Případová studie migrace z Cisco ACE a další možnosti nasazení

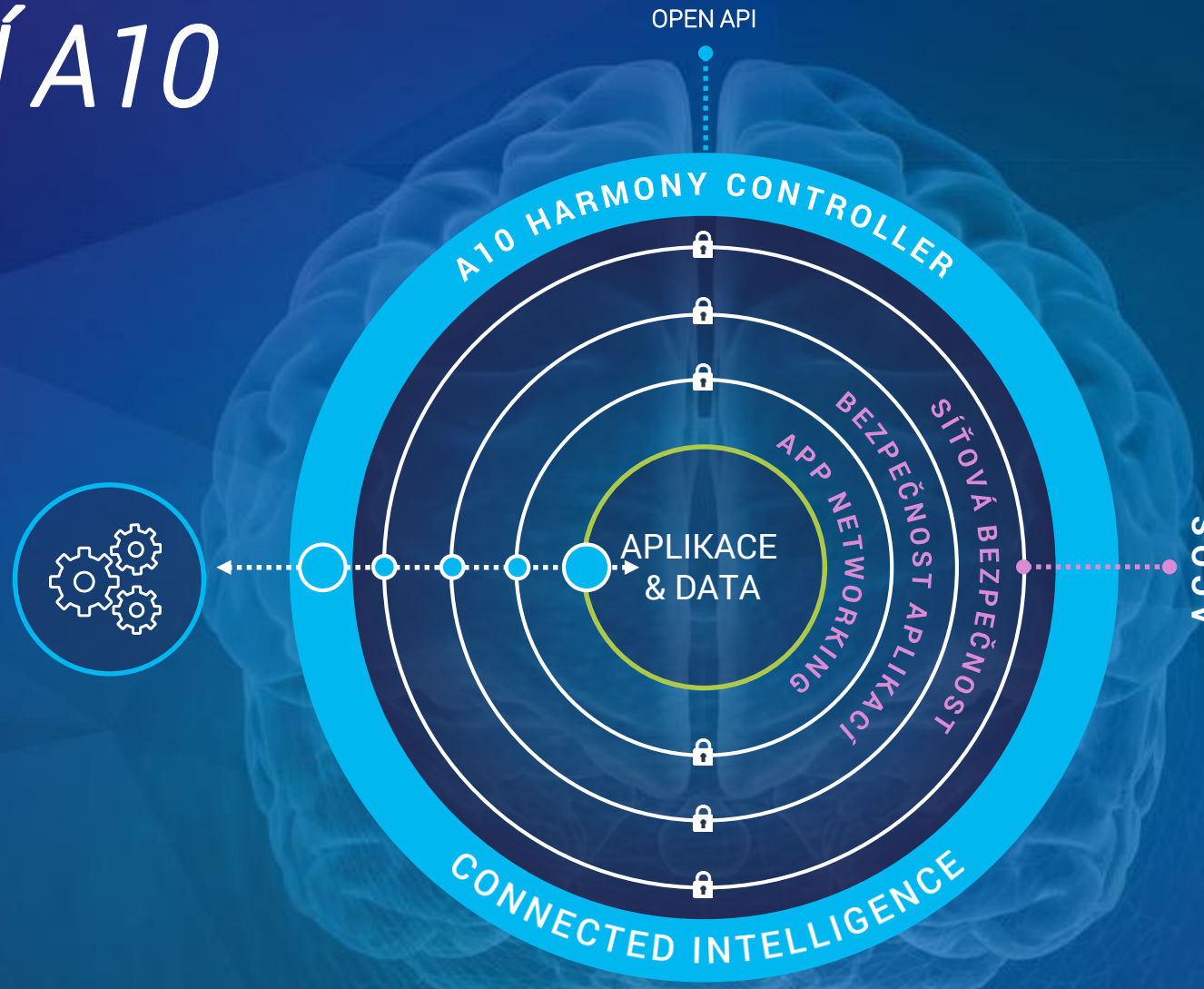
Ing. Jan Mazal, VPGC

- Mikulov, 5. 9. 2018

Reliable Security Always™

Konec podpory Cisco ACE

ŘEŠENÍ A10



Strojové učení
Analýza dat
Threat Intelligence

Bezpečné aplikační služby

- APP DELIVERY
- DDoS OCHRANA
- FIREWALL
- SSL VISIBILITY
- IPV4 PRESERVATION

ŘĚŠENÍ INTELIGENTNÍ AUTOMATIZOVANÉ BEZPEČNOSTI

Vybrané regionální reference

A10 Networks v ČR/SR

Distribuce a servis

VPGC
distinct.smart.innovative

Affinity Platinum

arreco

Akreditované školicí centrum

EDU Trainings

Affinity Gold

AUTOCONT

COMPAREX
Software · Consulting · Services

CGI

mainstream technologies

Případová studie: migrace z Cisco ACE

Zákazník:

Integrátor:

Výchozí situace se Cisco ACE

- Ukončení prodeje a podpory
  - Ukončení prodeje k 24. 1.2014
  - Ukončení podpory k 31. 1. 2019
- Slabý výkon systémů
  - Nedostatečná propustnost
  - Nízký SSL výkon
- Nevyhovující zabezpečení
  - Zranitelnost TLS (robotattack.org)
  - Absence funkcí Web Application Firewall
- Expertní znalost Cisco technologií
  - Certifikovaní in-house experti
  - Zachování kontinuity

