

NITROX™ *Lite* Security Macro Processor

IPsec Family Product Brief

PRODUCT FEATURES & BENEFITS

World's first Security Macro Processor developed using custom CPU design techniques

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

High performance, industry standard interfaces

- PCI-X (64bit, 133MHz, Master and Slave modes)
- PCI (32bit, 66MHz, Master and Slave modes)
- PCI (64bit, 66MHz, Master and Slave modes)

High performance Bulk Data Encryption

50 Mbps to 1 Gbps IPsec Packet Processing (Bulk Data Encryption + Hashing)

High performance Public Key Processor

- 500 to 12K 180bit Diffie Hellman operations/second
- 1K to 7K 1024bit RSA operations/second
- Up to 2000 IKE Main Mode (DH + RSA sig)/ sec

Multi Algorithm Support

- RSA and Diffie-Hellman
- DES/3DES, AES, ARC4
- MD5, SHA-1, HMAC-MD5, HMAC-SHA-1

High number of concurrent IPsec SAs supported

- Supports unlimited IPsec SAs with host memory

On Chip True Random Number Generator

128 LQFP (32bit PCI only) or 256 BGA

Typical Power 1.0W

Industrial temp version available

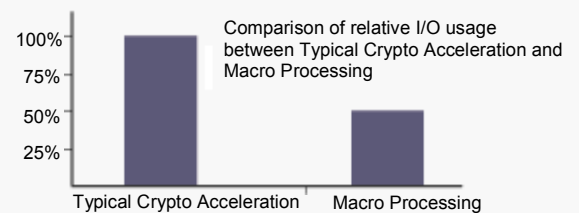
PROTOCOL & MANAGEMENT SUPPORT

Multi Protocol Support

- Macro support for IPsec and IKE

Full IPsec Protocol Processing with specialized TurboIPsec Macro API functions

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



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

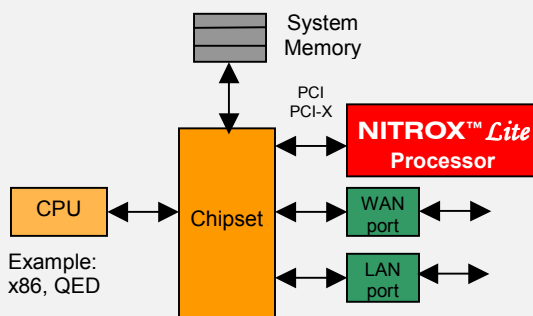
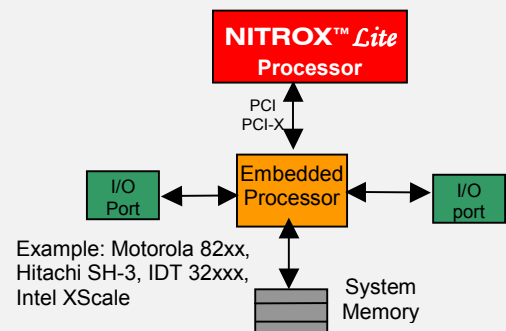


Figure 2: Example of NITROX *Lite* in embedded system using PCI bus interface



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)

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

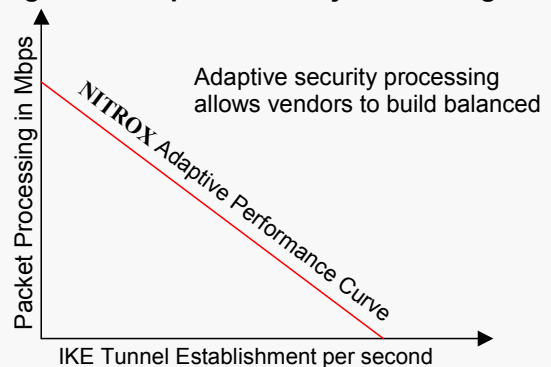
PRODUCT SUMMARY

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.

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.

Figure 3: Adaptive Security Processing



ORDERING INFORMATION

Part Number	Bus	Target Application Performance (packet processing)	Package
CN501-183LQ128	PCI 32bit, 33 or 66MHz	100Mbps 3DES+SHA1	128 LQFP
CN505-183LQ128	PCI 32bit, 33 or 66MHz	200Mbps 3DES+SHA1	128 LQFP
CN1001-350BG256	PCI 32 or 64bit 33 or 66MHz PCI-X 64 bit 133 MHz	200Mbps 3DES+SHA1	256 PBGA
CN1005-350BG256		400Mbps 3DES+SHA1	
CN1010-350BG256		1000Mbps 3DES+SHA1	

For PCI-X parts for CN1001, CN1005 and CN1010 add -X at the end