CryptoPanel

edycja #21

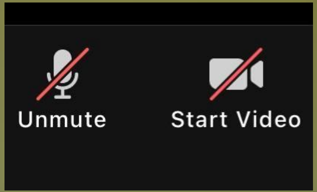
Już za moment zaczynamy!

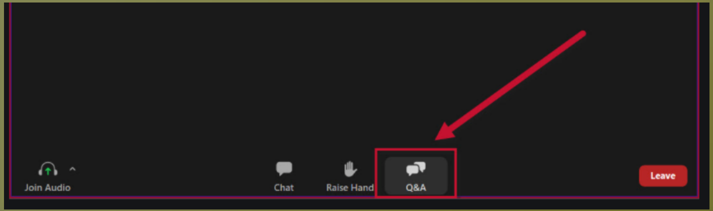
CryptoPanel

THALES

CLICO

CryptoPanel





CryptoPanel

edycja #21

Bezpieczna komunikacja cloud z on-prem bez degradacji przepustowości z możliwością wdrożenia bezpiecznej transmisji postkwantowej

CryptoPanel

dziś dyskutują

Piotr Majek

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

Artur Holeczek

Partner Account Manager /
Product Manager
artur.holeczek@clico.pl
mob. +48 667 699 444

CryptoPanel

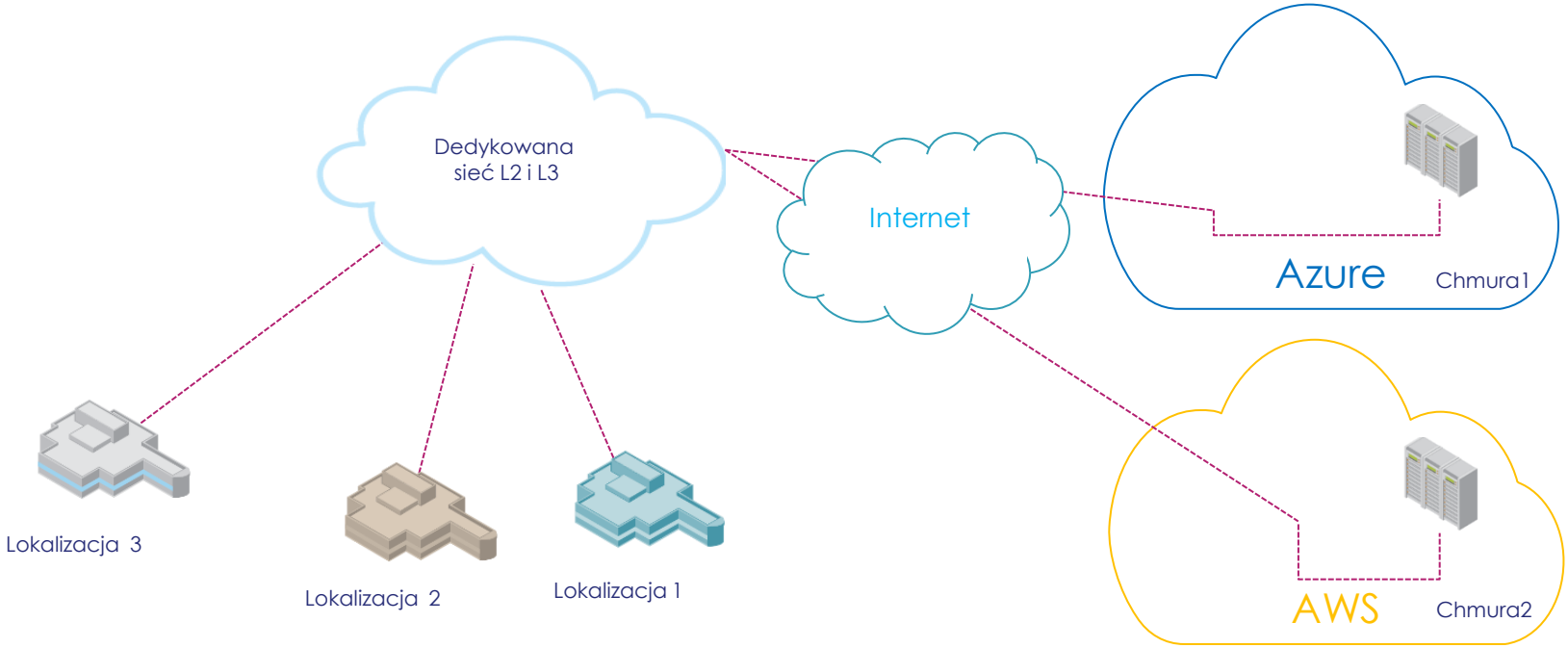
problem

Co nas boli...

- **Jesteśmy organizacją z sektora podlegającego NIS2**
- **Korzystamy z rozwiązań hybrydowych (miks on-prem oraz kilku chmur)**
  - AWS, Azure, w planach GCP
  - Mamy środowisko maszyn wirtualnych opartych o VMware
- **Chcemy zaszyfrować ruch pomiędzy swoimi zasobami on-prem, a zasobami w chmurze:**
  - Szyfrowanie na „naszych" zasadach
  - Bez spadku przepustowości
  - Bez instalowania urządzeń u dostawcy chmury
- **Mamy klasycznie zbudowaną infrastrukturę sieciową (połączenia między ośrodkami)**
  - Sieci oparte o L2 (Ethernet), L3 (IPSec) i MPLS

- **czy istnieje takie rozwiązanie dla chmur publicznych?**
- **jak zapewnić bezpieczeństwo ruchu do/z chmury bez korzystania z „ich VPN"?**
  - ale bez instalowania urządzeń w DC dostawcy, ze względu na wysokie koszty i ograniczoną dostępność
- **interesuje nas coś więcej niż „włącz szyfrowanie" – np. chcemy większej kontroli nad sposobem wymiany klucza.**
- **chcemy szyfrować ruch aż do „karty sieciowej serwera produkcyjnego", jeżeli to możliwe.**
- **w naszych serwerowniach (on-prem) chcemy używać dedykowanych urządzeń sprzętowych**

Nasza topologia



CryptoPanel

Dla kontekstu:

Kategorie podmiotów podlegających NIS2

Podmioty kluczowe są to podmioty, które dostarczają usługi niezbędne do funkcjonowania społeczeństwa i gospodarki. Podmioty kluczowe są zatem integralnym elementem infrastruktury krytycznej Unii Europejskiej, a ich działalność ma bezpośredni wpływ na stabilność i bezpieczeństwo społeczne i gospodarcze. W przypadku podmiotów kluczowych oczekuje się, że będą one przestrzegać najwyższych standardów bezpieczeństwa sieci i systemów informatycznych.

