**PRODUCT FEATURES & BENEFITS**

**In-line, Bump-in-the-Wire architecture**
- Inline processing, no CPU intervention required
- Programmable L2/L3 Parsing identifies traffic flows for specific processing paths
- Separate control/exception path to system controller
- Configurable look-aside operation option

**Tremendous interface flexibility**
- Single or Dual SPI3, Single or Dual SPI4, and SPI3/4 combo options
- All parts include PCI/PCI-X for control/data, and DDR SDRAM for session context storage

**High performance bulk data encryption**
- 1 to 10Gbps IPSec packet processing
- 1 to 20Gbps SSL record processing

**High performance Public Key operations**
- 10K to 40K 1024bit RSA's/sec
- 18K to 60K DH/sec (180-bit modulus)

**Multi-algorithm support**
- DES/3DES, AES (128, 192, 256), ARC4
- MD5/HMAC-MD5, SHA1/HMAC-SHA1
- DH(groups 1,2,5), RSA (to 4096 bits)

**On-chip true random number generator**
- Up to 320Mbps of verified-random data

**1096 BGA Package**

Typical Power - 6 W to 15 W

Available in Industrial temp version

---

**PROTOCOL & STATISTICS SUPPORT**

**Multiple protocols supported**
- IPSEC/IKE
- SSL/TLS
- Multiprotocol (CN2xxx p-version )
  - Both IPsec and SSL

**Support for high number of simultaneous sessions**
- 2M IPSec SAs with 512MB DRAM
- 4M SSL contexts with 4GB DRAM

**Rich statistics gathering capability**
- Per-packet, per-port, and/or per-tunnel statistics maintained on-chip
- Fully programmable/configurable

**Automatically adapts to changes in symmetric and asymmetric load conditions**
- Heavy tunnel establishment or heavy bulk data traffic processing loads

**Secure, trusted-path interface for smart cards or PED’s allows for FIPS 140-2 designs to level 4**

**Driver/API source for popular OSs, including Linux, VxWorks, Windows, and BSD**

**Modified IPsec and IKE software stack to incorporate Cavium’s TurboIPsec macro calls**

**Evaluation boards and HW design guidelines available**

---

**Figure 1 – Streaming Inline Architecture Example**

**Figure 2 – Inline “Smart-NIC” Architecture Example**
Cavium Network’s NITROX II Security Macro-Processors are the industry’s first family of Inline, Bump-in-the-Wire security protocol processors specifically designed to implement high-performance security protocol and algorithm processing for VPN, E-commerce, and storage applications. NITROX II processors support a wide variety of security protocols, including IPSec/IKE, SSL/TLS, and iSCSI.

NITROX II processors are available in five different interface options, based on different combinations of SPI3, SPI4, and PCI/PCI-X interfaces. Depending on system requirements and interfaces, NITROX II can be configured for any combination of SPI-to-SPI or SPI-to-PCI/PCI-X inline configurations, or in SPI or PCI/PCI-X look-aside configurations.

Different products within each device family offer a range of performance, with product offerings from 1 to 20Gbps of protocol-processing throughput. This tremendous breadth of interface, protocol, and performance options offers system architects a vast choice of configurations to match any application and system architecture.

The heart of all NITROX II processors are its micro-programmed GigaCipher cores, providing optimal flexibility in cryptographic and protocol layer functions, while allowing for future upgrades without costly hardware changes. Cores can also be allocated to specific groups, allowing optimization of data paths for high-priority traffic in designs requiring QoS. Using the NITROX II’s Plus feature, which combines Micro-programming with multi-core technology, allows all family members to optionally and simultaneously support multiple independent security and networking protocols in a single device.

Typical NITROX II applications include VPN gateway appliances, VPN-offload blades for routers & switches, secure NICs for IPSec or SSL-enabled servers, server load-balancers, or secure storage appliances.

### PRODUCT FAMILY OVERVIEW

<table>
<thead>
<tr>
<th>Part Number</th>
<th>Data Interface</th>
<th>Control Interface or alternate data path</th>
<th>Local DDR for IPSec SA or SSL Context (packet store on-chip)</th>
<th>Performance</th>
<th>Package</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>PCI-X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CN2120-350BG1096</td>
<td>1 x SPI3</td>
<td>yes</td>
<td>Max RSA 1024-bit Exponent</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Max DH 180-bit Exponent with 1024bit Mod(2)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Inline full IPsec Processing (includes inbound look-up, local SA storage, L2 handling etc.)(3)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Full SSL Record Throughput (w/ARC4 + MD5) (3)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CN2130-350BG1096(1)</td>
<td>1 x SPI3</td>
<td>yes</td>
<td>7K 12K 2Gbps 2Gbps</td>
<td></td>
<td>1096 BGA</td>
</tr>
<tr>
<td>CN2230-350BG1096</td>
<td>2 x SPI3</td>
<td></td>
<td>10K 18K 3Gbps 3Gbps</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CN2240-350BG1096(1)</td>
<td>1 x SPI3</td>
<td>yes</td>
<td>10K 18K 3Gbps 3Gbps</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CN2330-350BG1096</td>
<td>1 x SPI3 and SPI4.2</td>
<td></td>
<td>20K 36K 6Gbps 6Gbps</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CN2340-350BG1096(1)</td>
<td>1 x SPI4.2</td>
<td>yes</td>
<td>10K 18K 3Gbps 3Gbps</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CN2450-350BG1096(1)</td>
<td>1 x SPI4.2</td>
<td></td>
<td>20K 36K 6Gbps 6Gbps</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CN2530-400BG1096</td>
<td>2 x SPI4.2</td>
<td>yes</td>
<td>30K 50K 10Gbps 10Gbps</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CN2560-400BG1096(1)</td>
<td>2 x SPI4.2</td>
<td>yes</td>
<td>10K 18K 3Gbps 3Gbps</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>40K 60K 10Gbps 10Gbps</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(1) Bus limited
(2) For DH performance with 1024bit Exp, divide given numbers by 5
(3) Benchmarked on 256Byte Packets