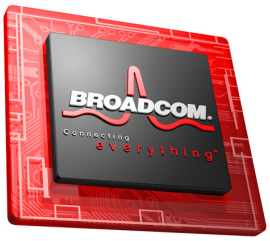
BROADCOM®
Connecting everything®

BCM5840 PRODUCT Brief



BCM5840 GIGABIT SECURITY PROCESSOR

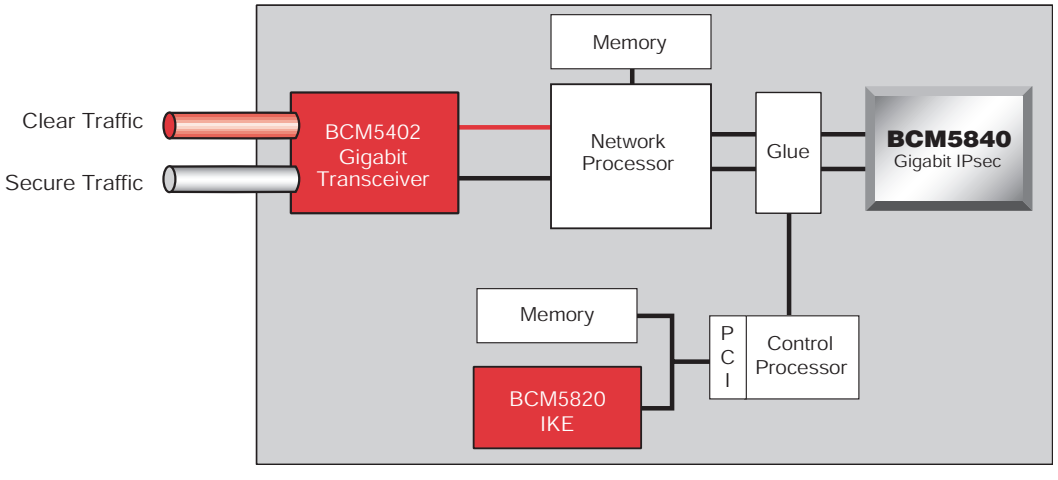
FEATURES

- **World's first multi-gigabit security processor**
  - 2.4-Gbps wirespeed IPsec acceleration (3DES-CBC, HMAC-SHA-1)
  - AH and ESP support (DES, 3DES, HMAC-SHA-1, HMAC- MD5)
- **Sustainable 2.4-Gbps wirespeed on small packets**
- **Flow-through architecture**
  - Order preservation logic on a per-direction basis
- **POS-PHY Level 3 interface**
  - 4.2 Gbps available bandwidth
- **On-chip security association storage and lookup**
  - CAM accelerated lookup supports 2048 SAs
- **Flexible packet processing options**
  - Can support unlimited SAs via in-band keying
  - SAs can be looked-up on chip
- **On-chip packet header processing**
  - Automatically handles mutable fields
  - Direct parsing of IPv4 headers
  - IPv4 header checksum calculation
- **Low-power 0.18µ, 1.8V operation**
- **208 MQFP package**