Podmioty ważne są nową kategorią wprowadzoną w Dyrektywie NIS 2 w celu uwzględnienia podmiotów, które nie spełniają rygorystycznych kryteriów podmiotów kluczowych, ale których działalność ma istotny wpływ na funkcjonowanie społeczeństwa i gospodarki Unii. Podmioty te pozostają jednak w dużej mierze zależne od bezpieczeństwa sieci i systemów informatycznych.

Analiza: www.traple.pl

Różnice w odpowiedzialności

Dyrektywa NIS2 dość precyzyjnie formułuje zapisy dotyczące nakładania sankcji za naruszenie jej przepisów. Podmioty kluczowe, które naruszą przepisy dyrektywy mogą otrzymać karę administracyjną w maksymalnej wysokości co najmniej 10 mln € lub co najmniej 2% łącznego rocznego światowego obrotu w poprzednim roku przedsiębiorstwa. Przy czym zastosowanie ma tu kwota wyższa. W związku z tym państwa członkowskie będą dysponowały dużą swobodą przy ustalaniu „widełek" i wspomniane kwoty mogą być znacznie wyższe.

naruszą przepisy dyrektywy , będzie mogła być nałożona kara administracyjna w maksymalnej wysokości co najmniej 7 000 0000 € lub co najmniej 1,4% łącznego rocznego światowego obrotu w poprzednim roku obrotowym przedsiębiorstwa. Przy czym zastosowanie ma kwota wyższa.

Artykuł 21 Punkt 2 – Środki zarządzania ryzykiem

„Bazują na podejściu uwzględniającym wszystkie zagrożenia
i mającym na celu ochronę sieci i systemów informatycznych (…), i obejmują co najmniej następujące elementy:

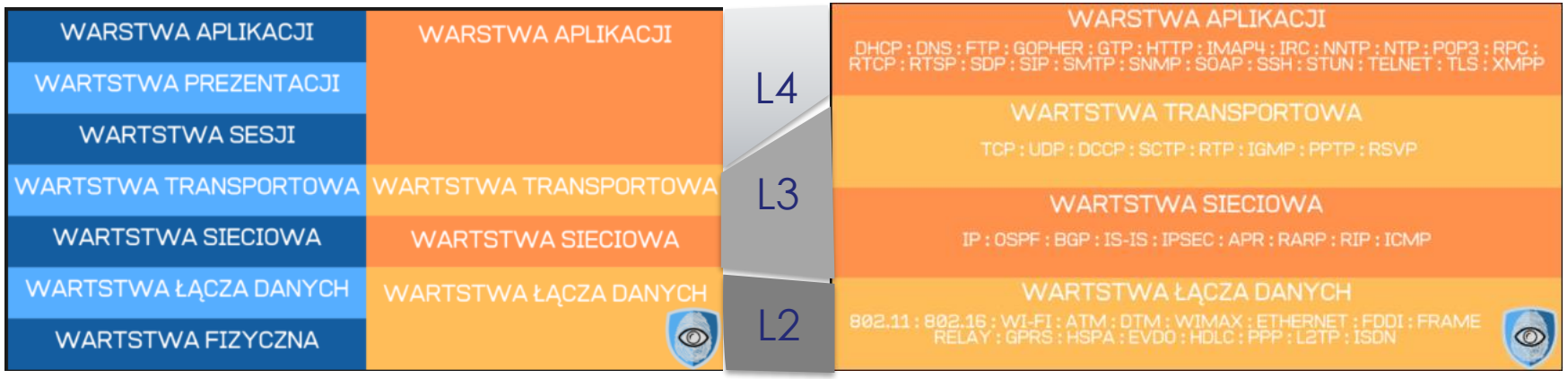
h) Polityki i procedury stosowania kryptografii i szyfrowania;

j) Procedury stosowania uwierzytelniania wieloskładnikowego lub ciągłego, zabezpieczonych połączeń głosowych, tekstowych i wideo oraz zabezpieczonych systemów łączności wewnątrz podmiotu w sytuacjach nadzwyczajnych.

CryptoPanel

rozwiązanie

Dla ustalenia uwagi: co mamy do szyfrowania transmisji?



L1 (szyfrowania łącza fizycznego)

- Multipleksery DWDM,
- Transcivery,
- Konwertery światłowodowe,
- Modemy, Itp..

L2 (MACSec)

L3 (IPSec)

L4 (TLS)

https://securitybeztabu.pl/model-iso-osi/

Rozwiązanie – wirtualne i sprzętowe szyfratory sieci

Szyfrator sprzętowy. Oraz do chmury. I do VMware.

