

# Typické problémy CGNAT a monitorování jeho využití v praxi

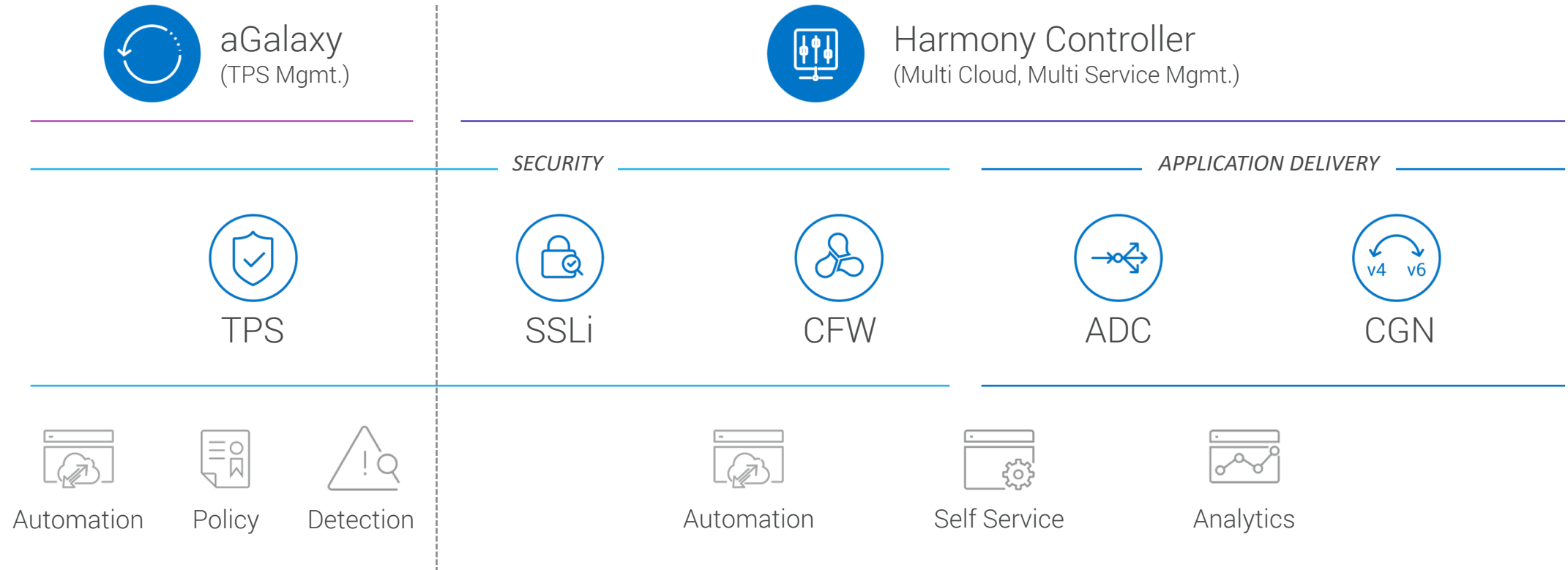
Václav Paur, CTO, VPGC



*Reliable Security Always™*

**VPGC**  
distinct.smart.innovative

# Portfolio A10 Networks



# Typické problémy dnešních implementací CGNAT



**Špatná škálovatelnost:** CGNAT zatěžuje páteřní směrovač; není v HA konfiguraci; nemá dostatečný výkon



**Funkcionalita:** malé možnosti NAT, chybějící ALG a další



**Bezpečnost:** Nulová ochrana veřejných adres proti DDoS útokům



**Složitá konfigurace:** Operační systém + aplikace, správa řešení



**Minimální analytika:** Informace o uživatelích a výkonu systému

# Řešení od A10 Networks pro ISP a Telco

A10 Networks Thunder 5440 CGN



100 Gb/s  
propustnost

250 mil.  
souběžných spojení

1U  
velikost

Anti-DDoS  
integrovaný

IPv4 / IPv6  
mnoho protokolů

1024  
kontexty



# Vybranné modely A10 Thunder CGN

| <b>VÝKON</b>                      | THUNDER<br><b>1040</b> CGN | THUNDER<br><b>3040</b> CGN | THUNDER<br><b>4440</b> CGN | THUNDER<br><b>5440</b> CGN |
|-----------------------------------|----------------------------|----------------------------|----------------------------|----------------------------|
| Propustnost                       | 20 Gbps                    | 30 Gbps                    | 80 Gbps                    | 100 Gbps                   |
