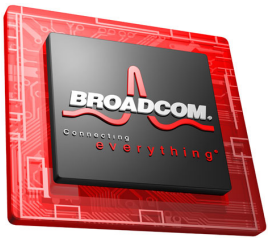
BROADCOM®
Connecting everything®

BCM5841 PRODUCT Brief



MULTI-GIGABIT SECURITY PROCESSOR

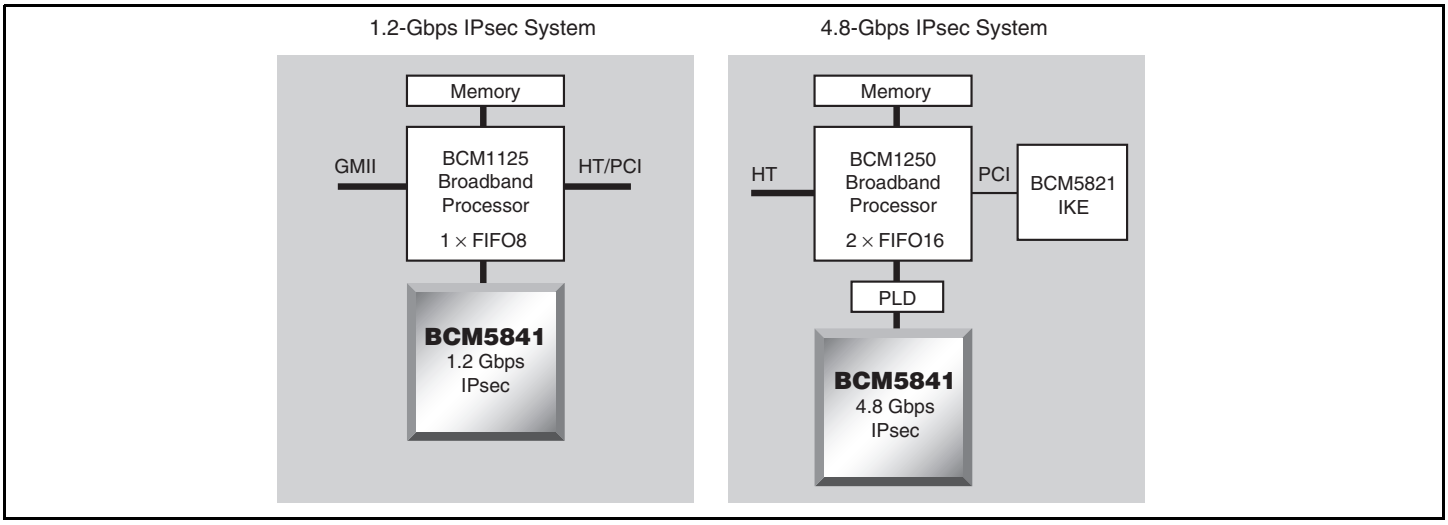
FEATURES

- **World's fastest IPsec security processor**
  - 4.8-Gbps IPsec acceleration
  - AES-CBC and AES-CTR modes
  - AH and ESP support
- **Multiple performance grades**
  - BCM5841-1: 4.8 Gbps
  - BCM5841-2: 2.4 Gbps
  - BCM5841-3: 1.2 Gbps
  - BCM5841-4: 0.6 Gbps
- **Sustainable performance on real-world traffic**
  - 4.8 Gbps on small packets
  - 4.8 Gbps on multiple or single flows
- **Compatibility across BCM584X product family**
  - Forward and backward compatible architectures
  - Common BCM584X API
- **Flexible interfaces**
  - POS-PHY level 3
  - FIFO interface
- **Support for unlimited SAs via in-band keying**
- **Package options**
  - 256-TBGA (27∞27 mm)
  - 256-FPBGA (17∞17 mm)
- **Low-power, 0.18-µm, 1.8V operation**

SUMMARY OF BENEFITS

- **Multiple BCM5841 performance versions offers flexibility**
  - Common IPsec solution across multiple platforms
  - Power consumption scales with performance
- **BCM584X common API protects software investment**
  - Leverage software across platforms
  - Easily migrate from previous generation solution
  - Future proof with next generation compatibility
- **Flexible interfaces minimize size and power requirements**
  - Seamless FIFO interface to Broadcom's broadband processors (BCM1250 and BCM1125)
  - POS-PHY L3 interface for backward compatibility
- **Highest performance security processor enables security in high-bandwidth applications**
  - Enterprise routers
  - Edge and core routers
  - Layer 3+ switches
  - Access concentration
  - VPN appliances
  - Firewalls
- **No performance degradation for small packets**
  - Ensures highest performance in realistic conditions
  - 3DES-CBC, AES-CBC, new SA per packet

