NITROX™ II

A Family of In-line Security Processors

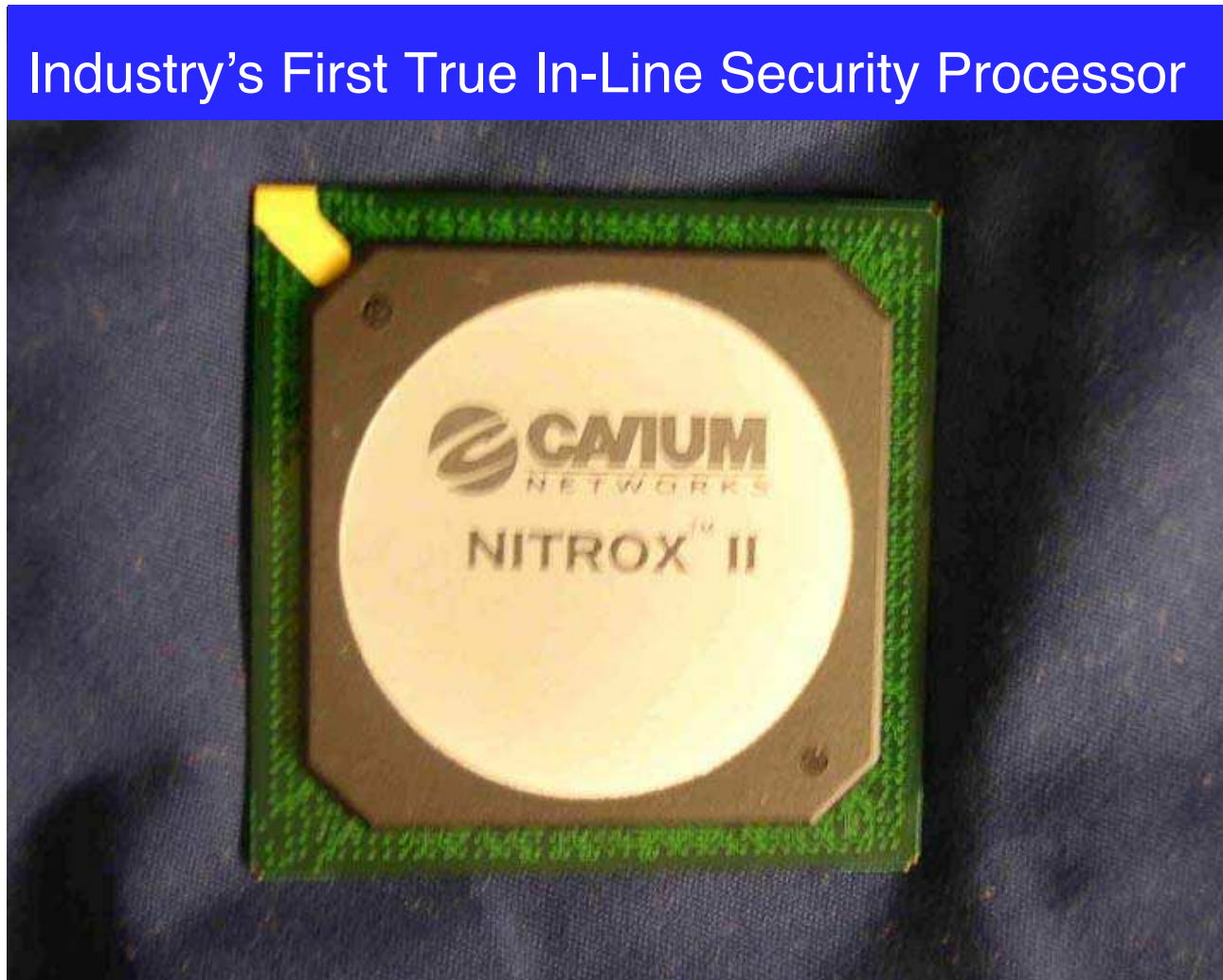Presented by:
Muhammad Raghib Hussain

Contributed by:
Bob Sanzone, Dan Katz, David Asher,
David Carlson, Gregg Bouchard,
Michael Bertone, Muhammad Hussain,
Richard Kessler, Tom Hummel