SUMMARY OF BENEFITS

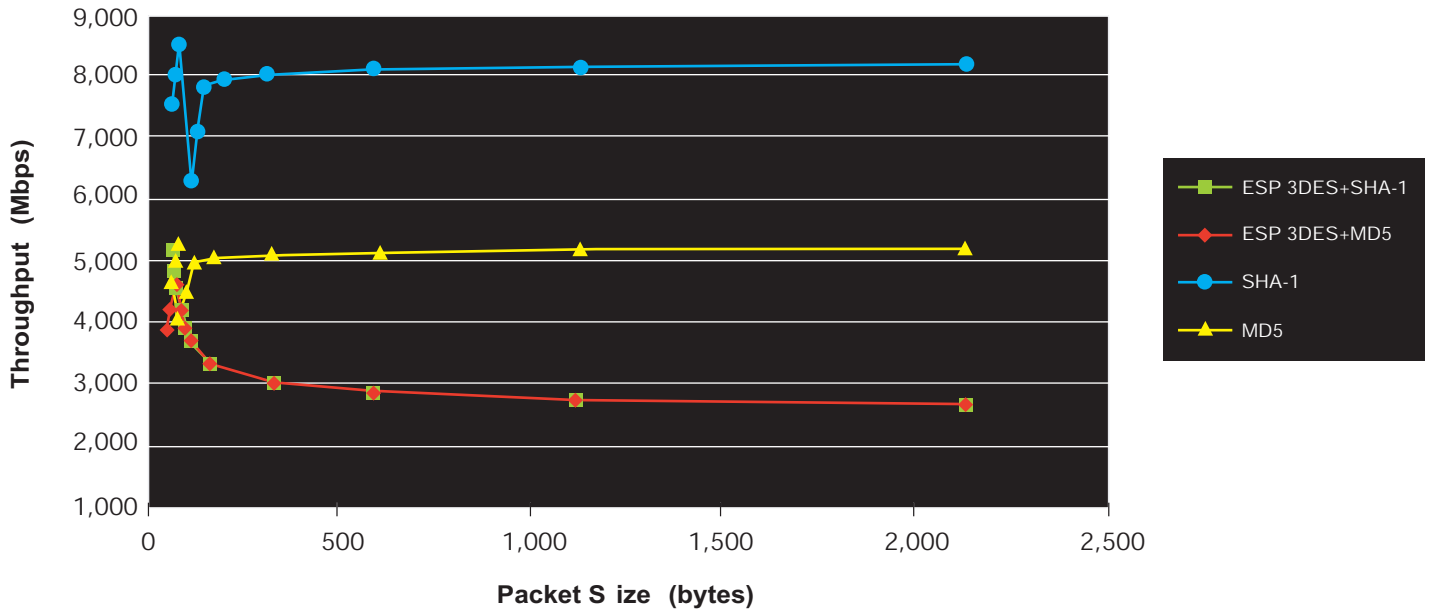
- **Highest performance security processor enables security in high-bandwidth applications**
  - Enterprise routers
  - Layer 3+ switches
  - VPN appliances
  - Edge and core routers
  - Access concentration
  - Firewalls
- **No performance degradation for small packets**
  - Ensures highest performance in realistic conditions
  - 3DES-CBC, new SA per packet
- **Fast path processing makes security ubiquitous**
  - Minimizes packet handling by processor
  - Security processing occurs in-line
- **IPsec-aware architecture optimizes security processing**
  - Flexible packet processing options
  - Packet header processing
  - On-chip SA storage and lookup
- **Scalability offers OC48 IPsec performance**
- **Complete high-performance VPN solution**
  - BCM5840 for high-speed IPsec functionality
  - BCM5820 for fast IKE (public key) functionality

GSM Handset Terminal Using BCM5840



BROADCOM®

OVERVIEW



The BCM5840, the world's first single-chip Gigabit security processor, removes barriers to providing efficient, wire-speed security across an entire LAN or WAN network infrastructure at multi-Gigabit data rates. Broadcom's latest security processor sustains throughputs of 2.4 Gbps for wirespeed IPsec encryption and authentication, regardless of packet size. The BCM5840 provides breakthrough performance, until now, unavailable in commercial products, thereby enabling ubiquitous wirespeed security in routers, firewalls, switches and accesses servers at data rates up to full-duplex OC-48 (4.8 Gbps) using a BCM5840 in each direction.

The innovative BCM5840 sustains multi-Gigabit performance for 3DES-CBC and HMAC-SHA-1 or HMAC-MD5 IPsec processing. The unprecedented performance levels of the BCM5840 are quickening the pace at which the Internet, in the form of virtual private networks (VPN), is replacing expensive, dedicated networks for remote access to corporate Intranets and business-to-business transactions.

Flexible enough to work in most applications, the BCM5840 utilizes a POS-PHY level 3 interface in its flow-through architecture. Multiple keying mechanisms are supported, allowing keys to be sent directly in-band with the packet or stored in the on-chip security association (SA) cache.

The BCM5840 device's on-chip SA storage utilizes a CAM accelerated lookup and supports as many as 2,048 SAs on-chip.

Packet header processing in the BCM5840 includes the IPv4 header checksum and the handling of mutable fields associated with the checksum calculation.

The BCM5840 is optimized to function as an IPsec co-processor that off-loads computationally demanding cryptographic operations for a host protocol processor. A typical application might utilize a custom ASIC or network processor unit (NPU) to receive outbound cleartext packets, perform Security Policy Database (SPD) lookup, insert security headers, access keys from a security association database (SAD), send encapsulated packets along with keys to the BCM5840 for encryption, receive encrypted packets from the BCM5840 and update the SAD as needed.

For inbound packets, the ASIC or NPU would lookup the security association and associated key vectors, send the packet and keys to the BCM5840 for decryption, receive decrypted packets back, perform decapsulation on the cleartext packets, update the SAD, verify that processing was consistent with the SPD, and return successfully processed packets to the system.

Connecting everything®

BROADCOM®

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

5480-PB03-R 04/08/04

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