Požadavky na nové řešení

Vysoká propustnost a SSL akcelerace

Vysoký počet souběžných L4 spojení

Vysoký počet nových L4 a L7 spojení za sekundu

Vysoký počet nových SSL spojení za s. při použití eliptických křivek

Web Application Firewall a DDoS ochrana

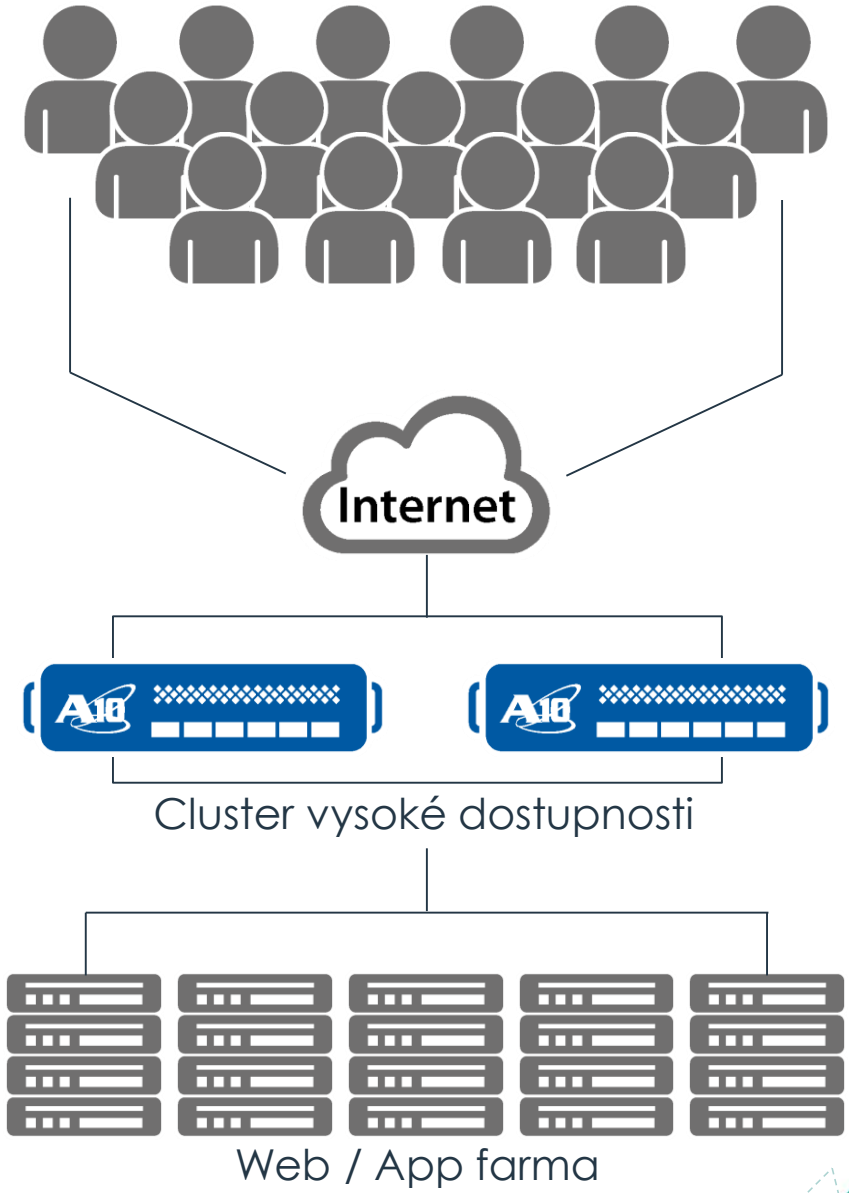
Samostatné konfigurační oddíly (virtual contexts)

Podpora skriptování v jazyku TCL

Sběr dat a napojení na monitoring pro plnění SLA

Navržené řešení

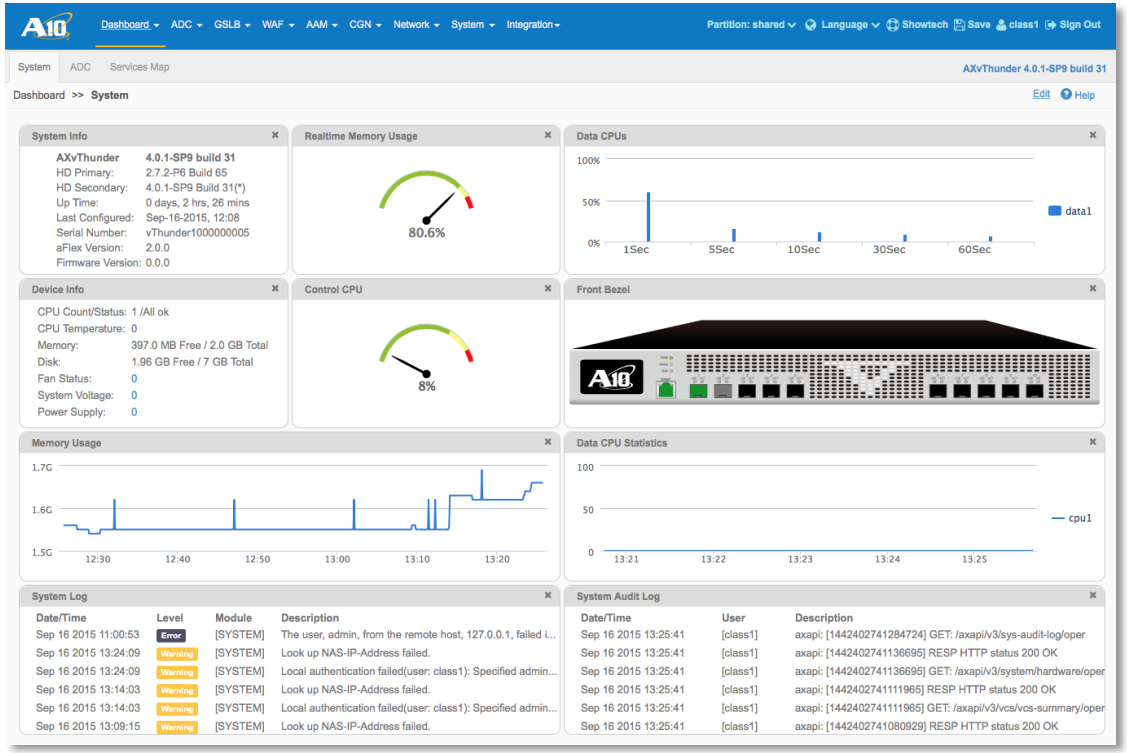
- 4× THUNDER 3040S
  (2× produkce + 1× dev/test + 1× záložní jednotka)
  - Propustnost 30 Gbps
  - Počet L4/L7 spojení 64 mil.
  - Počet nových spojení za sek. 750 tis.
  - Počet nových SSL spojení (ECDSA) 20 tis.
  - SYN flood DDoS ochrana 8 mil./s
- WAF a DDoS součástí all-in-one licence
- Průběžná podpora a monitoring řešení
- SLA 24×7 s garancí opravy do 4h



