CryptoPanel

edycja #12

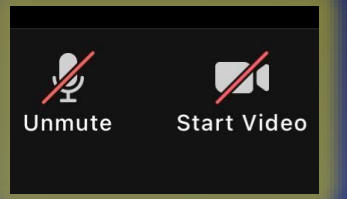
Już za moment zaczynamy...

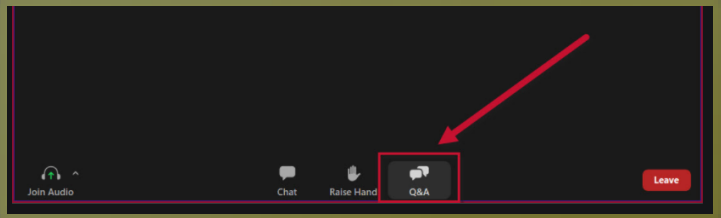
CryptoPanel

THALES

CLICO

CryptoPanel





CryptoPanel

edycja #12

W infrastrukturze hybrydowej: cloud in on-prem wymaga się wydajnej i niezawodnej a jednocześnie wysoce bezpiecznej transmisji danych pomiędzy zasobami.
Czy i jak można sobie z tym poradzić?

CryptoPanel

dziś dyskutują

Piotr Majek

Security Specialist
piotr.majek@clico.pl
mob. +48 663 994 996

Jarosław Ulczok

Pre-sales Consultant
Jaroslaw.Ulczok@thalesgroup.com
mob. +48 603 056 667

CryptoPanel

problem

co nas boli...

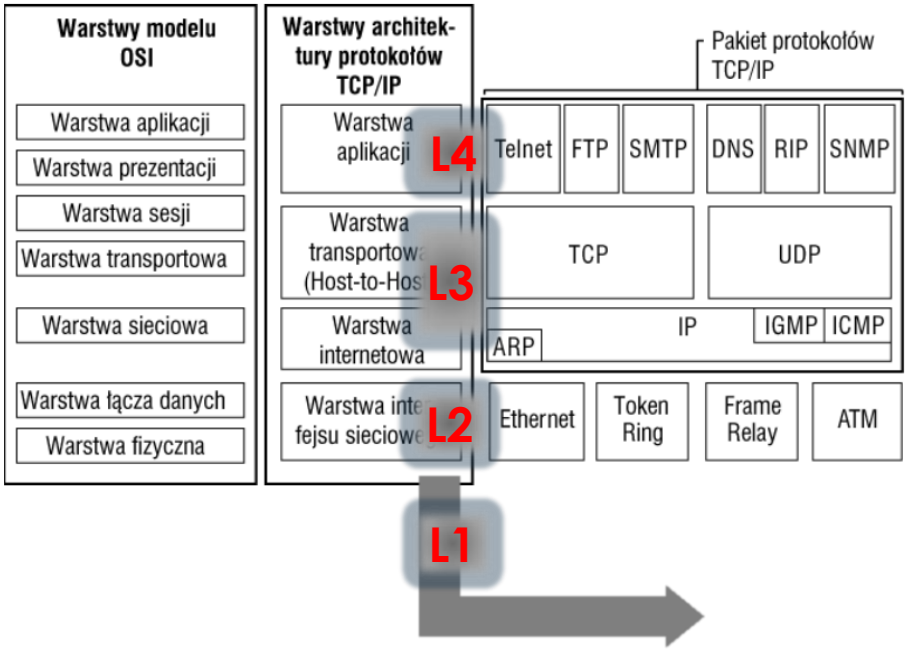
- **Jesteśmy przedsiębiorstwem z branży zbrojeniowej**
- **Korzystamy z zasobów lokalnych i kilku chmur**
- **Chcemy zaszyfrować ruch pomiędzy swoimi zasobami zarówno:**
  - Większymi lokalizacjami (zakłady, ośrodki badawcze)
  - Biurami
  - Chmurami (publiczne i „branżowe")
  - Pojedynczymi zasobami (lokalnie lub w chmurze)
- **Do ochrony komunikacji niejawnie/tajnej posiadamy osobną infrastrukturę**
- **Nie posiadamy infrastruktury sieciowej jednego typu**
  - Eksploatujemy m.in. Metroethernet, bezpośrednie łącza światłowodowe, MPLS, „IP-VPN", GSM, ..)
  - Planujemy jej rozbudowę

- **w jakie rozwiązanie zainwestować?**
- **jak zapewnić bezpieczeństwo ruchu do/z CSP bez korzystania z ich VPN?**
- **interesuje nas coś więcej niż „włącz szyfrowanie" na poziomie sieci (kontrola: algorytmu, kluczy, częstości zmiany kluczy, źródło entropii, itd.):**

- **no i jeszcze: odporność kwantowa?**

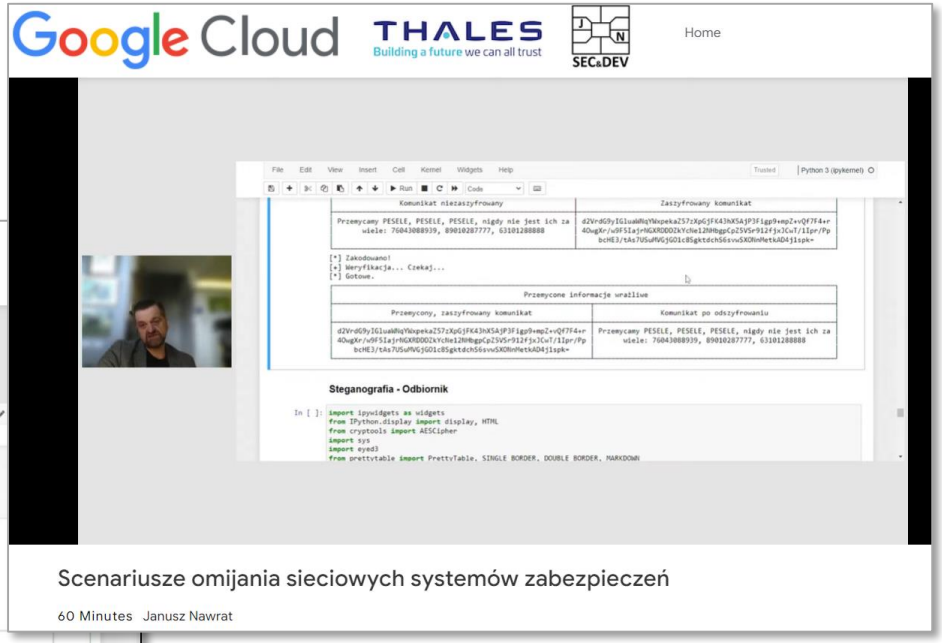
Dla ustalenia uwagi: co mamy do szyfrowania ruchu/łączy?

