Dpdk IPSec security gateway application

Intel NPG PMA, 3/2/2017

Legal Notices and Disclaimers

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Learn more at intel.com, or from the OEM or retailer.

No computer system can be absolutely secure.

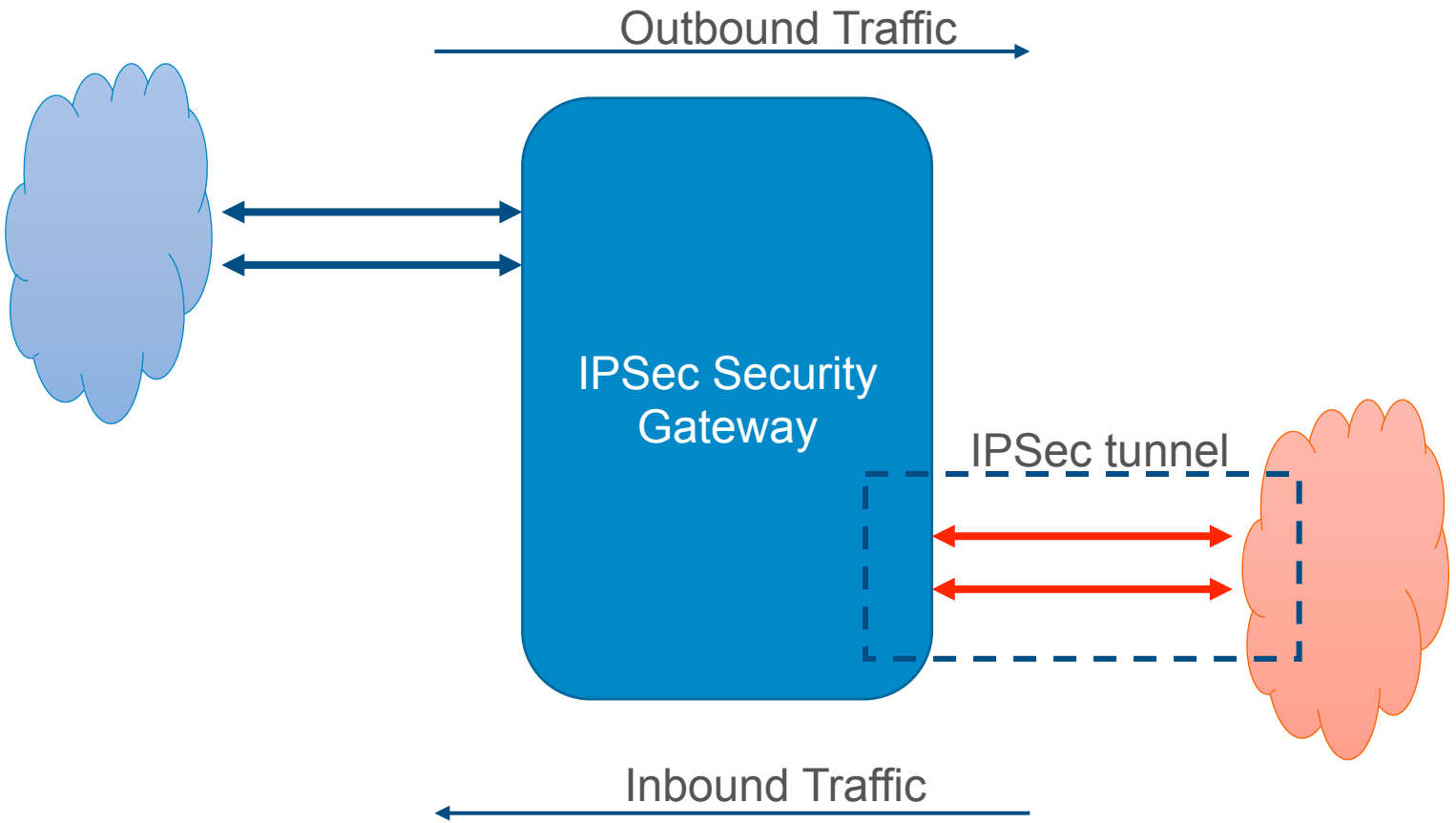
Tests document performance of components on a particular test, in specific systems. Differences in hardware, software, or configuration will affect actual performance. Consult other sources of information to evaluate performance as you consider your purchase. For more complete information about performance and benchmark results, visit **http://www.intel.com/performance**.

overview

- Example application providing guidelines for using the Cryptography Device Library framework.
- Showcase DPDK cryptodev framework performance with a real world use case scenario.