| Počet spojení za sekundu          | 0.8 mil.                   | 1.1 mil.                   | 2.5 mil.                   | 5 mil.                     |
| Počet full TCP spojení za sekundu | 0.3 mil.                   | 0.4 mil.                   | 1.1 mil.                   | 2.2 mil.                   |
| Počet současně navázaných spojení | 32 mil.                    | 64 mil.                    | 128 mil.                   | 256 mil.                   |
| Hardwarová akcelerace             | ne                         | ne                         | 2xFTA-4                    | 2xFTA-4                    |
| Počet kontextů (partitions)       | 32                         | 64                         | 128                        | 1024                       |

## **SÍŤOVÁ ROZHRANÍ**

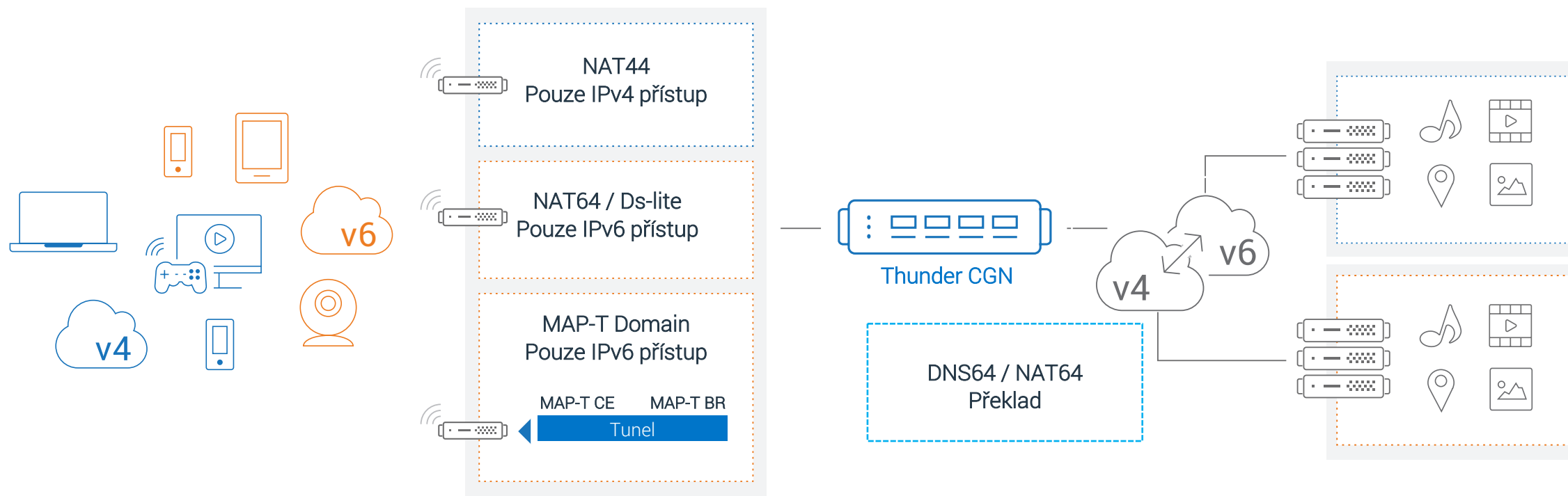
|                 |     |     |    |    |
|-----------------|-----|-----|----|----|
| 1 GE (RJ45/SFP) | 5/0 | 6/2 |    |    |
| 1/10 GE (SFP+)  | 4   | 4   | 16 | 24 |
| 40 GE (QSFP+)   |     |     | 4  | 4  |

## **FYZICKÉ PROVEDENÍ**

|            |      |      |      |      |
|------------|------|------|------|------|
| Rozměr     | 1U   | 1U   | 1U   | 1U   |
| Max. odběr | 110W | 240W | 445W | 445W |