Hot Chips 15
August 2003

securing networks with silicon

Introducing NITROX™ II

Industry's First True In-Line Security Processor

NITROX™ II"True bump-in-the-wire" Inline Architecture

- Can sit next to the framer/mac in IPsec applications acting as an intelligent wire
  - Eliminates the need of NPU or any extra logic to perform lookup and L2 processing for ingress IPsec packets.
  - Intelligent packet classification into pass-through, process-then-pass, exception and DOS categories.
- Highly scalable architecture with a mix of pipeline and parallel processing techniques

NITROX™ II I/O Interfaces

PCI/PCIX

SPI-3

OR

SPI-4

SPI-3

OR

SPI-4

TWSI

DDR SDRAM/
FCRAM
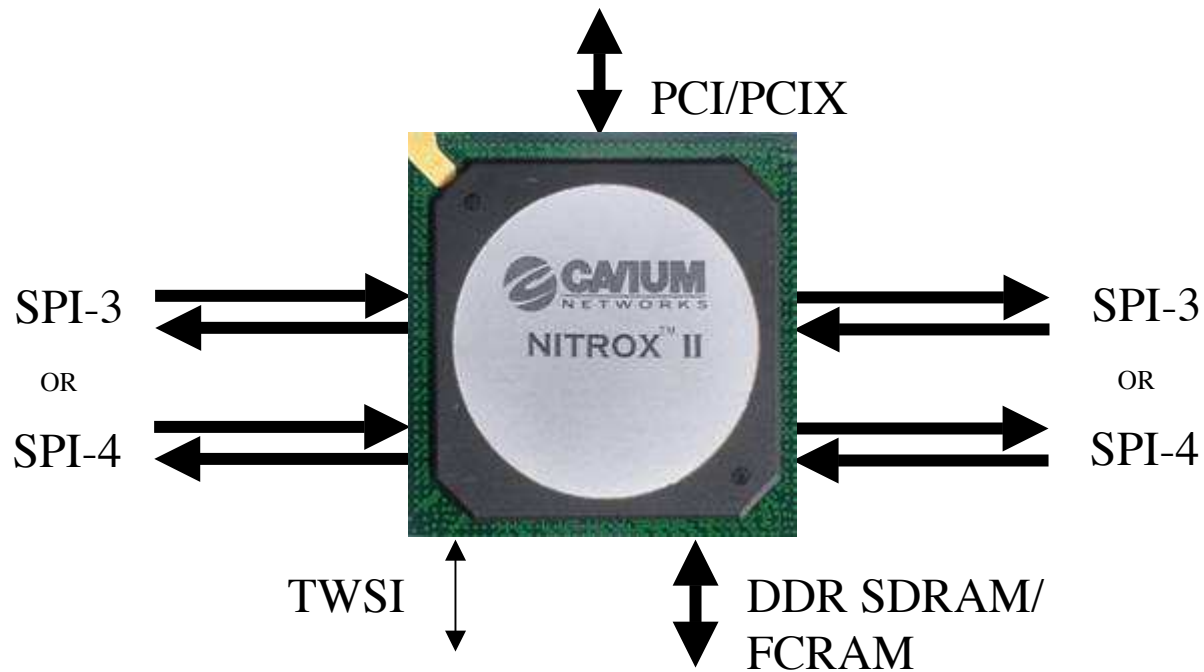
NITROX™ II Block Diagram
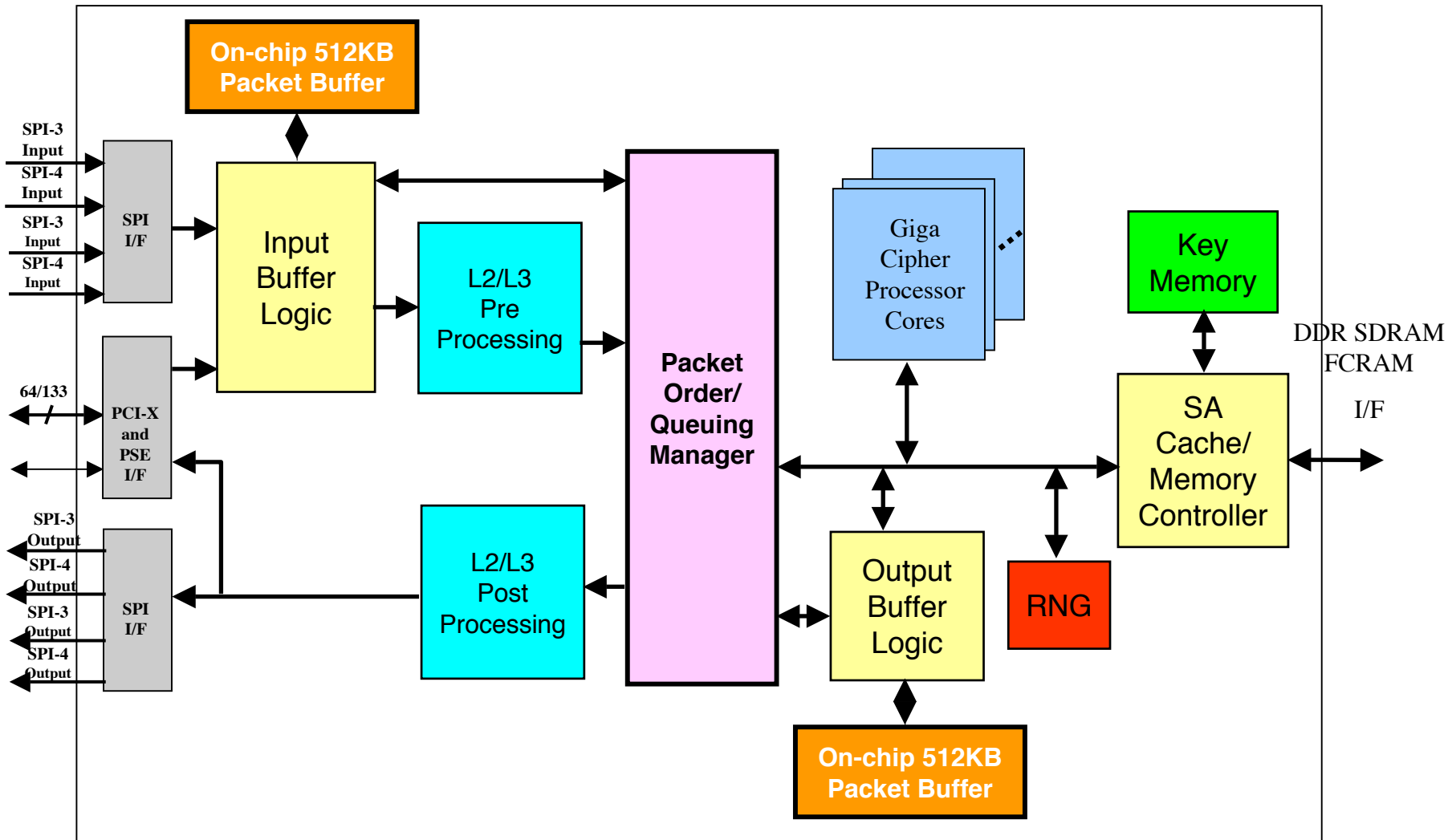
Inline IPsec Features in NITROX II