Zkušenosti uživatele

Rychlá orientace v novém prostředí

- Intuitivní GUI a snadné ovládání
- Méně konfiguračních kroků



- CLI podobné Cisco IOS
- Vestavěná detailní nápověda

```
vThunder#sh ver
AX Series Advanced Traffic Manager AXvThunder
  Copyright 2007-2015 by A10 Networks, Inc.  All A10 Networks products are
  protected by one or more of the following US patents:
  8918857, 8914871, 8904512, 8897154, 8868765, 8849938, 8826372, 8813180
  8782751, 8782221, 8595819, 8595791, 8595383, 8584199, 8464333, 8423676
  8387128, 8332925, 8312507, 8291487, 8266235, 8151322, 8079077, 7979585
  7804956, 7716378, 7665138, 7647635, 7627672, 7596695, 7577833, 7552126
  7392241, 7236491, 7139267, 6748084, 6658114, 6535516, 6363075, 6324286
  5931914, 5875185, RE44701, 8392563, 8103770, 7831712, 7606912, 7346695
  7287084, 6970933, 6473802, 6374300

      64-bit Advanced Core OS (ACOS) version 4.0.1-SP9, build 31 (Aug-24-2015,14
:34)
        Booted from Hard Disk secondary image
      Licenses:  Bandwidth
      Serial Number: vThunder1000000005
      aFleX version: 2.0.0
      aXAPI version: 3.0
      Hard Disk primary image version 2.7.2-P6, build 65
      Hard Disk secondary image (default) version 4.0.1-SP9, build 31
      Last configuration saved at Sep-16-2015, 12:08
      Virtualization type: VMware
      Hardware: 1 CPUs(Stepping 2), Single 8G Hard disk
      Memory 2054 Mbyte, Free Memory 395 Mbyte
      Hardware Manufacturing Code: N/A
      Current time is Sep-16-2015, 13:27
      The system has been up 0 day, 2 hours, 27 minutes
vThunder#
```

Zkušenosti uživatele

Snadná a rychlá migrace konfigurace (ilustrační příklad)

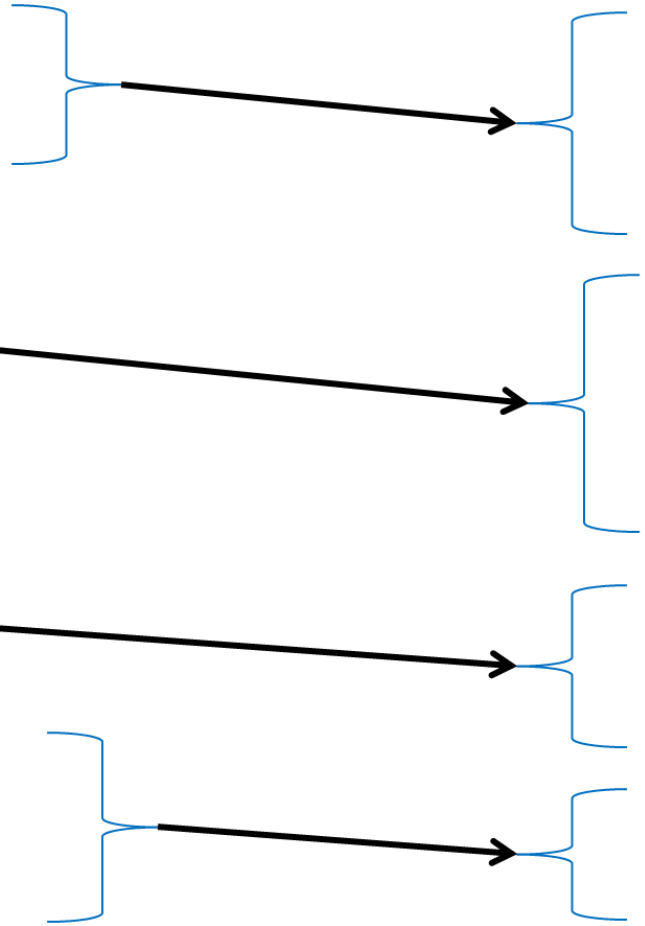
Cisco ACE

```
interface vlan 120
  description Upstream VLAN_120 - Clients and VIPs
  ip address 192.168.120.1 255.255.255.0
  fragment chain 20
  fragment min-mtu 68

rserver host SERVER1
  ip address 192.168.252.245
  inservice
rserver host SERVER2
  ip address 192.168.252.246
  inservice
rserver host SERVER3
  ip address 192.168.252.247
  inservice

serverfarm host SFARM1
  probe UDP
  rserver SERVER1
    inservice
  rserver SERVER2
    inservice
  rserver SERVER3
    inservice

class-map match-all L4UDP-VIP_114:UDP_CLASS
  2 match virtual-address 192.168.120.114 udp eq 53
policy-map type loadbalance first-match L7PLBSF_UDP_POLICY
  class class-default
    serverfarm SFARM1
```

