Disk Encryption Capability

All the data stored on the hardware RAID 5 and/or RAID 6 storage sub-system are real-time encrypted by the ***X-Wall MX*** real-time cryptographic processor sitting at the backplane controller. There is absolutely no clear text left unprotected in the ***SecureNAS T1***. The cryptographic processing is real-time and is totally transparent to all users, guaranteed.

Authentication and Access Control

Each SecureNAS T1 provides automatic yet secure authentication architecture for client access and storage management. As the data-at-rest cryptographic processing occurs at the backplane controller of the high performance hardware RAID 5 or RAID 6 storage sub-system, support for client access control of directory servers such as Active Directory Service (ADS) and LDAP is automatic thus doesn't complicate your existing network access control infrastructure. There are no extra software or drivers required to be installed, making the ***SecureNAS T1*** solution independent to commonly used operating systems. **On the NAS application, all clients with Windows, Linux, and MAC operating systems are allowed to conduct regular file access without complications.** The only difference is that all their data-at-rest are AES 256-bit secured. Moreover, as the ***SecureNAS T1*** also equips with SCSI 320 device controller on the hardware RAID 5 or RAID 6 storage sub-system controller unit, it is also a perfect candidate to serve as a Direct Attached Storage (DAS) in addition to its built-in Network Attached Storage (NAS) file level access support. **Over the DAS application, the *SecureNAS T1* simply serves as an AES 256-bit secure storage array for those application servers.**

Keys Recovery & Deletion

All important Keys, Certificates, Public and Private Keys are stored inside the Key Server encrypted and only the system Administrator has the right key to decrypt and to export. It can be transported to other Key Server to give you peace of mind. As all CERTIFICATES are delivered to the ***SecureNAS T1*** from the Key Server via a Secure Authentication Channel (SAC), the ***SecureNAS T1*** does not contain any credentials that could have harmed the sensitive data-at-rest, not even with the stolen of the entire system.

Optional Remote Secure File Backup

All encrypted files contained inside the ***SecureNAS T1*** can be exported encrypted to another designated ***SecureNAS T1*** through its powerful **Remote Secure File Backup** utility. The encrypted data-at-rest is firstly decrypted from the *X-Wall MX* of the backplane controller unit, re-encrypted then send through another ***SecureNAS T1*** encrypted using the KEY and CERTIFICATE of the designated ***SecureNAS T1***. The operation is totally transparent and does not require any user intervention. This utility provides a useful tool for disaster recovery as well as backing up important files remotely and securely. It is becoming critically important that important data to operate the daily business of an enterprise needs to be duplicated. The ***SecureNAS T1*** can definitely meet the strict requirement of demanding both security and performance.

