

NITROX™ Security Macro Processor SSL 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 complete SSL protocol

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 Public Key Processor

- 14K to 42K 1024bit RSA operations/second
- 24K to 72K 1024bit Diffie Hellman ops/sec
- Up to 34K full SSL or TLS Handshakes/sec (TPS)

High performance Bulk Data Encryption

- 1 Gbs to 4Gbps Record Processing (Bulk Data Encryption + Hashing)

Multi Algorithm Support

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

High number of concurrent SSL sessions supported

- Supports unlimited SSL sessions with host memory

Up to 200 Mbps On Chip True Random Number Generator

On-Chip Personal Security Environment (PSE)

- Separate interface for trusted path

On chip primality checking for RSA key generation

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

Industrial temp version available

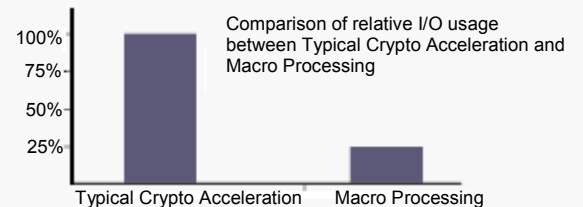
PROTOCOL & MANAGEMENT SUPPORT

Multi Protocol Support

- Macro support for SSL, TLS and WTLS

Full SSL Protocol Processing with specialized TurboSSL Macro API functions

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



Adapts to handle various bandwidth requirements of different cryptographic operations

- Truly balanced systems can be designed using NITROX that can adapt to various SSL handshakes/sec and SSL record processing loads based on website demand

Dedicated Resources for Administration & Management

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

Software drivers for popular operating systems such as Linux, BSD and Windows

Modified OpenSSL with Cavium's TurboSSL Macro API calls

Figure 1: Example of NITROX™ in an SSL offload application with optional context memory

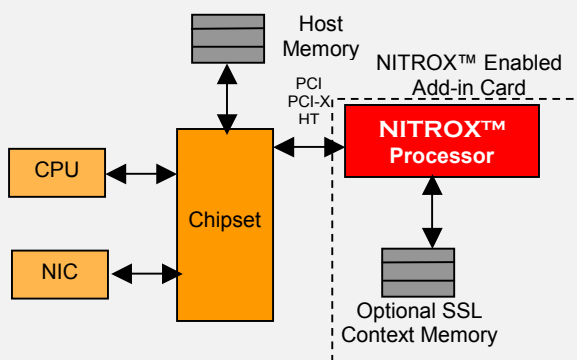
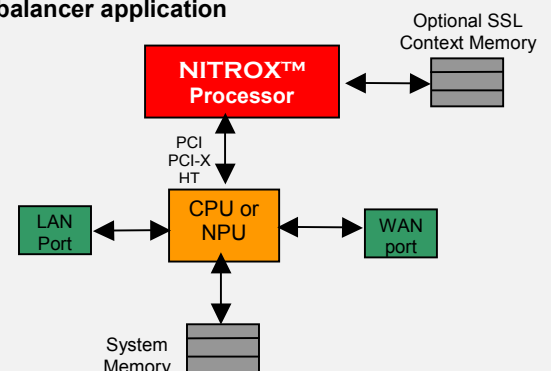


Figure 2: Example of NITROX in embedded load balancer application



APPLICATIONS

Servers

- SSL acceleration for Web Servers - Microsoft IIS and Linux Apache
- Signature verification for B2B exchanges

Web Switches and Appliances

- SSL/TLS Termination and Content Switching
- Content Aware Server Load Balancing
- SSL Proxy Server

Remote Access Servers using SSL

- Servers with SSL secure email and other web-enabled applications like CRM and ERP suites

Wireless WAP gateways

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 processing with field upgrade option

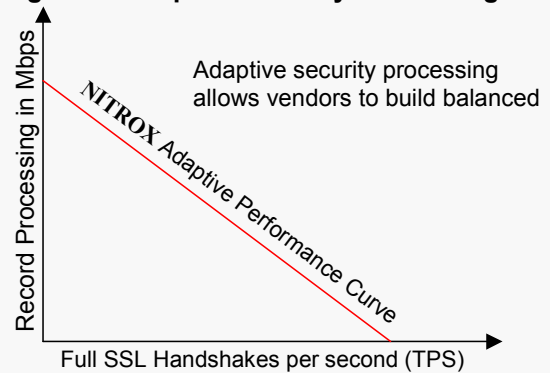
Designed for FIPS certification

PRODUCT SUMMARY

The NITROX Macro Security Processor is the industry's first processor exclusively targeted towards high performance SSL applications as opposed to plain cipher 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 the NITROX and allows for flexible response to dynamic load. For example, an e-commerce website requires a large ratio of SSL handshakes/sec Vs SSL record processing when compared to an online stock brokerage website that requires more SSL record processing vs SSL handshakes/sec. 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 SSL 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 OpenSSL using Cavium's TurboSSL Macro APIs and software drivers for popular operating systems such as Linux, BSD and Windows.

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	
		Yes	3,200Mbps 3DES+SHA1	