NITROX™ *Soho* CN220 & CN225 Secure Communication Processor Product Brief

PRODUCT FEATURES & BENEFITS

NITROX *Soho* CN220 & CN225 Overview

The NITROX *Soho* CN22x Secure Communication Processor (SCP) are the highest performing, value solution for Soho and Robo (remote office / branch office) IPSec and SSL VPN products. The NITROX *Soho* CN22x SCP incorporates the best elements of Cavium Networks' market leading security technology with a MIPS32 core and three Ethernet MACs. This combination provides the highest IPsec, SSL, Wireless security and tunnel set-up performance and the lowest system cost in the industry.

Market leading IPsec performance for all packet sizes
- Highest minimum size packet performance: >30 Mbps.
- Highest large packet performance: 170 Mbps.
- Multi-tunnel IPSec with no performance degradation

Highest SSL VPN performance for SoHo/SME
- High performance SSL VPN throughput of >25Mbps
- 900 1024bit-exponent RSA operations/second.

Highest performance Public Key Processor for target applications
- Hundreds of tunnels/second.
- 1550 ops/second at 180bit-exponent Diffie Hellman.
- Supports up to 2048-bit modulus size.

Provides IPv6 and IPv4 support (complete AH and ESP)

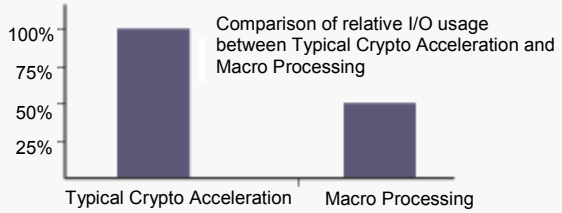
Multi Algorithm and Protocol Support
- RSA and Diffie-Hellman.
- 3DES, AES, ARC4.
- Modes: ECB, CBC; and 1, 8, 64-bit CFB (DES), 128-bit CFB (AES), CCMP.
- AES – supported key lengths: 128, 192, and 256-bit
- MD5, SHA-1, HMAC-MD5, HMAC-SHA-1.

Low System Power: <2.5W
Small package: 276 PBGA

PROTOCOL & MANAGEMENT SUPPORT

Multi Protocol Software Support
- SSL, IPsec and IKE. Wireless (802.11i) options.

Full IPsec Protocol Processing with specialized TurboIPsec and TurboSSL 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 *Soho* CN22x products' 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, and VxWorks

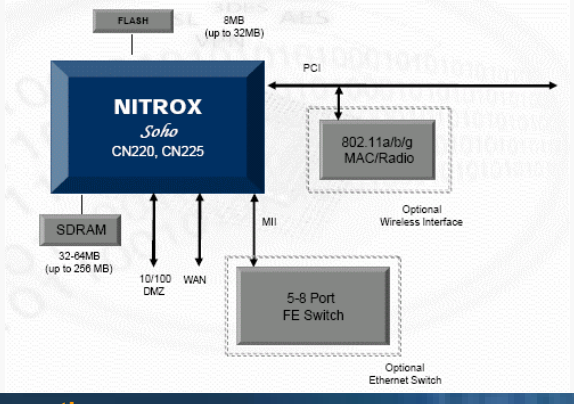
Modified IPsec, IKE and SSL software stack to incorporate Cavium Networks' macro calls
- FreeS/WAN, OpenSSL.

Processors and Interfaces

System Processors
- 166/200MHz MIPS32 4Km processor
  - 16KB I-Cache, 16KB D-Cache
- Cavium Networks' GigaCipher security processing core

Interfaces
- 3 independent MII/RMII 10/100 Ethernet MACs
  - Supports 802.1p VLAN tagging
- PCI v2.1 & 2.2 compatible (32-bit, 33MHz)
- Other: 2 x UART, SPI/MPI, Two-Wire

Figure 1: Example CN22x VPN Firewall Router



See over for more information

APPLICATIONS

SOHO and Small to Medium Enterprise
- SSL / IPSec VPN Gateways
- Remote Access Gateways, Residential Gateways
- Broadband Routers

Network Access
- DSL Modems, Cable Modems, FTTH
- 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 chip high performing solution with low power and small footprint

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

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

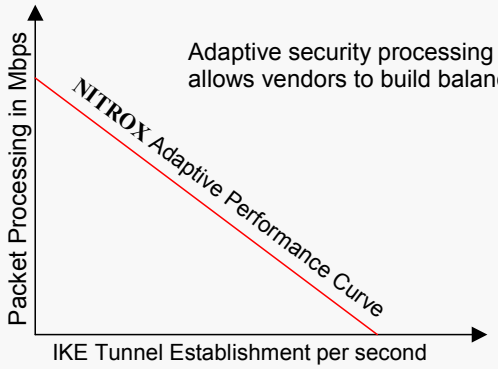
Highly Scaleable solution with NITROX *Soho* Family
- Common MIPS32 4Km Processor, API and Footprint

PRODUCT SUMMARY

The NITROX *Soho* CN22x Secure Communication Processors integrate Cavium Networks' widely deployed security technology with a MIPS32 CPU and several system peripherals. This combination results in a market leading product with high throughput multi-tunnel IPSec and SSL performance for Soho/SME VPN and IPsec Gateway solutions. Additionally, Cavium Networks complements this highly integrated solution with IPSec and SSL software solutions for fastest time to market for new products. The heart of NITROX *Soho* CN22x SCP are the MIPS32 CPU and the micro-programmed GigaCipher core, which allow for future upgrades and flexibility in supporting all cryptographic operations and protocol layer functions.

Figure 3 shows how the CN22x core provides adaptive processing power that can be used for all cryptographic operations and protocol processing. This feature is unique to NITROX family 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 *Soho* allows vendors to build balanced systems that can handle dynamic traffic conditions.

Figure 3: Adaptive Security Processing



NITROX *Soho* is the only processor to integrate a flexible MIPS32 4Km CPU, LAN interfaces and the innovative Cavium Networks GigaCipher security macro processor to enable systems designers to execute full Soho/SME SSL, IPsec and IKE protocol applications as an integrated security system in a single package. The NITROX *Soho* CDK includes an evaluation board with modified OpenSSL and Free S/WAN drivers using Cavium Networks' TurboIPsec and TurboSSL Macro APIs and software drivers for Linux, and VxWorks.

Ordering Information

Part Number	System Interfaces	Package	IPSec VPN performance	SSL VPN Performance	IKE Performance	Simultaneous Multi-Protocol (SSL & IPSEC)
CN225-200BG276	PCI 32bit 33MHz, 3 x RMII/MII	276 PBGA	170Mbps	>25Mbps	200tps	Yes
CN225-166BG276	PCI 32bit 33MHz, 3 x RMII/MII	276 PBGA	150Mbps	22Mbps	200tps	Yes
CN220-200BG276	PCI 32bit 33MHz, 3 x RMII/MII	276 PBGA	125Mbps	20Mbps	100tsp	No
CN220-166BG276	PCI 32bit 33MHz, 3 x RMII/MII	276 PBGA	100Mbps	15Mbps	100tsp	No

* All parts now available in lead-free packages

805 E. Middlefield Road, Mountain View, CA 94043, Phone: 650-623-7000, Email: sales@caviumnetworks.com, Web: http://www.caviumnetworks.com

CN220-CN225-PB-0.99 Printed in the USA