



IBM Software Group

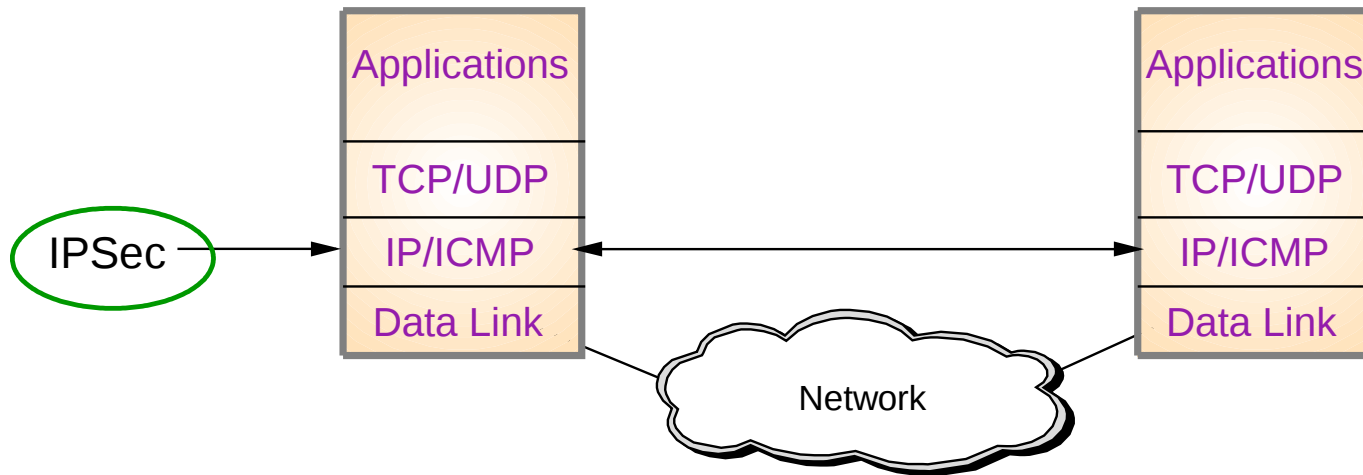
z/OS Communications Server zIIP Assisted IPsec