- L2 header/trailer processing
- IP header checks and processing
- Wire Speed Packet Buffering
- Inbound destination check and SA look-up
- Inbound IPsec selector checks
- Complete IPsec Packet Processing
  - IPSEC Transforms (AH, ESP, Tunnel, Transport)
    - 3DES, AES (all key sizes), HMAC SHA-1/MD5
  - UDP encapsulated IPSEC
- IKE packet detection and processing offload
- ICMP PMTU packet handling
- Robust Statistics for audit, billing and provisioning
- SA Mirroring for High-Availability
- IPsec exception processing and error handling

Inline SSL Features in NITROX II

- SSL 3.0 / TLS record transformations and exception processing
- Inline handshake record processing
- On-chip key material generation and context management
- Inline alert detection
- Session Resumption without CPU intervention
- TCP acceleration support
- Security Context Mirroring for High-Availability

NITROX™ II Raw Performance

- DES/3DES   48 Gbps
- AES   48 Gbps
- ARC4   20 Gbps
- SHA-1   60 Gbps
- MD5   38 Gbps
- 1024-bit private-key RSA   60K per sec.
- 1024-bit public-key RSA   300K per sec.
- True Random Numbers   320 Mbps

NITROX™ II System Performance

- Greater than 10Gbps of complete IPSEC packet processing (3DES/SHA-1, ESP/Tunnel)
  - ~20Gbps for large packets
- 10K IKE sessions per sec.
- 40 K per sec. Full SSL Handshake
- Line rate 49B pass-through packet support at 10Gbps
- SSL (ARC4/MD5) record processing at 10Gbps for average size (512B) records

NITROX™ II High Level Specs

- Core Frequency — 400MHz
- Core Voltage — 1.0V (Nominal)
- Technology — 0.13 CMOS
- Metal layers — 8
- Package — 1096 TSBGA
- Transistors — over 100 million
- Power — 6W to 15W
- Status — Sampling now, production Q303

NITROX™ II I/O Details

- 36G full duplex of flexible data I/Os
  - Dual SPI-3 up to 133Mhz clock
  - Dual SPI-4 up to 500Mhz DDR (1G data words/sec)
  - 64-bit PCI/PCI-X up to 133MHz
- High bandwidth Memory Interface
  - 72-bit DDR SDRAM (w/ ECC) 200Mhz DDR
  - 72-bit FCRAM (w/ ECC) 200Mhz DDR
- Highly configurable I/Os
  - SPI interfaces supports both Link and PHY mode
  - SPI-4.2 interface supports dynamic de-skewing
  - 32 virtual ports on SPI interfaces
  - 3 virtual ports on PCI interface
- Any port to any port flow through architecture
  - Bridging function between SPI-3, SPI-4 and PCI I/Os.

NITROX™ II
GigaCipher Processor Core (GPC)

- Stand Alone Custom Processor RISC core with SIS (Security Instruction Set) extension
  - Accelerates various ciphers, mod exp and CRC calculation
  - Micro code engine coordinates operations and implements actual algorithms
  - Flexible to adapt emerging standards and protocols
  - Local Micro code and scratch buffer memory increases efficiency
  - Micro code overlay support
  - Efficient Power Management
  - Any algorithm using the same primitive cipher permutation can be implemented
    - Data Integrity and Privacy: HMAC (SHA-1, MD5 etc.), 3DES(ECB, CBC), AES (CBC, XCBC, Counter)
    - Authentication: Public-key cryptography (RSA/DH)
    - Key management (e.g RSA key generation, key backup etc.)
  - Protocol processing (e.g. IKE, IPsec, SSL, WEP, TKIP, SRTP etc.)
  - Programmable CRC
- Direct Access to on-chip resources (e.g key memory, random number)

NITROX™ II L2/L3 Processing

- Fully Configurable L2 Support
  - Ethernet (w/ VLAN), MPLS, PPPoE, PPPoA, PPPoS, PPPoEoA …..
- L2 CRC Check and Generation
  - Three inline polynomials (CRC32, CRC16, CRC16/CCITT) configurable per-interface
  - Flexible CRC support present in GPC
- Custom Link Layer Header Support
  - Skip N byte (programmable)
- IPv4 and IPv6 Packet Processing
- IP header checksum and error checks

NITROX™ II Memory Management

- **Packet Buffer Management**
  - On-chip 1MB packet buffer with complete hardware management.
  - Fully ECC protected memory with repair
  - Highly optimized linked list architecture
  - Extensive configurable flow control
    - Per input port/interface buffer thresholds
    - Per output port/interface buffer thresholds
- **SA/Context Management**
  - On-chip SA/Context cache
  - Hardware locks for SA/Context sharing

NITROX™ II Packet Synchronization

- **Hardware based semaphores and synchronizing logic**

- **Tag based Synchronization**
  - Flexible software controlled tags
  - Packet processing serialization based on tags
  - Excellent fit for SSL and similar applications

- **Hardware based Atomic Order**
  - Tag is assigned by the hardware
  - Dynamic synchronization under GPC control
  - Supports lock/release, Fetch and Add etc.
  - Great fit for IPSEC

NITROX™ II Robust Statistics

- Global Counters
  - 32 64-bit counters accessible by GPC
  - Fetch and Add operation
  - Primarily implemented for global statistics
- Per session (SA) counters
  - Management of per session statistics counters with hardware synchronization
 - Excellent for billing and provisioning

NITROX™ II
QOS and Multi-service Support

- ● **Quality-of-service support**
  - – Per virtual port queues
  - – Per virtual port back pressure mechanisms.
  - – Thresholds for denial-of-service type of traffic.

