

Security Processors

NITROX[®] III Family of Security Processors

Product Brief



OVERVIEW

The NITROX III single chip, security processor family delivers the world's highest security and compression performance for application delivery, cloud computing and WAN optimization equipment. Its unmatched performance provides up to 300K SSL Ops/s, 40Gbps Security and 25 Gbps Compression along with virtualization and very low power consumption.

The NITROX III security processor family integrates 16 to 64 purpose-built security RISC cores with high performance compression engines and virtualization hardware and supports the PCI-Express Gen 2 interface. All NITROX III chips are fully software compatible with Cavium Networks' NITROX family of security processors.

Target applications for NITROX III Security Processors include enterprise, data center and service provider equipment such as Application Delivery Controllers, UTM Gateways, WAN Optimization Appliances, servers, routers and switches and are ideally suited to secure and virtualized cloud computing and the borderless enterprise environments.

FEATURES

High performance security processing for look-aside architecture

- Scalable from 5 Gbps – 40 Gbps Security Performance
- 35K -300K RSA Ops/s (1024bit keys)
- 6K – 52K RSA Ops/s (2048 bit keys)
- 16 – 64 security RISC engines with 16K instructions/engine

High-performance, industry standard compression

- 5 – 25 Gbps GZIP / LZS Compression

Virtualization

- Single Root – IO Virtualization (SR-IOV) support in hardware
- 8, 16, 32, 64 Virtual Functions

High-performance, industry standard interfaces

- PCI-Express Gen 2 x4, x8, x16 interfaces (up to 80 Gbps)

Wide variety of algorithms supported

- IPsec, SSL, TLS 1.2, DTLS, ECC Suite B
- DES, 3DES, ARC4, AES 256-bit (ECB, CBC, XCBC, CNTR, GCM)
- MD5, SHA-1, SHA-2, MAC-MD5/SHA-1/SHA-2, HMAC-MD5/SHA-1/SHA-2 (including SHA-224, SHA-256, SHA-384, SHA-512)
- RSA 2049, RSA 4096, Diffie-Hellman, KASUMI

Random Number Generator

- FIPS 140-3 compliant True RNG

Software compatibility

- Fully compatible with existing NITROX families

Power and Package

- 10 – 20 W power dissipation, all of the family is pin compatible
- No external memory required
- Package: 27 x 27 mm FCBGGA

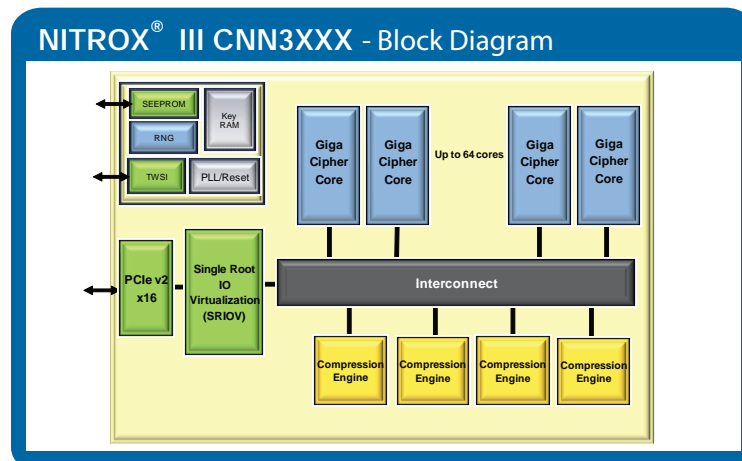
Scalability

- Top to Bottom HW & SW compatibility

BENEFITS

- Fifth Generation Security processor with proven feature set and quality software
- Delivers high throughput and broad scalability for next-generation wired and wireless - Enterprise, Data Center and Telco appliances
- Combines key functionality into a single, high-performance, low-power chip – Security, Compression, Virtualization, & Random Number Generator
- Provides flexible options for popular current and next-generation system interconnects
- Ideal for Virtual environments
- Enables easy migration, and protects customer investment in existing NITROX Security Processor based designs
- Meets security acceleration needs of several next-generation applications with latest security algorithm support

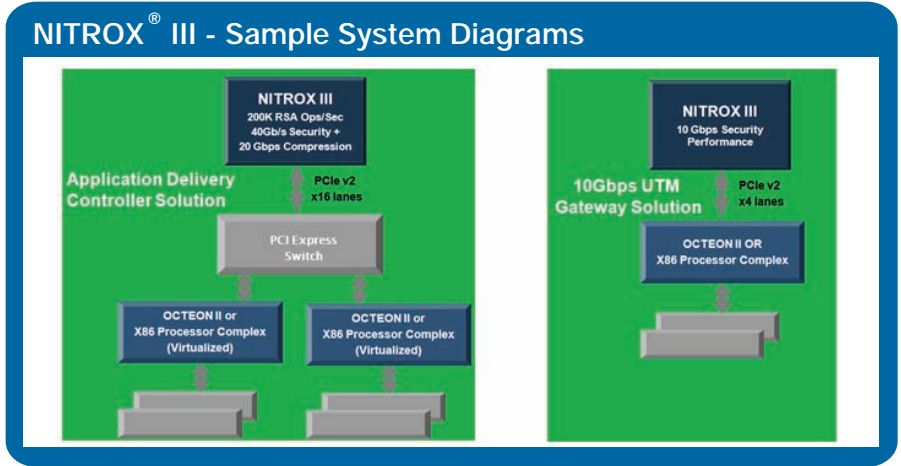
NITROX[®] III CNN3XXX - Block Diagram



Security Processors

NITROX[®] III Family of Security Processors

Product Brief



NITROX III Applications

Data Center

- Application Delivery Controllers (ADC)
- WAN Optimization
- Cloud Computing
- Storage Appliances

Server Offload

- Web, Mail, Search

Enterprise

- UTM Gateway
- Routers
- WAN Optimization
- VPN/Firewall
- Intrusion Prevention Appliances

NITROX III Software Support

Multi Protocol Support

- SSL, TLS, and IPsec

Full Protocol Processing with specialized Macro API functions

Adapts to handle various bandwidth requirements of different cryptographic operations

NITROX can adapt to various asymmetric (tunnel setup/handshake) and symmetric (encryption) processing loads based on application demand

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

NITROX[®] III CNN35XX - Product Family

Device	Data Interface	Local Memory for SA or Context	Performance				
			Max RSA 1024-bit Exponent	RSA 2048bit Exponent	Inline full IPsec Processing Throughput Mbps (w/AES +SHA2)	Full SSL Record Throughput Mbps	Compression
NITROX III PCI-Express CNN35XX - PCIe Look-aside Processor - Crypto, Compression & Virtualization							
CNN3510 -C5	PCI Express Gen 2 x4, x8, x16	No	35K	6K	5 Gbps	5 Gbps	5 Gbps
CNN3530 -C10		No	75K	13K	10 Gbps	10 Gbps	10 Gbps
CNN3550 -C20		No	150K	26K	20 Gbps	20 Gbps	20 Gbps
CNN3550-C20 (Boost)		No	200K	35K	28 Gbps	28 Gbps	20 Gbps
CNN3560-C20		No	230K	41K	32Gbps	32Gbps	25 Gbps
CNN3560 -C20 (Boost)		No	300K	52K	35 Gbps	35 Gbps	25 Gbps