# Network Overlay and Crypto Service

Heqing Zhu & Ping Yu
Intel

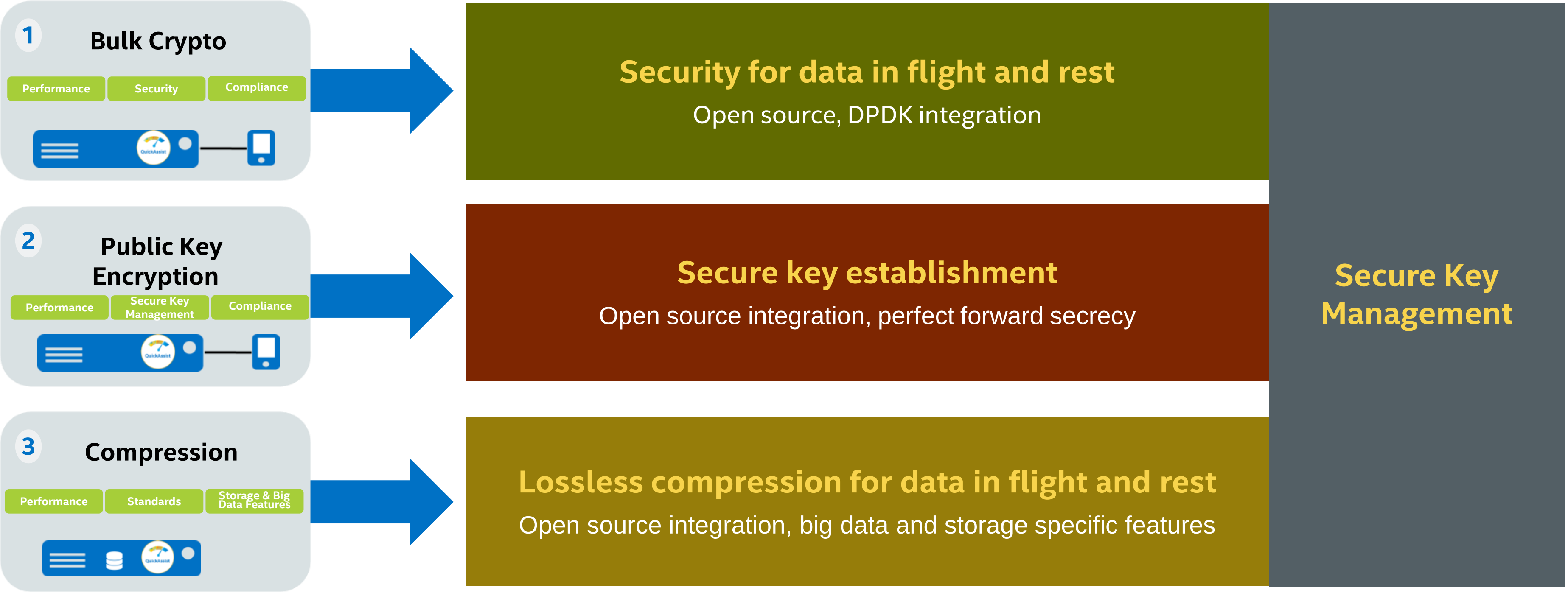
# Agenda

- Ingredient introduction
  - Intel QAT Overview
  - Intel AES-NI introduction
  - DPDK Cryptodev Framework
  - Intel hyperscan framework
- Crypto service in network overlay
  - overlay security
  - content security
  - application security
- Key Takeaway

# PART 1: INTEL INGREDIENT

# Intel® QuickAssist Technology

## Designed to optimize the use and deployment of crypto and compression hardware accelerators



1 Bulk Crypto

Performance | Security | Compliance

2 Public Key Encryption

Performance | Secure Key Management | Compliance

3 Compression

Performance | Standards | Storage & Big Data Features

**Security for data in flight and rest**

Open source, DPDK integration

**Secure key establishment**

Open source integration, perfect forward secrecy

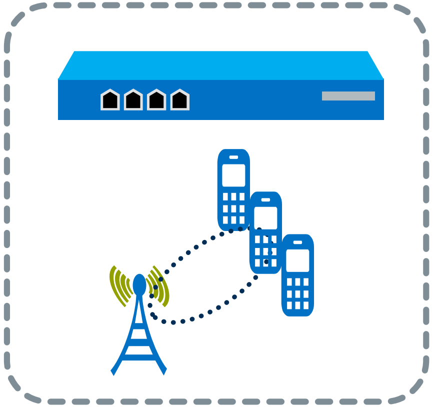
**Lossless compression for data in flight and rest**

Open source integration, big data and storage specific features

**Secure Key Management**

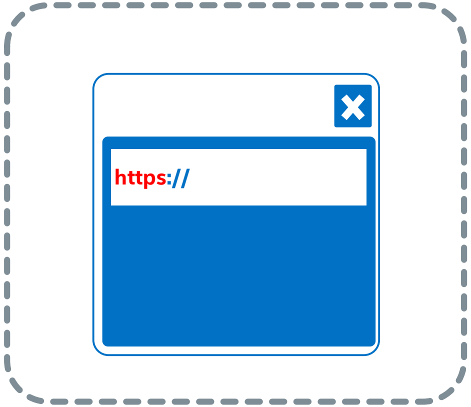
# Intel® QAT Use Cases

## Packet Processing



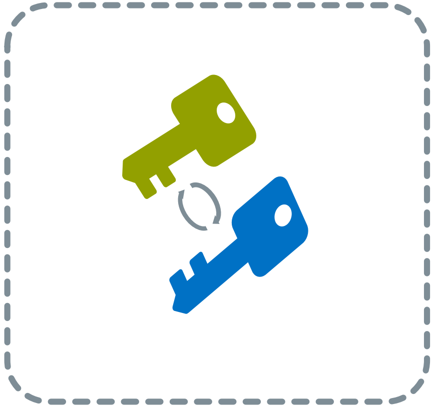
- Wired and Wireless
- Routers
- Gateways
- 3G / 4G LTE Infrastructure
- Firewalls
- Security Appliances