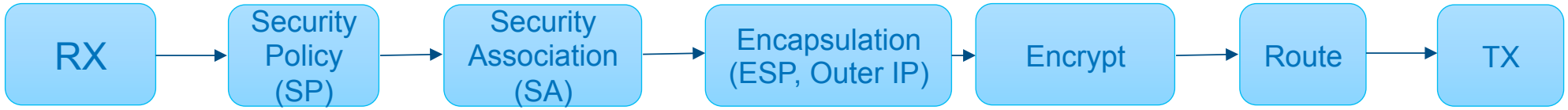
- http://dpdk.org/doc/guides-16.04/sample_app_ug/ipsec_secgw.html (Google DPDK IPSec sample application)

Overview cont.



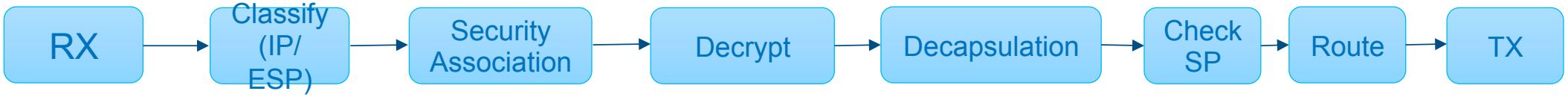
Application Flow

Outbound



- Check destination
- Encrypt, Encapsulate
- Route

Inbound



- Classify
- Decrypt, Decapsulate
- Check SP
- Route

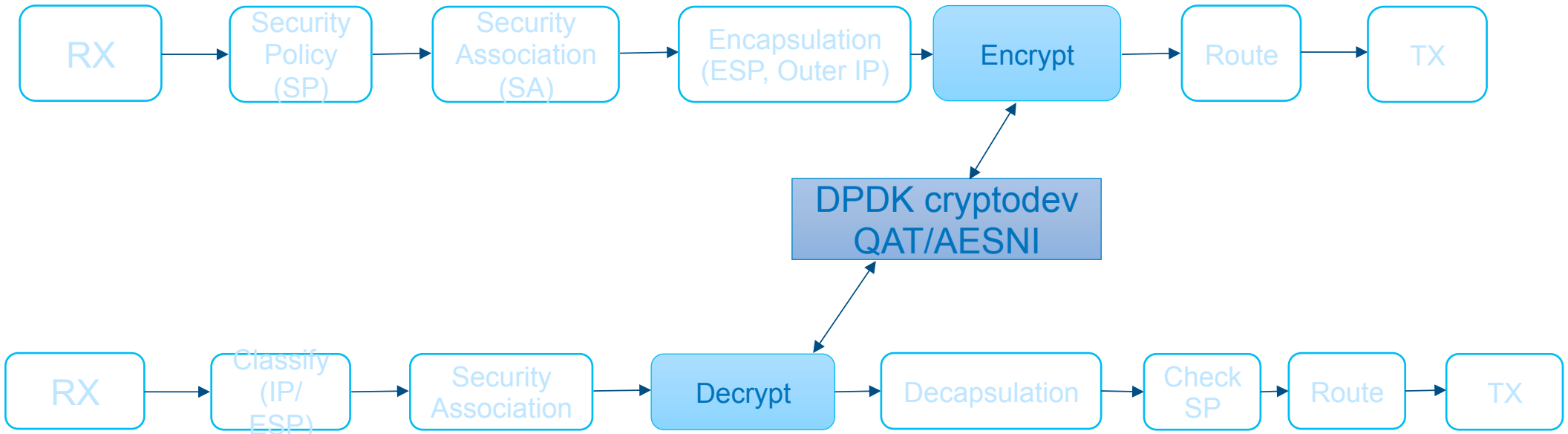
security policy

Src	Dst	proto	SA idx
Any	192.168.115.0/24	Any	5
Any	192.168.116.0/24	Any	6
Any	192.168.117.0/24	Any	BYPASS