- ● **Multi-service and multi-protocol support**
  - – GPCs can be grouped into 8 different groups
  - – Each group can process a unique protocol

- ● **Guaranteed bandwidth support**
  - – Guaranteed bandwidth can be achieved with the help of per port queues and groups
  - – Queues/groups can be dynamically allocated for bandwidth provisioning
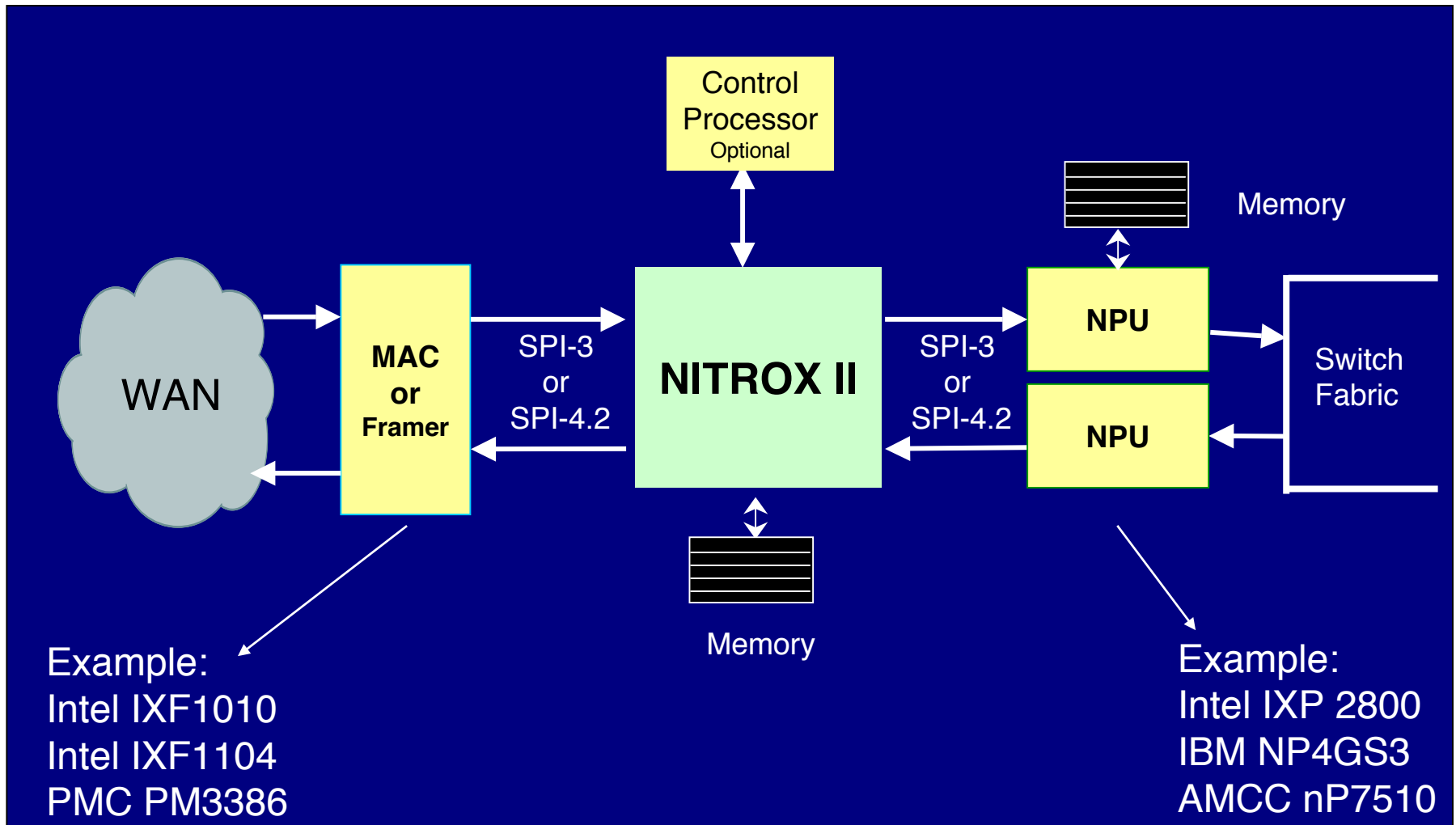
