



NEXT-GENERATION CRYPTONETX™ IPSEC/SSL SECURITY PROTOCOL PROCESSOR PRODUCT LINE

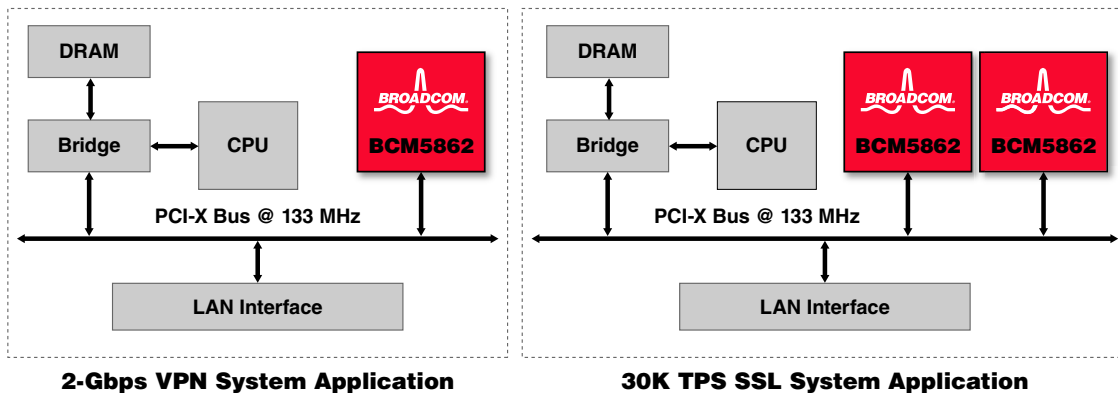
FEATURES

- **High-performance VPN and SSL security processor**
- **Up to 2 Gbps IPsec packet protocol processing**
 - IPv4 and IPv6 header encapsulation/decapsulation
 - AH, ESP, transport and tunnel modes supported
 - 5-tuple-based inbound security policy verification
- **Two Gbps SSL/TLS record layer processing**
 - Record encapsulation and decapsulation
 - Session key derivation
 - SSL/TLS finished message computation
- **High-performance public key processor**
 - 15,224,1024-bit RSA transactions per second
 - 15,224 Diffie-Hellman transactions per second
 - Support for IKE and SSL/TLS modes
- **BroadSAFE™ enabled**
 - OTP to protect private keys
 - Secure assurance logic
- **Software-compatible with the entire CryptoNetX™ security processor family**
- **Cryptographic functions**
 - 3DES/DES, AES, HMAC-SHA-1
- **True hardware random number generator**
- **Optimized PCI-X® or PCI Express® interface**
- **0.13-mm CMOS technology**
- **Low power consumption: <5W**
- **400-pin PBGA package**

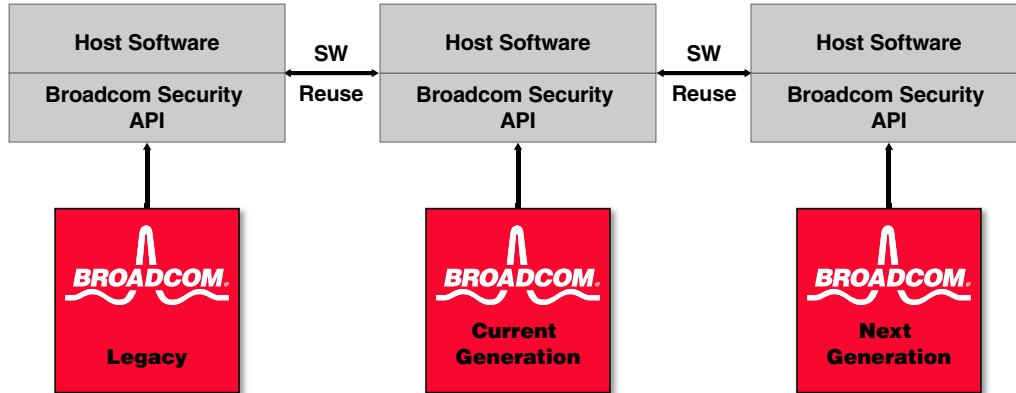
SUMMARY OF BENEFITS

- **High-performance security processor enables both secure web and high-performance VPN applications**
 - Web servers
 - VPN-enabled routers
 - Layer 4+ switches
 - VPN appliances
 - Web appliances with integrated SSL
 - Access devices
 - Firewalls
- **Extensive embedded software development kit**
 - Linux®, VxWorks®, BSD® support
 - Software reference library
 - Full OpenSSL integration
 - Complete reference design
- **Easy upgrade from BCM5821, BCM5823, and BCM5825**
- **Compatible with other Broadcom devices, enabling optimal system-level form factor, costs, and power dissipation**
- **Software compatibility across entire family protects customers software investment and enables fast time-to-market of next-generation solutions.**
- **BroadSAFE benefits**
 - Keys and identity stored in on-chip memory
 - Provides a secure key management
 - Strong device authentication
 - Secure key distribution coupled with strong hardware encryption (AES) ensures true link privacy
 - Secure software distribution for safe in-field upgrades and patches of software