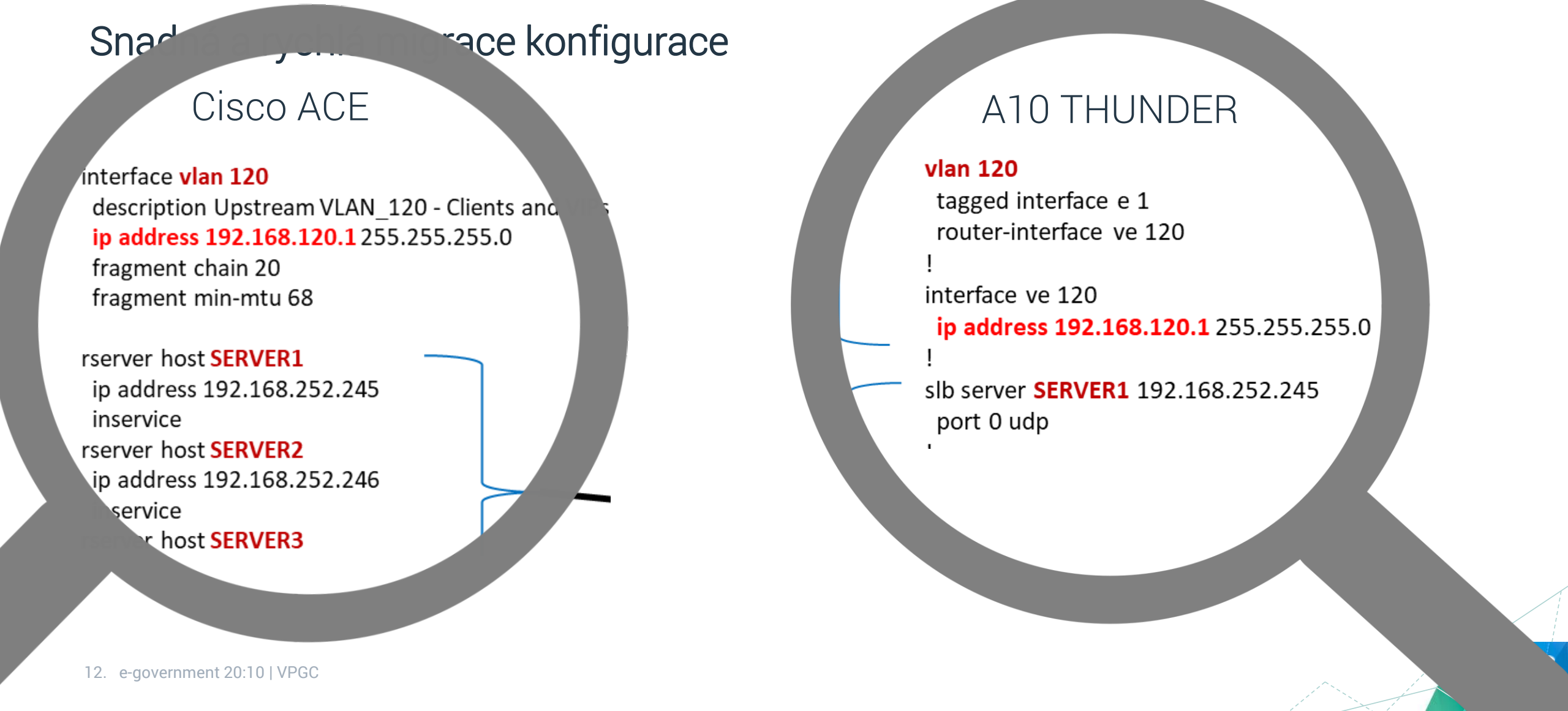


A10 THUNDER

```
vlan 120
  tagged interface e 1
  router-interface ve 120
!
interface ve 120
  ip address 192.168.120.1 255.255.255.0
!
slb server SERVER1 192.168.252.245
  port 0 udp
!
slb server SERVER2 192.168.252.246
  port 0 udp
!
slb server SERVER3 192.168.252.247
  port 0 udp
!
slb service-group SFARM1 udp
  health-check UDP
  member SERVER1:None
  member SERVER2:None
  member SERVER3:None
!
slb virtual-server vs_192_168_120_114 192.168.120.114
  port udp
    name L4UDP-VIP_114:UDP_CLASS
    service-group SFARM1
```

Zkušenosti uživatele

Snadná a rychlá migrace konfigurace



Zkušenosti uživatele

Vysoký výkon při testování převyšující udávané parametry

- Ve specifikaci A10 TH3040 je k počtu 30 000 new SSL / sec informace:
  *performance pro nejhorší kombinaci s RSA

Dle tabulky total SSL sessions s četností typů z reálného provozu:
- nejhorší kombinace bude zřejmě tls1-rsa-aes-256-gcm-sha384
- největší četnost klientů je tls1-ecdhe-rsa-aes-128-gcm-sha256
- ecdhe-rsa je 3x rychlejší než prostý dhe-rsa
- nejčetnější klienti používají s ecdhe-rsa jen rsa-aes-128
- gcm má opět menší overhead v komunikaci

výkonový limit A10 bude zřejně pro nejčetnější typ až 4x vyšší

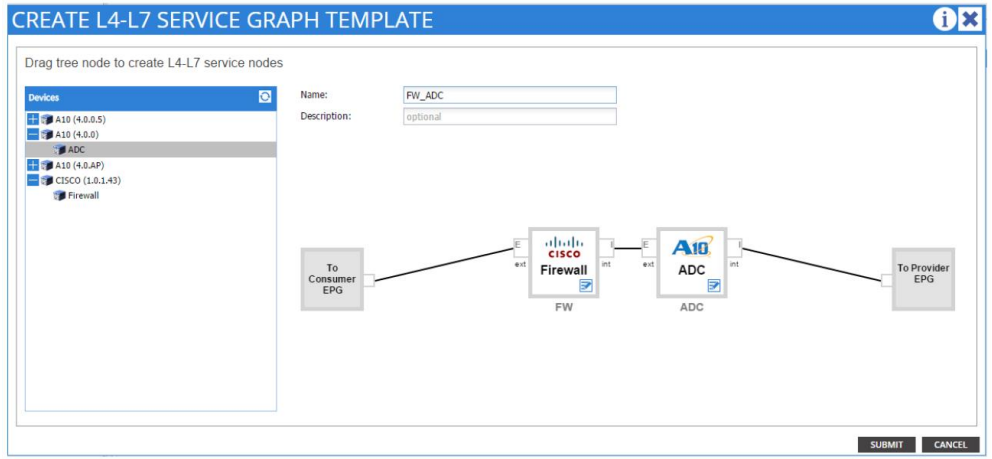
0x0300C02F	tls1-ecdhe-rsa-aes-128-gcm-sha256	341758
0x0300C013	tls1-ecdhe-rsa-aes-128-sha	254
0x0300C027	tls1-ecdhe-rsa-aes-128-sha256	0
0x0300C030	tls1-ecdhe-rsa-aes-256-gcm-sha384	2932
0x0300C014	tls1-ecdhe-rsa-aes-256-sha	749
0x0300009C	tls1-rsa-aes-128-gcm-sha256	343
0x0300002F	tls1-rsa-aes-128-sha	55
0x0300003C	tls1-rsa-aes-128-sha256	1
0x0300009D	tls1-rsa-aes-256-gcm-sha384	655
0x03000035	tls1-rsa-aes-256-sha	13
0x0300003D	tls1-rsa-aes-256-sha256	0