## Security Protocol



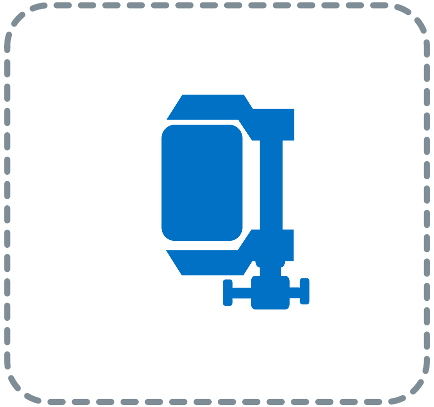
- Secure Browsing
- Email
- Search Results
- BYOD
- HTTP 2.0
- Secure Socket Layer (SSL)
- Transport Layer Security (TLS)

## Key Exchange



- RSA Public-Key Exchange
- Perfect Forward Secrecy

## Compression



- Big Data Analytics
- Storage

**Security and Compression Workloads—Ready for Optimization**

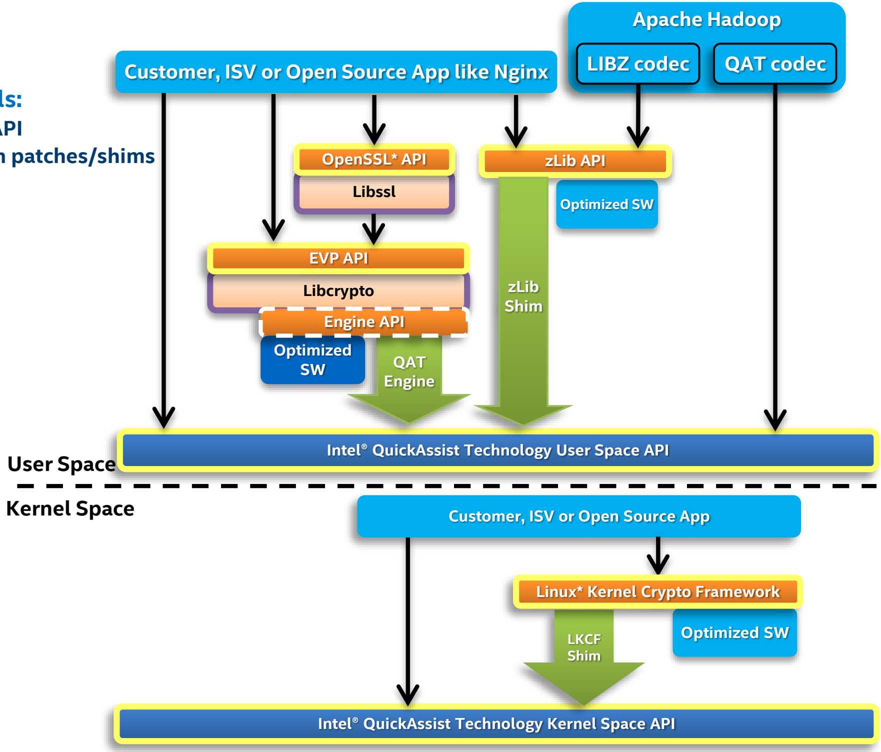
# Intel® QAT Software Architecture

**Application may integrate at multiple levels:**

1. Program to Intel® QuickAssist Technology API
2. Program to open source framework through patches/shims

- Application Layer
- Open Source SW
- QA Offload Shim
- IA Optimized SW
- Intel® QuickAssist Technology API

| Service | Open Source Frameworks | Open Source Applications |
|---|---|---|
| Cryptography | • OpenSSL* libcrypto<br>• Linux* Kernel Crypto API (scatterlist) | • IPsec (NETKEY) |
| Data Compression | • Zlib<br>• Apache Hadoop<br>• Linux Kernel Crypto API (scatterlist) | • File compression (minigzip)<br>• IPComp (NETKEY) |



Apache Hadoop
LIBZ codec
QAT codec
Customer, ISV or Open Source App like Nginx
OpenSSL* API
Libssl
zLib API
Optimized SW
EVP API
Libcrypto
zLib Shim
Engine API
Optimized SW
QAT Engine
Intel® QuickAssist Technology User Space API
User Space
Kernel Space
Customer, ISV or Open Source App
Linux* Kernel Crypto Framework
LKCF Shim
Optimized SW
Intel® QuickAssist Technology Kernel Space API