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

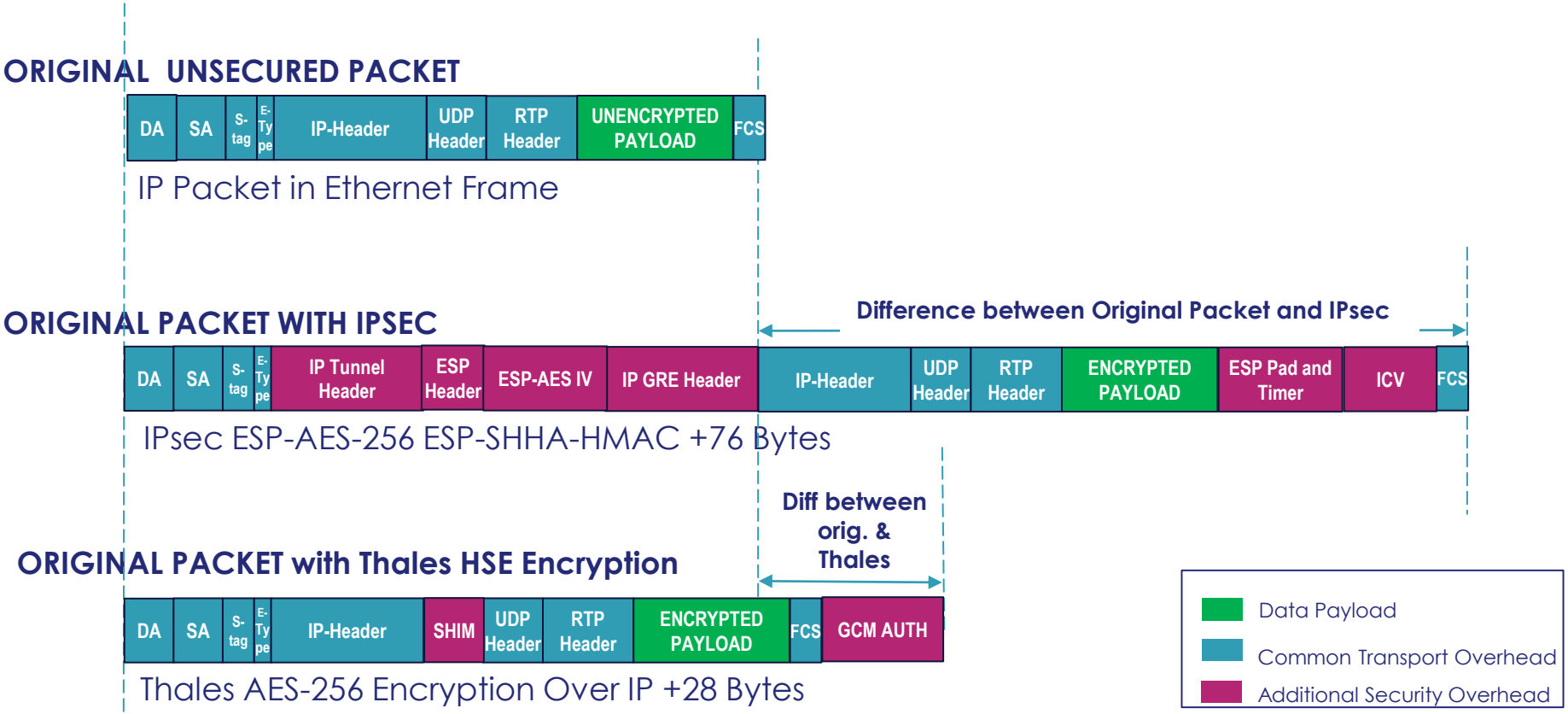
CN6000

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

CN9000

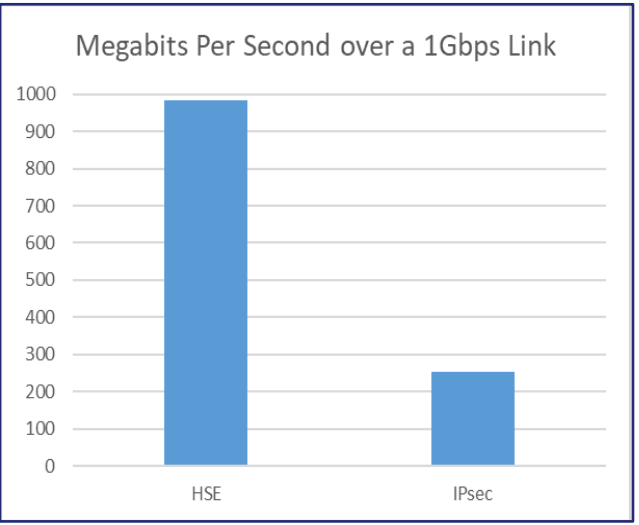
- Certified multipoint 100 Gbps encryptors
- Designed for next gen datacenters and core networks

Porównanie wielkości pakietów – IPsec vs. HSE

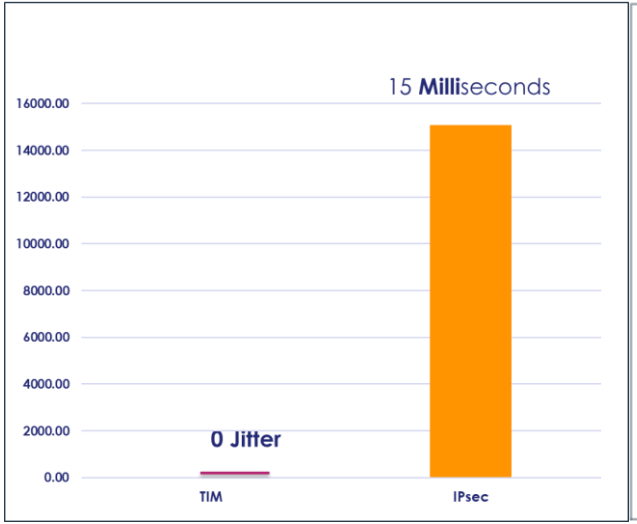


Rzeczywiste testy rozwiązania 5G – HSE vs. IPsec

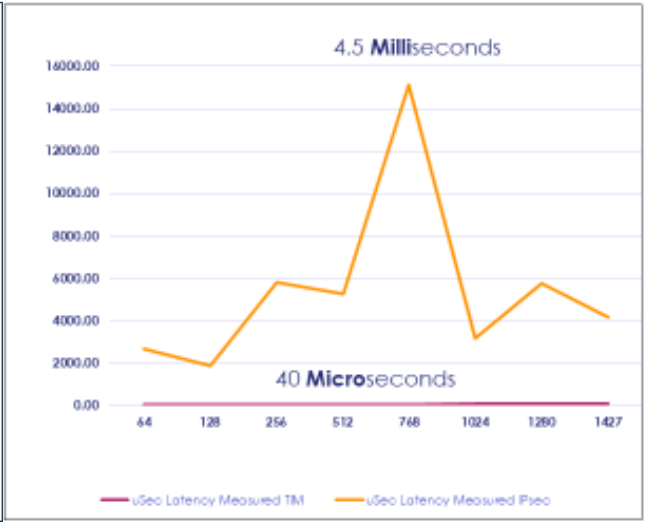
Measured Throughput (1427 Frame)