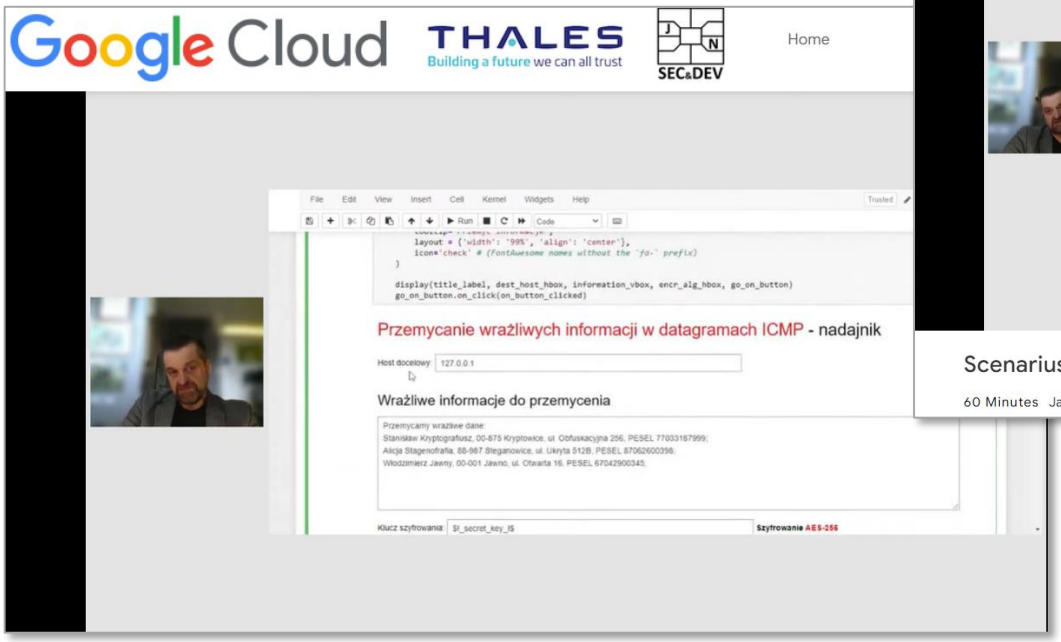
- **L1 (szyfrowania łącza fizycznego)**
  - Multipleksery DWDM
  - Transcivery, konwertery światłowodowe,
  - Modemy, …
- **L2 (MACSec)**
- **L3 (IPSec)**
- **L4 (aplikacja)**
  - Np. S/MIME,



https://www.soisk-me.pl/klasa-iv-sieci/model-iso-osi-i-tcp-ip

Czy VPN nie wystarczy?





ICMP, UDP, ARP, DNS, Broadcast, Multicast, Unicast, NTP, Steganofonia, …

Pakiet/ramka wcale nie musi dotrzeć do odbiorcy wystarczy go „podsłuchać"…

https://cloudonair.withgoogle.com/events/june_bezpiecznik_w_chmurze_google/watch?talk=talk3

THALES

CryptoPanel

rozwiązanie

Rozwiązanie – szyfratory wysokich prędkości

Przegląd

CV1000

- Hardened virtual encryption function
- Ideal for Cloud, Software Defined Networks (SDN) and Server-to-Server communications, East-West connectivity

CN4000 Series

- Up to 1 Gbps Encryptor
- Certified, low-cost, high-performance
- Small form factor ideal for remote locations such as Critical Infrastructure, SCADA, Energy, remote video feeds

CN6000

- Up to 4x10 Gbps Encryptor
- Rack-mountable, fully redundant robust design
- Ideal for private networks and datacenter interconnects

CN9000

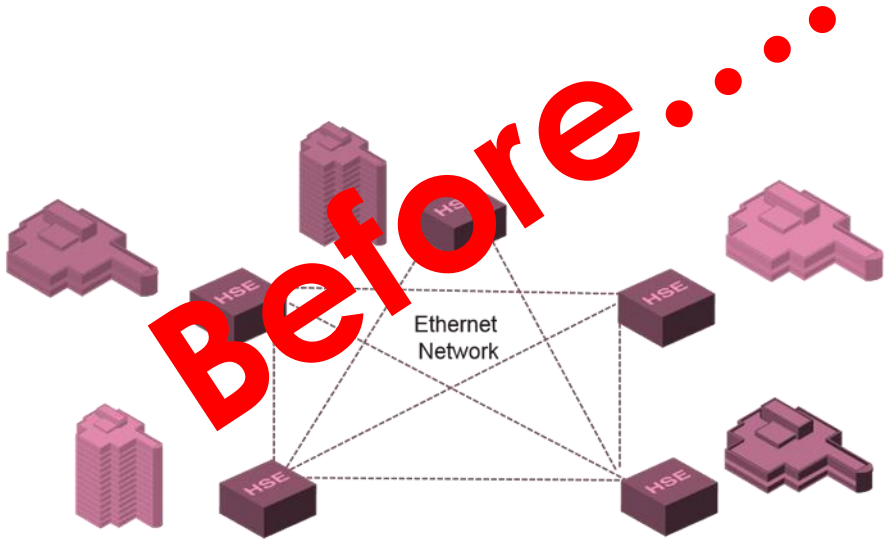
- Certified multipoint 100 Gbps encryptors
- Designed for next gen datacenters and core networks

THALES

Kiedyś

A family of dedicated appliances that encrypt data at wire speed across:

- Carrier Layer 2 services
- Metro Area Networks
- Ethernet Wide Area Networks
- Data Centre Interconnects

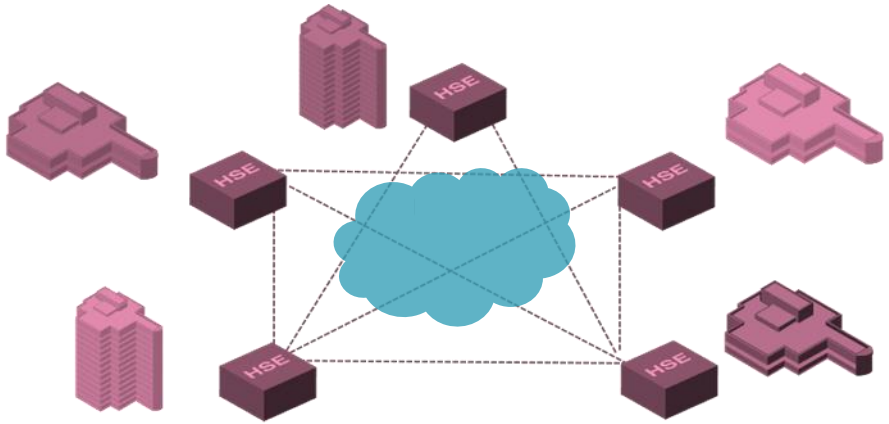


Dziś z TIM

A family of dedicated appliances that encrypt data at wire speed across:

Any network !