security association

SPI	Cipher	Auth	Tunnel src	Tunnel dst
5	AES-CBC	HMAC-SHA1	172.16.1.5	172.16.2.5
6	AES-CBC	HMAC-SHA1	172.16.1.6	172.16.2.6
9	NULL	NULL	172.16.1.5	172.16.2.5

cryptography

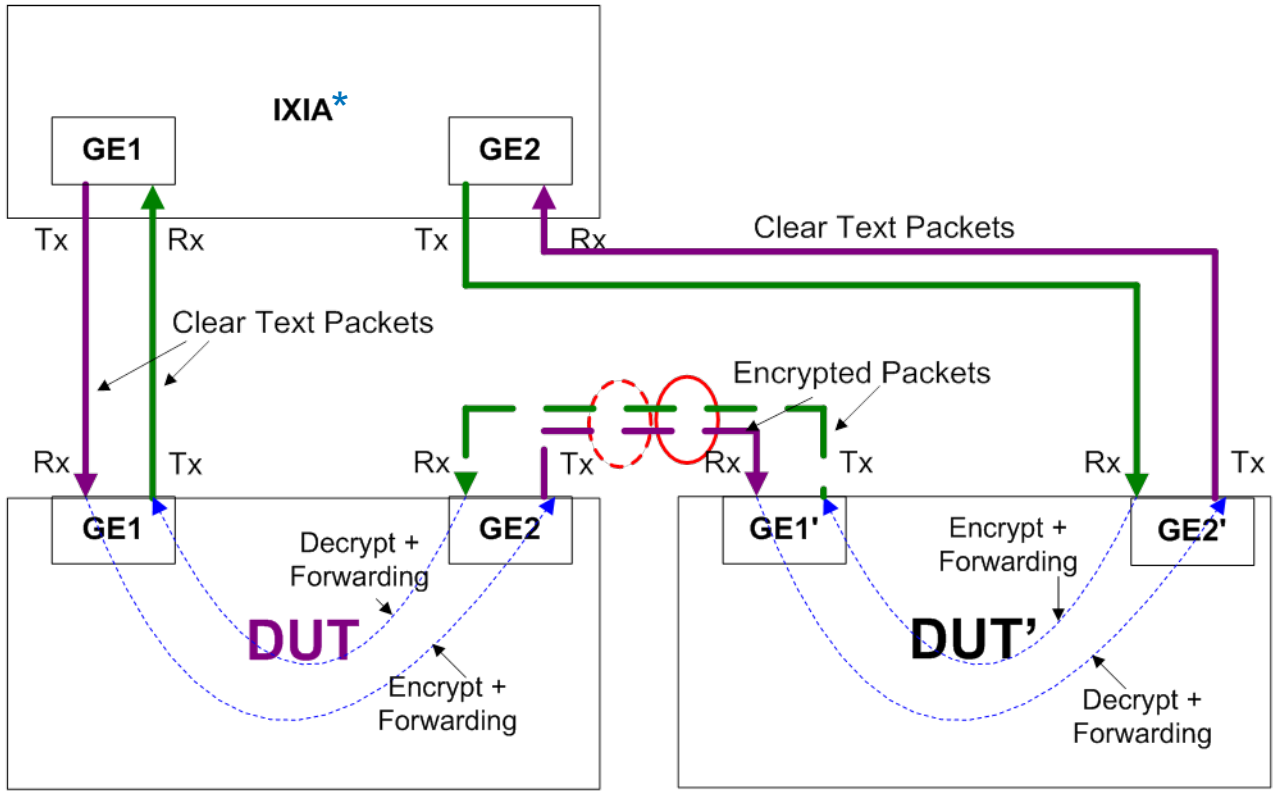


DPDK cryptodev

- Crypto PMD framework – similar to DPDK NIC drivers
- Same generic API for HW and SW crypto devices
  - No change to code to switch between QAT and AESNI libraries
- Supports
  - Symmetric Crypto
  - Authentication
  - Chained crypto/authentication
  - Asymmetric Crypto

http://dpdk.org/doc/guides-16.04/prog_guide/cryptodev_lib.html (Google DPDK cryptodev libraries)