# Data Protection with Intel® AES-NI

Enhanced

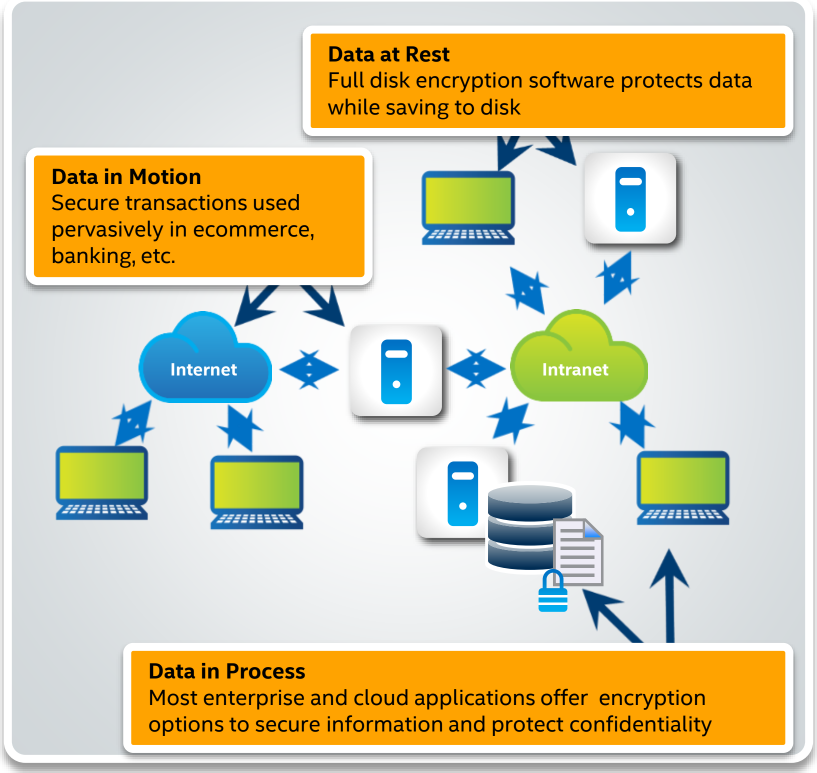
*Efficient Ways to Use Encryption for Data Protection*

**Intel® AES-NI**:

Special math functions built in the processor accelerate AES

- Includes 7 new instructions

Makes enabled encryption software faster and stronger

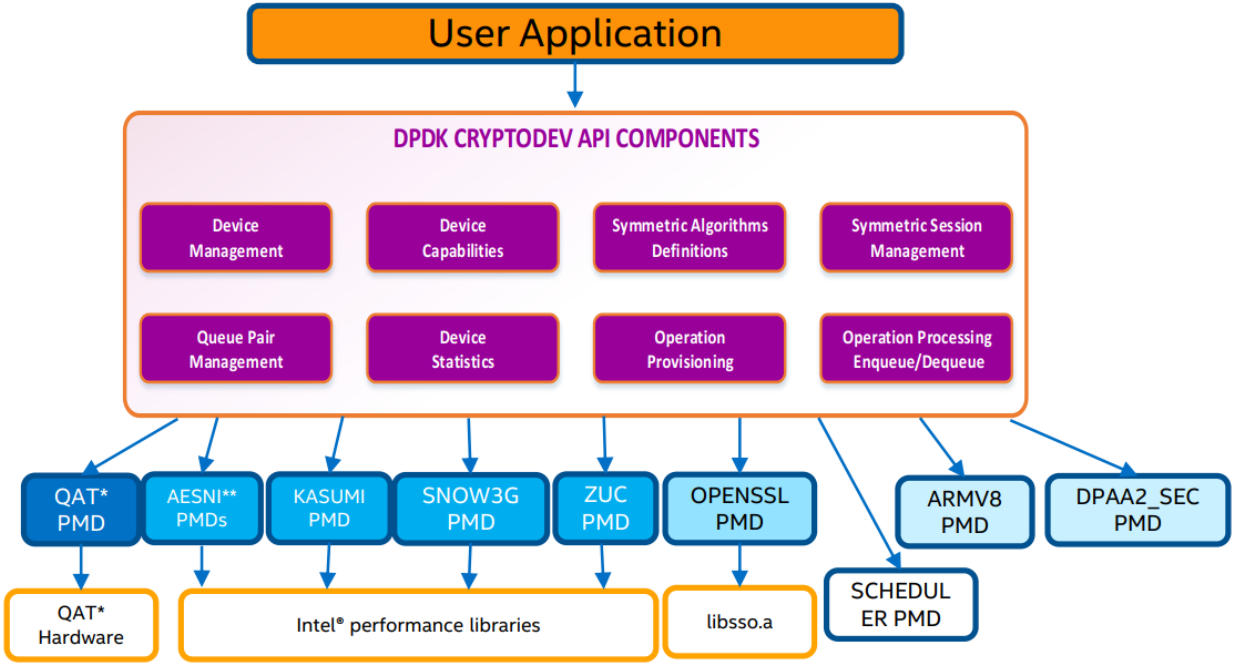


**Data at Rest**
Full disk encryption software protects data while saving to disk

**Data in Motion**
Secure transactions used pervasively in ecommerce, banking, etc.

**Data in Process**
Most enterprise and cloud applications offer  encryption options to secure information and protect confidentiality

# DPDK Cryptodev Framework



- Crypto framework for processing symmetric crypto workloads.
- DPDK Cryptodev consists of:
  - SW and HW Crypto PMDs
  - A standard API supports all PMDs
  - Multi-queues for multi-thread sharing
- Effortless migration (SW-HW)

# Hyperscan Overview

- Hyperscan is a regular expression matching library
  - Zero cost Software-only, IA specific (requires SSSE3 as a baseline!)
  - Open Source (BSD), Business friendly
  - Run seamlessly on Xeon, Core and Atom processors
  - Match “Rulesets” on data blocks or packet streaming
  - Callback if match found. Flexible and powerful

SNORT® SURICATA

3~6x

IDS/IPS

ntop

**Linear Core Scaling**

SD-WAN/DPI

NGiNX modsecurity Open Source Web Application Firewall NAXSI

Network and Web Security Save CPU cycles about 20%

# Hyperscan: An industry fastest Regular Expression, Literal Matching Algorithm on Intel platform, BSD License, Free open source project