Auditing and Logging

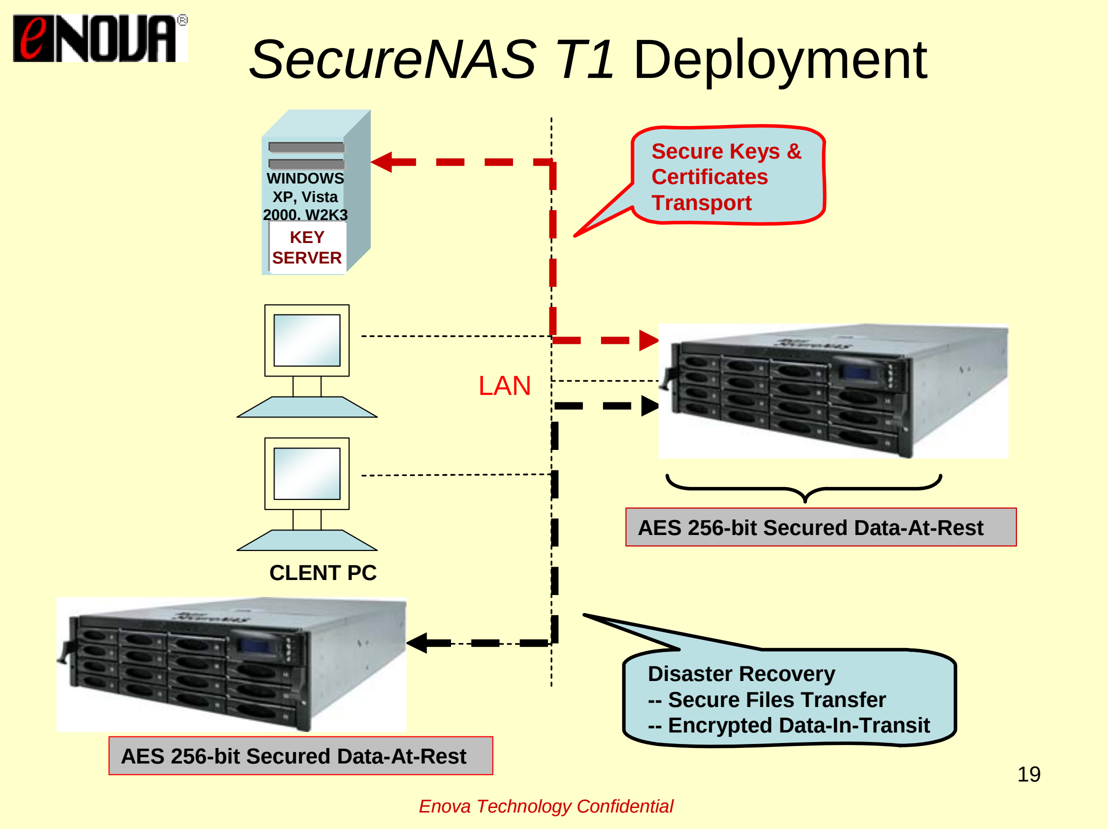
The ***SecureNAS T1*** offers auditing and logging capability for which a system administrator can view all important security events including client access log.

Deployment Made Easy with *SecureNAS T1*

SecureNAS T1 Deployment

Deployment through the Standard Gigabit Ethernet

The ***SecureNAS T1*** is a real-time encrypted networked storage file server that equips with proven data-at-rest security, advanced security architecture, secure authentication, and access control. It can fit seamlessly into the existing Gigabit-based networked storage infrastructure while providing advanced real-time data-at-rest security without system complications. There is no software to be installed on the client side other than the Key Server that needs to be running under Windows platforms. The implementation does not require users to alter their regular computing behavior. See below the deployment using standard Gigabit Ethernet (the LAN and WAN) if the ***SecureNAS T1*** is intended for Network Attached Storage (NAS) file server.



SecureNAS T1 Deployment

Transparent Operation

Upon initializing the ***SecureNAS T1***, ongoing system management is simple and straight forward via a web-based interface.

No System Complications

As the data-at-rest security is done through the backplane controller, the ***SecureNAS T1*** behaves just like a networked storage file server performing regular data read/write. Unlike other product that encrypts the TCP/IP payload, which causes unforeseen system complications, ***SecureNAS T1*** can completely eliminate the system complications and perform transparent hardware level data-at-rest AES 256-bit encryption. Support of user access control such as Active Directory Service and LDAP is automatic and transparent.

The ***SecureNAS*** natively supports CIFS, NFS and AppleTalk filers. iSCSI support is an option.

Easy to Expand Capacity

The ***Enova SecureNAS T1*** features 16TB to start with. Future models may extend the capacity in the magnitude of 2 or more. Capacity can be easily added with additional purchase of a SATA compliant disk drive.

Reliable and Durable

The ***SecureNAS T1*** is built for robust data-at-rest encryption. There are more advanced features such as redundant power supply, hot plug, hot spare, and heat dissipation that would sustain the ***SecureNAS T1*** a durable life of operation. The hot-pluggable hardware RAID 5 or RAID 6 storage sub-system that accommodates SATA disk drive design enables quick data recovery and repair, making the regular maintenance job much less challenged.

Contact Information

Dennis Chen at dennis.chen@enovatech.com or info@enovatech.com
Account Manager
Enova Technology Corporation www.enovatech.com
1st Floor, #11, Research & Development 2nd Road
Science-based Industrial Park, Hsin-Chu City
Taiwan 30076, Republic of China
Tel. +886 3 577 2767 Fax +886 3 577 2770
http://www.enovatech.com info@enovatech.com