

NITROX™ 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

- Hyper Transport™ (8 bit, Full Differential, 500 MHz, DDR)
- PCI-X (64bit, 133MHz, Master and Slave modes)
- PCI (64bit, 66MHz, Master and Slave modes)

High performance Bulk Data Encryption

1 Gbps to 4 Gbps IPsec Packet Processing (Bulk Data Encryption + Hashing)

High performance Public Key Processor

- 24K to 72K 180bit Diffie Hellman operations/second
- 14K to 42K 1024bit RSA operations/second
- Up to 14000 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
- Support for local 64bit DDR DRAM (optional)

Up to 200 Mbps On Chip True Random Number Generator

On-Chip Personal Security Environment (PSE)

- Separate interface for trusted path

600 TSBGA with <10W; 256 PBGA with <6W

Industrial temp version available

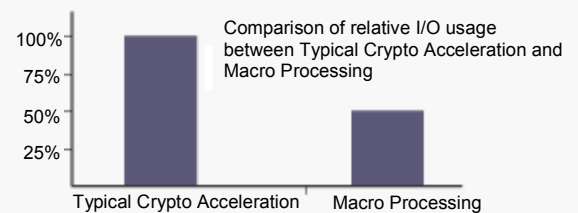
PROTOCOL & MANAGEMENT SUPPORT

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 bandwidth requirements of different cryptographic operations

- Truly balanced systems can be designed using NITROX'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 in Firewall or IPsec off-load application

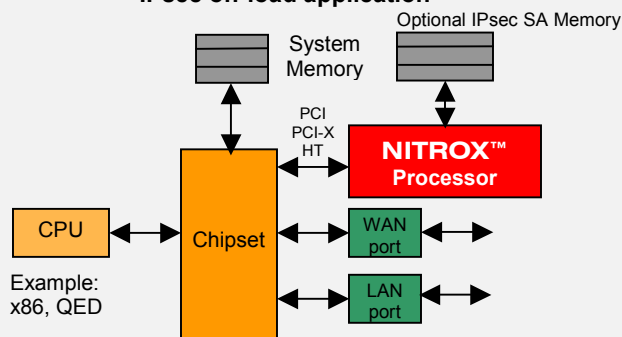
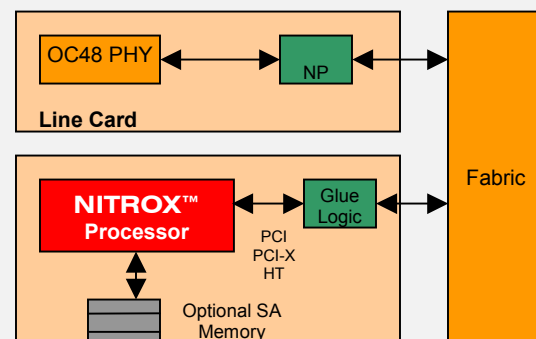


Figure 2: Example of NITROX™ in a Service Card Application



APPLICATIONS

Dedicated VPN Gateways

- Firewalls
- Remote Access Gateways

Network Access

- Switches
- Routers

Network Storage Devices

- Network Attached Storage Systems (NAS)
- Storage Area Networks (SAN)

BENEFITS TO DESIGNERS

Reduced system cost and complexity

- Single custom processor solution

Quick time to market with complete solution

- Evaluation board, processor, software & documentation
- Software driver and application

Flexible Protocol Processing with simple upgrade

- Flexible microcode allows for advanced protocol processing with field upgrade option

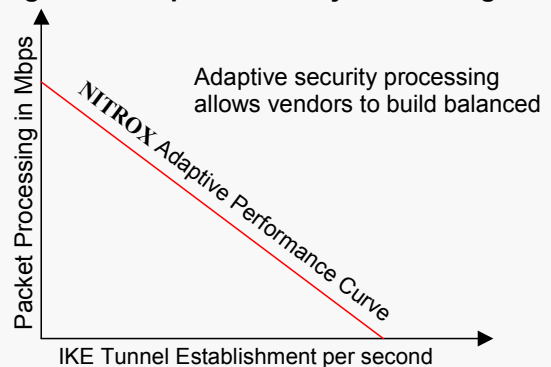
Designed for FIPS certification

PRODUCT SUMMARY

The NITROX Security Macro Processor is the industry's first custom processor exclusively targeted towards acceleration. The NITROX custom designed processor provides lowest area, cost and power consumption when compared to ASIC based security chips. The heart of NITROX 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 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 allows vendors to build balanced systems that can handle dynamic traffic conditions.

Figure 3: Adaptive Security Processing



NITROX 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 SDK includes an evaluation board with modified KAME and Free SWAN drivers using Cavium's TurboIPsec Macro APIs and software drivers for Linux, BSD and VxWorks.

ORDERING INFORMATION

Part Number	Bus	Local DDR (optional)	Target Application Performance	Package
CN1120-350BG256	PCI-X 64bit, 100MHz	No	1,000Mbps 3DES+SHA1	256 PBGA
CN1220-350BG600	PCI-X 64bit, 133MHz	Yes	1,200Mbps 3DES+SHA1	600 TSBGA
CN1230-350BG600		Yes	2,000Mbps 3DES+SHA1	
CN1320-350BG600	HyperTransport 200 MHz DDR	Yes	2,000Mbps 3DES+SHA1	
CN1330-350BG600		Yes	3,200Mbps 3DES+SHA1	
CN1340-350BG600		Yes	3,200Mbps 3DES+SHA1	