## Applications

Integrated Open Source Solutions and User Cases (40+ Customers, 37 Open Source Projects)

SNORT SURICATA

IDS/IPS

ntop

SD-WAN/DPI

modsecurity Open Source Web Application Firewall NGINX NAXSI

Network and Web Security

## Language Bindings

golang Java python

Extensive, Seamless, Software Acceleration With Intel

Email Virus, Network visibility, Data Analytic

MariaDB

## Operating Systems

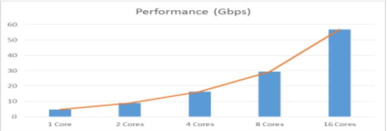
FreeBSD fedora ubuntu debian gentoo linux Windows OS X

## Intel Architectures

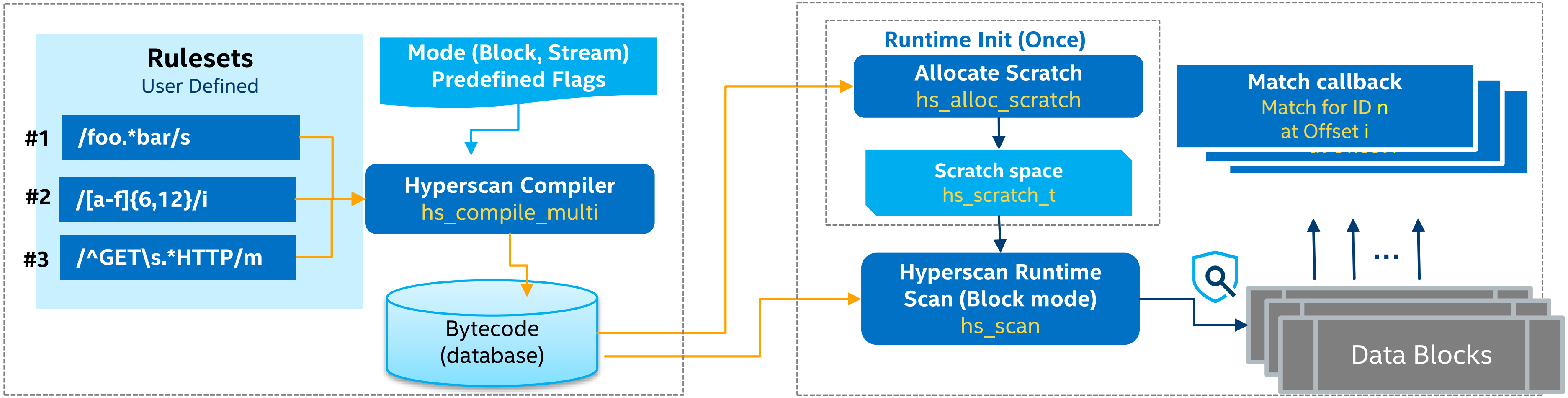
Seamless Support from Atom to Xeon processor

intel inside ATOM … intel inside CORE i5 … intel inside XEON

Linear Core Scalability, Intel Optimized



# How Hyperscan works: Repeatable process



Rulesets

User Defined

#1 /foo.*bar/s

#2 /[a-f]{6,12}/i

#3 /^GET\s.*HTTP/m

Mode (Block, Stream)
Predefined Flags

Hyperscan Compiler
hs_compile_multi

Bytecode
(database)

Runtime Init (Once)