Enterprise Network and Transformation Solutions

Michael Fitzpatrick

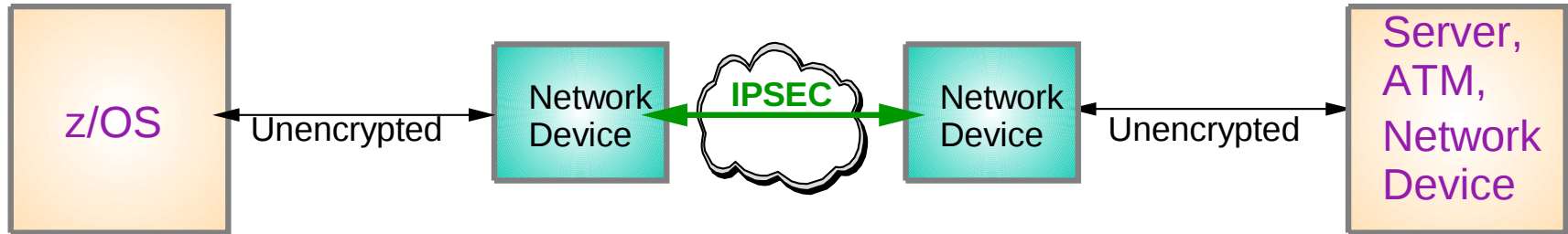
mfitz@us.ibm.com

IPSec Overview

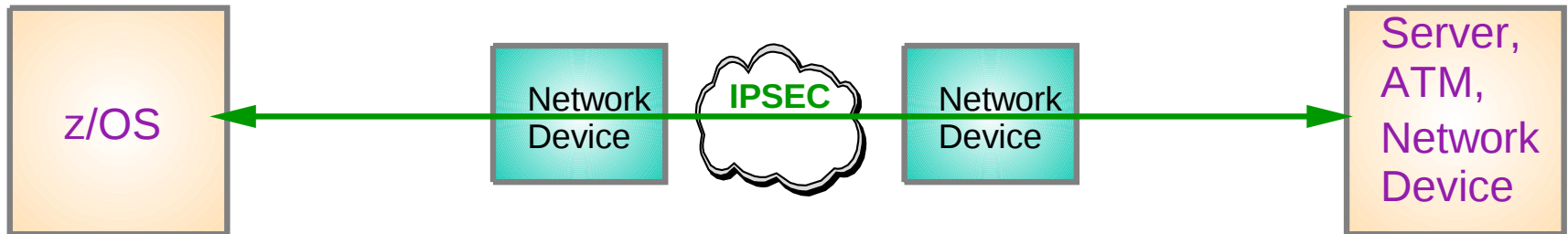


- Open network layer security protocol endorsed by IETF
- Provides authentication, integrity, and data privacy via IPSec security protocols
 - ▶ Authentication Header (AH) - provides authentication / integrity
 - ▶ Encapsulating Security Protocol (ESP) - provides data privacy with optional authentication/integrity
- Secures traffic between any two IP resources
 - ▶ Security Associations (SA)
- Management of crypto keys and security associations can be
 - ▶ manual
 - ▶ automated via key management protocol (IKE)

IPSec Overview...



- IPSec provides end-to-end network encryption
- End-to-end network encryption is becoming more pervasive due to regulatory security policies
- End-to-end network encryption is also becoming a requirement for companies that outsource/share part of their network with business partners and need to have greater control of access to confidential data



Specialty Engines

- Integrated Facility for Linux (IFL)
 - ▶ Provides additional processing capacity for Linux workloads without affecting IBM software charges

- System z Application Assist Processor (zAAP)
 - ▶ Provides ability to lower costs of CPU-intensive web-based applications (i.e. Java, XML)

- System z9 Integrated Information Processor (zIIP)
 - ▶ Provides ability to lower costs for select data and transaction processing workloads
 - ▶ DB2/DRDA exploits zIIPs for portions of their workloads
 - ▶ Communications Server exploits zIIPs for portions of their IPsec workloads

Cryptographic Hardware

■ Crypto coprocessors

- ▶ Available on previous generations of zSeries
 - General CP with “built-in” crypto functions
- ▶ Provides hardware encryption/decryption
 - Unit of work must be running on this processor

■ Crypto cards

- ▶ Available on z/990, z/9, and z/10
 - PCIX Cryptographic card (PCIXCC)
 - CryptoExpress2 card (CEX2C)
- ▶ Provides hardware RSA signature generation/verification for peer authentication during IKE negotiations

■ Hardware instructions

- ▶ Available on z/990, z/9, and z/10
 - CP Assist for Cryptographic Function (CPACF)
- ▶ Provides hardware encryption/decryption and authentication
 - Unit of work can be running on any general CP

What is zIIP-Assisted IPsec?