NITROX™ II Trusted Path Support
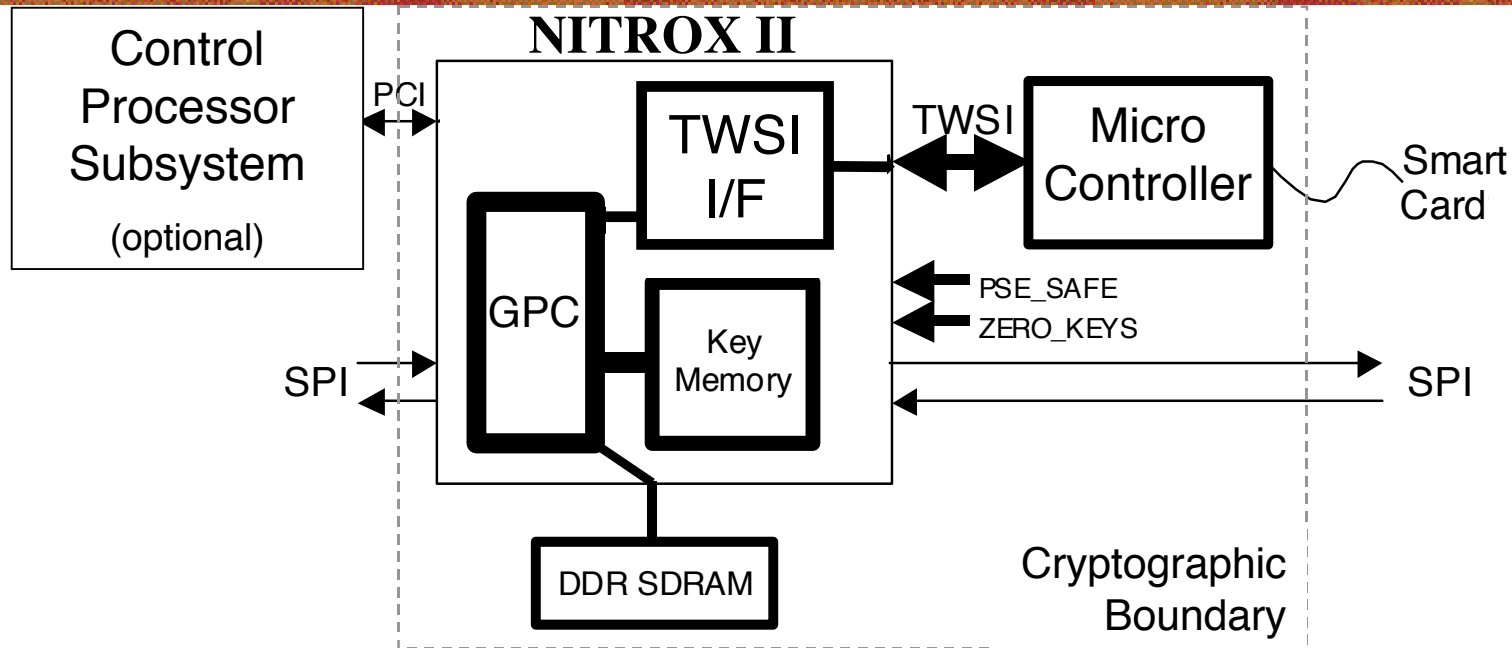
- Trusted hardware interface and tamper-proof key zeroization
- Full support for FIPS 140-2 system design
- Support for key backup, key restore and key pair generation
- Easy power-on device authentication and key management
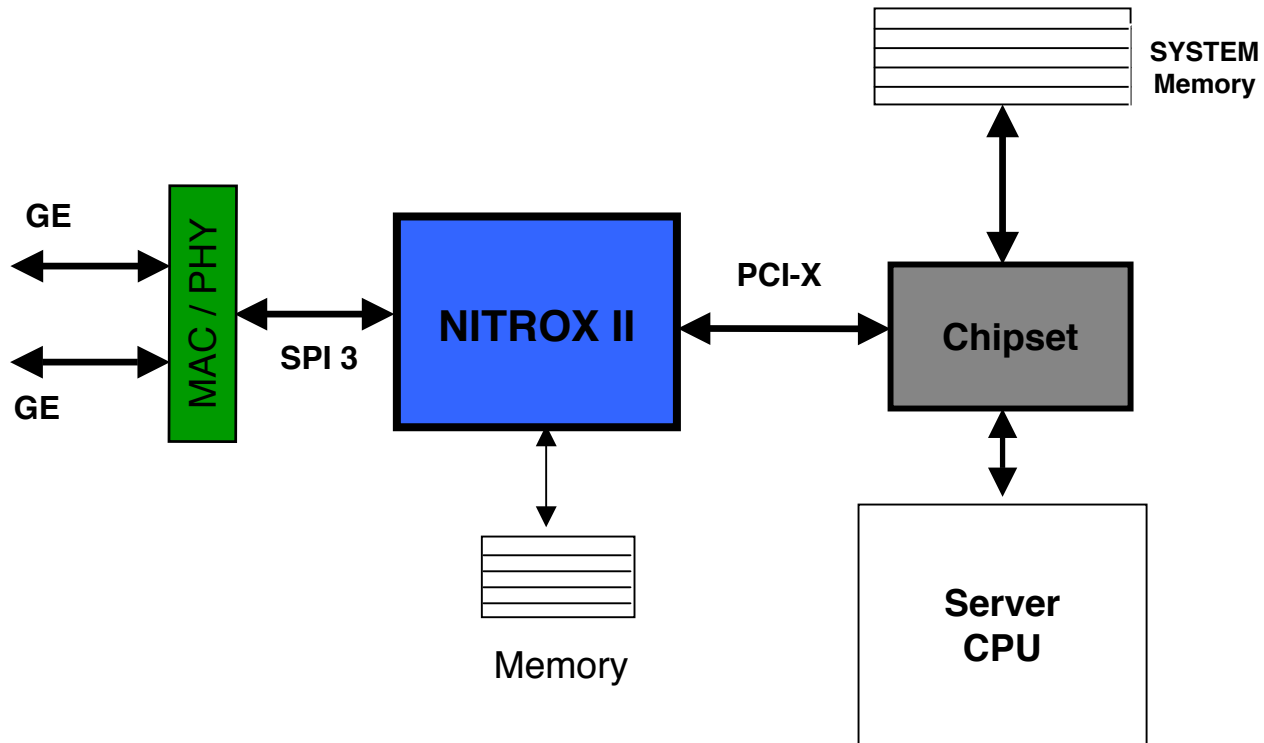
NITROX™ II Low Power Design