Allocate Scratch
hs_alloc_scratch

Scratch space
hs_scratch_t

Hyperscan Runtime
Scan (Block mode)
hs_scan

Match callback
Match for ID n
at Offset i

…

Data Blocks

Phase 1: Compilation
at initialization phase

Phase 2: Data Searching & Match, Further
Processing Phase

**From 0 to 5K servers**

Quick POC with Simple APIs, 1 week integration

From integration to full validation 3~6 months

Online adoption from 1 to 5K servers, 6~9 Months

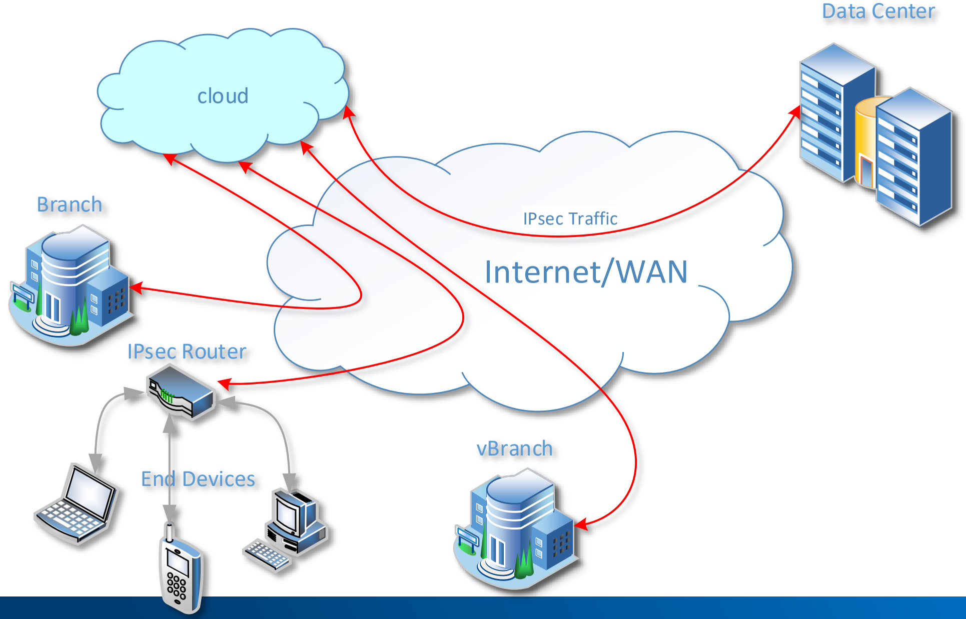
# PART 2: CRYPTO SERVICE IN NETWORK OVERLAY

# Crypto service in network

- Overlay security
- Content security
- Application security

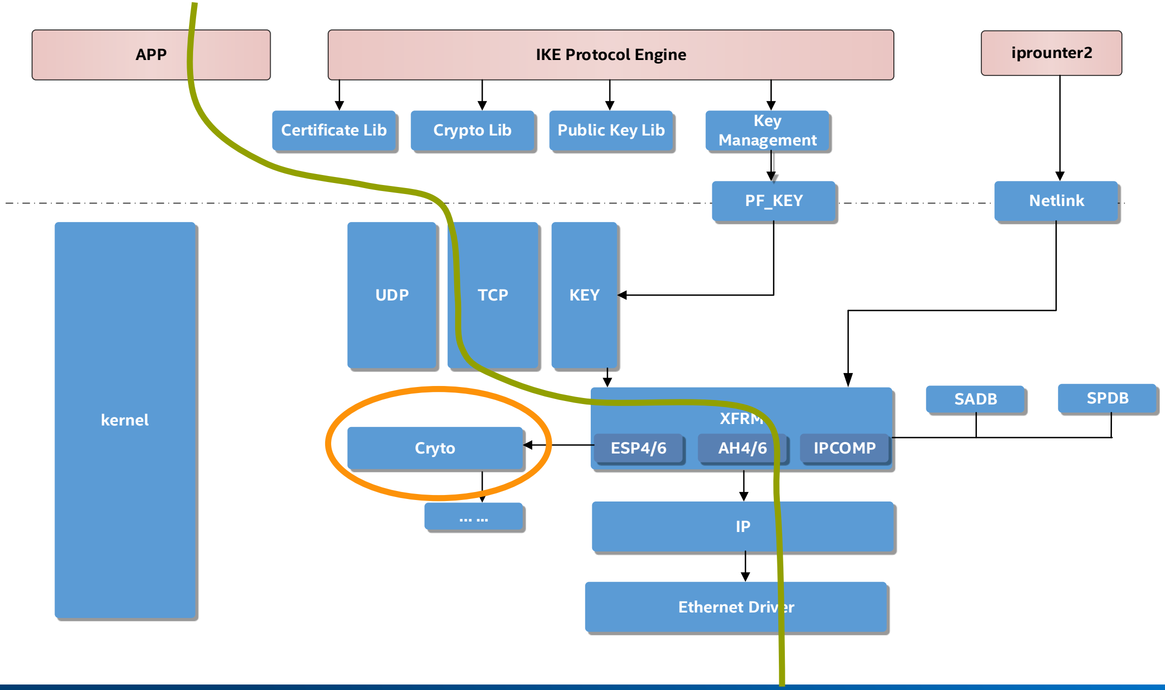
# Let’s take IPSec as an example

- > 20 years old but is still extremely popular
- Playing the role of security guardian in many network applications



# IPSec Overhead

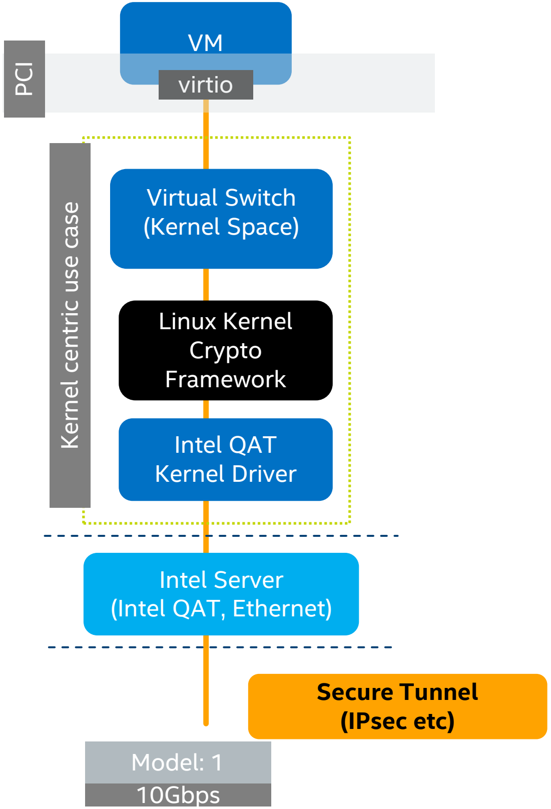
- Memory movements between User/Kernel
- Cost of crypto operations