Flow Traffic Configuration



DUT and DUT' are the identical platforms

* Other names and brands may be claimed as the property of others.

running the application

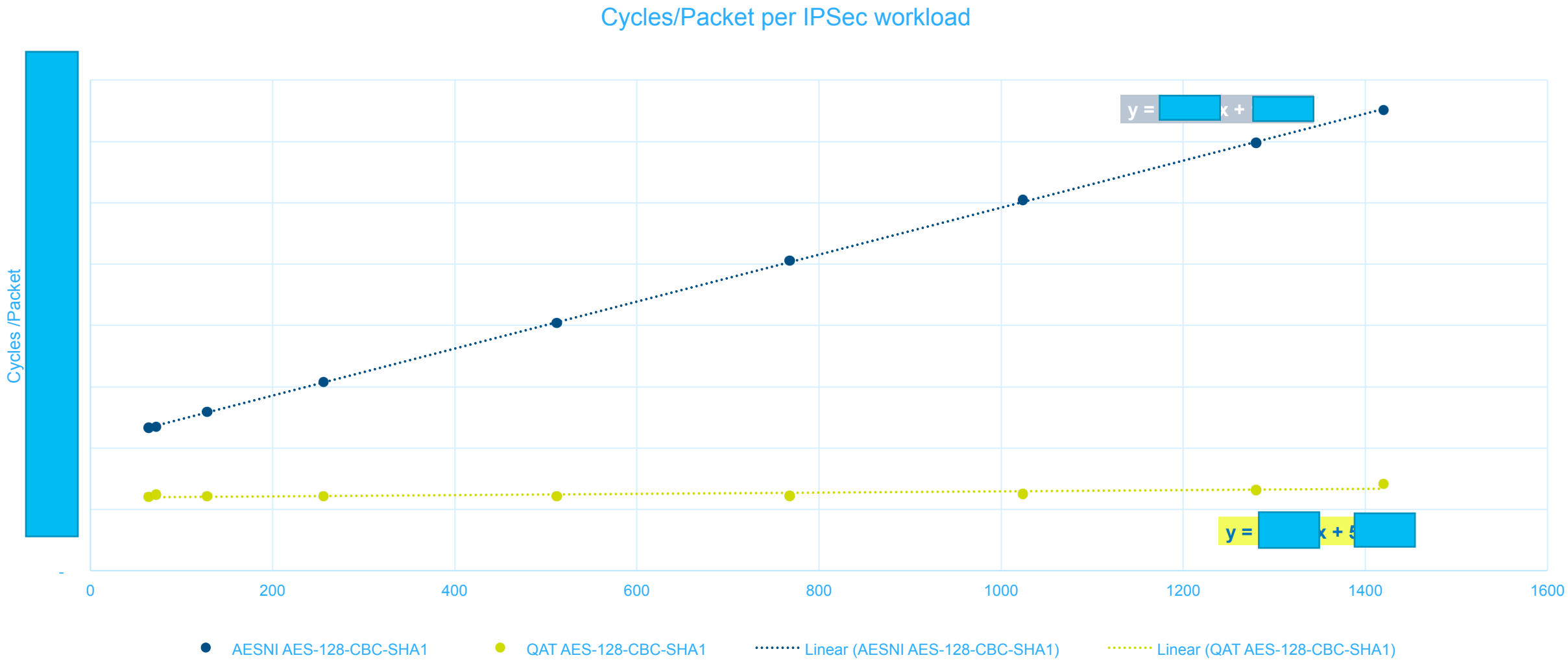
- Pass number of cores
  - -l 1,2-5
- Pass NICs
  - -w 02:00.0 …
- Pass encryption device
  - -w b3:00.0 … or --vdev='crypto_aesni_mb'
- Allocate ports and cores
  - --config=(port,queue,core)
- Provide IPSec config
  - EP0 or EP1

