NITROX™ *Lite* CN501 Security Macro Processor
IPsec Product Brief

PRODUCT FEATURES & BENEFITS

Worlds first Security Macro Processor developed using custom CPU design techniques (.13µ)

- Single chip solution that accelerates all cryptographic operations and IPsec / IKE protocols

High performance, industry standard interfaces

- PCI v2.2 (32bit, 66MHz, Master and Slave modes)
- 2.2Gbps burst throughput

High performance Bulk Data Encryption

- 100 Mbps IPsec performance

Highest performance/price Public Key Processor

- 1550 180bit-exponent Diffie Hellman operations/second
- 900 1024bit-exponent RSA operations/second
- Supports up to 2048-bit modulus size

Multi Algorithm Support

- RSA and Diffie-Hellman
- 3DES, AES, ARC4
- Modes: ECB, CBC; Can support 64, 128-bit OFB, and 1, 8, 64-bit CFB (DES), 128-bit CFB (AES)
- AES – supported key lengths: 128, 192, and 256-bit
- MD5, SHA-1, HMAC-MD5, HMAC-SHA-1
- IPv4 and IPv6, complete IPsec AH and ESP

Typical Power <1.0W

100Mbps Random Number Generator

**Available in industrial temp**

PROTOCOL & MANAGEMENT SUPPORT

Multi Protocol Support

- IPsec and IKE. Wireless (802.11i) option available

Full IPsec Protocol Processing with specialized TurboIPsec Macro API functions

- Macro API functions result in dramatic reduction of required I/O bus bandwidth

Comparison of relative I/O usage between Typical Crypto Acceleration and Macro Processing
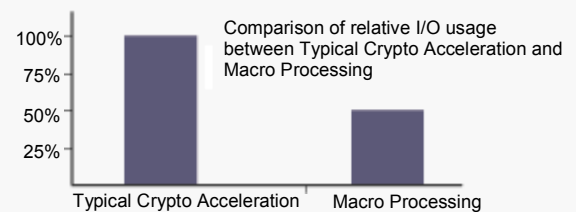
Adaptive capability to handle various bandwidth requirements of different cryptographic operations

- Truly balanced systems can be designed using NITROX *Lite's* flexibility to perform asymmetric, symmetric, hash and protocol processing in a single chip

Dedicated Resources for Administration & Management

- Extensive functionality to assist a range of functions including statistics collection, logging, etc.

Software driver support for Linux, BSD and VxWorks

Modified IPsec and IKE software stack to incorporate Cavium's TurboIPsec macro calls

- KAME, FreeS/WAN

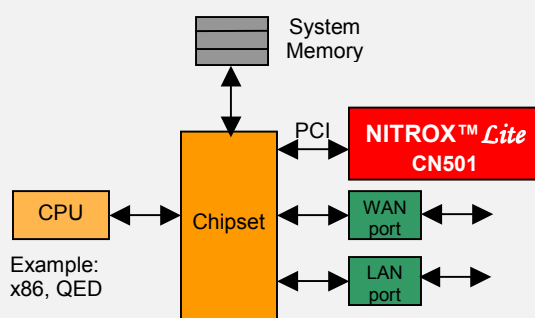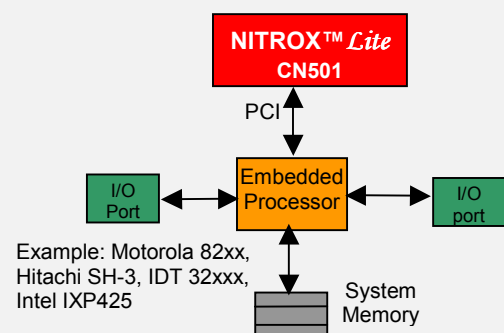**Figure 1: Example of NITROX *Lite* as an IPsec accelerator using PCI bus interface**

Figure 2: Example of NITROX *Lite* in embedded system using PCI bus interface

Example: Motorola 82xx, Hitachi SH-3, IDT 32xxx, Intel IXP425

See over for more information

APPLICATIONS

SOHO and Small to Medium Enterprise
- VPN Gateways
- Remote Access gateways, Residential Gateways

Network Access
- DSL Modems, Cable Modems
- Switches, Routers

Wireless LAN / WAN
- 802.11 gateways (supports AES acceleration and 802.11i security protocols)

BENEFITS TO DESIGNERS

Reduced system cost and complexity
- Single custom processor solution

Quick time to market with complete
- Evaluation board, processor, software
- Software driver and application

Flexible Protocol Processing
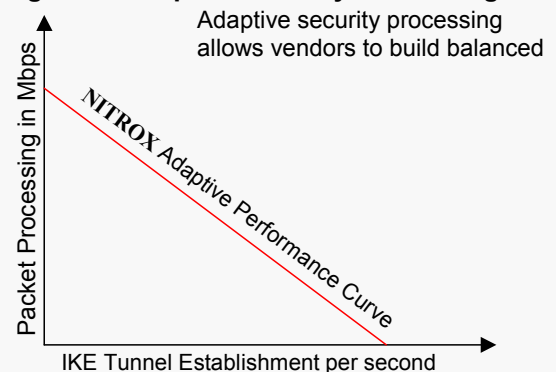- Flexible microcode allows for advanced processing with field upgrade option

PRODUCT SUMMARY

The NITROX *Lite* Security Macro Processor is the industry's first custom processor exclusively targeted towards acceleration.The NITROX *Lite* custom designed processor provides lowest area, cost and power consumption when compared to ASIC based security chips. The heart of NITROX *Lite* is the micro-programmed GigaCipher core, which allows for future upgrades and flexibility in supporting all cryptographic operations and protocol layer functions.

Figure 3 shows how multiple cores provide adaptive processing power that can be used for all cryptographic operations and protocol processing. This feature is unique to NITROX *Lite* and allows for flexible response to dynamic load. Dynamic Adaptive processing is enabled by the GigaCipher's ability to accelerate both the asymmetric algorithms used for tunnel establishment and the symmetric ciphers + hashing algorithms used in bulk data encryption. This adaptive nature of NITROX *Lite* allows vendors to build balanced systems that can handle dynamic traffic conditions.

Figure 3: Adaptive Security Processing

Adaptive security processing allows vendors to build balanced

NITROX *Lite* is the only processor that has the capability to process high-level IPsec and IKE protocol macro commands that reduce the host I/O traffic and dramatically offload the system processor to increase the total system throughput. The NITROX *Lite* SDK includes an evaluation board with modified KAME, Free S/WAN drivers using Cavium's TurboIPsec Macro APIs and software drivers for Linux, BSD and VxWorks.

Ordering Information

Part Number	System Interface	Package
CN501-183LQ128	PCI 32bit 66MHz	128 LQFP

Actual Size