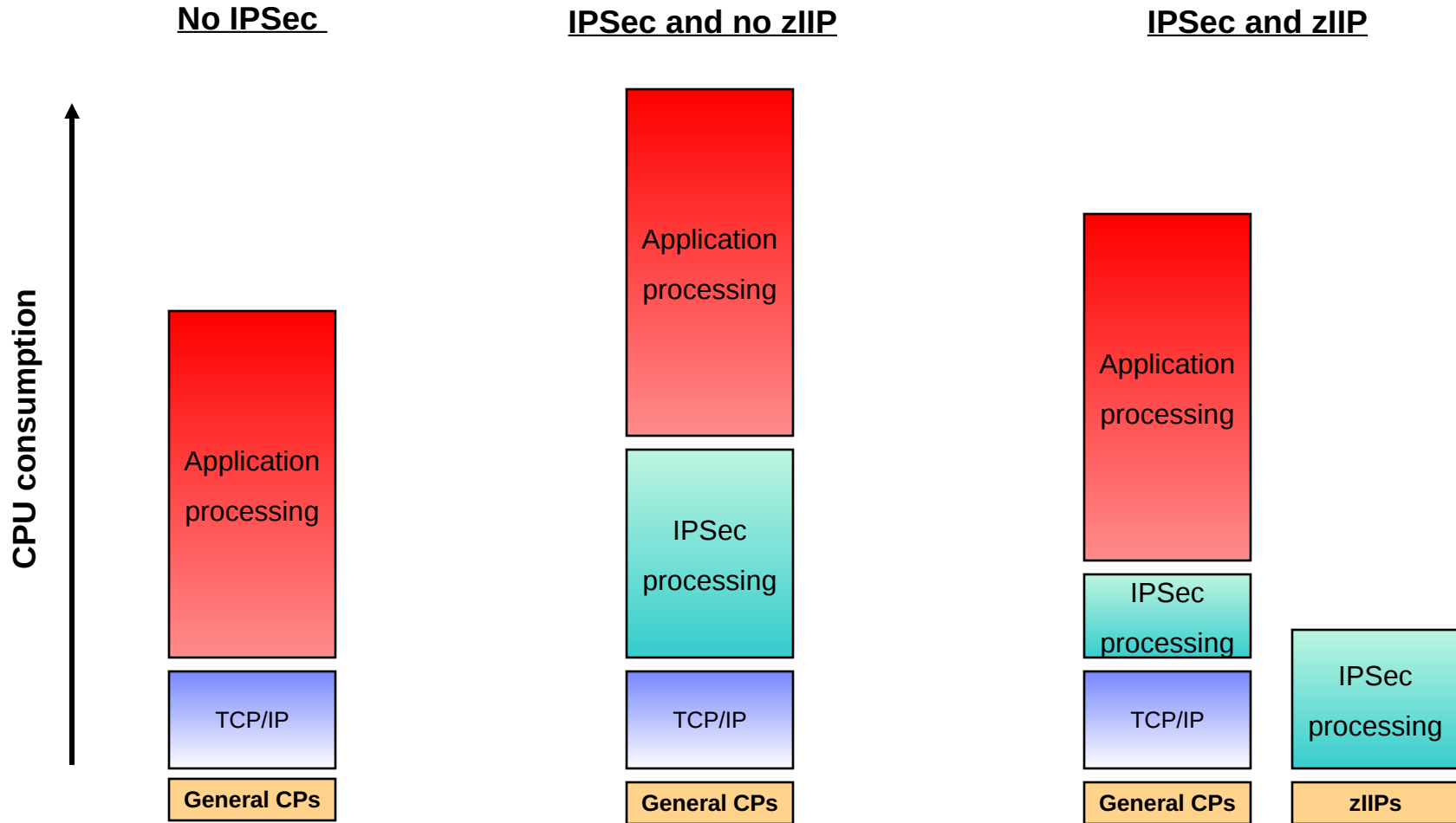
- Even with zSeries specialized Crypto hardware, data encryption/decryption and authentication processing can incur very heavy CPU consumption
- zIIP-Assisted IPsec allows for the movement of the bulk of Communications Server IPsec processing from general CPs to zIIPs
 - ▶ SRB-mode IPsec protocol traffic directed to zIIPs
 - Encryption/decryption, message authentication, and IPSEC header processing
 - Work is assigned to an independent WLM enclave
- Will provide CPU-busy relief on general CPs for customers already running IPsec on z/OS
- Makes z/OS IPsec deployment more attractive for customers concerned about IPsec CPU consumption
 - ▶ IBM does not impose software charges for zIIP capacity
- Does not replace CPACF
 - ▶ Simply performs CPACF instruction on zIIP rather than on a general CP

Performance impact of zIIP-Assisted IPsec

- When compared to using no network security protocols, enabling IPsec using zIIPs on z/OS V1R10
 - ▶ For interactive traffic
 - 5% increase in CPU on general CP per transaction
 - ▶ For inbound bulk transfers
 - 4% increase in CPU on general CP per Mbyte
 - ▶ For outbound bulk transfers
 - 14% increase in CPU on general CP per Mbyte
 - ▶ For inbound and outbound bulk transfers
 - 4% drop in throughput

More details on measurement environment and what was measured are on page “Performance Measurements”