# Crypto service in both Kernel space and user space

- Linux Kernel
  - LKCF
  - QAT kernel space SDK
- User space:
  - Cryptodev

# Secure Virtual Switching with QAT/IPsec in Kernel



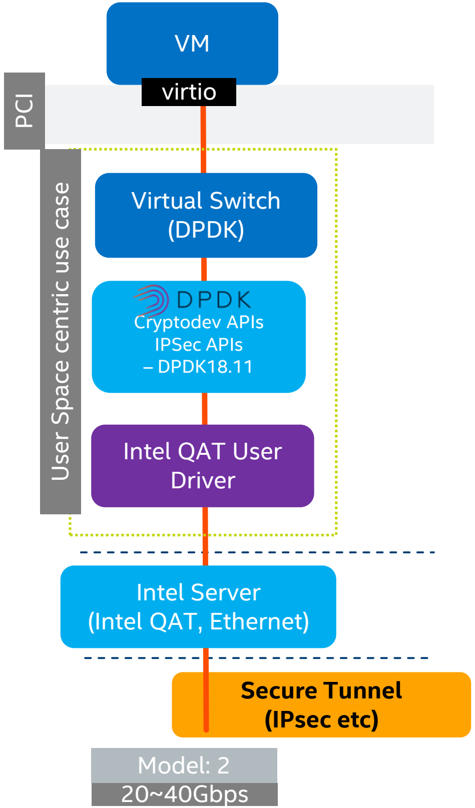
VM
virtio
PCI
Kernel centric use case
Virtual Switch (Kernel Space)
Linux Kernel Crypto Framework
Intel QAT Kernel Driver
Intel Server (Intel QAT, Ethernet)
Secure Tunnel (IPsec etc)
Model: 1
10Gbps

- Guest is not aware of QAT acceleration
- Host leverages Linux kernel for IPsec
- QAT driver is staying behind Linux stack, integrated.
- Out of box experience or pre-configured

**Status:**

- Technical ingredients are ready
- Not integrated /tested with OVS and TF yet

# Secure Virtual Switching with QAT/IPsec in User space



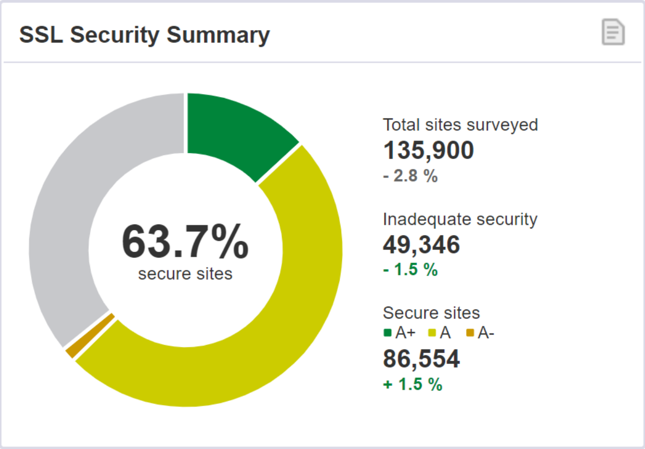
- Guest is not aware of QAT acceleration
- Host leverages IPSec APIs in DPDK 18.11
- QAT driver is hidden under DPDK Cryptodev APIs

**Status:**

- Technical ingredients are Not ready
- Not integrated /tested with OVS and TF yet.