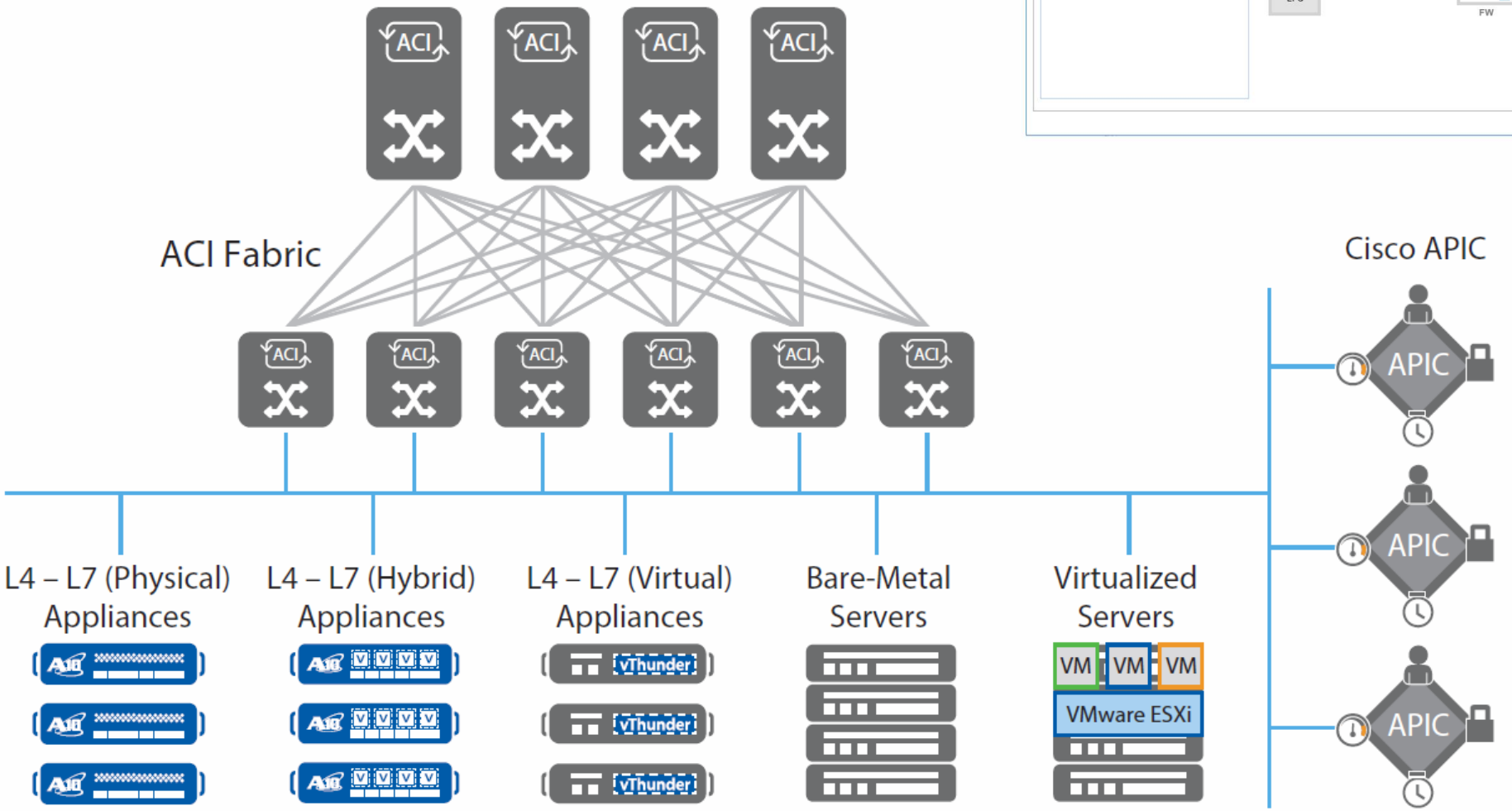
Výsledné shrnutí

1. Rychlá orientace v novém prostředí
2. Snadná a rychlá migrace konfigurace
3. Vysoký výkon převyšující udávané parametry
4. Integrace s monitoringem a napojení systému prostřednictvím REST API
5. Plná podpora lokálního integrátora Asseco