Potential benefit of zIIP-Assisted IPSec



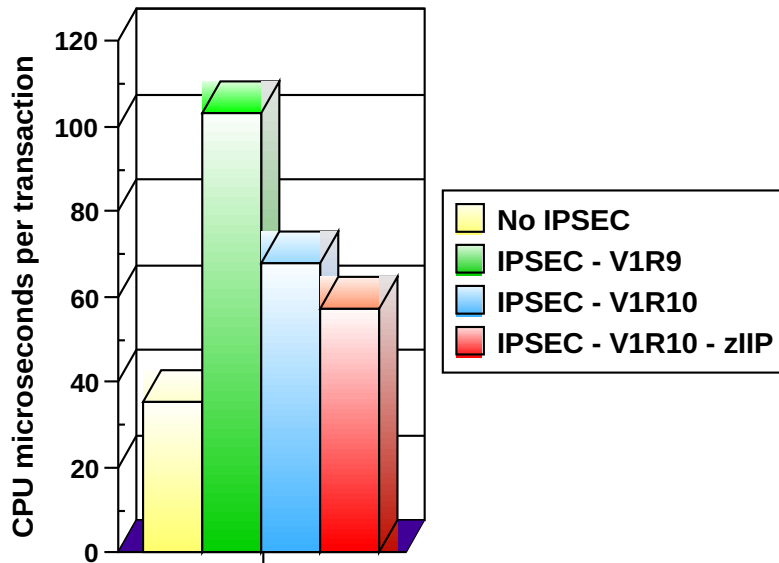
Performance Measurements

- Disclaimer
 - ▶ The performance data discussed in this presentation was collected using a dedicated system environment, so the results obtained in other configurations or operating system environments may vary
- The benchmarks used in this presentation were obtained using the Application Workload Modeler (AWM) for z/OS
 - ▶ For more information, visit the Application Workload Modeler website at <http://www.ibm.com/software/network/awm/index.html>
- All CPU consumption measurements are for networking CPU
 - ▶ Refers to CPU used in the TCPIP stack, Unix System Services, and MVS IOS, Scheduling, and Dispatcher cycles involved in networking flows
 - Typically contributes 8% of total CPU for interactive workloads
 - Typically contributes 30% of total CPU for bulk workloads
- All measurements collected on z/10 model 2097-752 LPARs with 2 dedicated general CPs and 0 - 1 dedicated zIIPs per LPAR running Communications Server
 - ▶ IPsec configuration utilized Triple-DES encryption with SHA authentication
 - ▶ V1R10 provides optimizations for IPSEC versus V1R9
 - ▶ zIIP-assisted IPSEC provides TCP flow-control changes for bulk data transfers