# TLS everywhere

## Monthly Scan: October 03, 2018



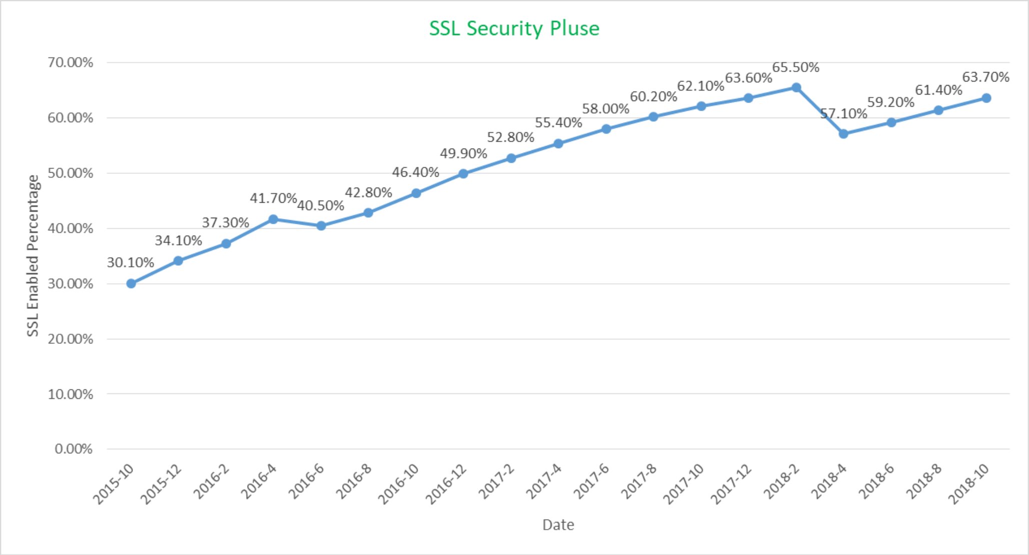
### SSL Security Summary

63.7%
secure sites

Total sites surveyed
**135,900**
- 2.8 %

Inadequate security
**49,346**
- 1.5 %

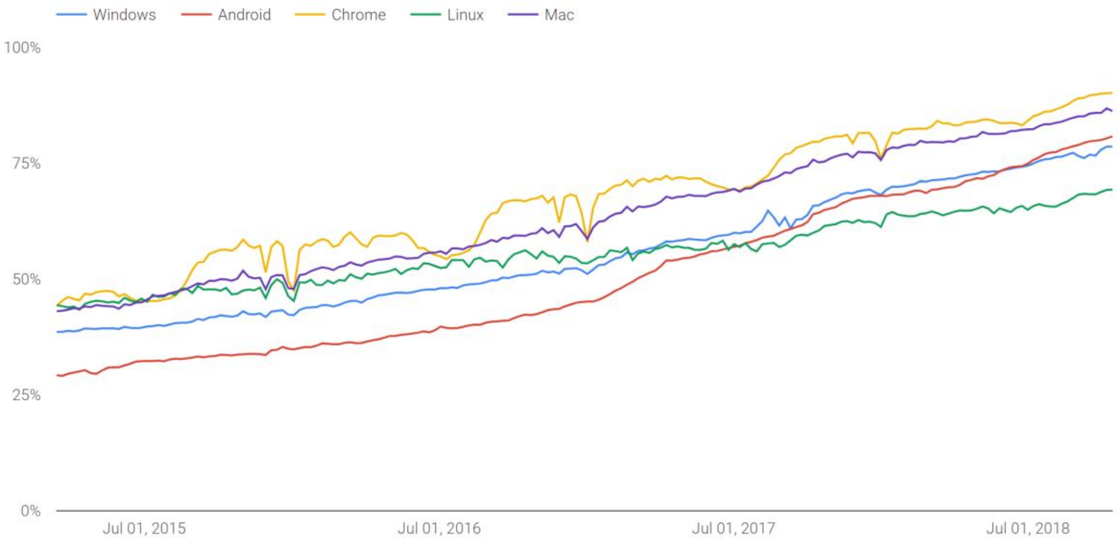
Secure sites
🟩 A+ 🟨 A 🟧 A-
**86,554**
+ 1.5 %



https://www.ssllabs.com/ssl-pulse/

# TLS traffic increases

Percentage of pages loaded over HTTPS in Chrome by platform

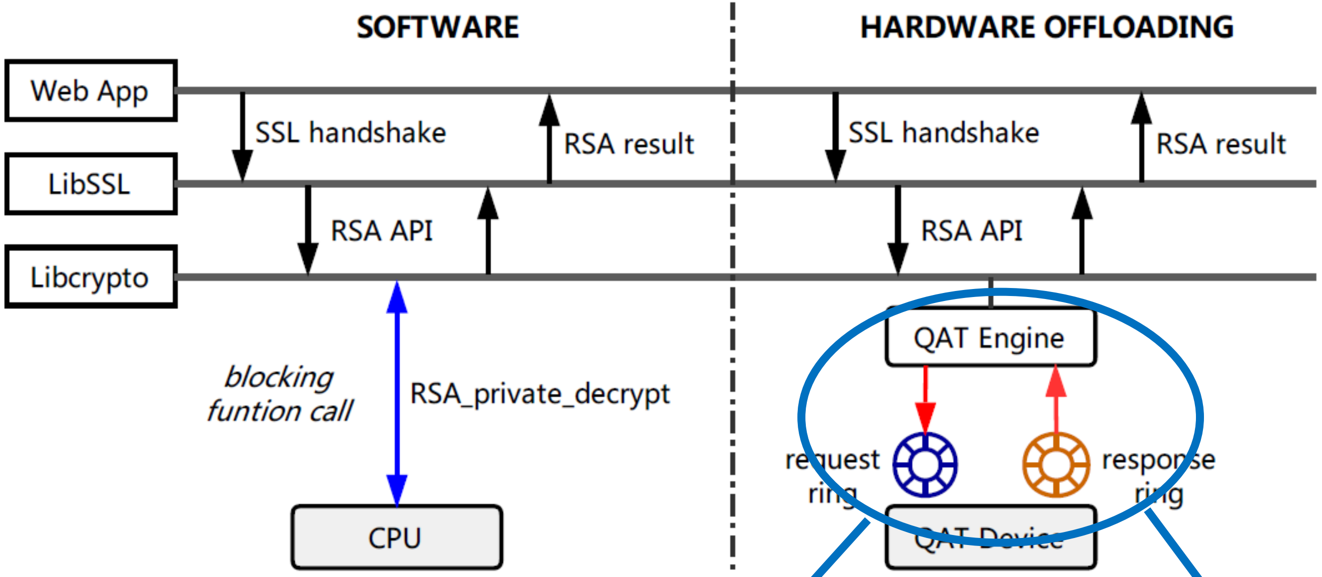


Fragment navigations, history push state navigations, and all schemes besides HTTP/HTTPS (including new tab page navigations) are not included.