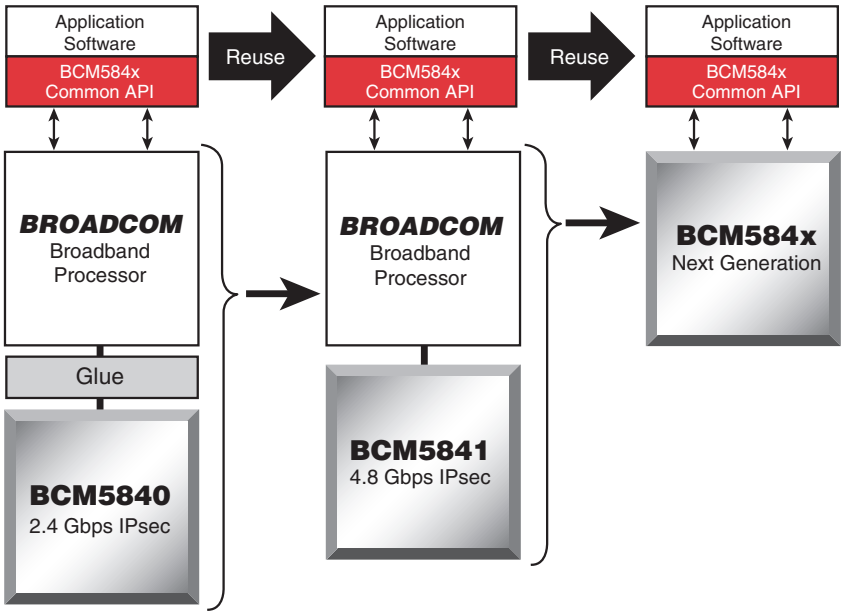
VPN Applications Using the BCM5841



BROADCOM®

OVERVIEW

Broadcom BCM584X Common API



The Broadcom **BCM5841** is a follow-up to the BCM5840, the world's first single-chip Gigabit security processor. Offering increased performance, additional functionality, and more flexible interfaces, the **BCM5841** is the most versatile, highest performance IPsec processor in the world. The **BCM5841** is software and mode-compatible with the BCM5840 processor, thus protecting the software investment of Broadcom's current BCM5840 customers.

Flexible enough to span multiple applications and address a variety of throughput requirements, the **BCM5841** is available in four different versions. The various versions of the **BCM5841** are 600 Mbps, 1.2 Gbps, 2.4 Gbps, and 4.8 Gbps. Such versatility allows customers to address an entire product line's security requirements with a common security solution in a cost-effective manner.

The **BCM5841** architecture provides backward and forward compatibility with Broadcom's BCM5840 Gigabit processor and the next-generation multi-gigabit solution. Furthermore, migration from the BCM5840 or **BCM5841** to Broadcom's next-generation solutions is simplified through a common software API.

Broadcom's BCM584X common API protects customers' software investments while providing the flexibility to migrate to higher performance, and more highly-integrated, next-generation solutions. This common API allows customers to migrate from previous generations to current generations to future generations, while eliminating the impact on their existing software.

The **BCM5841** is able to sustain throughputs of 4.8 Gbps for IPsec encryption and authentication, regardless of packet size. The innovative **BCM5841** sustains multi-gigabit performance for 3DES-CBC/AES-CBC and HMAC-SHA-1/HMAC-MD5 IPsec processing.

Flexible enough to work in most applications, the **BCM5841** utilizes a POS-PHY level 3 interface with the ability to seamlessly interact with Broadcom's family of broadband processors (BCM1250, BCM1125) via the FIFO interfaces of the NPU.

The **BCM5841** is optimized to function as an IPsec coprocessor that offloads computationally demanding cryptographic operations from a host protocol processor. Typical applications might utilize a network processor (NPU) to perform the IPsec protocol processing, including Security Policy Database (SPD) lookup, header encapsulation and de-encapsulation, security association lookup/update, and forwarding to the **BCM5841**.

Applications requiring FIPS140-1 level 2 or 3 can benefit from the ability of the **BCM5841**'s ability to handle encrypted security associations. External security associations can be stored encrypted in a secure manner and forwarded to the **BCM5841** for processing without any performance penalties.

Connecting everything®

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

5841-PB03-R 02/13/04

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