Now….



Nowy tryb pracy: ‘Transport Independent Mode’

Line & MAC mode

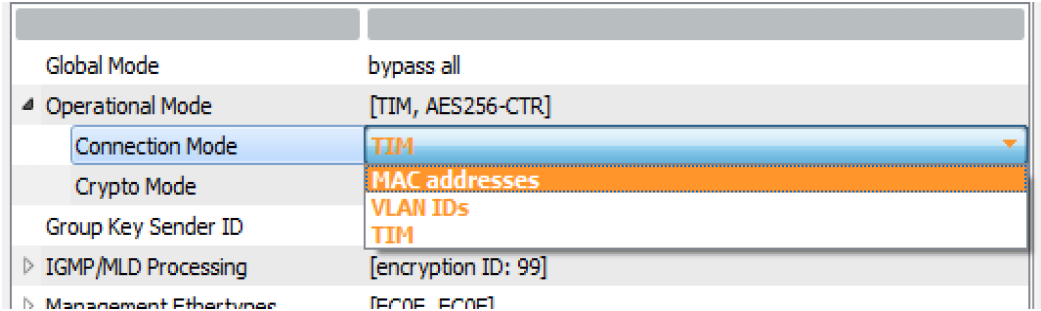
- Layer 2 Ethernet encryption only
- Policy based on remote MAC address in frame (MAC mode)

VLAN mode

- Layer 2 Ethernet encryption only
- Policy based on VLAN ID in frame

Transport Independent Mode

- Layer 2 Ethernet OR layer 3 IP OR layer 4 TCP/UDP encryption
- Policy based on IP address and/or port numbers

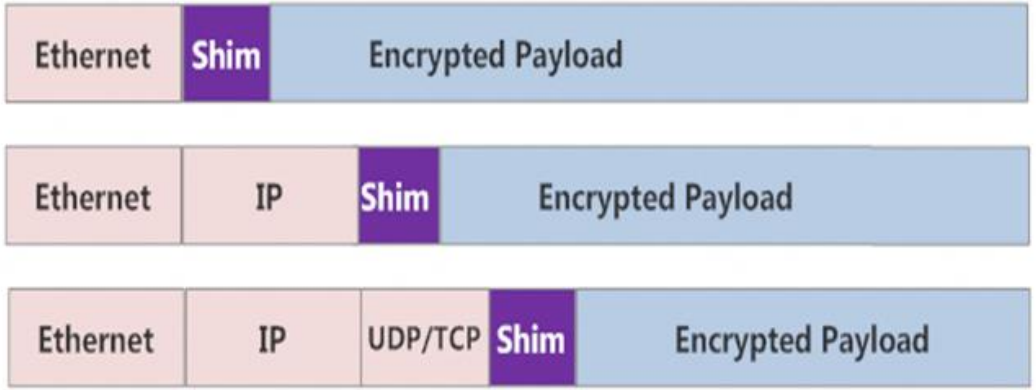



```
CV1000>con

Connection mode: TIM

CV1000>con -h

Usage: con  <CR>          Display current Connection mode status
            -m            Enable MAC Connection mode
            -v            Enable VLAN Connection mode
            -T            Enable TIM Connection mode
            -h            This help message
```


THALES

Network Independent = Smart network encryption

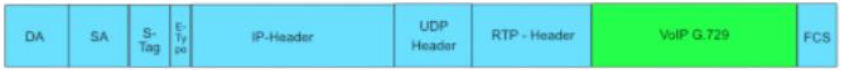
- Tunnel free payload encryption where it makes sense
  - *For performance*
  - *For security*
  - *For network*
- AES-256 CTR/GCM mode:
  - *Confidentiality only OR*
  - *Confidentiality + Authentication*
- Simple key management
- Per traffic flow encryption policies:
  - *Layer 2 – Ethernet*
  - *Layer 3 – IPv4/v6*
  - *Layer 4 (IP + Port)*
    - *NAT pass-through*
    - *Netflow/Jflow support*
    - *Policy based routing*



THALES

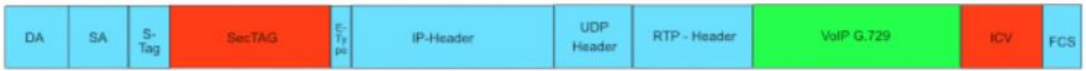
Przykład: VoIP encryption – MacSec, IPSec & HSE TIM