performance considerations

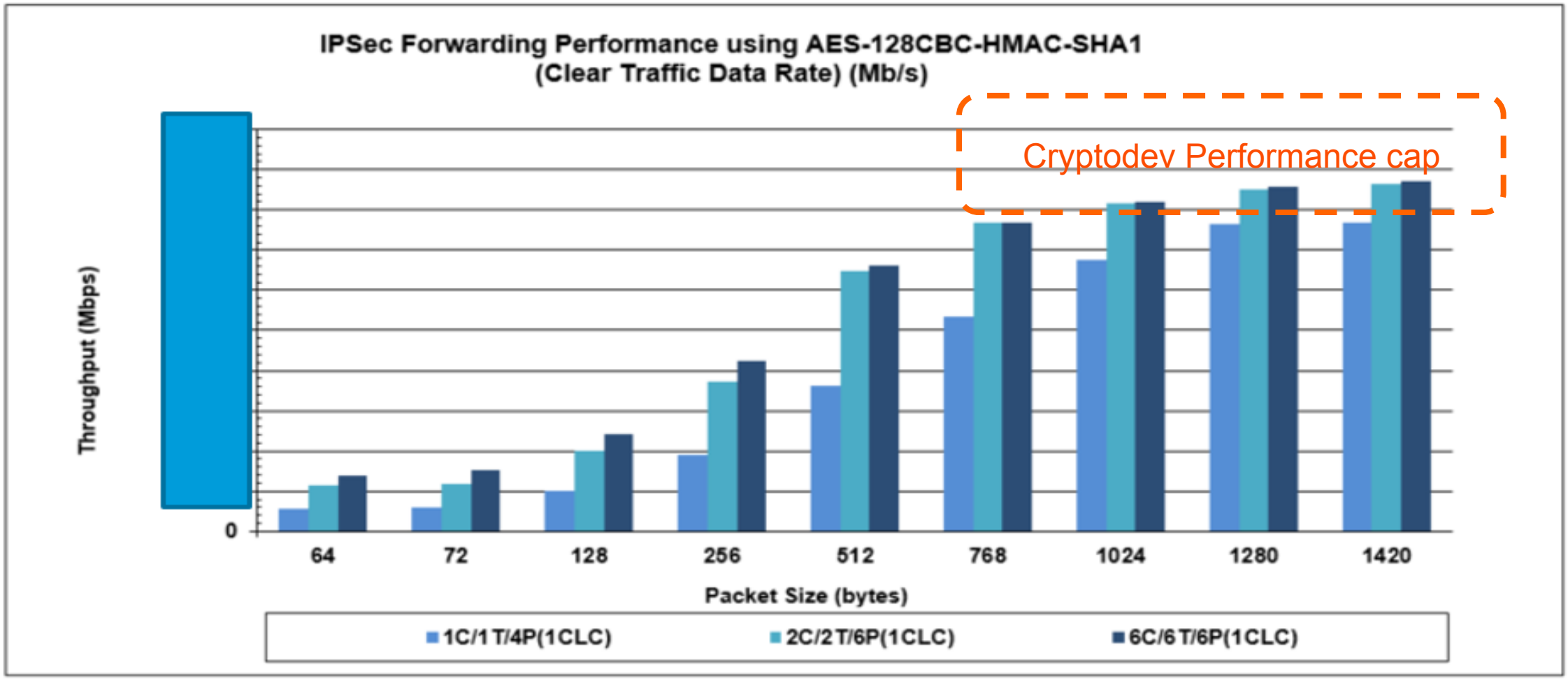
system resources

- **Cores**
  - Run to completion
  - Packets/Sec/Core varies
- **Memory**
  - Large amount of data traveling through memory (2x memory accesses vs L3fwd)
  - Beware of NUMA
- **Cryptodev**
  - QAT has a limit based on packet size
- **NIC line rate**
  - Encapsulated packet is larger than original