- Low Vdd
  - 1.0 Volts (Nominal)
- Extensive Power Management
  - Conditionally clocked architecture
  - Functional Block Clocks turned off when not in use
- Fully Static Design
- Full custom design yields better smaller circuits saving power.
- Full custom layout reduces spaghetti routing also saving power.
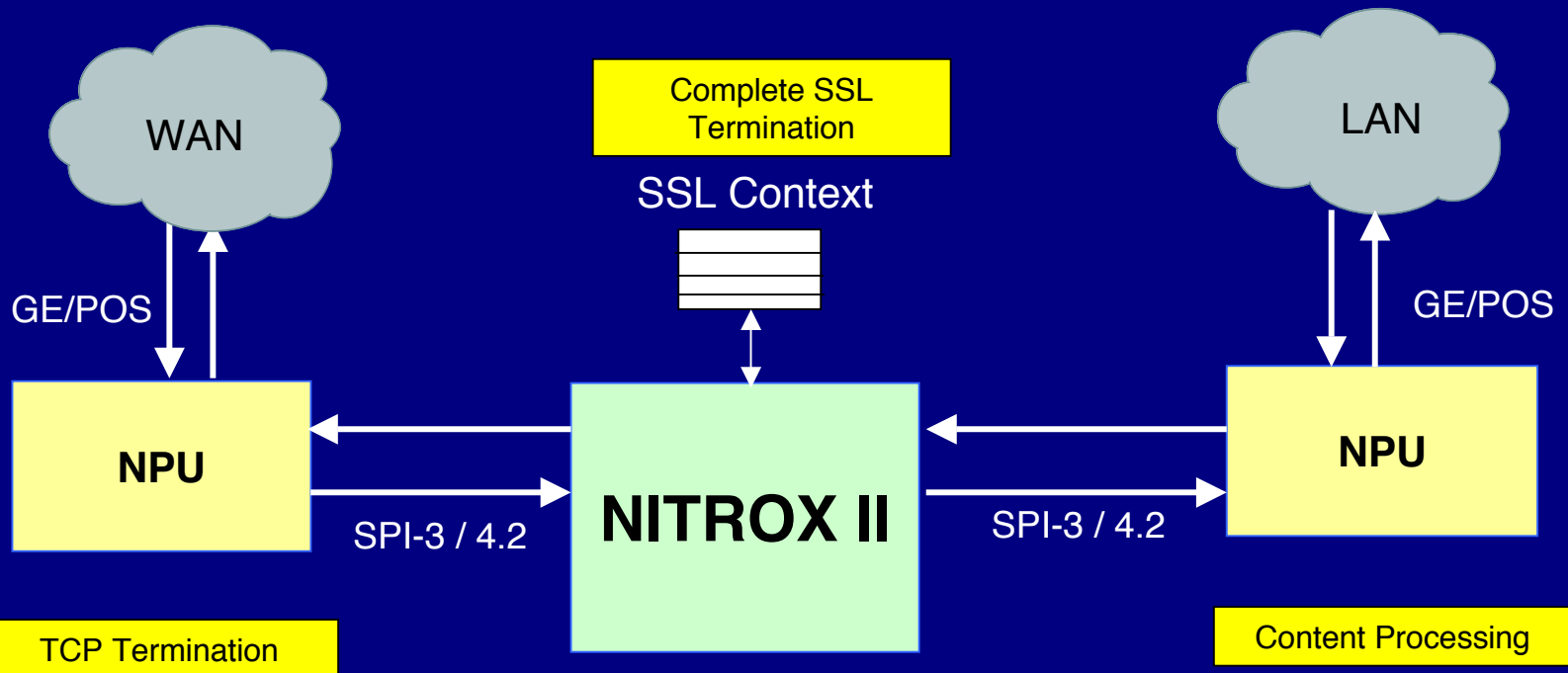
Inline IPsec Solution using NITROX™ II

