3GPP TSG SA WG3 Security — S3#21 **S3-010582**

26 - 30 November, 2001

Sophia Antipolis, France

Source:	**Telenor**
Title:	**NDS/IP suggestions**
Document for:	**Discussion and decision**
Agenda Item:	**tbd**

Dear all,

I have gone through the meeting report from SA3#20 and the present draft of TS33.210 NDS/IP.
Based on this I have the following suggestions for how we proceed with TS33.210 in Sophia Antipolis next week. I have also tried to give my impression on some of the contributions.

Intial reactions to some of the contributions

- **S3-010529 (Huawei/CWTS)**
  This is a clarification to do with security domains vs operator subnets.
  The clarification seem appropriate to me.

- **S3-010489 (Nokia)**
  The suggestion is about seeing the SEG as a BG with additional security functionality.
  This makes a lot of sense to me and I will support the idea.

- **S3-010490 (Nokia)**
  The suggestion here is to add support for the GGSN - P-CSCF interface.
  See comments under the "suggestions" heading.

- **S3-010496 (Nokia)**
  This is a contribution about GTP-U. I don't support the pCR as such.
  I have however changed my mind over GTP-U and I think we should allow the possibility of GTP-U protection. More on this under the "suggestions" heading.

Some suggestions for TS 33.210 NDS/IP

1) To keep TS 33.210 NDS/IP as a framework for use of IPsec in the UMTS core network

What do I mean by this?
Well, I think it will be a lot easier to complete 33.210 on time if we keep 33.210 free from specific information about the protocols that it shall be used to protect. Maintenance of 33.210 will also benefit from this since fewer CRs will probably then be required. In the present draft of 33.210, only GTP and IMS protocols/interfaces will be affected. So to be specific, all IMS related information in 33.210 should be moved to 33.203.

What about GTP then?

Well, ideally one might want to have all GTP related information moved to 29.060.
And indeed, this would be the natural solution if we were only concerned with GTP Rel5.
However, since NDS/IP really is a very simple application of IPsec we will have to opportunity to protect previous version of GTP if we take a little care.

This means that NDS/IP could very easily be used to protect previous versions of GTP given that one configures the right port number etc. But, since we are very unlikely to be able to change/update the older versions of GTP, we cannot rely on moving the NDS/IP GTP specific material to those TSs. So, I suggest that we consider keeping the legacy GTP specific material in 33.210. That is, we should move it to an annex in 33.210 to keep the main body of 33.210 as conceptually clean as possible.

2) Support for GTP-U and GTP Release 97/98 ?

I have come to the conclusion that we should allow for the possibility of using NDS/IP for ***all*** IP based control plane core network protocols.

We might have to include a word or two in 33.900 about the consequences of using/not using NDS/IP, but apart from that we should probably not restrict the use of NDS/IP.

Today it is possible to get high-performance crypto-processor that easily keeps up with a 100 Mb pipe. See the attached PDFs for some examples from Broadcom. OpenBSD developers have reported that they have achieved 3DES 122 Mb in real-life with the BCM5805 processor (see OpenBSD.pdf file). More OpenBSD crypto info: http://www.openbsd.org/crypto.html#hardware . Broadcom also has a faster crypto-processor (see BCM5840.pdf) if people think that 122 Mb is a bit on the slow side[1]. The advent of AES should make it even easier to provide high-speed encryption.

So, in short, I feel it would be wrong of us to disallow the possibility of protecting GTP-U. I think, in fact, that we may even allow for protection of GTP for Release 97/98 (where there is no port number distinction between GTP-C and GTP-U).

All of this could then be described in an annex to 33.210. We should take care not to mandate GTP-U and/or GTP-rel97/98 support, but rather give a description of how it can be done by means of NDS/IP.

3) Clause 5.3.1

We have said that we ***shall not*** support IP payload compression (IPCOMP). We may want to reconsider this position if we are to allow NDS/IP to protect GTP-U etc.

For while we argued that GTP-C packets were generally very short and would benefit for IPCOMP, the same cannot be said for GTP-U and probably not for other protocols either. We should therefore probably open up for IP payload compression as an option. Since that is the default case for IPsec anyway, we may consider deleting clause 5.3.1

4) SEG discovery function

This was brought up by Alcatel in S3-010348 (SA3#19, Newbury).
Although I don't think it is strictly needed, it could be a useful feature for larger networks.
I have the feeling this might be a candidate for the Rel6 version of 33.210

5) Minor clarifications on IKE

The statement "Support of Notifications shall be mandatory" in clause 6.5 should perhaps be clarified. What it actually implies is that the IKE SA must be persistent and live at least as long as the derived IPsec SA.