Average Jitter uSec



Measured Latency uSec

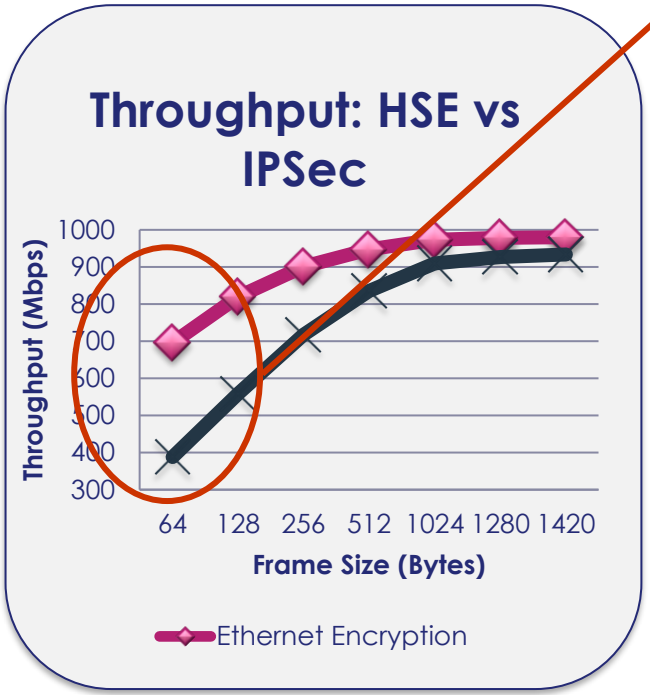


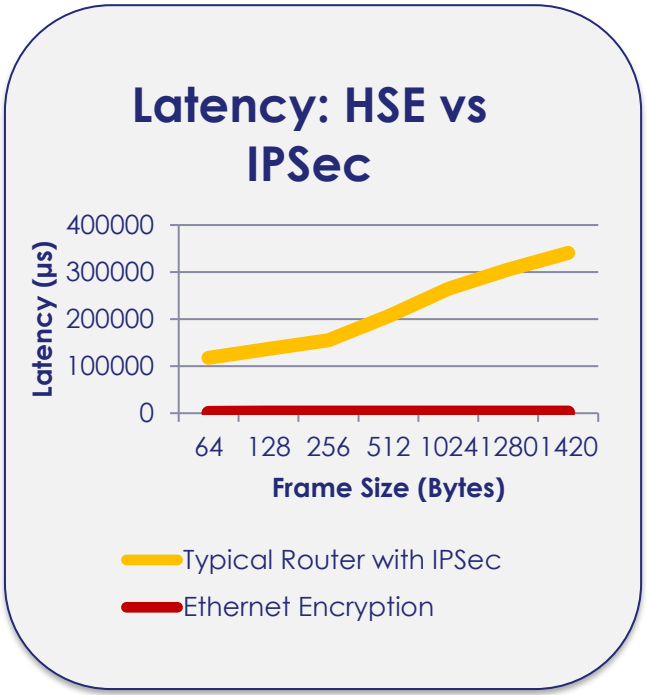
Toronto to Quebec City through wired ENCQR 5G Transport Core

Źródło: Senetas.com

Przepustowość niczym rozmiar - ma znaczenie!