Application security protect for QUIC/HTTPS/SSH

https://transparencyreport.google.com/https/overview?hl=en

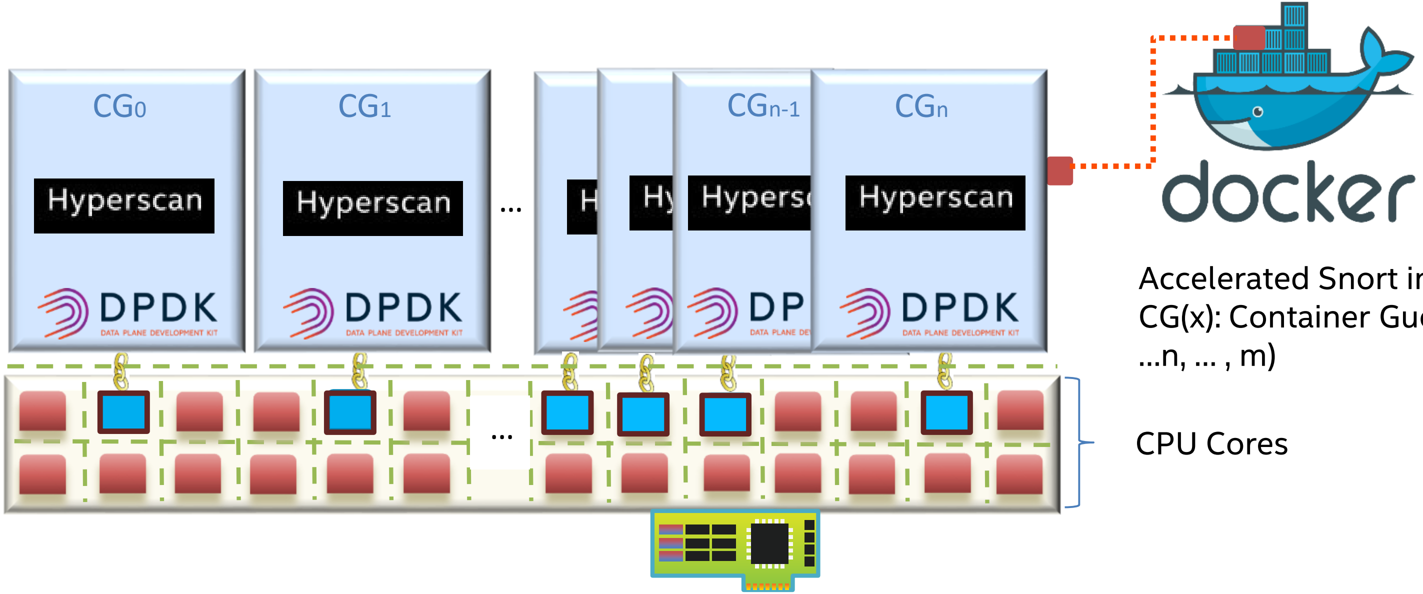
# Hardware Acceleration



**Blocking?**
**Synchronous Mode**

**Non-blocking?**
**Asynchronous Mode**

# Accelerated IDS Container Instances

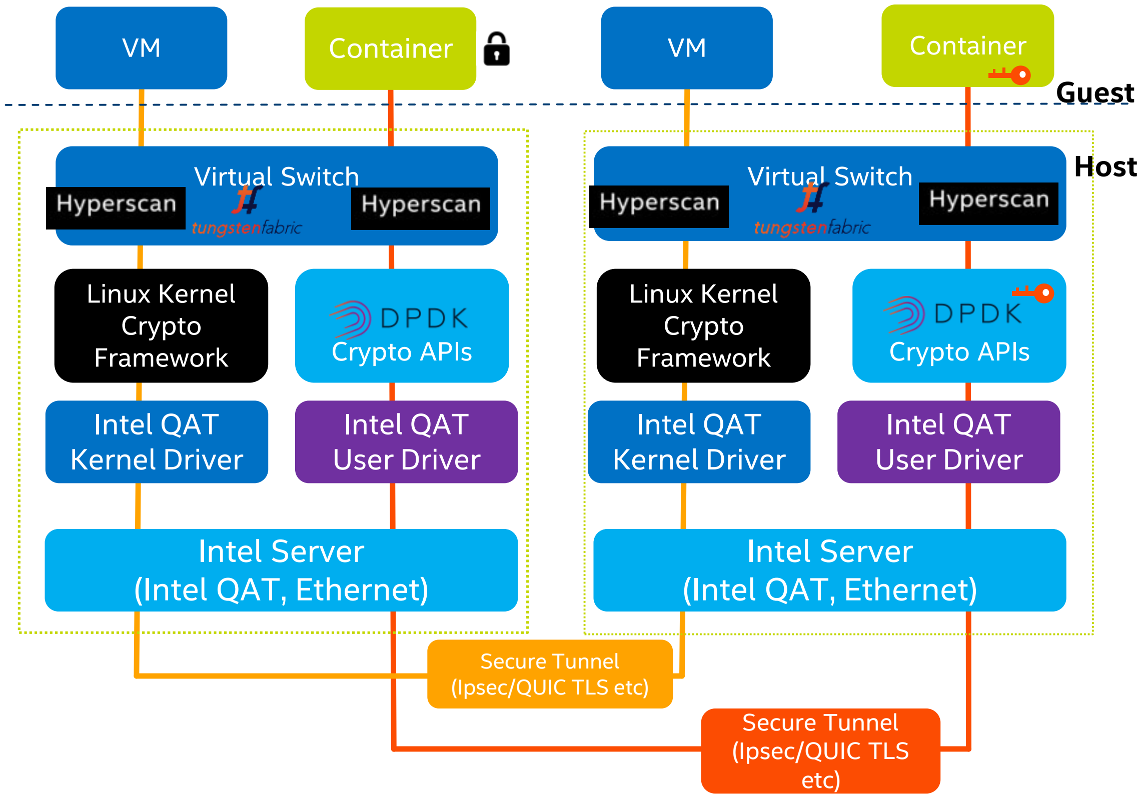

CG0
Hyperscan
DPDK
DATA PLANE DEVELOPMENT KIT
CG1
Hyperscan
DPDK
DATA PLANE DEVELOPMENT KIT
…
CGn-1
Hyperscan
CGn
Hyperscan
DPDK
DATA PLANE DEVELOPMENT KIT
…
docker

Accelerated Snort instances
CG(x): Container Guest x (x=1,2, …n, … , m)

CPU Cores

**Running Multiple IDS instances in NFV/Container with DPDK/Hyperscan**
**Linear core performance scalability**

# Deploy Model of network overlay crypto service



# Key takeaway

- Intel provides rick hardware and software ingridients for network overaly crypto service, such as QAT, AES-NI, DPDK Cryptodev, hyperscan.
- Provide solution to different crypto service model, such as overlay security, content security & application security.

# Thank you !

# Q & A