6) Support of PKI for authentication of IKE phase 1

In the current version of 33.210 we rely on the use of preshared secrets for IKE phase-1 authentication. IKE also support authentication by means of digital signatures and PKI.

---

[1] No, Broadcom doesn't pay me in any way.

I suggest that we include support of PKI in 33.210, and that this work is put into Rel6.

/Geir M. Køien, Telenor R&D

The IPSec Architecture in OpenBSD

Niels Provos
CITI, University of Michigan
provos@citi.umich.edu

Overview

- Introduction
- History
- Kernel Details
- IKE
- Policy using Keynote
- Crypto Acceleration Framework
- Bridging with IPSec
- Conclusion

Introduction

- OpenBSD is a free UNIX-like operating system with a strong emphasis on security.
- We realized early that many security problems can be solved only by using cryptography.
- Cryptography is integrated seamlessly into the system and is an essential component:
  - IPSec, IPv6, key management daemons,
  - Cryptographic Acceleration Framework
  - Kerberos, AFS, OpenSSH, etc...

History

- July 1997: OpenBSD 2.1 with IPSec support
  - Based on BSD/OS code by John Ioannidis,
  - Ported to OpenBSD by Angelos Keromytis,
  - no automatic keying, only manual setup.
- December 1997: OpenBSD 2.2
  - Photuris key management daemon,
  - new ESP and AH support according to RFC 2406 + 2402.

History

- May 1998: OpenBSD 2.3
  - more encryption and authentication transforms, e.g. Blowfish,
  - `PF_ENCAP` notifications for key management daemon.
- May 1999: OpenBSD 2.5
  - `isakmpd` as IKE daemon,
  - `PFKEYv2` as generic key management API.

History

- December 1999: OpenBSD 2.6
  - support kernel acquire messages.
- June 2000: OpenBSD 2.7
  - support IPSec tunnels for bridging,
  - hardware acceleration for IPSec,
  - ACLs for ingress flows,
  - IPv6 IPSec support.

History

- December 2000: OpenBSD 2.8
  - AES (Rijndael) support,
  - Support for automatic IKE setup (no configuration).
- December 2001: OpenBSD 3.0
  - Path MTU discovery for IPSec,
  - IPCOMP (Payload compression) support.

Kernel Details

- Incoming IPSec packets are decapsulated and processed in ipsec_common_input(), and passed pack into the IP input queue.
- Outgoing packets are IPSec processed and encapsulated in ipsp_process_packet().
- SPD is stored in the BSD routing radix tree:
  - SA selection can be based on protocol and port numbers.
  - Supported attributes (ingress and egress):
    - acquire, require, dontacq, permit, and bypass.

Kernel Details

- Prevent source address spoofing by specifying permitted source addresses for specific SAs.
- Cryptographic processing of packets is done asynchronously, so that network stack processing does not block:
  - just by itself caused a performance improvement.
- Hard- and soft-expirations based on SA life time, processed bytes, etc...

Kernel Details

- Flows specify IPSec policy:
  - acquire/require flows send `PFKEY_ACQUIRE` messages to registered key management daemons,
  - permit/bypass either make use of existing IPSec SAs or bypass IPSec completely.
- Multiple key management daemons can run at the same time, e.g. photuris and isakmpd.

IKE

- isakmpd, new implementation started in 1998 since our IKE daemon had to be
  - scalable:
    - needs to support thousands of SAs.
  - flexible:
    - the standard was still evolving.
- Protocol complexity mandates modular design.
- isakmpd is an event driven UNIX daemon using `select(2)`

IKE

- Features
  - Main Mode, Aggressive Mode.
  - Diffie-Hellman groups 1 - 5, including elliptic curve cryptography.
  - Authentication via pre-shared pass phrases and RSA signatures with X509 certificates.
- Main abstraction is the exchange:
  - Provides the context for negotiations as script-driven state machine.
  - Enables high-level syntax checking of messages.

IKE

- Configuration:
  - Very flexible, allows for good interoperability, but too complex.
  - PFKEY extensions permit mode without configuration file:
    - Identities and policies are communicated via PFKEY.
- Portable with system dependency layer. Runs on *BSD and Linux.
- About 42 KLOC code size (12% platform dependent, 4% regression tests).