Typowy profil ruchu sieciowego

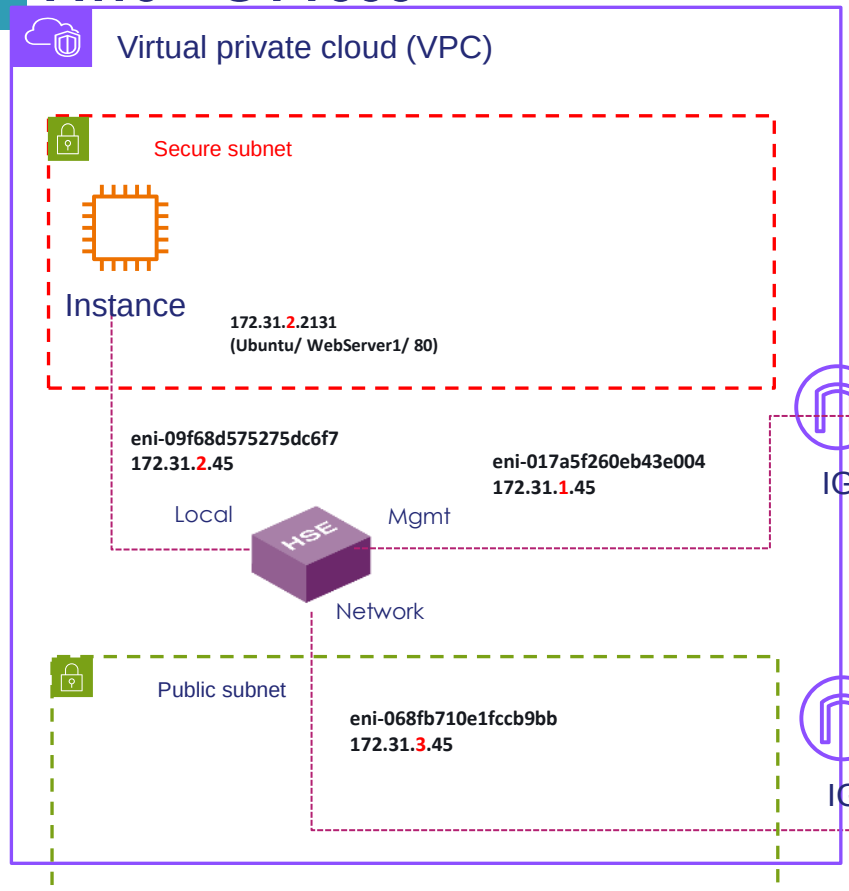




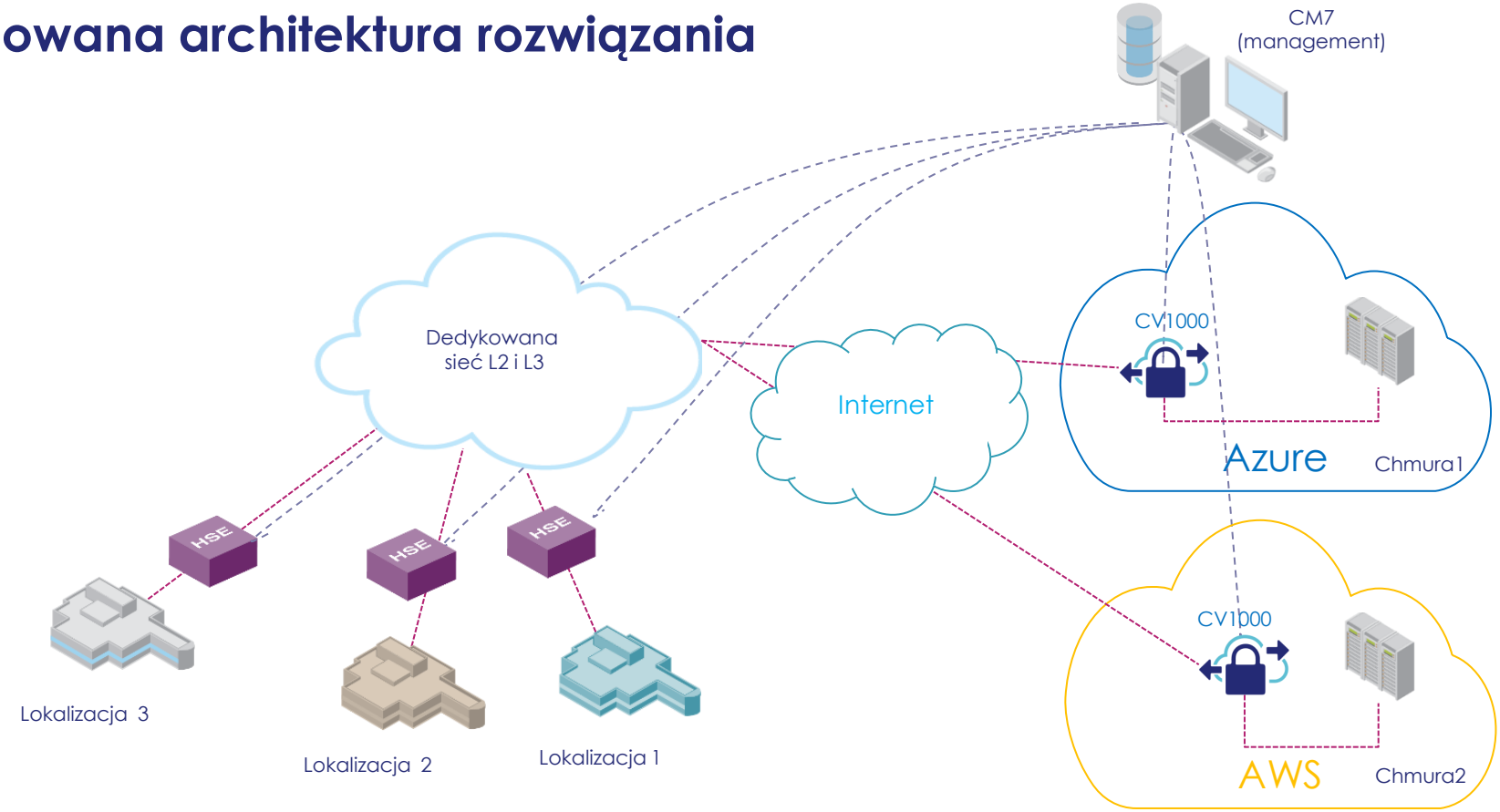
HSE ma lepsze parametry przepustowości i opóźnienia w stosunku do IPSec

Szkice architektury

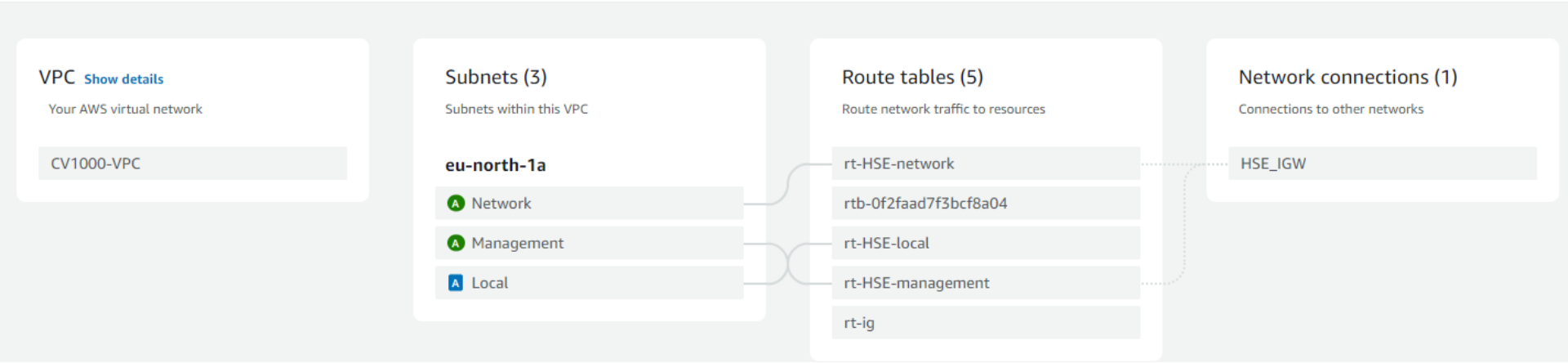
AWS – CV1000


Virtual private cloud (VPC)
Secure subnet
Instance
172.31.2.2131
(Ubuntu/ WebServer1/ 80)
eni-09f68d575275dc6f7
172.31.2.45
eni-017a5f260eb43e004
172.31.1.45
Local
Mgmt
HSE
Network
Public subnet
eni-068fb710e1fccb9bb
172.31.3.45
IG
IG
51.21.81.40
93.179.251.225/27
13.50.144.130
NAT
Azure
On-prem
10.2.99.236
Secure Client
CM7
10.2.99.102
10.2.99.0/24
10.2.99.235
Local
Mgmt
Network