IP Packet in Ethernet Frame



IPsec ESP-AES-256 ESP-SHA-HMAC +76 Bytes

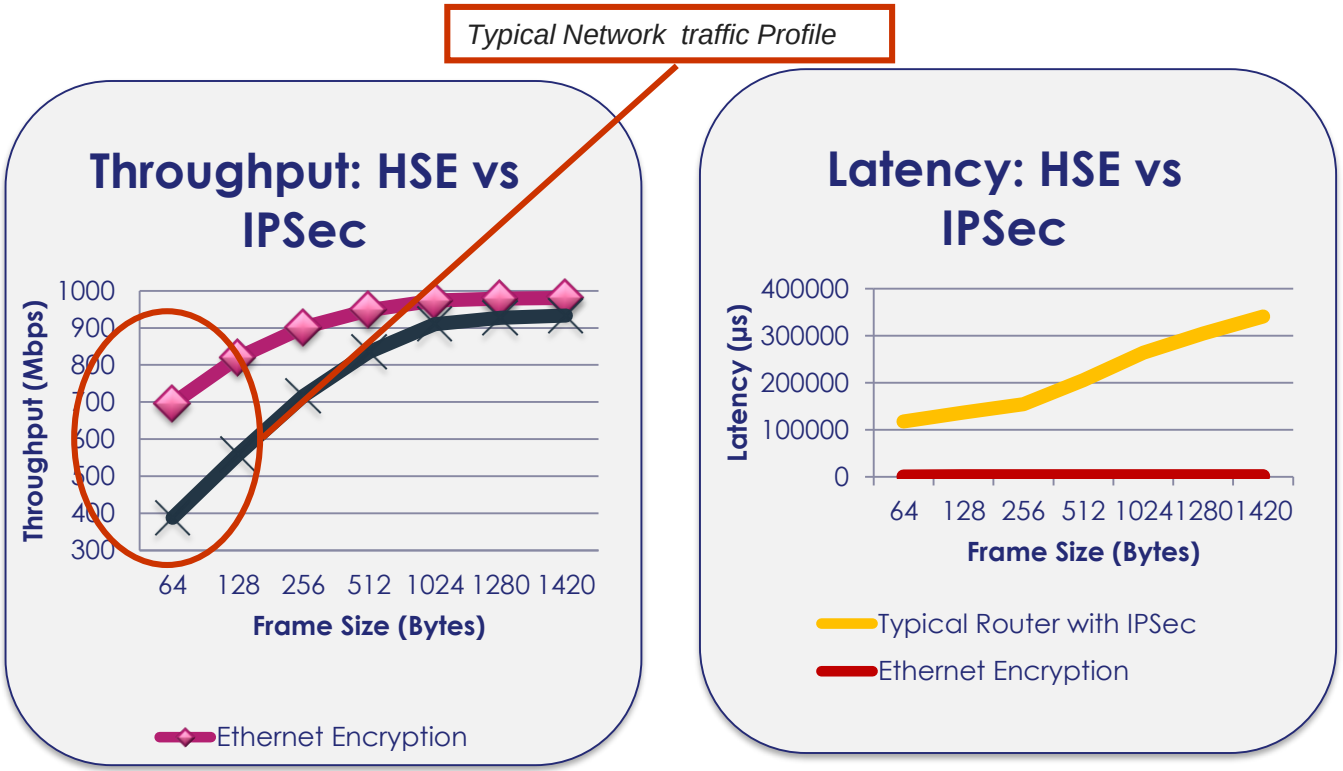
MACsec pr Ethernet +24 Bytes



TIM – Ethernet 8 bytes (+ 16 for confidentiality)

THALES

Performance



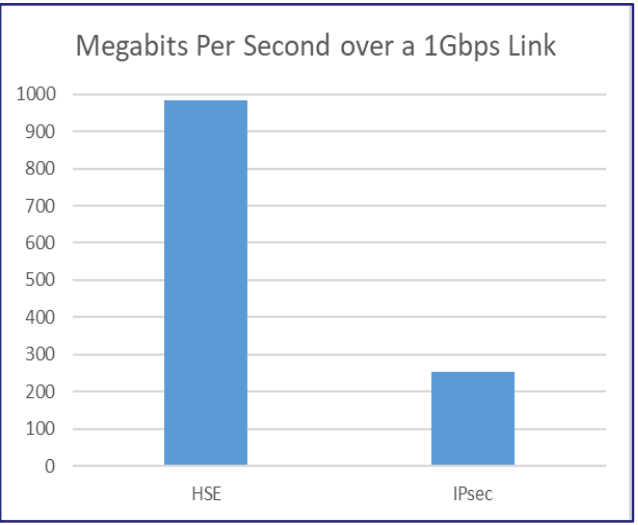
Thales High Speed Encryption Offers

Better Bandwidth Efficiency and Latency Performance

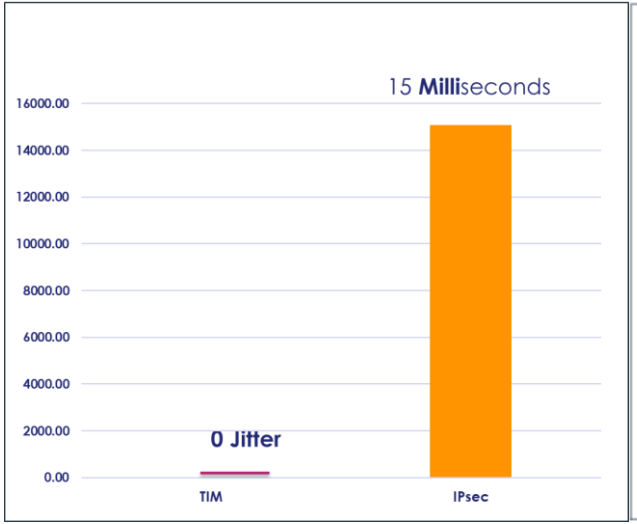
THALES

Rzeczywiste testy 5G – HSE vs. IPsec

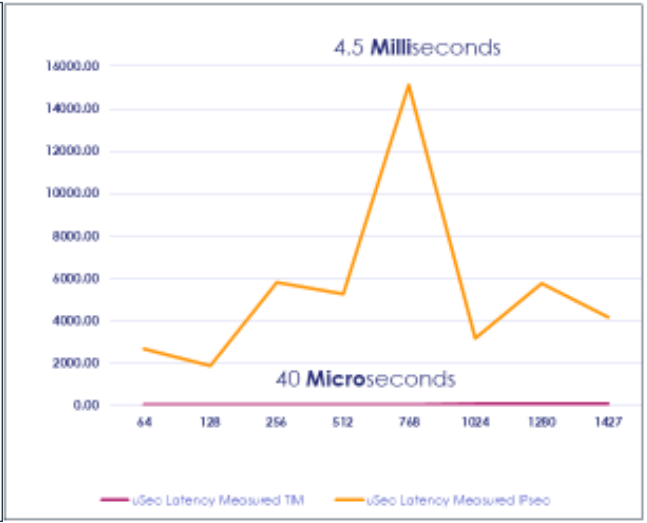
Measured Throughput (1427 Frame)