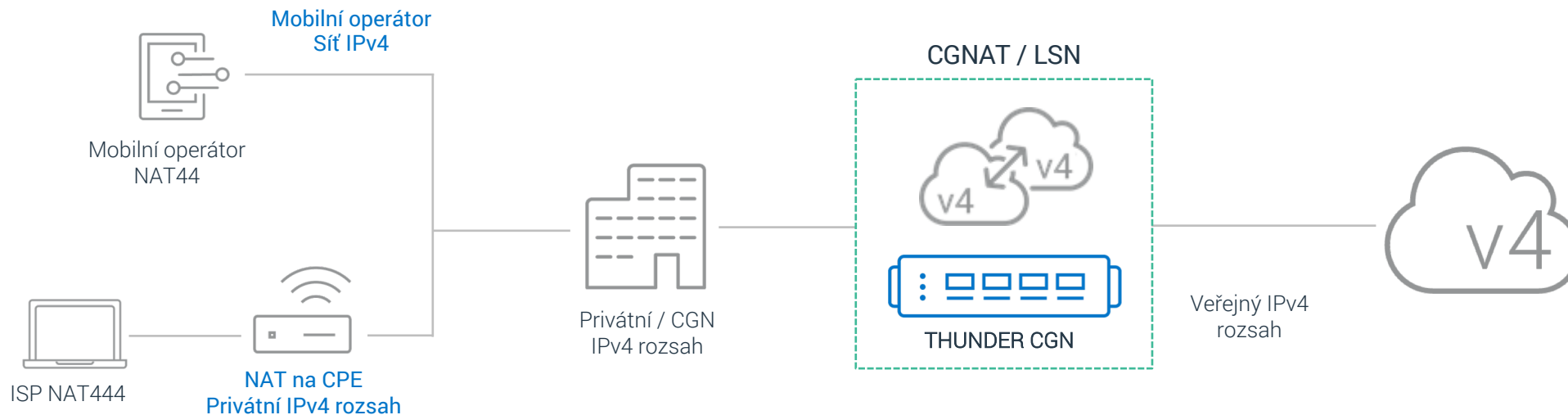


# Funkce NAT



Ověřené řešení pro postupnou migraci na IPv6

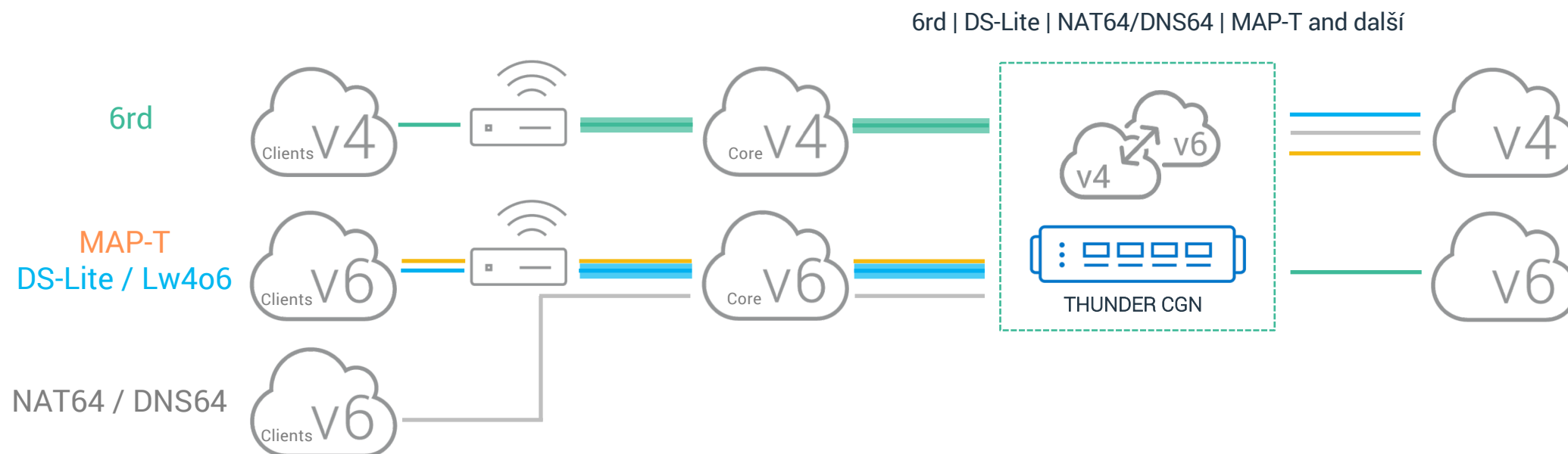
# Řešení A10 Networks pro ISP/Telco operátory