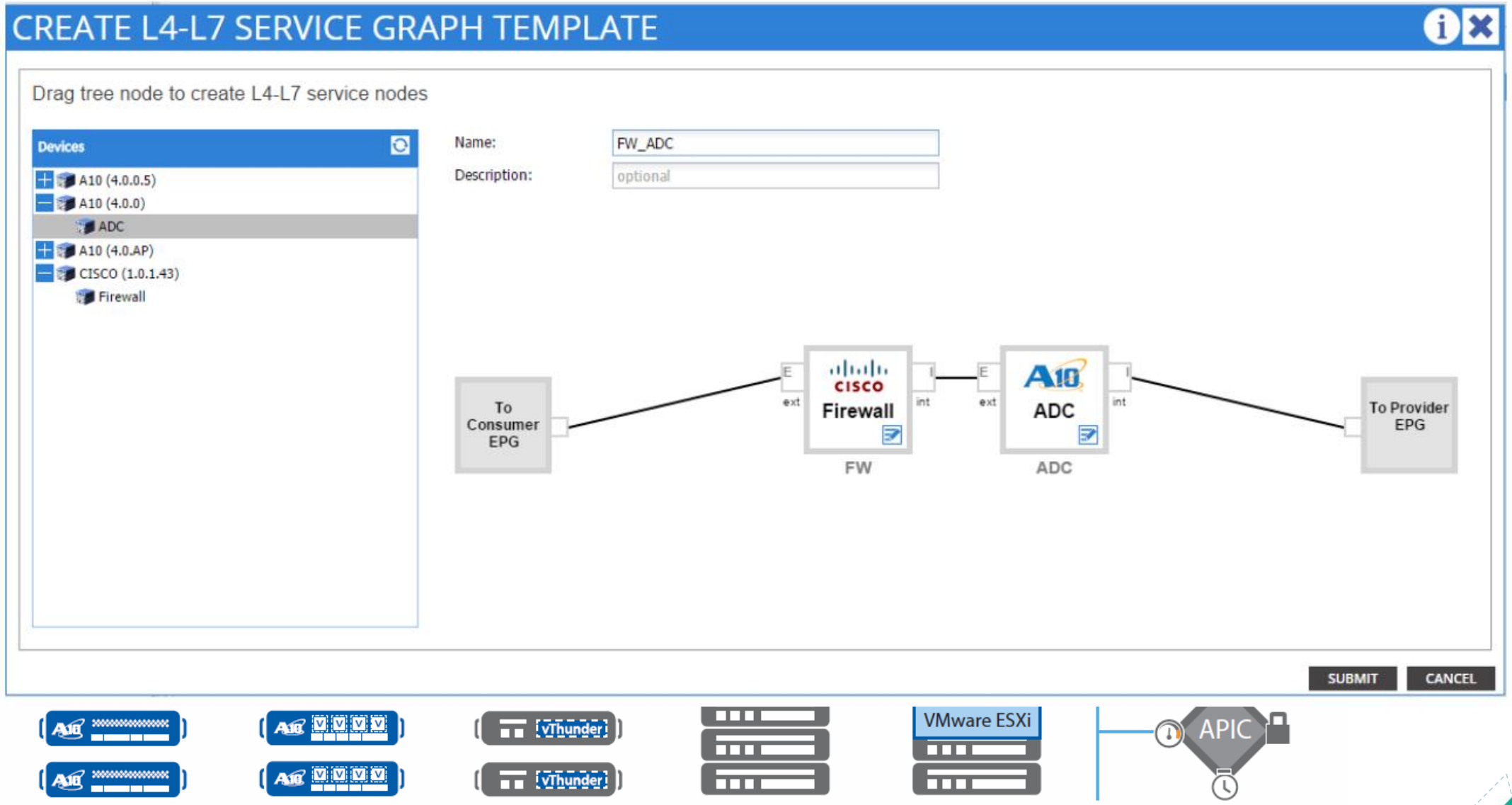
Další možnosti nasazení

Integrace se Cisco ACI



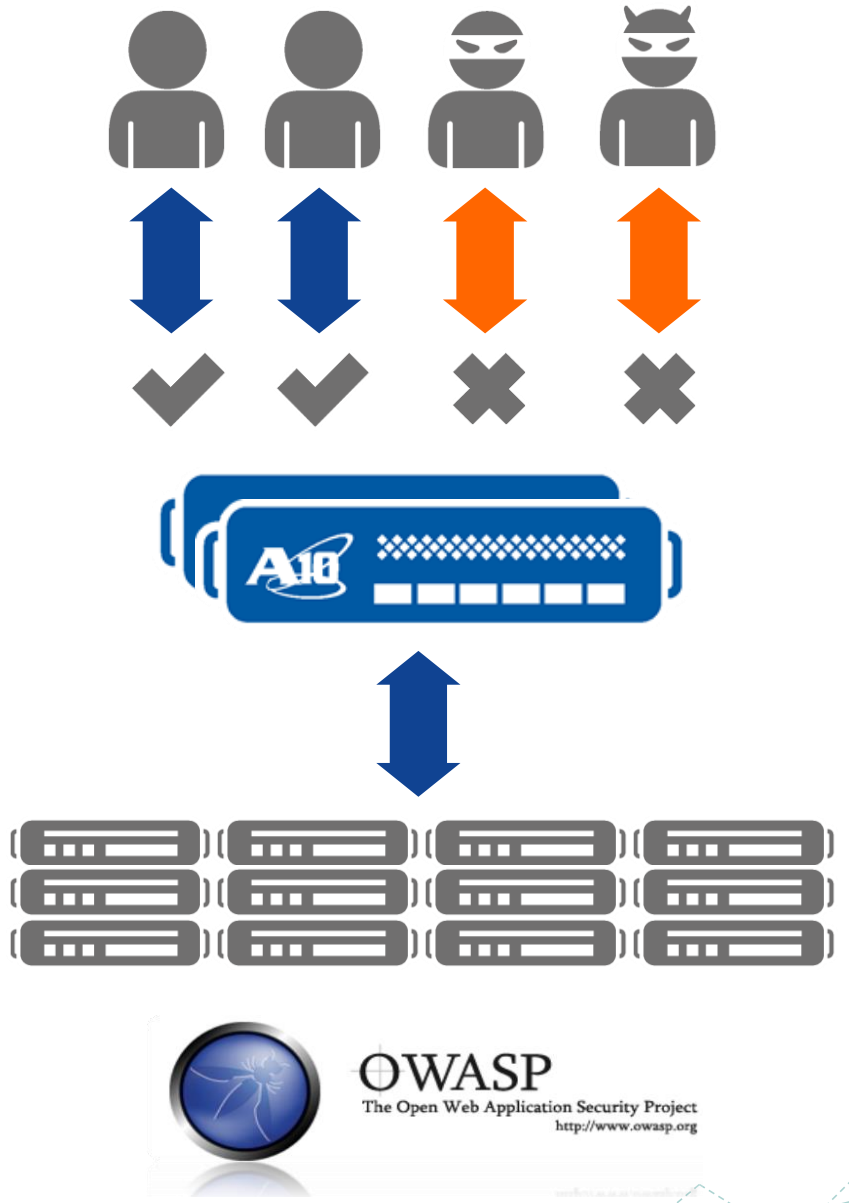


Integrace se Cisco ACI

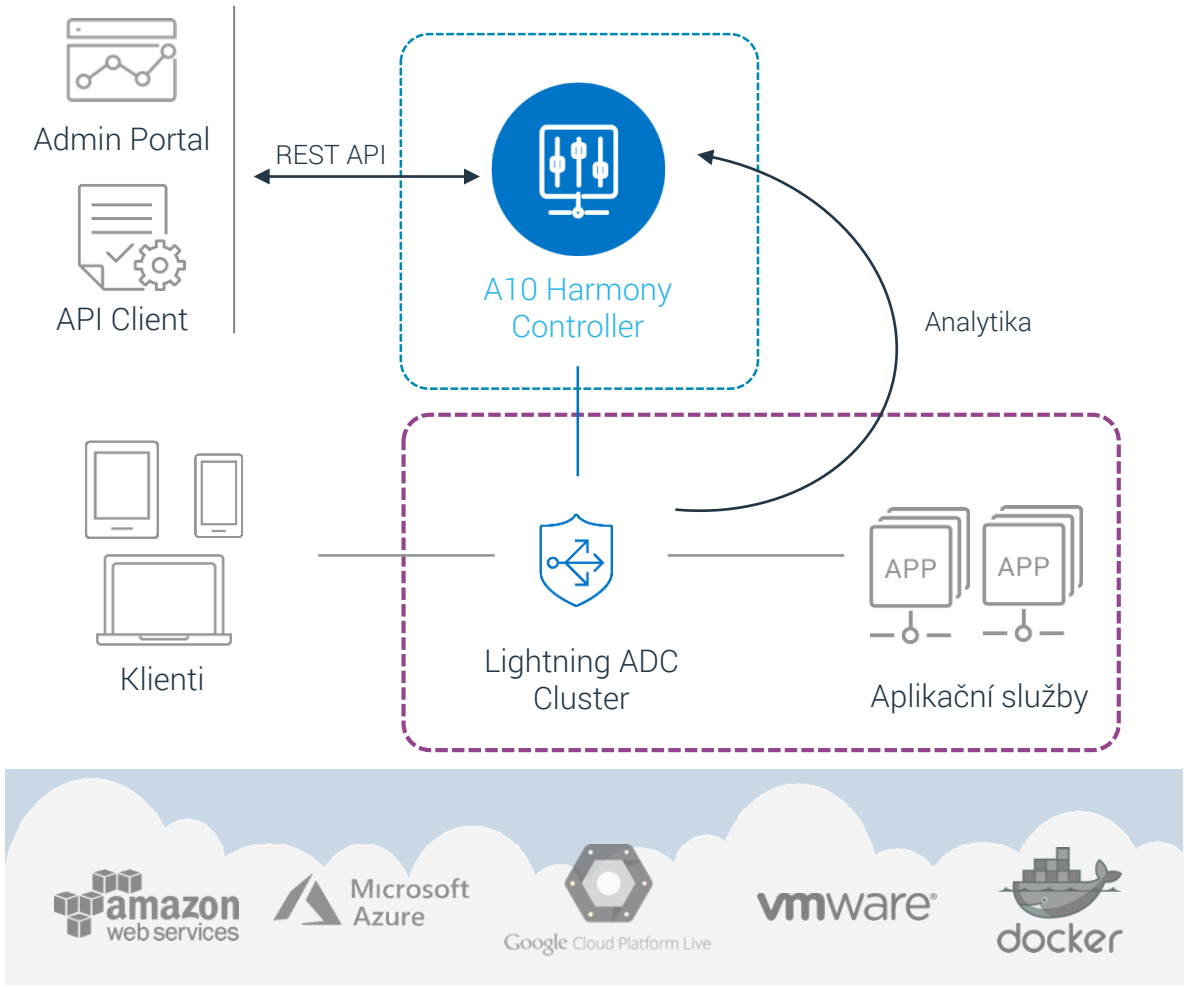


Web Application Firewall (WAF)