Average Jitter uSec



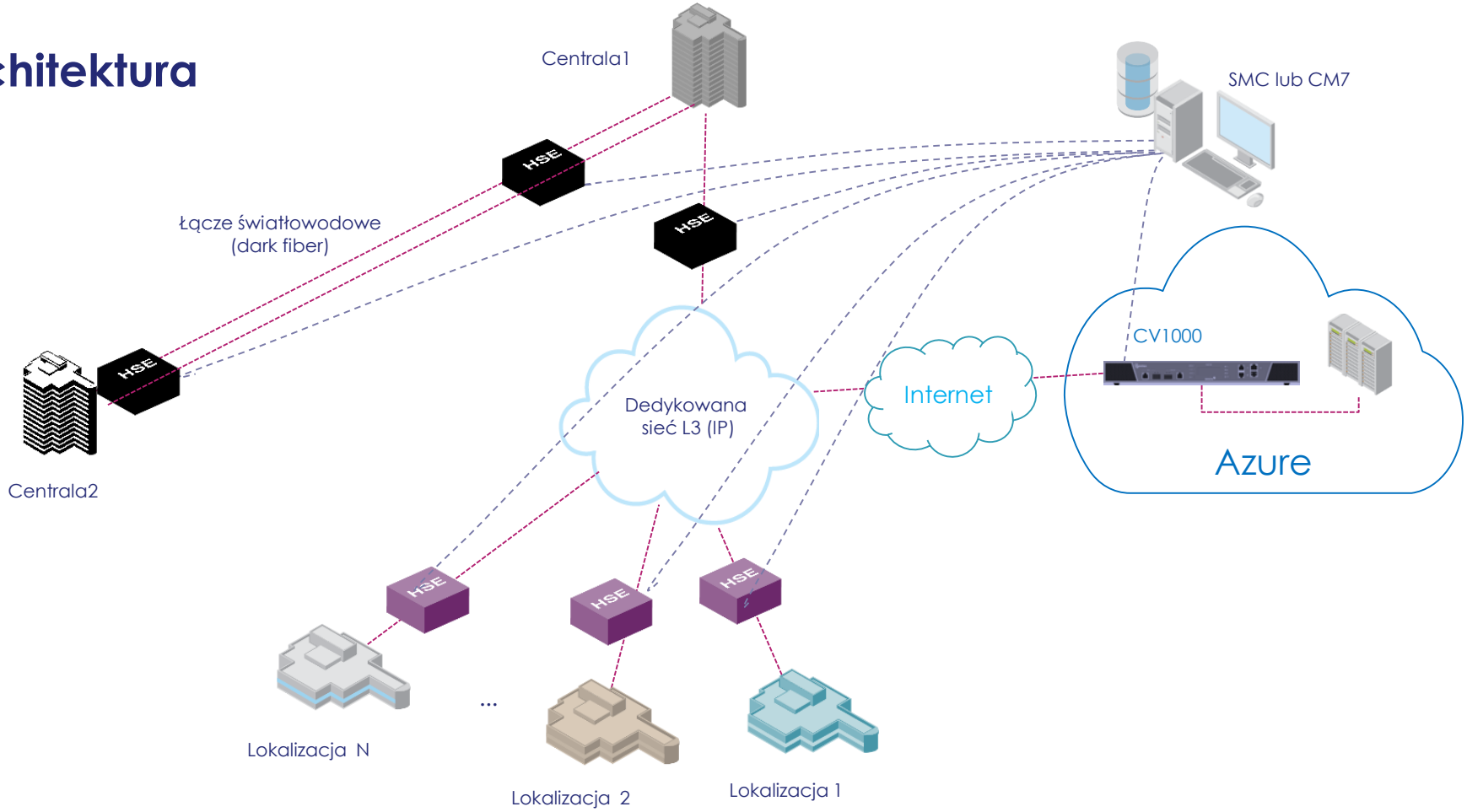
Measured Latency uSec



Toronto to Quebec City through wired ENCQR 5G Transport Core

THALES

Architektura



THALES

Do czego może służyć wirtualny szyfrator?

CV1000 is NOT a cheap HSE

- It has been designed for specific use cases
- Suitable only for existing virtualized environments
  - *Please don't try to fit a square peg in a round hole*

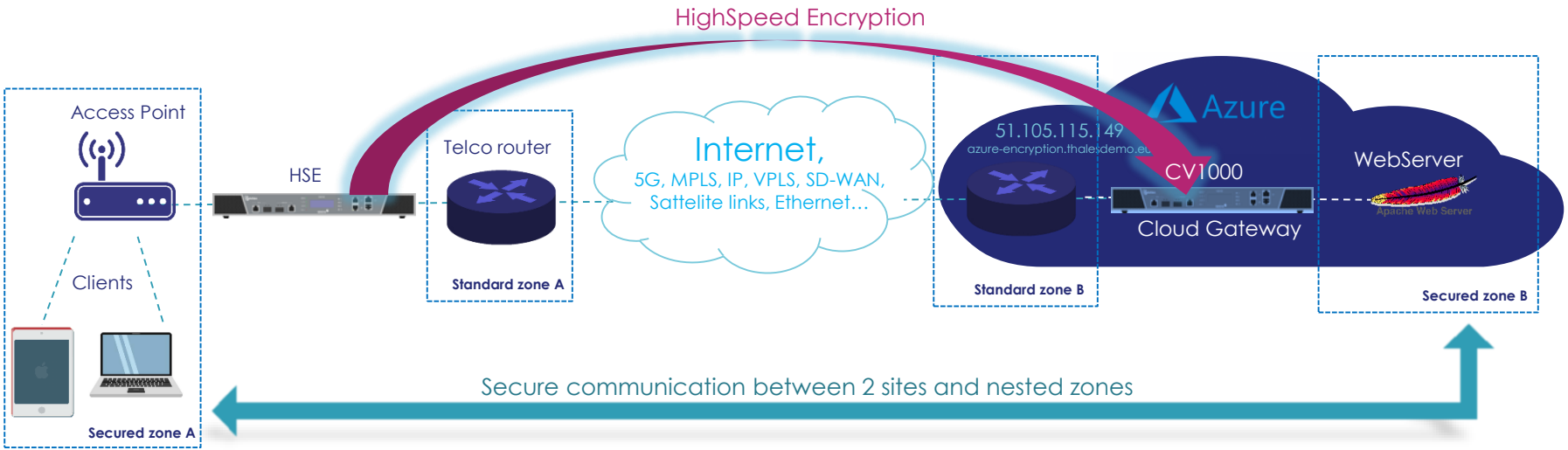
Possible use cases …..

- East-West encryption inside a data centre
- North-south encryption in/out of data centre
- SD-WAN environments
- Cloud gateway
- Other….