Proponowana architektura rozwiązania



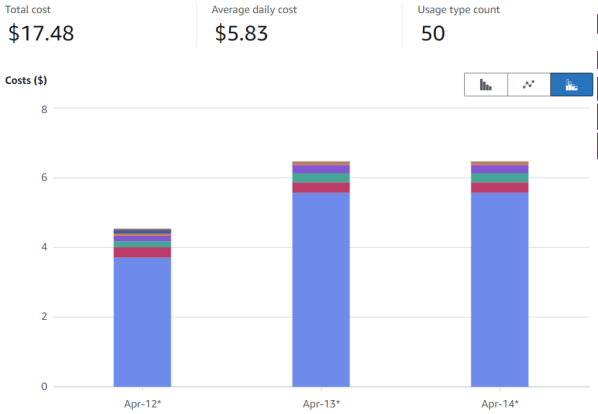
Tablice routingu na przykładzie AWS



CV wymaga mocy i … $ €

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
CV2000	i-0d5c0a082081f9c07	Running	c5n.xlarge	2/2 checks passed	View alarms	eu-north-1a
WebServer1	i-02fa9216f2225b167	Running	t3.micro	2/2 checks passed	View alarms	eu-north-1a

24h pracy CV1000 + 2x EIP + 1x Ubuntu (t3.micro) w AWS to 5,83 $



Instance Type	vCPUs	GB RAM	Max NICs	Bandwidth
c5n.xlarge	4	10.5	4	25 Gbps
c5n.2xlarge	8	21	4	25 Gbps
c5n.4xlarge	16	42	8	25 Gbps

Do czego może służyć wirtualny szyfrator?

CV1000 rozszerza bezpieczeństwo na środowiska zwirtualizowane

- Został zaprojektowany do konkretnych zastosowań
- Nadaje się środowisk, w których nie ma możliwości instalacji urządzeń fizycznych (VMware, AWS, Azure)
- *Nie próbuj wkładać kwadratowego kołka w okrągły otwór*

Możliwe przypadki użycia

- Szyfrowanie wschód-zachód w centrum danych
- Szyfrowanie północ-południe w centrum danych/na zewnątrz
- Środowiska SD-WAN
- Brama w chmurze

Wszystkie inne przypadki - Sprzętowe urządzenie!

Nauczki i to, czego raczej nie znajdziecie w dokumentacji

A co z wydajnością przy dużych pakietach?

- Wspieramy ramki jumbo

Uwaga na transcivery światłowodowe!

- Testujemy i wspieramy tylko „nasze" (z cennika)
- Transcivery innych dostawców mogą działać ale nie odpowiadamy za wsparcie!

I coś i jeszcze: podczas PoC nie zrób sobie pętli na przełączniku ☺ gdy włączasz ***BypassAll***

- Zalecenie: sieci **Local** i **Network** w oddzielnych VLAN-ach.

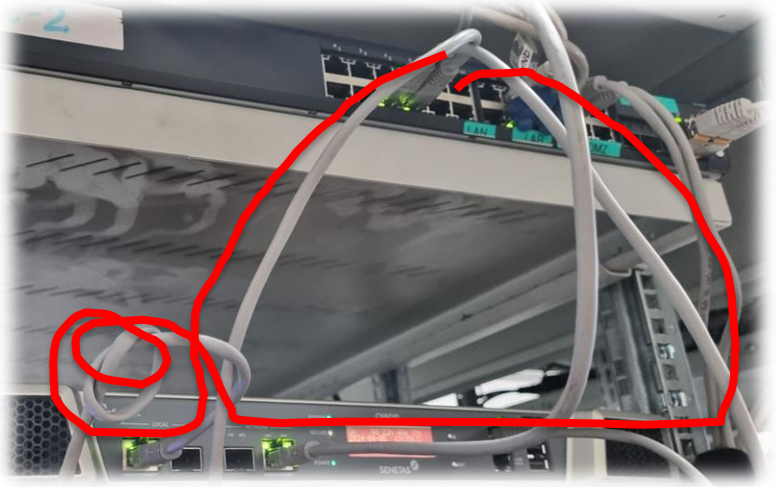
Przed przejściem do konfigurowaniem szyfrowania upewnij się, że poprawnie działa połączenie sieciowe między obszarami bezpieczeństwa (tu: klient serwer)

- Odpowiednie przypisanie interfejsów (AWS)
- Odpowiednie tablice routing (AWS)
- Prawdowo skonfigurowane bramy internetowe (AWS)
- Poprawne reguły IP Rules (uwaga na zewnętrzne IP w on-prem)

The experience gathered so far:

Before encrypting any traffic, make it work in "bypass all" mode.

thank you!

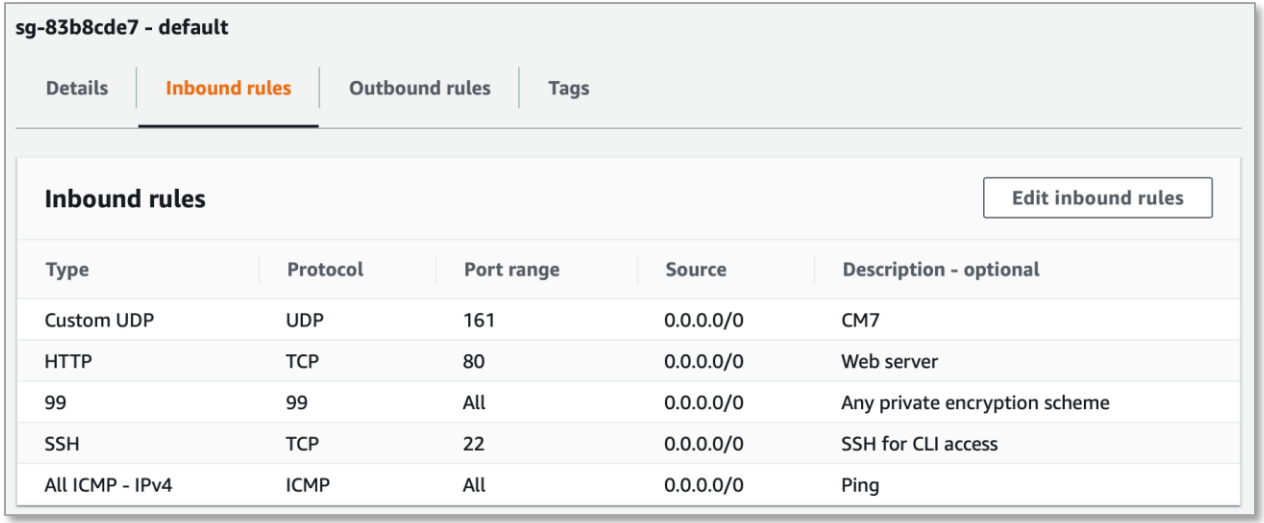


Nauczki i raczej nie znajdziecie w dokumentacji 2/3

Uwaga na AWS – Security Group i definicje Protocol # 99

- Momentami bywa śmiesznie w pracy informatyka ☺
  - you may encounter putting 99 as Protocol Type (in AWS GUI since 2024-04-04] try this: put 99 you will get “IGP (9)9” and move cursor within brackets and delete unnecessary characters.