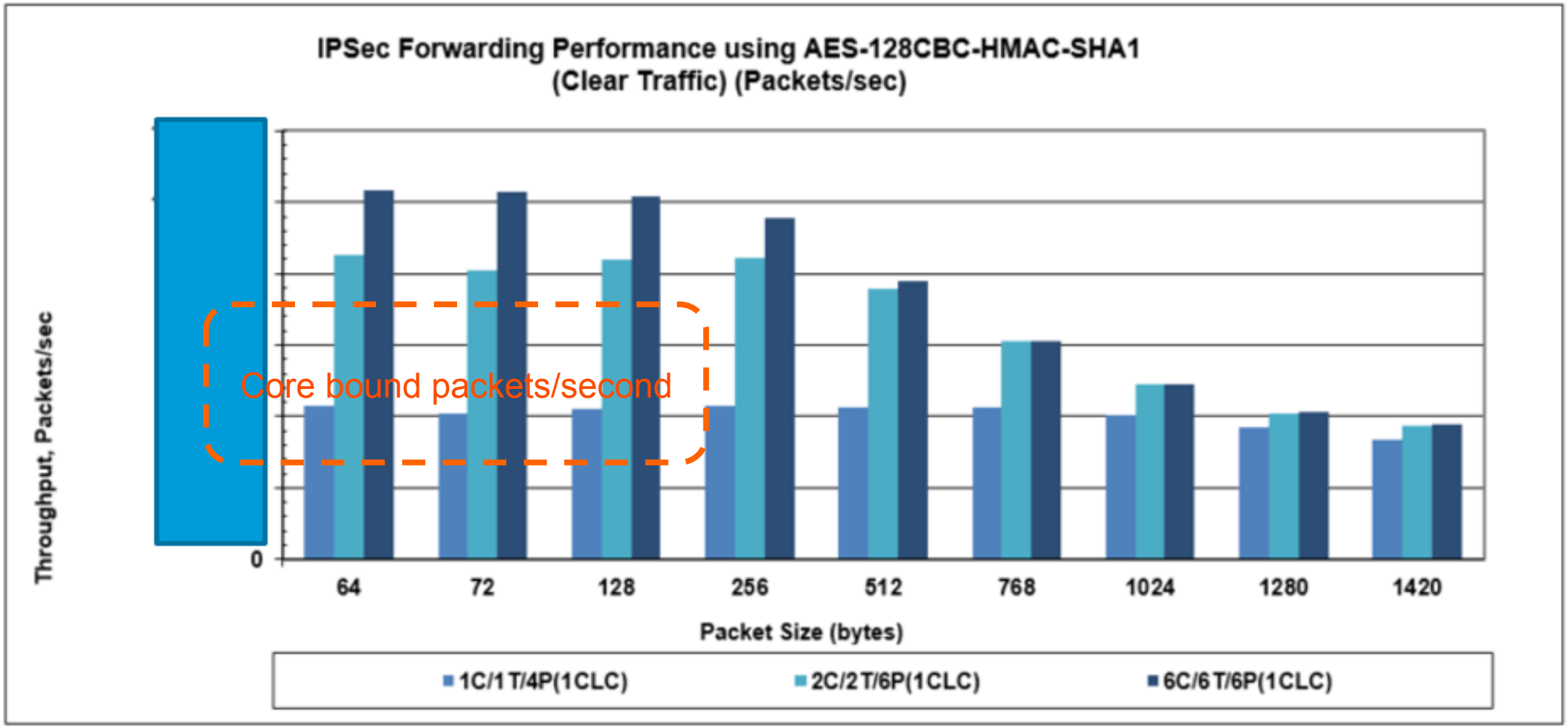
Understanding IPSEC performance numbers



Understanding IPSEC performance numbers

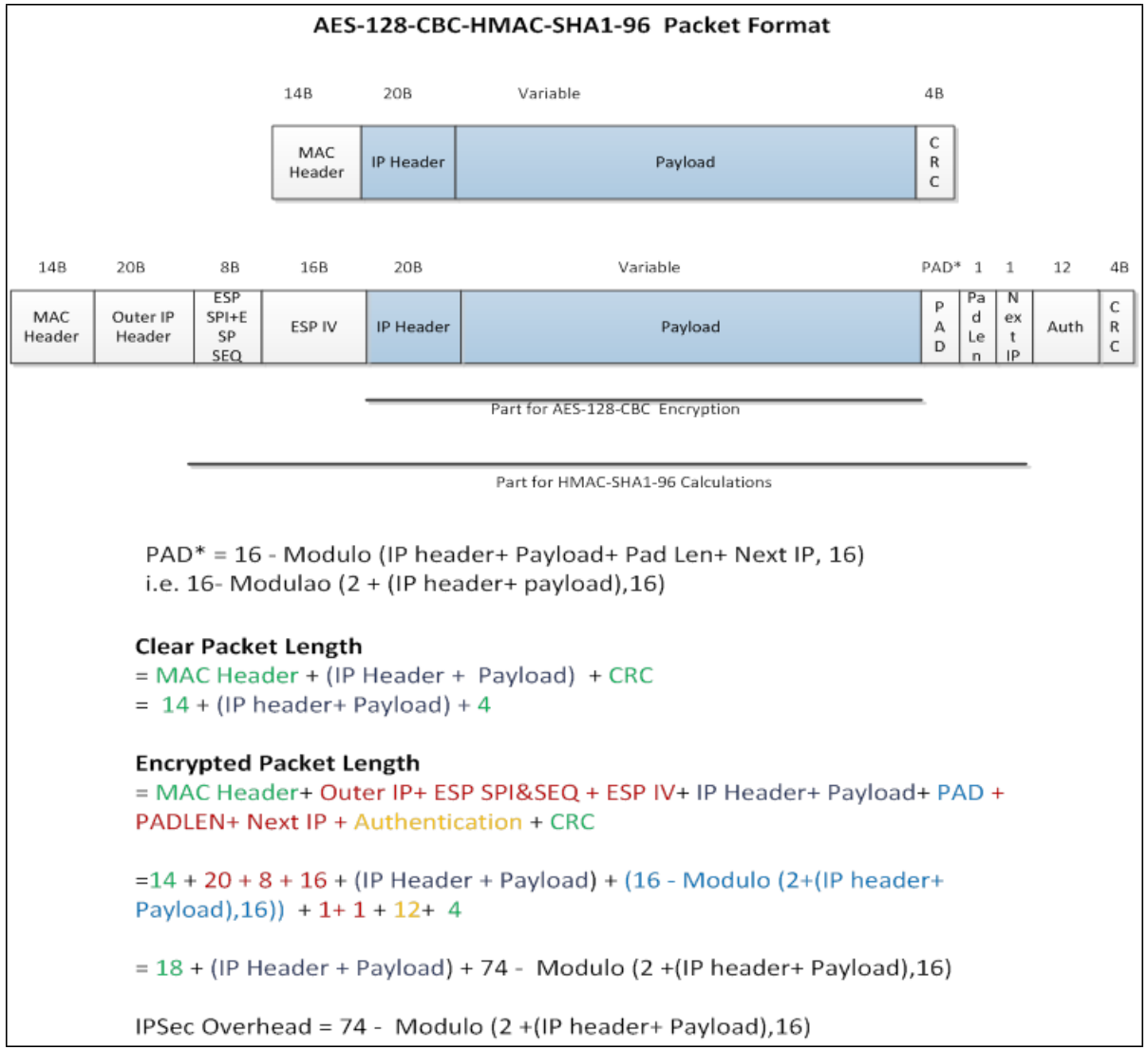


Understanding IPSEC performance numbers



Backup

IPSec Packet Format



PAD* = 16 - Modulo (IP header+ Payload+ Pad Len+ Next IP, 16)
i.e. 16- Modulao (2 + (IP header+ payload),16)

Clear Packet Length
= MAC Header + (IP Header + Payload) + CRC
= 14 + (IP header+ Payload) + 4

Encrypted Packet Length
= MAC Header+ Outer IP+ ESP SPI&SEQ + ESP IV+ IP Header+ Payload+ PAD + PADLEN+ Next IP + Authentication + CRC

=14 + 20 + 8 + 16 + (IP Header + Payload) + (16 - Modulo (2+(IP header+ Payload),16)) + 1+ 1 + 12+ 4

= 18 + (IP Header + Payload) + 74 - Modulo (2 +(IP header+ Payload),16)

IPSec Overhead = 74 - Modulo (2 +(IP header+ Payload),16)