Everything else …….. hardware

THALES

Konfiguracja



SITES A and B

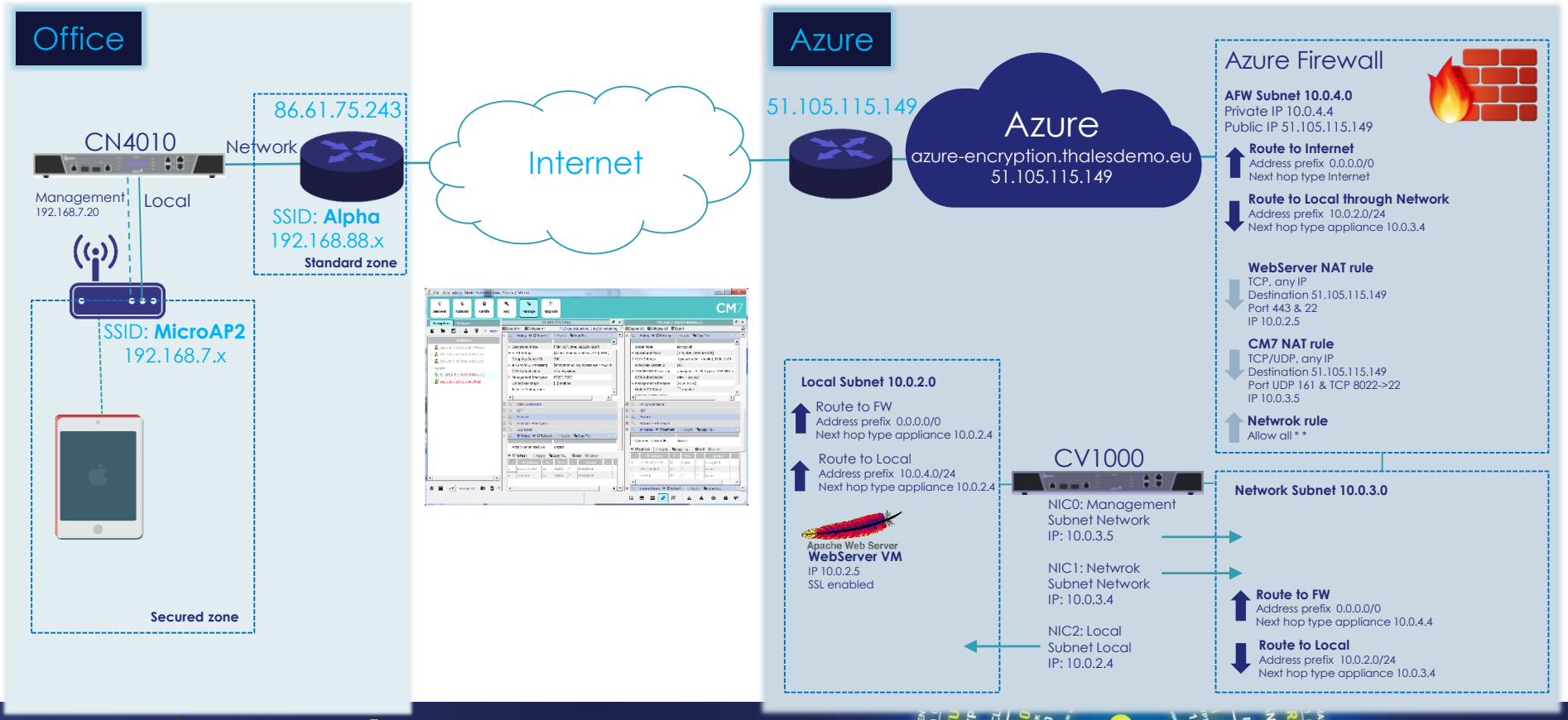
- Azure is hosting WebServer with sensitive content
- Multiple machines from Office want to access WebServer

SECURE COMMUNICATION

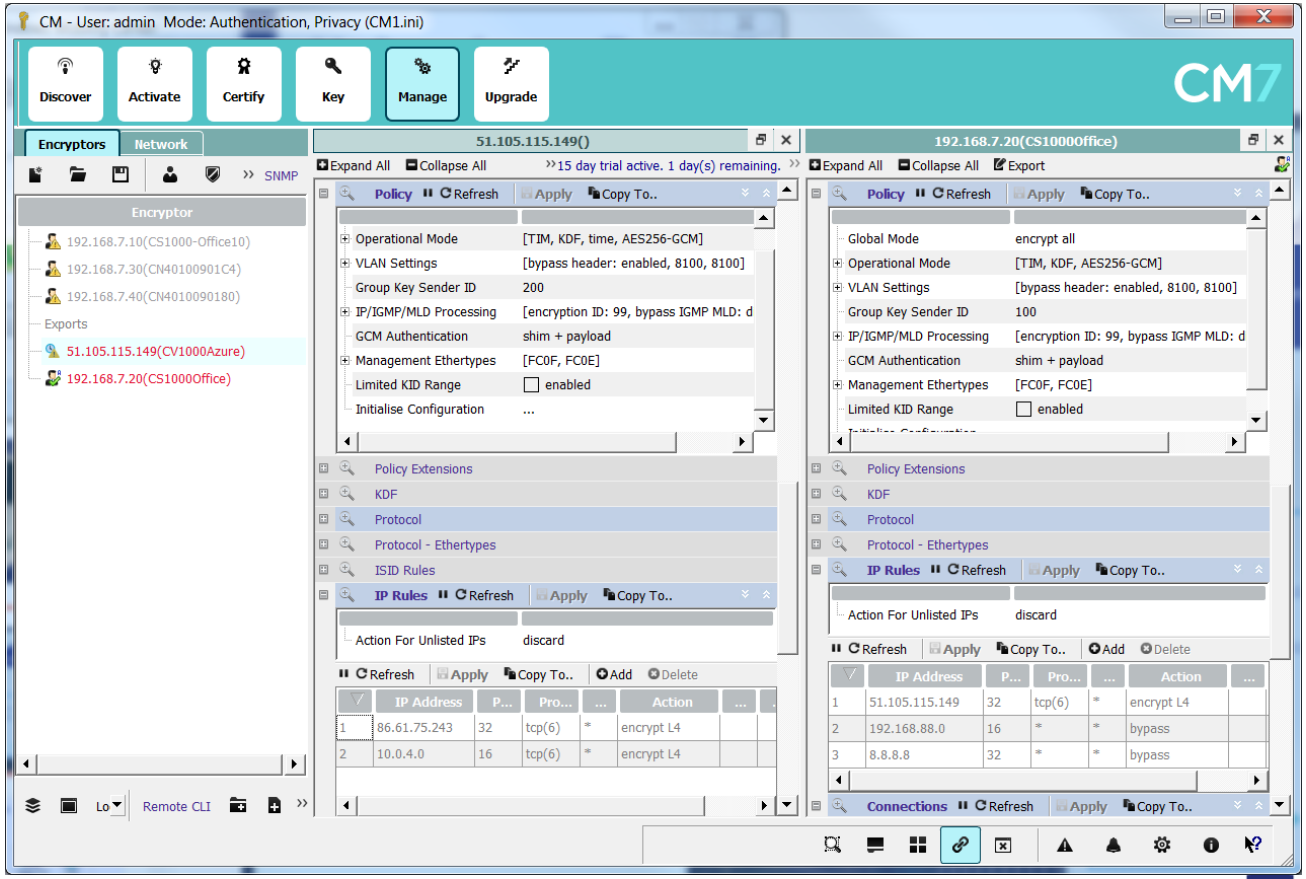
- Only machines in Secured A can talk to machines in Secured zone B
- Machines outside of Secured zone A can‘t talk to machines in Secured zone B as they receive AES encrypted traffic they don‘t understand