https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml



sg-83b8cde7 - default

Details | **Inbound rules** | Outbound rules | Tags

Inbound rules — Edit inbound rules

Type	Protocol	Port range	Source	Description - optional
Custom UDP	UDP	161	0.0.0.0/0	CM7
HTTP	TCP	80	0.0.0.0/0	Web server
99	99	All	0.0.0.0/0	Any private encryption scheme
SSH	TCP	22	0.0.0.0/0	SSH for CLI access
All ICMP - IPv4	ICMP	All	0.0.0.0/0	Ping

99	any private encryption scheme	[Internet_Assigned_Numbers_Authority]

Nauczki i raczej nie znajdziecie w dokumentacji 3/3

„Ale przecież można znaleźć klucz w zrzucie pamięci w AWS…?”

CV1000 Memory Dump

- ”CV1000 is a hardened Linux image. It’s far from trivial to perform a AWS memory dump for Linux images and I’d argue that if someone was in a position to do this then a customer has far bigger security problems – the access rights and utilities required are significant (if someone has such access to infrastructure to do memory dumps then CV1000 is not their biggest problem).

AES Encryption Key

- Either AES-CTR or AES-GCM are used with the CV1000-AWS. With both of these algorithms and the use of a FIPS-approved Key Derivation Function (KDF), compromise of one key does not degrade prior or future derived keys (the AES session keys are changed on a regular basis).

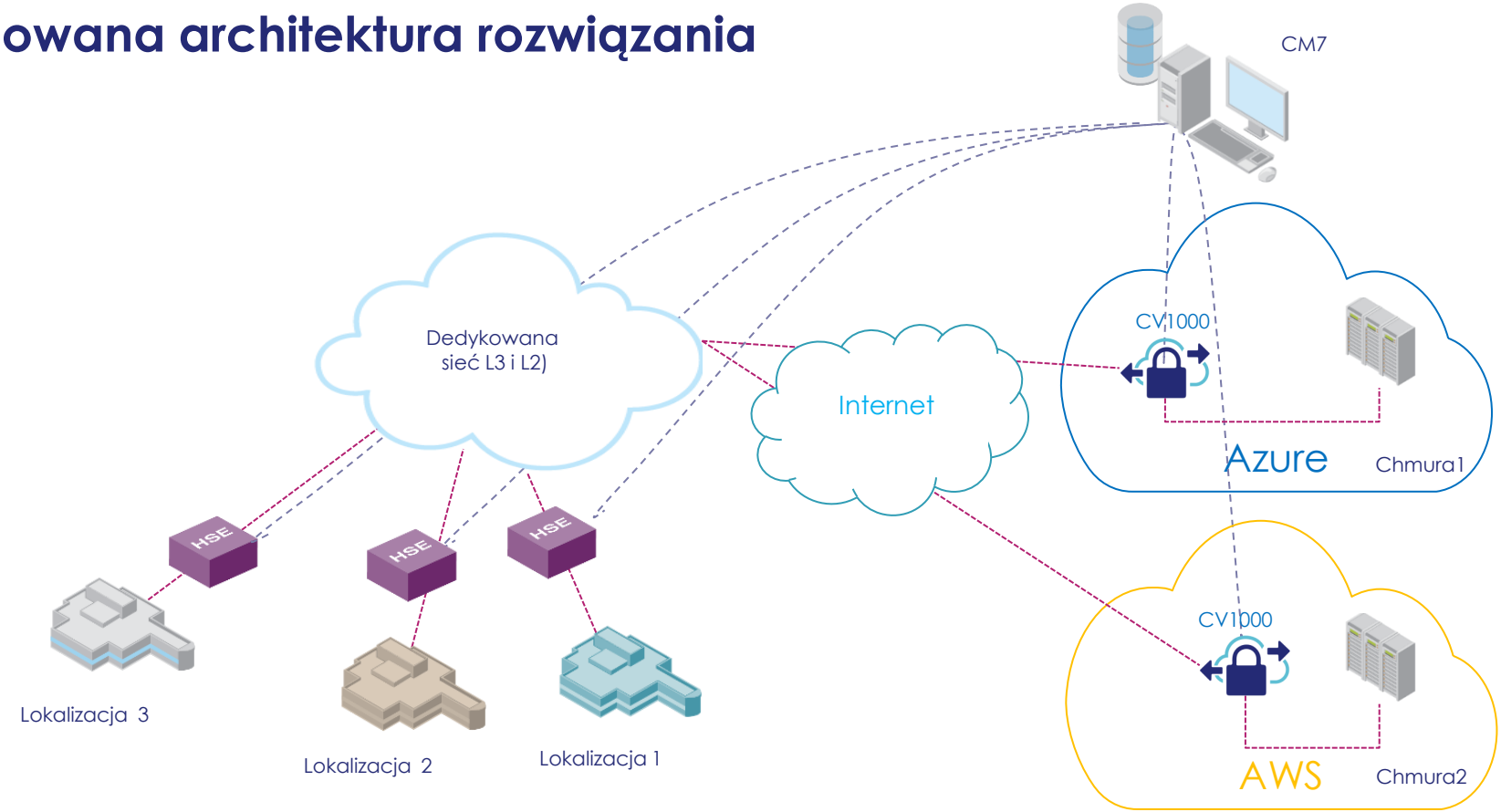
FIPS

- Senetas are currently seeking FIPS 140-3 Level 1 certification for the software crypto

CryptoPanel

podsumowanie

Proponowana architektura rozwiązania



Podsumowanie, czyli co potrzeba…

Do 1 GBps (dla lokalizacji)

1GBPS + Products	
Network Encryptor,1 GBPS,External AC,CN4010	10 300,00
Network Encryptor,1 GBPS,External AC,CN4020	10 900,00
STEP 2 SELECT TRANSCEIVERS	
KIT,XCVR,SFP,1000BASE-SX,LC,MM,850NM,ROHS	104,00
KIT,XCVR,SFP,1000BASE-T,10/100/1000,RJ-45,ROHS	202,00
KIT,XCVR,SFP,1000BASE-LX,LC,SM,1310NM,ROHS	214,00
KIT,XCVR,SFP,1000BASE-[ZX],LC,SM,1550NM,ROHS	954,00

- A macie szybsze?

