Nitrox™ XL FIPS 140-2 Level 3 Compliant Acceleration Board

Product Brief

Features & Benefits

SSL/TLS Performance
- 10,000 1024-bit RSA operations/sec
- 500 Mbps SSL record processing
- 8,000 full SSL Transactions/sec (with 1024 bit RSA handshake plus 1KB record transfer)

Macro-processing for optimal system efficiency
- Complete SSL handshake processing in a single API call
- Complete SSL record processing in a single API call

API's backward compatible with existing, non-FIPS, Nitrox XL SSL/TLS accelerator cards

Multiple algorithms supported
- RSA up to 2048 bits w/out CRT (4096 w/CRT)
- ARC4*, DES, 3DES, AES
- MD5*, SHA1

*Only accelerated in a non-FIPS mode

On-board storage for up to 100,000 (est.) concurrent SSL sessions & 4096 (est.) concurrent server private keys
Maintained and managed on-board by local subsystem

Industry-standard system interface
Universal 3V/5V, 32/64 bit, 33/66 MHz PCI plug-in card

Separate "Trusted-Path" Administration Interface
Serial interface for connection to PIN Entry Device (PED) for FIPS Level 3 configurations

Physical and Logical Cryptographic Boundaries
Secure, tamper-proof enclosure provides a barrier. All components are encompassed within the Cryptographic boundary. Keys cleared if enclosure is breached.

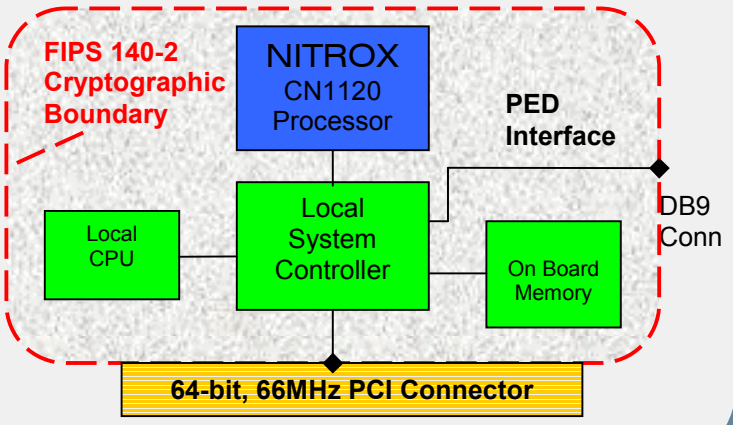
Configurable security modes
Operates in FIPS 140-2 modes, either level 2 or level 3. Mode is set by Security Officer during initialization.

Authenticated Operator Roles
User - normal operational role on the module
Security Officer - configures module for operation and performs security administration tasks such as User creation

Unauthenticated Operator Role
Public User - for access to status information and diagnostics before authentication

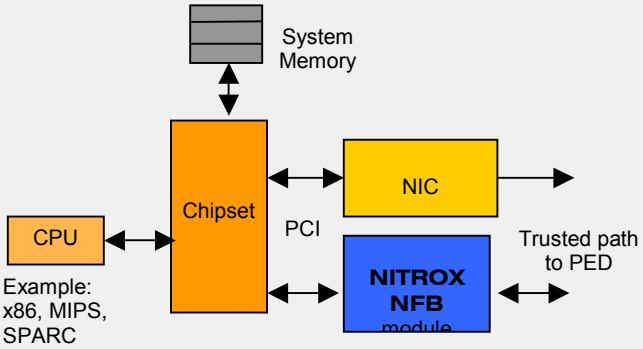
IPsec Acceleration
All algorithms required for IPsec also accelerated in a FIPS compliant fashion.

Module Architecture



Simplified CN1120-NFB Block Diagram

System Concept



Example of NITROX NFB in SSL offload applications

APPLICATIONS

Servers

- Web-Servers used in e-Commerce
- 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

BENEFITS TO DESIGNERS

Short development time for quick time to market

- Complete hardware module
- Same API as non-FIPS SSL API from Cavium Networks
- Complete C Software Kit including source code
  - Driver & Utilities
  - Reference Application

Reduced system complexity

- Entire SSL security implementation on single module

PRODUCT SUMMARY

Cavium Network's **Nitrox FIPS 140-2 Compliant Acceleration Board** brings together the high performance hardware acceleration of Cavium's Nitrox security macro-processors, and the trusted strength and security of the FIPS 140-2 standard.

The Federal Information Processing Standard (FIPS) has become a fundamental component of best practices for the rating of cryptographic accelerators. These security requirements are used to validate the performance of cryptographic modules, so that the trust model can be confidently deployed based on established security standards. It is these standards that have been leveraged in order to create an acceleration module for vendors of highest-security SSL e-Commerce, e-Business, and SSL and IPsec VPN equipment.

The Nitrox XL Accelerator Board is a comprehensive security subsystem, combining high performance hardware-cryptographic acceleration with a complete high-security hardware and software system. The resulting module creates a tight FIPS140-2 level 3 cryptographic boundary around the modules card-edge.

The module comes complete with a rich, full-featured set of software drivers, utilities, and reference application software, all delivered in C source code.

The hardware module with a FIPS compliant security boundary, ensures the integrity of the cryptographic material. Together with a complete software development kit, it significantly reduces the cost, complexity, and time to develop products targeted at high-value, high-security e-commerce and e-business applications.

ORDERING INFORMATION

Part Number	System Interface	Separate Trusted-Path Interface	Performance	Package
CN1120-350-NFB	64 bit, 66 MHz PCI	Serial Pin Entry Device (PED) interface	10,000 1024 bit RSA Ops/sec 8,000 SSL Transactions per second, with 1KB record 500 Mbps sustained throughput	full-length PCI Card
CN1010-350-NFB	64 bit, 66 MHz PCI	Serial Pin Entry Device (PED) interface	6,000 1024 bit RSA Ops/sec 250 Mbps sustained throughput	full-length PCI Card
CN1005-350-NFB	64 bit, 66 MHz PCI	Serial Pin Entry Device (PED) interface	3,000 1024 bit RSA Ops/sec 125 Mbps sustained throughput	full-length PCI Card

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

CN1120-NFB-PB-005 Printed in the USA