Policy using Keynote

- Uses the Keynote trust management system for policy decisions.
- Keynote determines who can negotiate what kind of SAs.
- Allows very fine grained access controls:

```
KeyNote-Version: 2
Authorizer: "POLICY"
Licensees: "passphrase:blubberdubber"
Conditions: app_domain == "IPsec policy" &&
            pfs == "yes" && esp_present == "yes" &&
            esp_enc_alg != "null" -> "true";
```

  - Requires the use of PFS and ESP, where the ESP algorithm is not null.

Crypto Acceleration Framework

- Cryptographic framework manages available hardware accelerators:
  - Asynchronous interface,
  - Callbacks on completion of cryptographic operation.
- Software cryptographic engine as fallback.
- Currently supports:
  - HiFn 7751 (e.g. Powercrypt),
  - Broadcom BCM5805 (ubsec).

Crypto Acceleration Framework

- Performance:

Engine	Transform	Spee
software (P3/550)	3DES	11 MBit/
software (P3/550)	Blowfish	34 MBit/
HiFn	3DES	70 MBit/
BCM5805	3DES	122 MBit/

  - Broadcom card has no problems dealing with 100 MBit ethernet.

Crypto Acceleration Framework

- `/dev/crypto` allows userland to access cryptographic framework:
  - Supports currently only symmetric ciphers and message authentication codes.
  - Acceleration for asymmetric operations planned:
    - Speedup for Diffie-Hellman and RSA.
- OpenSSL abstracts access to `/dev/crypto`:
  - Standard applications will automatically use hardware acceleration
    - OpenSSH, isakmpd, etc...

Bridging with IPSec

- In OpenBSD, a bridge device creates a logical link between a set of network interfaces.
- The bridge copies frames read from one interface to the other interfaces associated with the bridge device.
- Supports filtering on Layer-2 and Layer-3 -> transparent firewall.

Bridging with IPSec

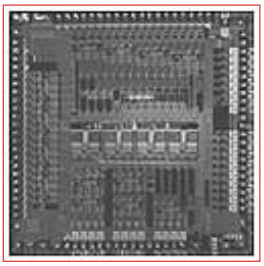
- Supports extended LAN over the Internet.
  - Ease of administration, no routing required.
- Uses IPSec as encapsulation mechanism:
  - Set up a tunnel via generic tunnel interface `gif`:
    - IPv4 or IPv6.
  - Set up IPSec flows between tunnel endpoints.
  - `gif` interface may become a bridge member.
  - Ethernet in IP over IPSec.

Conclusion

- OpenBSD has state-of-the-art IPSec architecture:
  - IPSec is part of every OpenBSD installation,
  - Very fast with hardware acceleration,
  - Bridge and IPSec allow easy to administrate VPNs.
- OpenBSD code and information can be found at `http://www.openbsd.org/`.
- Further reading: `http://www.openbsd.org/crypto.html`.