THALES

Szczegółowa konfiguracja

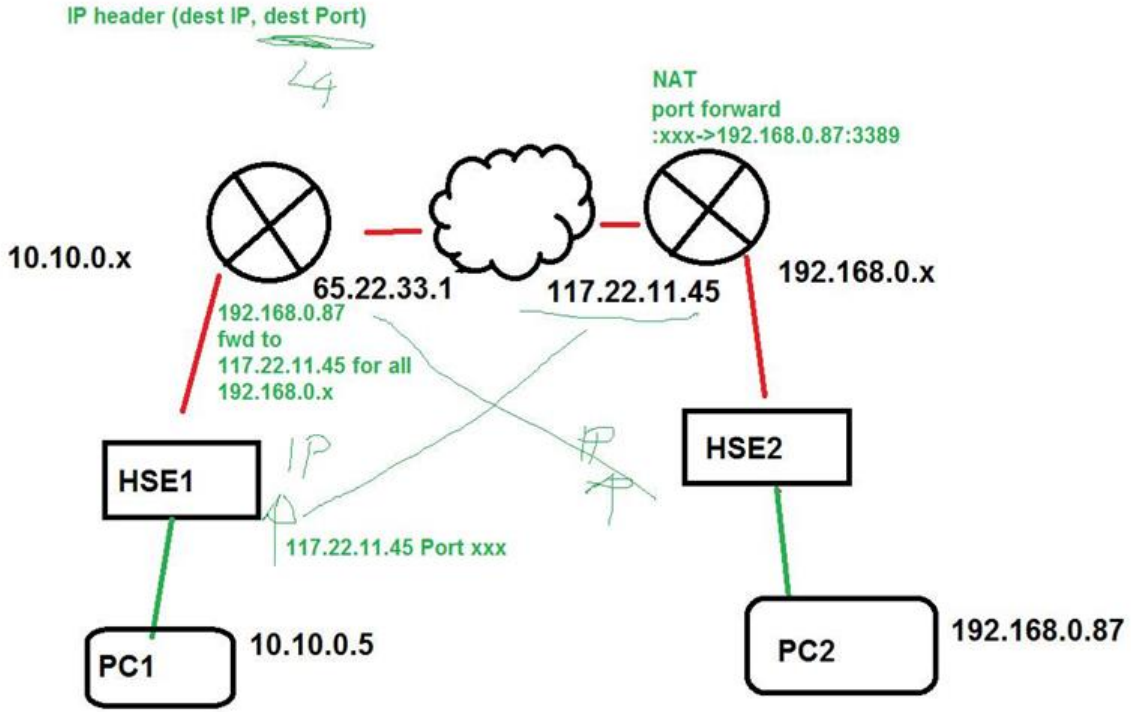


CM7


CM - User: admin Mode: Authentication, Privacy (CM1.ini)
Discover
Activate
Certify
Key
Manage
Upgrade
CM7
Encryptors
Network
SNMP
Encryptor
192.168.7.10(CS1000-Office10)
192.168.7.30(CN40100901C4)
192.168.7.40(CN4010090180)
Exports
51.105.115.149(CV1000Azure)
192.168.7.20(CS1000Office)
Remote CLI
51.105.115.149()
Expand All
Collapse All
15 day trial active. 1 day(s) remaining.
Policy
Refresh
Apply
Copy To..
Operational Mode [TIM, KDF, time, AES256-GCM]
VLAN Settings [bypass header: enabled, 8100, 8100]
Group Key Sender ID 200
IP/IGMP/MLD Processing [encryption ID: 99, bypass IGMP MLD: d
GCM Authentication shim + payload
Management Ethertypes [FC0F, FC0E]
Limited KID Range enabled
Initialise Configuration ...
Policy Extensions
KDF
Protocol
Protocol - Ethertypes
ISID Rules
IP Rules
Action For Unlisted IPs discard
Add
Delete
IP Address P... Pro... ... Action
1 86.61.75.243 32 tcp(6) * encrypt L4
2 10.0.4.0 16 tcp(6) * encrypt L4
192.168.7.20(CS1000Office)
Export
Global Mode encrypt all
Operational Mode [TIM, KDF, AES256-GCM]
VLAN Settings [bypass header: enabled, 8100, 8100]
Group Key Sender ID 100
IP/IGMP/MLD Processing [encryption ID: 99, bypass IGMP MLD: d
GCM Authentication shim + payload
Management Ethertypes [FC0F, FC0E]
Limited KID Range enabled
Action For Unlisted IPs discard
1 51.105.115.149 32 tcp(6) * encrypt L4
2 192.168.88.0 16 * * bypass
3 8.8.8.8 32 * * bypass
Connections

THALES

TIM w praktyce – kolega od firewall…



Nauczki i raczej nie znajdziecie w dokumentacji…

A co z wydajnością przy dużych pakietach?

- Wspieramy ramki jumbo

Uwaga na transcivery!

- Testujemy i wspieramy „nasze”
- Innych firm mogą działać ale nie odpowiadamy za to!

no i jeszcze: odporność kwantowa?

Comparison of conventional and quantum security levels

1

Table 1 - Impact of Quantum Computing on Common Cryptographic Algorithms

Cryptographic Algorithm	Type	Purpose	Impact from large-scale quantum computer
AES	Symmetric key	Encryption	Larger key sizes needed
SHA-2, SHA-3	----------	Hash functions	Larger output needed

2

RSA	Public key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, key exchange	No longer secure
DSA (Finite Field Cryptography)	Public key	Signatures, key exchange	No longer secure

THALES

Thales HSE - Quantum Safe strategy

Providing a transition path to Post Quantum Security

- Quantum entropy sources
- Quantum Key Distribution
- Quantum Resistant Algorithms

OPEN QUANTUM SAFE

software for prototyping quantum-resistant cryptography

aws

evolution

IBM Research

Microsoft

SENETAS
Security without compromise

THALES

NIST Search NIST Menu

NEWS

NIST's Post-Quantum Cryptography Program Enters 'Selection Round'

Chosen algorithms will become part of first standard devised to counter quantum decryption threat.

July 22, 2020

Credit: B. Hayes/NIST

A select few algorithms, some of which fall into one of three mathematical "families," are undergoing a final leg of review. Some will form the core of the first post-quantum cryptography standard.