- Funkce
  - Zabezpečení webových aplikací
  - Prevence úniku dat, duševního vlastnictví
  - Ochrana proti zranitelnostem podle OWASP
  - Zajištění souladu se standardy PCI/HIPAA
- Výhody
  - Není potřeba žádná další licence
  - Podpora všech transportních vrstev
  - Škálovatelné a vysoce výkonné řešení

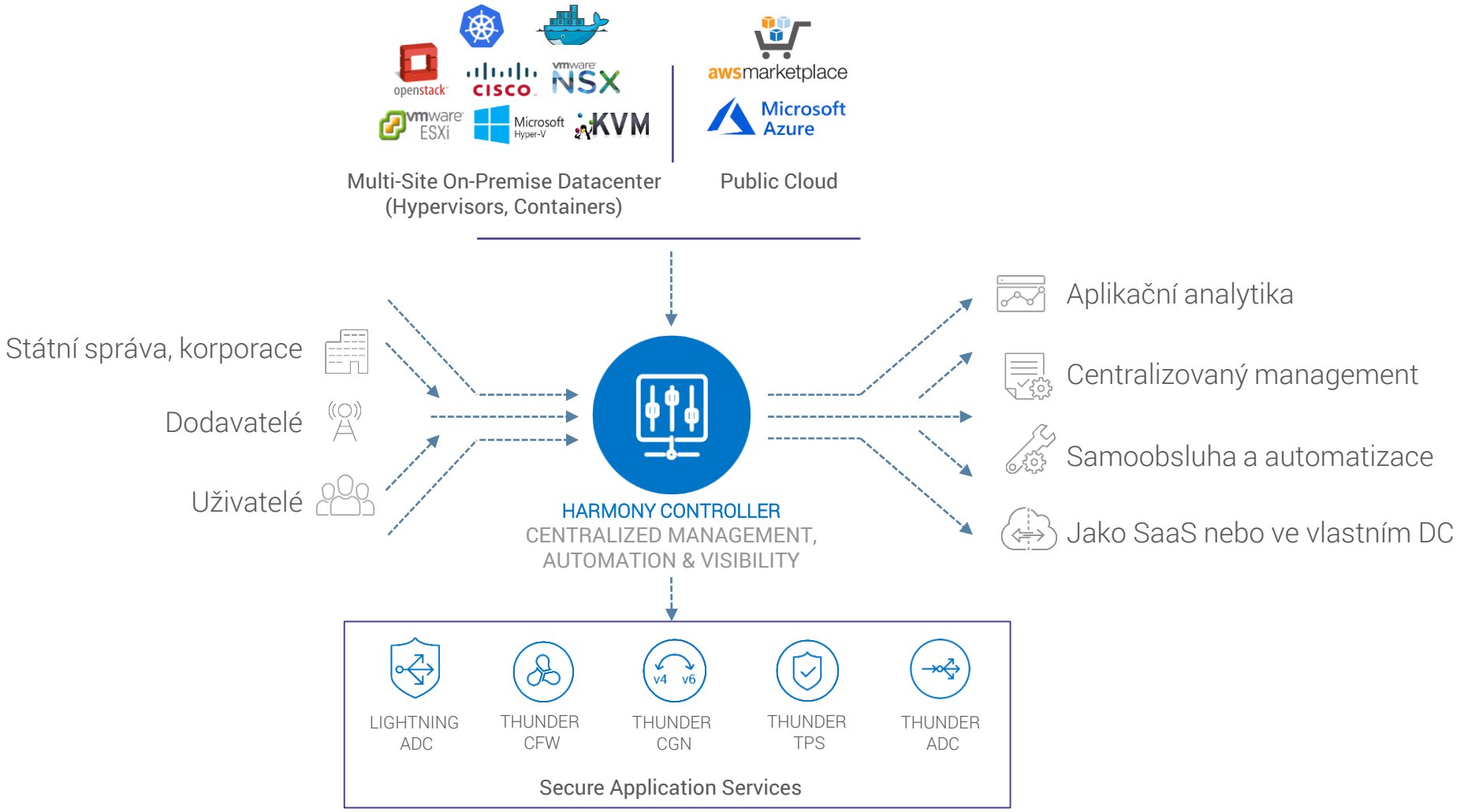


A10 Lightning pro kontejnery a cloud

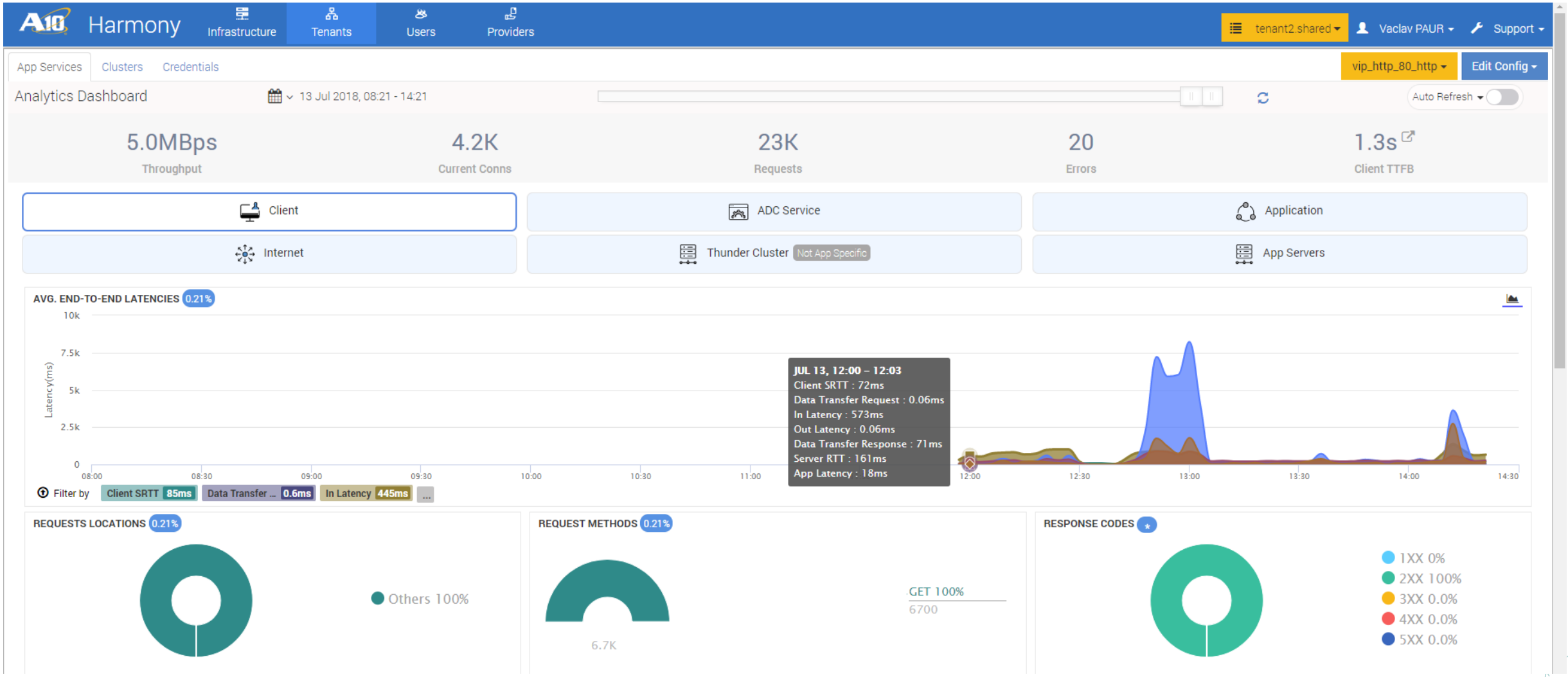


- Elastický ADC & aplikační firewall
- Vyvinutý na míru pro
  - Cloudové aplikace
  - Mikroslužby a kontejnery
- Dostupný v MS Azure, AWS, Google Cloud
- Jednodušší a levnější proti jiným řešením
  - Integrace s DevOps a CI/CD procesy