BCM5805

PRODUCT Brief



BCM5805 SECURITY PROCESSOR

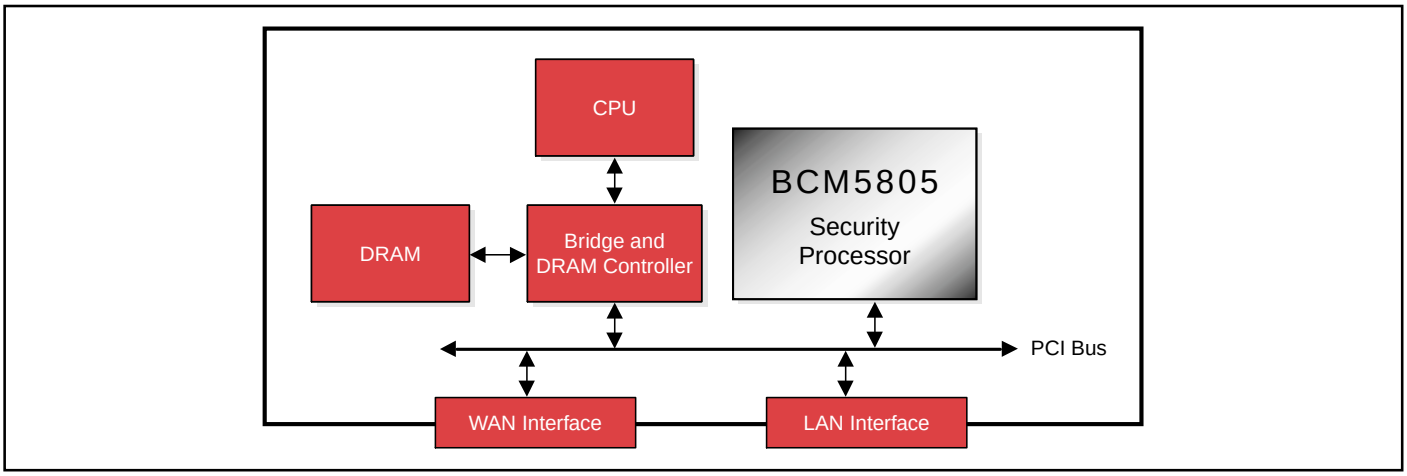
BCM5805 FEATURES

- **High-performance Single-Chip Security Processor Integrating Full IPSec Acceleration**
- **Supports DES, 3DES, HMAC- SHA-1 and HMAC-MD5**
- **310 Mbps IPSec (3DES, SHA-1) "In-System" Performance, with New Security Association (SA) per Packet**
- **Unlimited SA Support via System Memory**
- **Extensive HW Acceleration Support for IKE/SSL/TLS Key Setup**
- **Public Key Acceleration Unit Supports Over 250 Diffie-Hellman Key Exchanges/second**
- **Compatible with Industry Standard SSH IPSec & IKE Software**
- **True Hardware Random Number Generator**
- **Supports Multi-Packet Processing & Pre-Fetch of Packet Data and Context**
- **Multi-Threaded DMA allows Multi-Packet Processing with Single PCI Writes**
- **Accommodates Most PCI Latency Problems Without Performance Degradation**
- **PCI 2.1 Interface, 32-bit, 33/66 MHz**
- **Low-Power 3.3V Design**
- **144-pin LQFP Package**

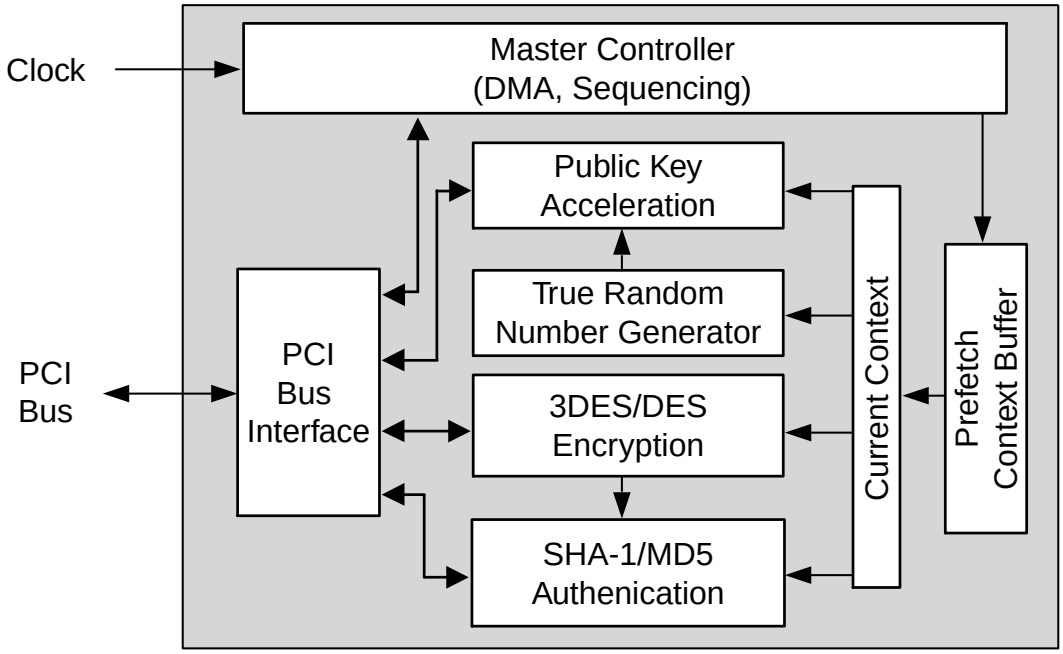
SUMMARY OF BENEFITS

- **Highly integrated security processor**
  - Single-chip IPSec, IKE, SSL/TLS accelerator
  - Multi Threaded DMA Engine
  - True Hardware Random Number Generator
  - On-chip context buffer memory
  - Lowest system cost
- **Sustainable performance in real-world conditions**
  - DMA supports multi-packet processing
  - Pre-fetch of new context and packet
- **Flexible, easy to use PCI 2.1 interface**
  - No external components required
  - Ideal for low-cost add-in card applications
  - Compatible with all existing PC systems
- **Complete product solution minimizes time-to-market**
  - Software Reference Library (SRL) including a hardware abstraction software layer
  - Compatible with industry standard SSH IPSec & IKE Software
  - Compatible with OpenSSL
- **Flexible VPN solution for all data security applications:**
  - VPN appliances
  - SOHO routers and appliances
  - Access concentrators
  - IPSec acceleration