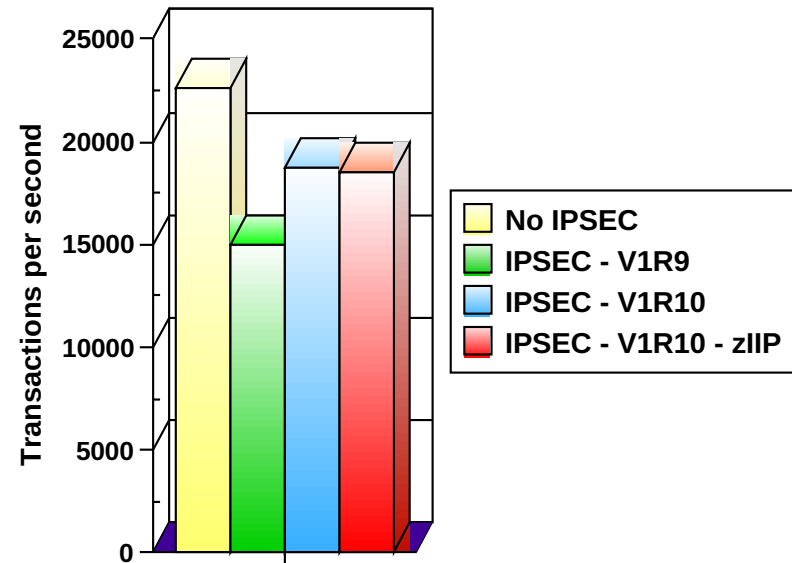
Interactive workload Measurements

- 10 concurrent interactive sessions sending/receiving 100 bytes

General CPU Consumption



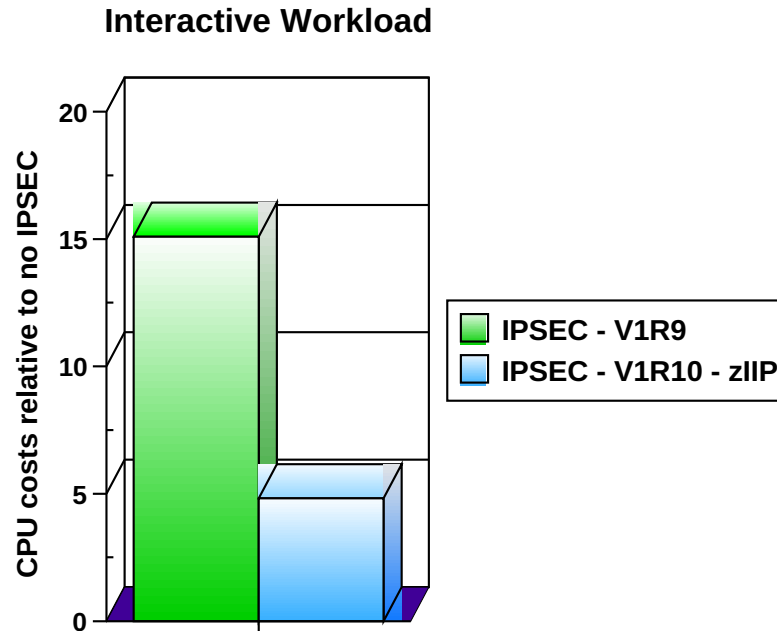
Raw Throughput



- With zIIPs and V1R10, networking CPU for IPsec drops from an 189% increase to a 61% increase compared to non-secured
- Regardless of zIIPs, overhead of IPsec processing adds latency which results in 17% lower transaction rate compared to non-secure

“Normalized” Interactive workload Measurements

- IPSEC impact to CPU consumption (based on 8% networking costs)

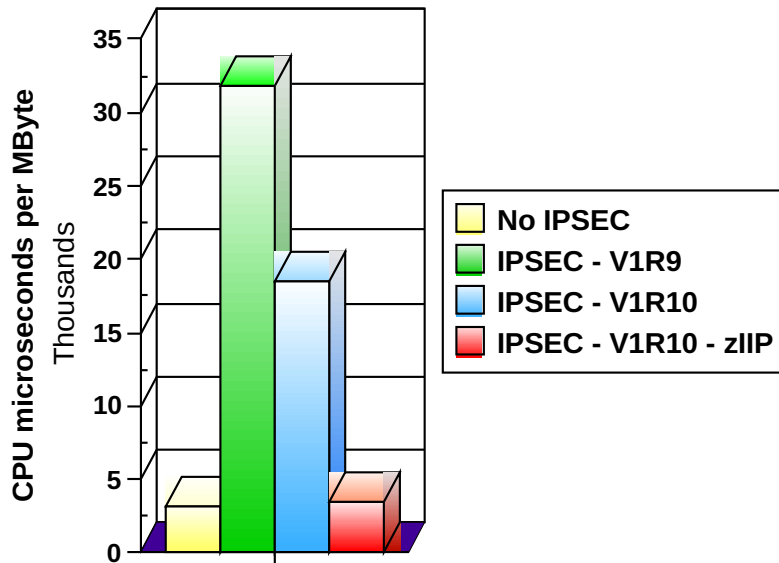


- For interactive traffic, enabling IPSEC results in a 5% increase in CPU per transaction when using zIIPs on V1R10

