ENOVA

Enova *SecureNAS T1*
Now FIPS 140-2 Compliant

Secure Network Storage & File Server Specification 1.2

*T*he **SecureNAS T1** is a FIPS 140-2 compliant real-time encrypted networked storage server (NAS) that equips with **FIPS 140-2 certified crypto module** responsible for en/decrypting the disk array (data-at-rest) real-time, in addition to its PKI implementation for authentication. It integrates Enova Technology's latest FIPS 140-2 certified **X-Wall MX**®[1] on the backplane of a high performance hardware RAID 5/6 controller to encrypt entire disk array. The AES secret keys and CERTIFICATES are delivered securely via a remote Key Server which runs under Windows XP Pro, Windows Vista, and/or Windows Server 2003. The entire hardware RAID 5/6 disk array is secured by the **FIPS 140-2 certified**[2][3] **X-Wall MX** **real time**

crypto modules such that overall disk IO throughput is unaffected. Each of the SATA disk drive that connects to the RAID 5/6 disk array is real-time encrypted with AES ECB/CBC 256-bit strength. As the AES secret keys that operate the disk array 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 encrypted data stored inside the disk drives as the AES secret keys and CERTIFICATES are not stored inside the system. The Key Server at power on reset performs certificate exchange to authenticate each connected **SecureNAS T1** system.

The **SecureNAS T1** boasts a 32TB[4] capacity and can be extended more with upcoming models. The high performance hardware RAID configuration is set at either RAID 5 or RAID6. 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 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; User authentication service such

---

[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.
[2] The *X-Wall MX-256* (ECB 256-bit) and *X-Wall MX-256C (CBC 256-bit)* are FIPS 140-2 certified with level 3 for physical security.

[3] The *X-Wall MX* family is protected by US patents: 7,136,995; 7,386,734; and 7,900,057.
[4] Disk drives may or may not be included in the **SecureNAS T1 System**

ENOVA

as Active Directory Service (ADS) can be integrated nicely with the **SecureNAS T1** as the cryptographic operations are done on the data read/write commands and are not on the Packet level thus compliance to the ADS a is automatic and transparent; Encryption is done real-time with dedicated FIPS 140-2 certified crypto module with AES ECB/CBC 256-bit strength to ensure that all Data-At-Rest (DAR) are properly secured; No performance degradation over disk IO operations due to heavy cryptographic operations; An automated key Server is provided for authentication and key management to each network connected **SecureNAS T1**.

Security Features

- Dedicated hardware real-time <u>FIPS 140-2 certified X-Wall MX-256 or X-Wall MX-256C Crypto Module</u> that offers AES ECB/CBC 256-bit cryptographic strength for the entire disk array, encrypting every data block written to the disk while decrypting every data block read out from the disk drive without performance degradation;
- Key Server, at power on reset, authenticates the *SecureNAS T1* remontly through certificate exchanged. The AES secret keys and credentials that operate the *SecureNAS T1* stays on the Key Server. The *SecureNAS T1* does not have any secrets left after powering down;
- The Key Server can be installed on a standard laptop running Windows XP or Vista; or on a high end machine running Windows 2003 Server;
- Optional Backup Key Server can duplicate

every security parameters that Key Server is opearting;
- The optional License Server, which operates separately from the Key Server, creates licenses files for each connected **SecureNAS T1** and Key Server such that only pre-defines functions and features can be properly executed;
- Optional Secure File Transfer Protocol allow secure transportation of selected files and folders remotely from **SecureNAS T1** to another through standard Ethernet connection;

NAS Features

- 19" rack-mountable 3U chassis with up to Sixteen (16) hot-swappable SATA II hard drives
- Generic CIFS, NFS, and AppleTalk file protocols;
- Hot spare and automatic hot rebuild;
- Two standard Gigabit Ethernet ports that allows standard LAN or WAN configurations; Trunking/ Failover/Load-balance modes for option;
- High performance hardware RAID 5 and 6 configurations;
- Front-end LCD panel for RAID setting & ENC status;
- Java-based GUI for centralized data and storage management;
- Share management and permission with advanced ACL setting;

eNOVA

Hardware Technical Specifications

Model Name: *SecureNAS* T1
Product Description: Secure Network Storage File Server
◆ Powered by Enova **FIPS 140-2 certified crypto modules** that offer AES ECB/CBC 256-bit hardware cryptographic strength to the entire disk array.
◆ Key Server offers remote key management to all properly licensed *SecureNAS T1*:
◆ Default two Gigabit Ethernet ports
◆ Up to Sixteen hot-swappable SATA II (3Gb/s, NCQ support) hard drives
◆ High performance hardware RAID 5 and RAID 6 configuration to ensure data integrity
◆ Two(2) redundant 700W hot-swappable power supplies with PFC
◆ Real-time drive activity and status indicators and environmental monitoring unit

Connectivity
◆ SMB
◆ CIFS over TCP/IP
◆ NFS over UDP/IP (Optional)
◆ Novell Netware (Optional)
◆ AFP over Apple Talk (Optional)
◆ Mac Zones (Optional)
◆ FTP & HTTP file transfer (Optional)
◆ DHCP, NAT, Internet gateway, & WINS Server

General
◆ File Server Independent and peer-to-peer operation

◆ Localized and multiple language support with multi-node Management GUI
◆ Supports NIC, trunking, load balance, and fail over
◆ Supports Microsoft ADS / PDC and Unix NIS accounts import
◆ SNMP/MRTG management and notification
◆ Online firmware upgrade
◆ CLI management via Telnet or SSH

Power requirements
◆ AC 90V ~ 264V Full range
◆ 10A ~ 5A, 47 ~ 63Hz

Physical Dimension
◆ 133(H) x 482(W) x 730(D) mm