  - Podpora Server-less prostředí

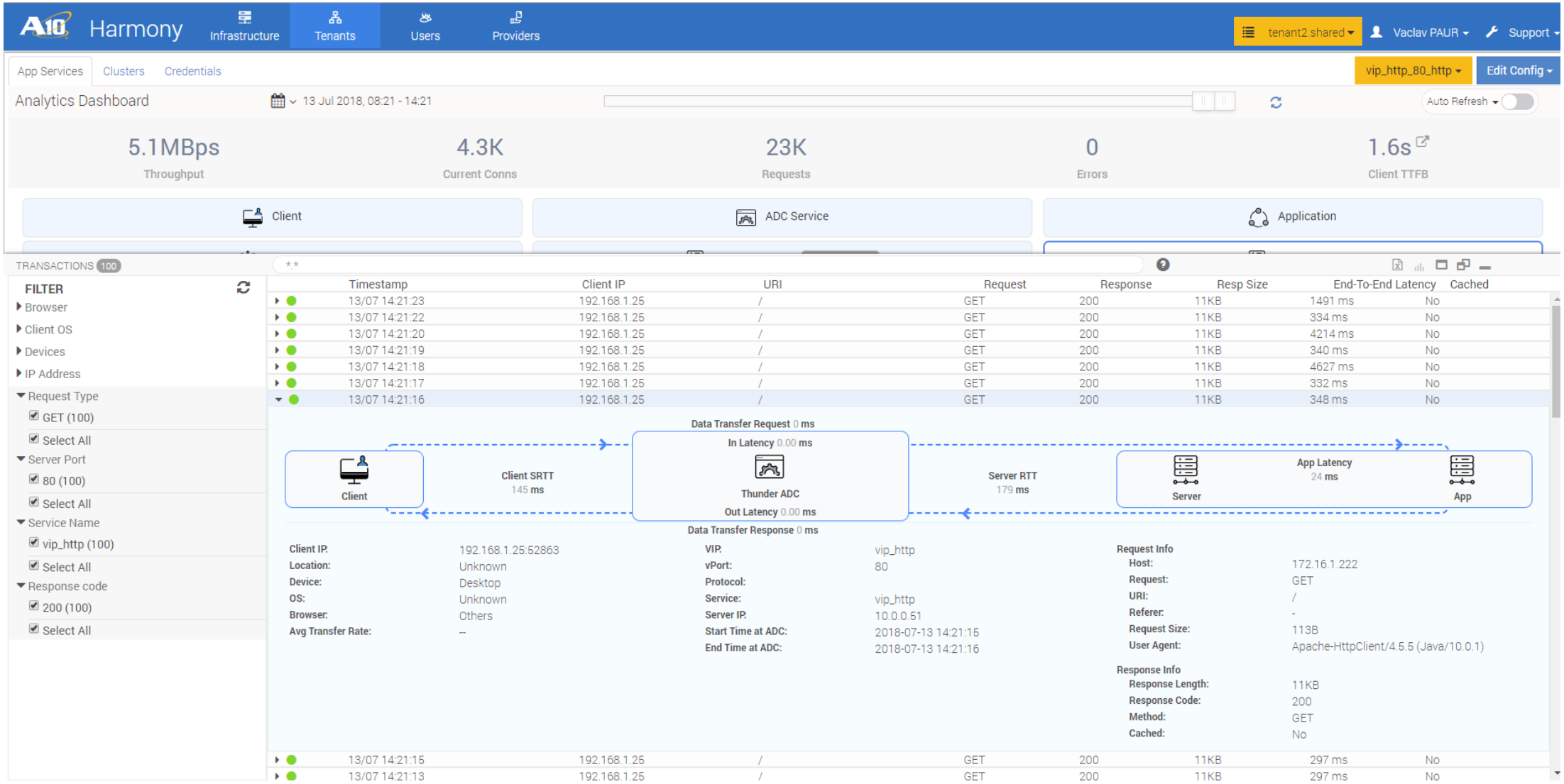
Harmony Controller



Harmony Controller – ukázka



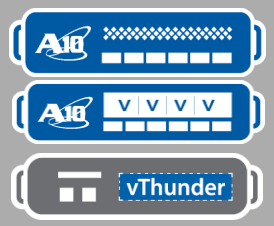
Harmony Controller – ukázka



Shrnutí

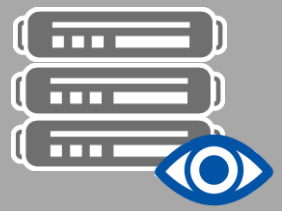
Čeho si uživatelé nejvíc cení

Vysoký výkon daný architekturou OS ACOS



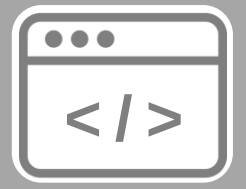
Funkcionality pro dostupnost, akceleraci a zabezpečení

Všechny funkce součástí jedné licence



Monitoring aplikací v centrálním managementu

100% otevřenost systému přes REST API



Možnosti skriptování – jazyk aFlex TCL

Kontakty

- VPGC – www.vpgc.com
- Asseco – ce.asseco.com

Děkujeme