Jeszcze jak! Ale czy to potrzebne? ☺

Podsumowanie, czyli co potrzeba…

Do chmury (CV1000) 1x

Thales Virtual Encryptor,CV1000, DPDK, Term Limited, 1-year, Enhanced Support	**1 070,00**
Thales Virtual Encryptor,CV1000, DPDK, Term Limited, 3-year, Enhanced Support	**2 130,00**
Thales Virtual Encryptor,CV1000, DPDK, Perpetual	**1 430,00**

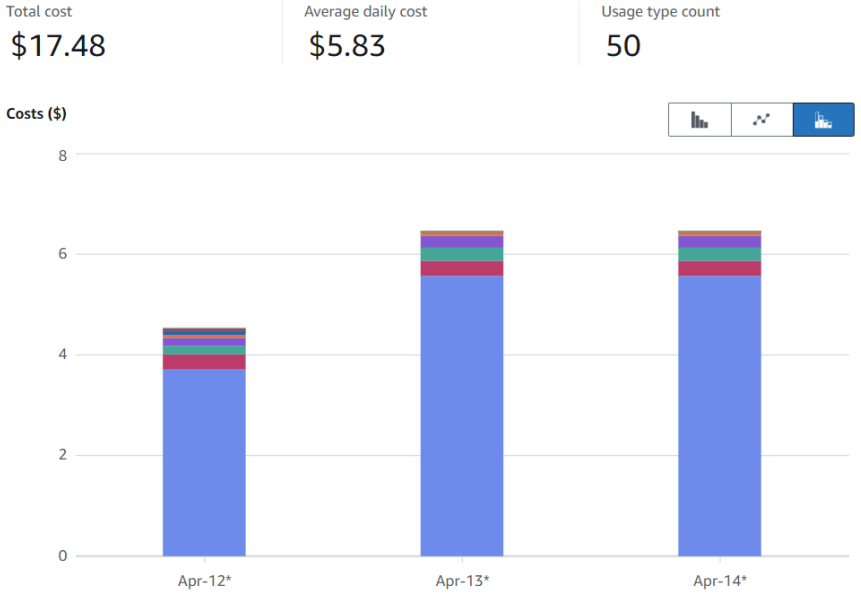
Zarządzanie:

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

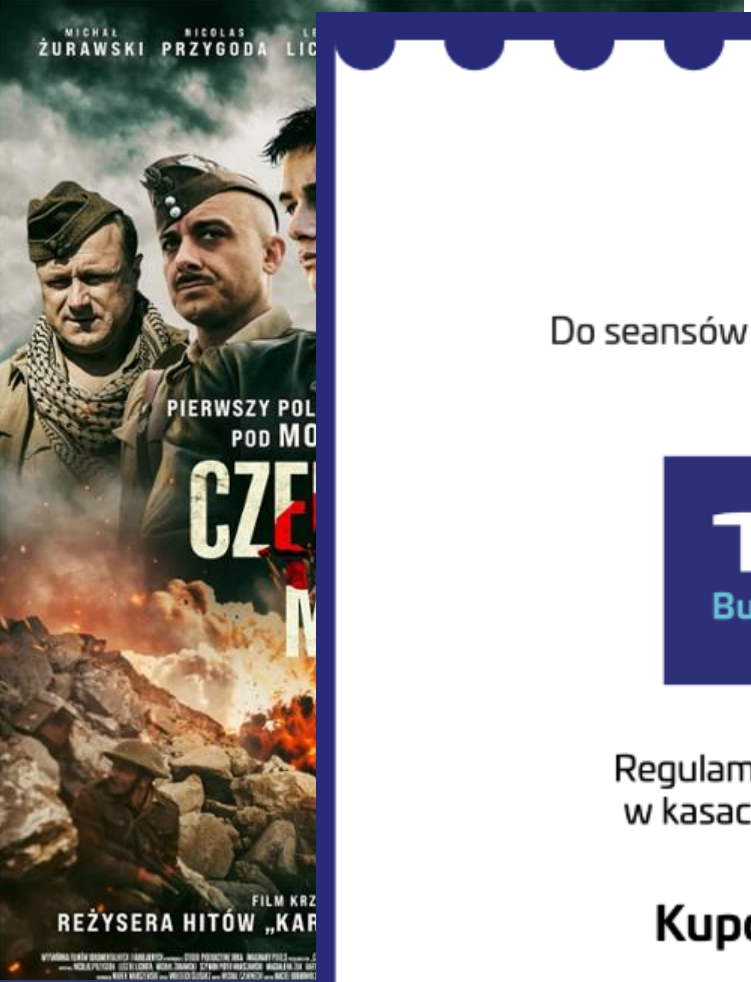
Koszty po stronie AWS?

Średnio 5,83 $/24h (mierzone przez 72h na działającym i obciążonym lekko środowisku)

- Za całość CV1000 (x.large) + 2x Elastic IP (Public IP) + Ubuntu (t5.micro)



CryptoPanel



Multikino

Ważny w całej Polsce.
Do seansów 3D oraz miejsc VIP obowiązuje dopłata.

NA FILM ZAPRASZA

THALES
Building a future we can all trust

Regulamin wykorzystania kuponu dostępny
w kasach kina oraz na stronie internetowej.

Kupon: XXXXXXXXXXXXXX

CryptoPanel

A teraz quiz