## CGNAT v prostředí IPv4

- Transparentní IPv4 konektivita
- Možnost omezení počtu portů na uživatele
- Podpora uživatelských aplikací

# Snadná migrace na IPv6

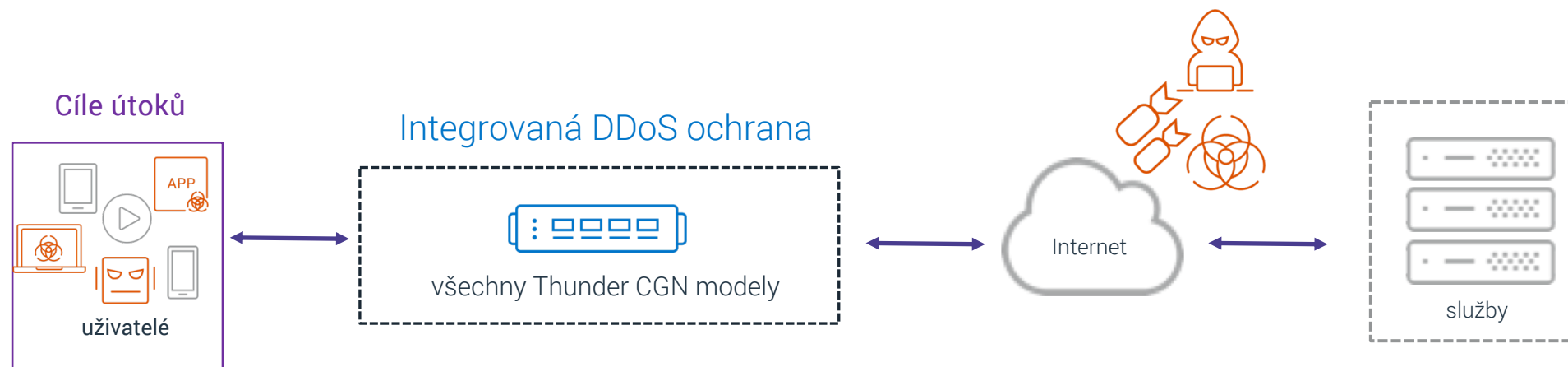


## Podpora mnoha strategií migrace na IPv6

- Souběh obou protokolů
- Zajištění konektivity mezi IPv6 klientem a IPv4 obsahem
- Snadný postupný přechod
- Bez dopadu na uživatele