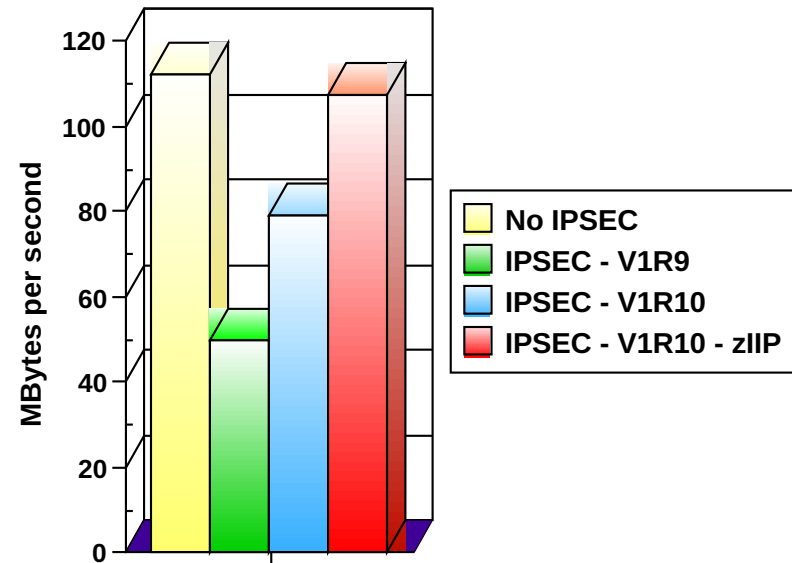
Inbound Bulk workload Measurements

- 5 concurrent streaming sessions sending 1 byte and receiving 20 Mbytes

General CPU Consumption



Raw Throughput

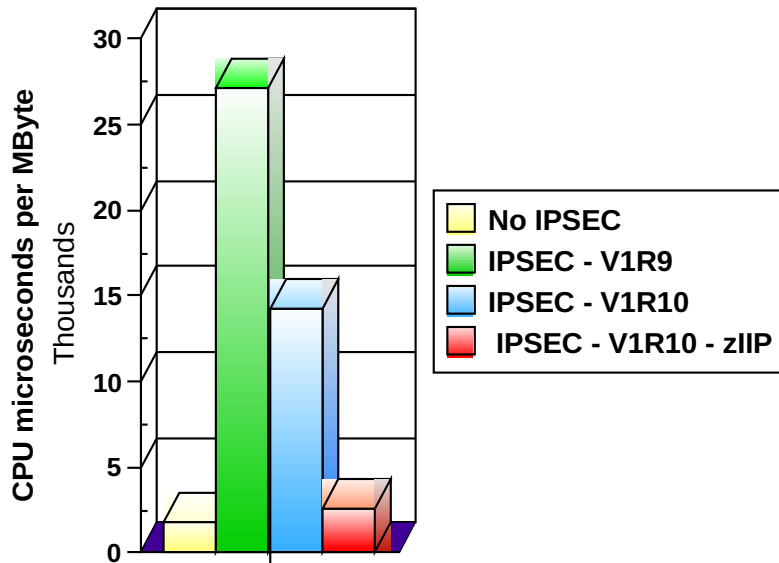


- With zIIPs and V1R10, networking CPU for IPsec drops from a 912% increase to a 13% increase compared to non-secured
- Algorithm changes with zIIP and V1R10 optimizations reduces throughput gap from 56% to 4% compared to non-secure

