

IPSEC Packet Processor

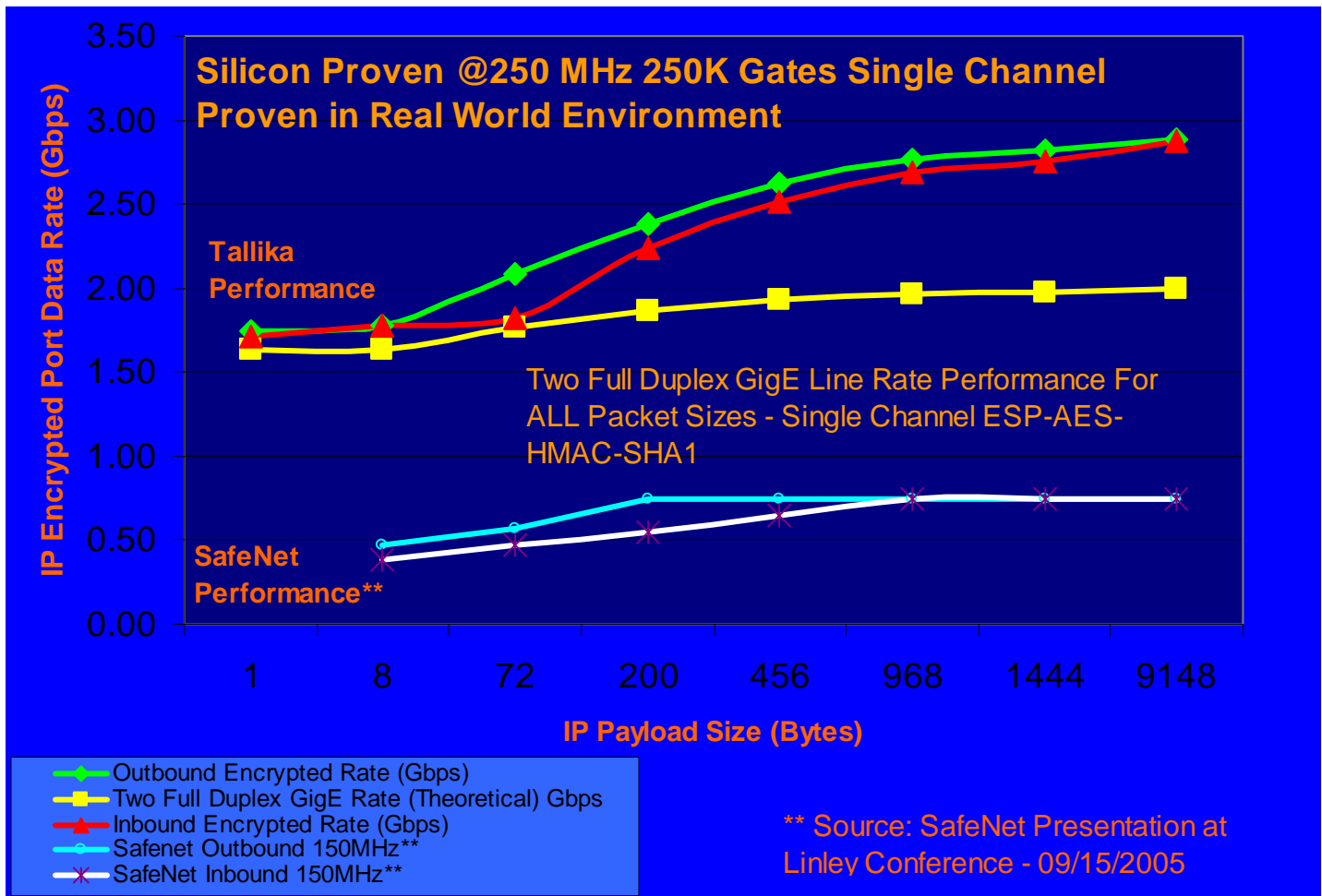
TALLIKA CORPORATION

2222 S. Dobson Rd, Suite 1103
Mesa, AZ 85202

Phone: 480 231 2074
www.tallika.com

Email: sales@tallika.com

Tallika's IPSEC Packet Processor core sustains two full duplex GigE ports performance even for short packets. It is a silicon proven, flexible and scalable solution built by experts with years of experience in building security solutions for commercial as well as government applications in Networking, Storage and Consumer market segments. The core has been validated in a real world environment with a real world software stack.



Product Brief

Features:

- Silicon Proven in 250 MHz Operation in 0.13u technology
- Validated at system level with real world software stack
- Performs line rate for two full duplex Gigabit ports for short packets with a single channel and approximately 500K gates
- The IPSEC block supports Ethernet In (cleartext or ciphertext) and Ethernet Out (ciphertext or cleartext) —Fully Compliant with RFC 2401.
- IPv4 with IP option headers
- Automatic insertion/deletion of ESP/AH headers and trailers
- ESP Cipher algorithms supported are DES, 3DES, AES128, AES192, AES256 in CBC Mode, and AES128, AES192, AES256 in Counter Mode
- ESP and AH Authentication algorithms supported are HMAC-SHA1, HMAC-MD5, HMAC-SHA1-96, HMAC-MD5-96, AES-XCBC-MAC-96
- Anti-Replay Option Per Security Association (SA)
- IPSec Sequence Number overflow detection/event generation
- Transmit SA Lifetime time-timeout and byte-timeout checks.
- “Soft” (early warning of SA expiration, creating event) and “hard” (drop all further datagrams) timeout limits.
- Supports Ethernet frames of type DIX, IEEE 802.3 SNAP with optional VLAN
- Ethernet Jumbo frame support supports frame size upto 9200B
- Support for configurable number of Security Associations, each based on an SA index resulting from an external IPV4 classification
- Local storage/maintenance of statistics compatible with Microsoft’s security APIs.
- Aggregate 200 Mbps to 2.7 Gbps IPSEC throughput per channel for AES-SHA1 as measured on the encrypted port.

Deliverables:

- ◆ Verilog RTL
- ◆ Primitime and DC scripts—support available for Synopsys, Magma and Cadence design flows
- ◆ Complete documentation with Integration Guide