BCM586X Application Block Diagram



OVERVIEW



BCM586X Compatibility

The BCM586X protocol processors are capable of providing up to 2 Gbps of IPsec protocol processing as well securing 15,224 RSA transactions per second. Ideal for high- and mid-end virtual private networking (VPN), firewall appliances, and SSL-based appliances, this new low-power security protocol processing family provides software compatibility with Broadcom's popular CryptoNetX™ security processor chip family.

For VPN applications, this BCM586X product line offers protocol processing and acceleration for symmetric key functions at significantly increased performance rates. The BCM586X products support bulk AES encryption and authentication up to 2 Gbps, bulk SSL encryption and authentication (ARC4, SSL-MAC-MD5/SHA-1) up to 2 Gbps, and Ipsec (3DES, HMAC-SHA-1) in-system performance up to and greater than 2 Gbps. The product line is also capable of performing security association (SA) lifetime checking for both inbound and outbound SAs and anti-replay checking for inbound packets, supporting 5-tuple-based inbound policy verification. A true hardware random number generator is convenient for initialization vector seeding and secret key generations.

For SSL applications, a single BCM5862 (see table) can support 15,224 SSL sessions per second, which dramatically improves the response time of layer 4+ switches, server load balancers, servers, and other appliances with integrated SSL capability. The BCM586X devices perform all of the protocol processing required for SSL record layer processing: encapsulation/decapsulation, authentication/verification, encryption/decryption of SSL/TLS records at up to 2 Gbps, key derivation, finished message processing, and client certificate verification operations for SSL/TLS. The BCM586X processors support public key operations used in IKE and SSL/TLS handshake protocols: Diffie Hellman (DH), RSA, and DSA.

The BCM586X processors include BroadSAFE™, an automated FIPS 140-2 level 3 certifiable key management subsystem. BroadSAFE enables strong cryptographic authentication, automatic device enrollment, and easy in-field upgrades. In addition, BroadSAFE can be

used to distribute private keys and symmetric keys securely in public networks.

Depending on the chip bonding options, the BCM586X processors connect directly to either the PCI/PCI-X bus or the PCI Express bus without external logic/memory. This new product line is software-compatible to the entire security processor family in either bus configuration.

The BCM586X family is ideal for embedded applications with strict board space and power requirements because it requires no external components. Additionally, the integrated PCI-X interface makes the BCM586X the solution for all high-performance yet cost-sensitive security applications. In the unlikely event that more performance is required, the BCM586X processors can be scaled to further increase both public key and bulk crypto (IPsec and AES) processing performance. System memory is optimized to maximum throughput in real-world applications with unlimited security association (SA) support via system memory and a multithreaded DMA engine. Concurrent public key and bulk payload processing minimizes latency and improves system performance dramatically.

The next-generation CryptoNetX BCM586X devices address a broad range of performance points and leverage a common software base, enabling customers to develop families of products with common architectures and software platforms.

Application program interface (API) support through Broadcom's renowned Software Reference Library (SRL) for IPsec and SSL application software offers BCM586X users a complete system solution. The BCM586X SDK includes support for VxWorks, Linux, and BSD.

Part Number	IPSec and SSL Performance	RSA Performance
BCM5860	500 Mbps	4,600
BCM5861	1 Gbps	7,000
BCM5862	2 Gbps	15,224

Broadcom®, the pulse logo, Connecting everything®, and the Connecting everything logo are among the trademarks of Broadcom Corporation and/or its affiliates in the United States, certain other countries and/or the EU. Any other trademarks or trade names mentioned are the property of their respective owners.

Connecting
everything®



BROADCOM CORPORATION
16215 Alton Parkway, P.O. Box 57013
Irvine, California 92619-7013

© 2006 by BROADCOM CORPORATION. All rights reserved.

586X-DS02-R 04/07/06

Phone: 949-450-8700
Fax: 949-450-8710
E-mail: info@broadcom.com
Web: www.broadcom.com