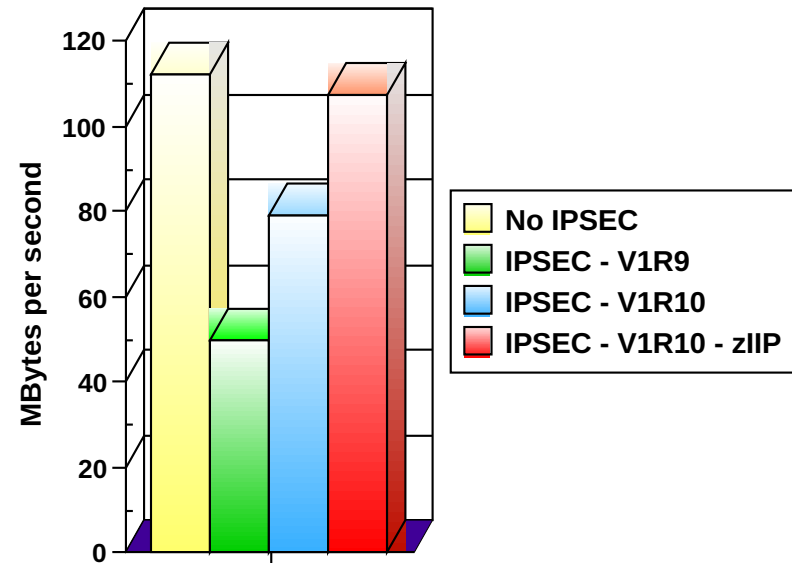
Outbound Bulk workload Measurements

- 5 concurrent streaming sessions sending 20 Mbytes and receiving 1 byte

General CPU Consumption



Raw Throughput

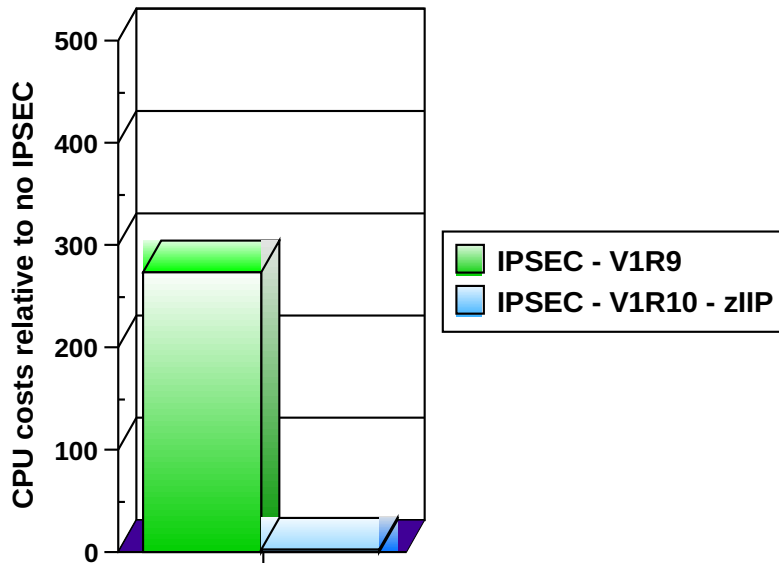


- With zIIPs and V1R10, networking CPU for IPsec drops from a 1405% increase to a 45% increase compared to non-secured
- Algorithm changes with zIIP and V1R10 optimizations reduces throughput gap from 56% to 4% compared to non-secure

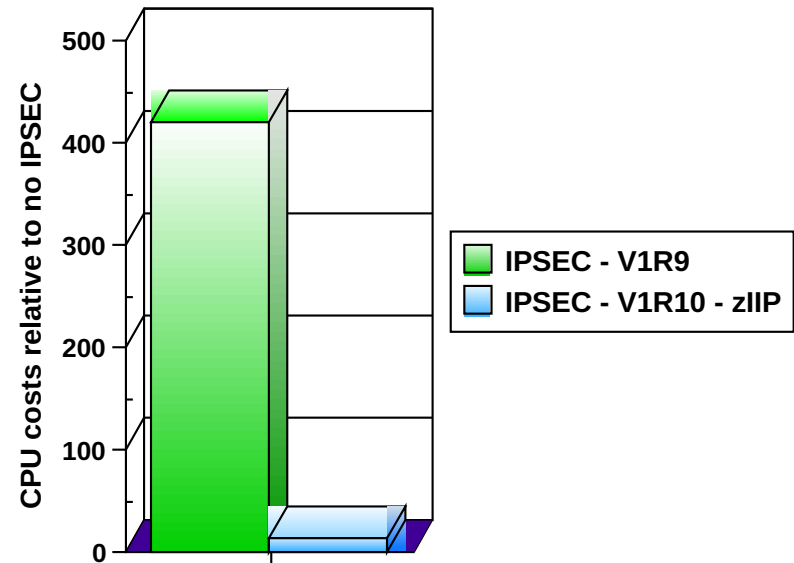
“Normalized” Bulk workload Measurements

- IPSEC impact to CPU consumption (based on 30% networking costs)

Inbound Bulk Workload



Outbound Bulk Workload



- For inbound bulk transfers, enabling IPSEC results in a 4% increase in CPU per Mbyte when using zIIPs on V1R10
- For outbound bulk transfers, enabling IPSEC results in a 14% increase in CPU per Mbyte when using zIIPs on V1R10