Seven algorithms are finalists:

- Classic McEliece
- CRYSTALS-KYBER
- NTRU
- SABER

- CRYSTALS-DILITHIUM
- FALCON
- Rainbow

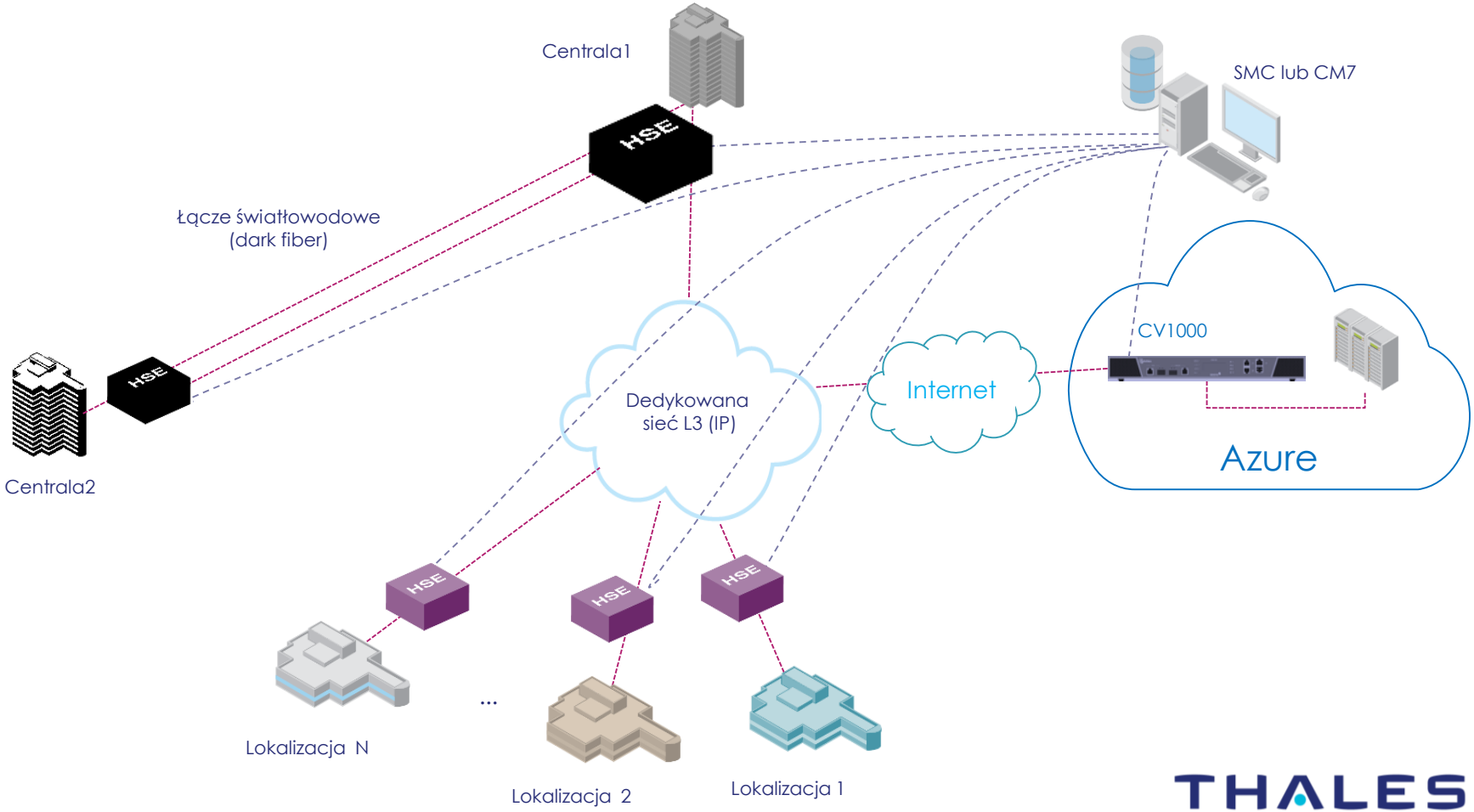
HSE 5.2.0 firmware will support all seven algorithms in all products

THALES

CryptoPanel

podsumowanie

Architektura – propozycja rozwiązania



THALES

Podsumowanie, czyli co potrzeba…

Do 1 GBps (dla lokalizacji)

- 3x…
- Ethernet Encryptor,1 GBPS,External AC,CN4020 **8 910,00** 943-000276-001-000

Do 2 GBps (z możliwością podniesienia przepustowości do 10Gbps)

- 2x (6140 – to 4 w jednym!)
- Network Encryptor, 5.0 GBPS, RATE LIMITED, DUAL AC, CN6140 **26 200,00** 943-000120-001-000
- Network Encryptor,1.25GBPS rate upgrade **2 240,00** 943-000182-001-000

STEP 2 SELECT TRANSCEIVERS

XFP for 10GB (CN6100 Only)		
XFP, 10GBASE-SR (300M), Multi-Mode, 850NM	**470,00**	904-40004-001-000
XFP, OC192 SR-1 & 10GBASE-LR/LW (10KM), Single Mode, 1310NM	**650,00**	904-40001-001-000
XFP, OC192 IR-2 & 10GBASE-ER/EW (40KM), Single Mode,1550NM	**1 500,00**	904-40002-001-000
XFP, OC192 LR-2A & 10GBASE-ZR/ZW (80KM), Single Mode, 1550NM	**2 980,00**	904-40003-001-000
SFP+ for 1/10GB (CN6140 Only)		
Transceiver, 1G/10G,LC,Multimode, 850NM, SFP+	**85,03**	943-000216-001-000
Transceiver, 1G/10G,LC,10KM,Single Mode, 1310NM, SFP+	**225,00**	943-000241-001-000
Transceiver, 10G,LC,40KM,Single Mode, 1550NM, SFP+	**805,00**	943-000255-001-000
Transceiver, 10G,LC,80KM,Single Mode, 1550NM, SFP+	**1 210,00**	943-000267-001-000

Podsumowanie, czyli co potrzeba…

Do chmury (CV1000) 1x

- 1x… do wyboru do koloru:
- Thales Virtual Encryptor,CV1000, DPDK, Term Limited, 1-year, Enhanced Support **875,00** 943-000019-001-000
- Thales Virtual Encryptor,CV1000, DPDK, Term Limited, 3-year, Enhanced Support **1 750,00** 943-000012-001-000
- Thales Virtual Encryptor,CV1000, DPDK, Perpetual **1 170,00** 943-000114-001-000

Zarządzanie:

- **CM7 za darmo**
- **SMC:**
- SMC,Small Deployment,up to 10 Encryptors,Electonic Delivery **3 010,00** 906-000063-001-000

CryptoPanel

CryptoPanel

A teraz quiz

https://forms.office.com/r/PPaKkghaT3

THALES