Control Processor Optional

WAN

MAC or Framer

SPI-3 or SPI-4.2

NITROX II

SPI-3 or SPI-4.2

NPU

NPU

Switch Fabric

Memory

Memory

Example:
Intel IXF1010
Intel IXF1104
PMC PM3386

Example:
Intel IXP 2800
IBM NP4GS3
AMCC nP7510

2xGE Server Secure IPsec NIC

Cavium's Flow Through SSL Solution

High End SSL Based Secure Content Processing

WAN

Complete SSL Termination

SSL Context

LAN

GE/POS

GE/POS

NPU

NITROX II

NPU

SPI-3 / 4.2

SPI-3 / 4.2

TCP Termination

Content Processing

Cavium Summary
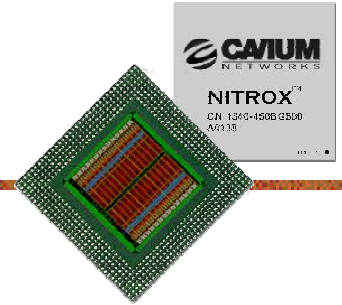
✓ **Industry's Largest family of security processors**

    Family for Low (50Mbps) to High (over 10Gbps) Performance security

    True Inline high performance security processor

✓ **Aggressive Roadmap to extend lead ahead of competitors**

    Reducing cost, driving features, horizontal integration, and performance

✓ **Flexible Solution to support emerging standards for Security centric applications**

✓ **Well Positioned to take lead in security processing market by 2004**

Thank You

securing networks with silicon