Virtual Private Network Appliance System Diagram



BCM5805 OVERVIEW



The **BCM5805** Security Processor integrates a high-performance IPSec engine (DES, 3DES, HMAC-SHA-1, HMAC-MD5), public key processor, true random number generator, PCI interface and context buffer memory onto a single chip. The highly integrated **BCM5805** Security Processor is an ideal solution for VPN-enabled networking products such as SOHO routers and gateways, VPN appliances, access concentrators and network interface cards.

Accelerating bulk cryptographic functions (DES, 3DES, SHA-1 and MD5) and public key operations, the **BCM5805** is a streamlined design ideally suited for all cost sensitive applications. Extensive hardware support for processing intensive public key operations, minimizes the user software required for IKE and SSL/TLS key negotiations.

The **BCM5805** offers full-duplex OC3 IPSec processing (310 Mbps - 3DES, HMAC-SHA-1) performance, and in excess of 250 Diffie-Hellman key exchanges per second (1024-bit public key, 180-bit private key). IPSec performance is measured "in-system" on outbound packets, with new security associations per packet.

A true hardware random number generator on the **BCM5805** is well suited for IV seeding and secret key generation.

The **BCM5805**'s PCI interface makes it a perfect solution for all cost-sensitive security applications. Requiring no external components, the **BCM5805** is ideal for add-in card applications requiring IPSec acceleration. Unlimited security association (SA) support via system memory and a multi-threaded DMA engine utilizes system memory to maximize throughput in real-world applications. The ability to pre-fetch packet contexts minimizes the performance degradation when processing small packets.

Application program interface (API) support through Broadcom's Software Reference Library (SRL) for IPSec and SSL application software offers **BCM5805** users a complete system solution. Compatibility with OpenSSL and industry standard IPSec software from SSH Communications eases integration and reduces time-to-market.

For more information please contact us at:
Phone: 949-450-8700, FAX: 949-450-8710
Email: info@broadcom.com

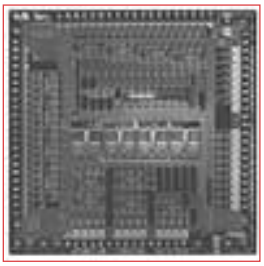
Visit our web site at: www.broadcom.com

5805-PB00-R-04.24.00

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

BROADCOM®

BCM5840
PRODUCT Brief



BCM5840 GIGABIT SECURITY PROCESSOR

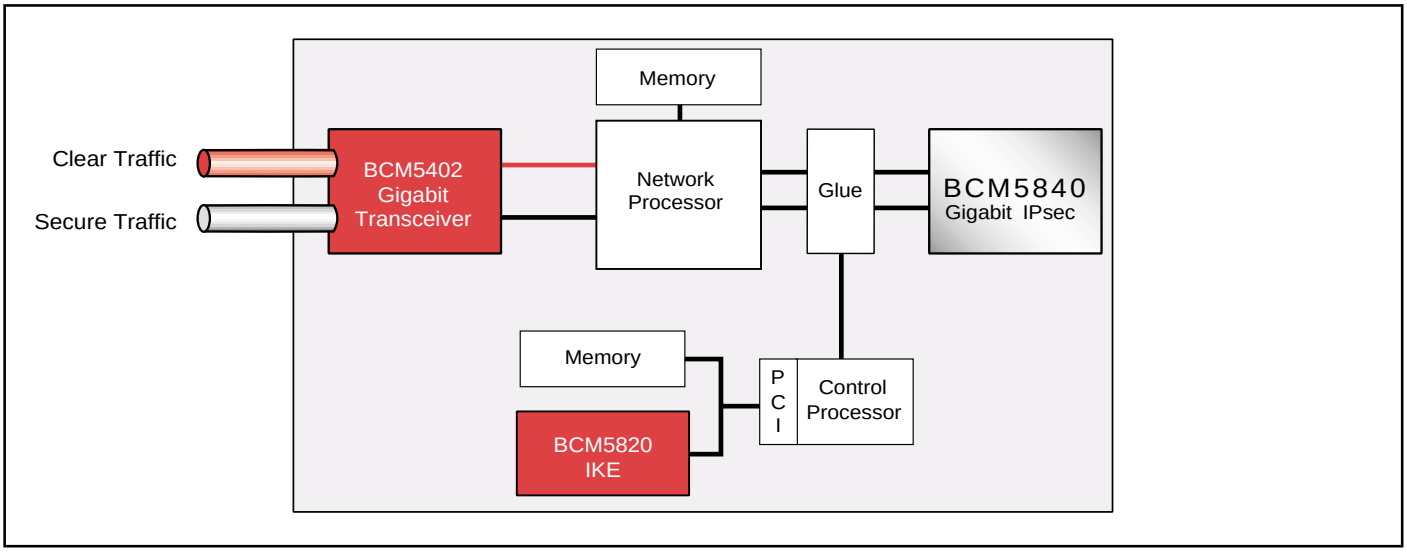
BCM5840 FEATURES

- **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 look-up**
  - CAM accelerated look-up 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 0.18u, 1.8V operation in 208 MQFP Pkg**

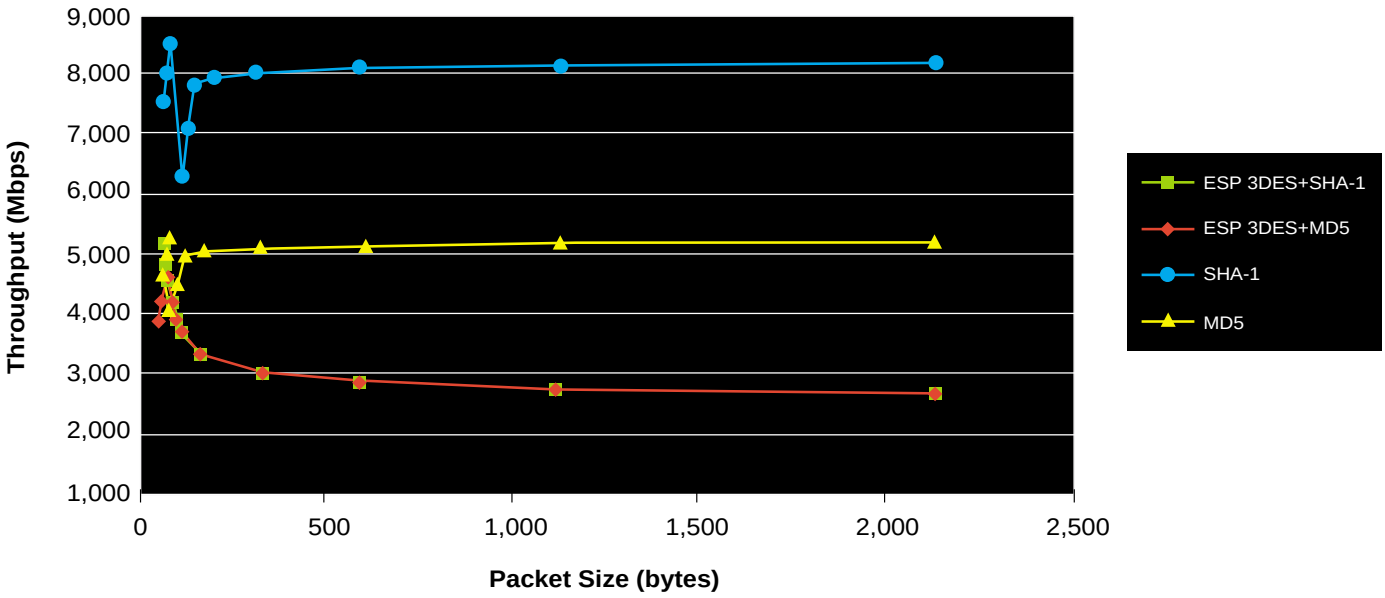
SUMMARY OF BENEFITS

- **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, 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 look-up
- **Scalability Offers OC48 IPsec Performance**
- **Complete high-performance VPN solution**
  - BCM5840 for high-speed IPsec functionality
  - BCM5820 for fast IKE (public key) functionality

VPN Gigabit Tunnel Server Application



BCM5840 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 accesses servers at data rates up to full-duplex OC-48 (4.8 Gbps).

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's** on-chip SA storage utilizes a CAM accelerated look-up 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 units (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.

For more information please contact us at:
Phone: 949-450-8700, FAX: 949-450-8710
Email: info@broadcom.com

BROADCOM®

Visit our web site at: www.broadcom.com

5840-PB00-R-12.6.00

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