# Multivektorové DDoS útoky jsou větší a komplexnější



## Integrovaná DDoS ochrana v prostředí poskytovatele telekomunikačních služeb

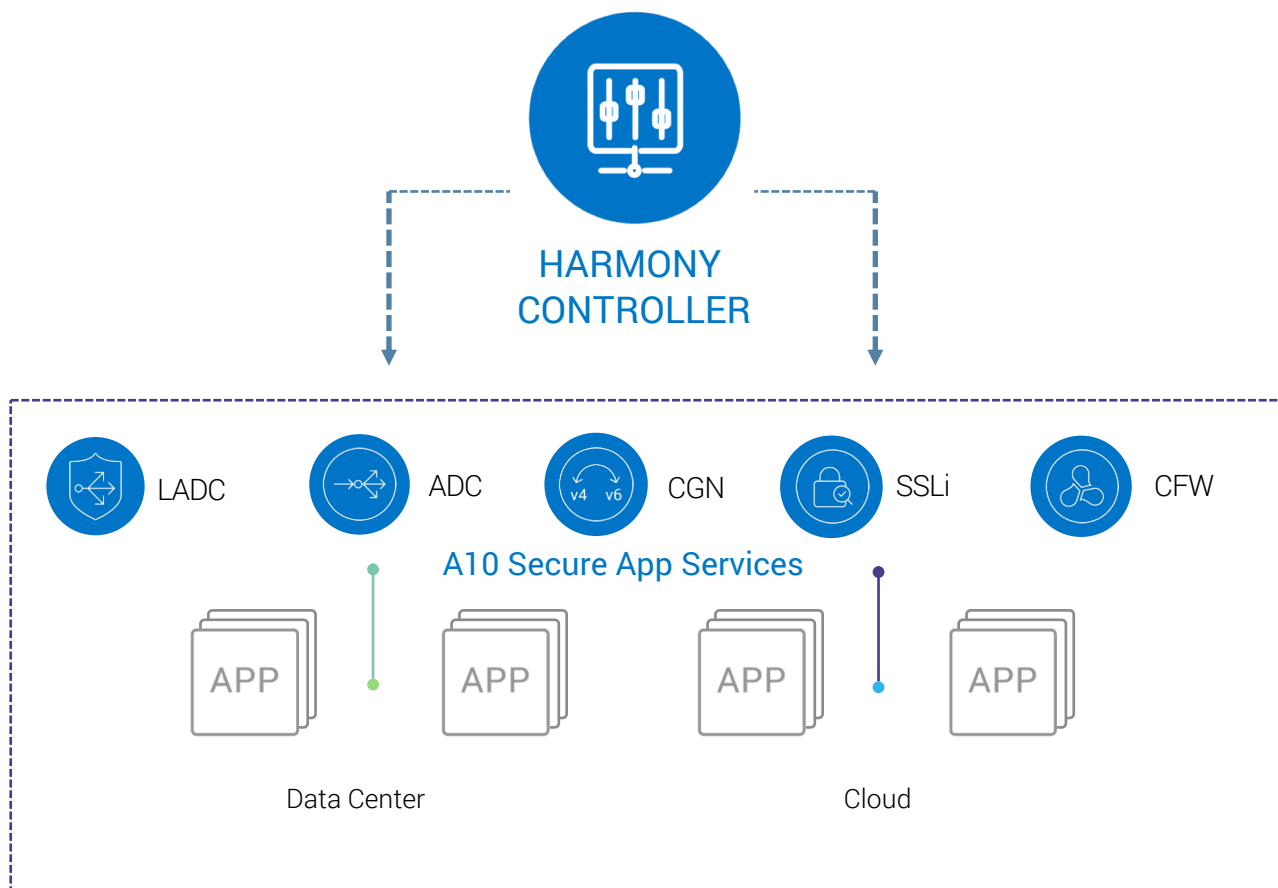
- IP Black List DDoS Protection – ochrana NAT poolu
- IP Anomaly Filtering – ochrana proti útokům na bázi deformovaných paketů
- Connection Rate Limiting – ochrana proti volumetrickým útokům
- Selective Filtering – ochrana proti známým zdrojům útoků

# Složitá konfigurace?

```
class-list CLIENTS ipv4
  10.0.0.0/8 lsn-lid 1
interface management
  ip address 192.168.1.18 255.255.255.0
  ip default-gateway 192.168.1.254
interface ethernet 1
  enable
  ip address 100.64.0.1 255.255.255.0
  ip nat inside
interface ethernet 2
  enable
  ip address 198.18.0.1 255.255.255.0
  ip nat outside
ip route 10.0.0.0 /8 100.64.0.254
ip route 0.0.0.0 /0 198.18.0.254
```

```
cgnv6 server LOG_SERVER 192.168.1.222
  port 514 udp
cgnv6 service-group LOG_SG udp
  member LOG_SERVER 514
cgnv6 template logging LOGGING
  service-group LOG_SG
cgnv6 lsn inside source class-list CLIENTS
cgnv6 nat pool POOL 172.16.1.1 172.16.1.254
  netmask /24
cgnv6 lsn logging default-template LOGGING
cgnv6 lsn-lid 1
  name LSN_1
  source-nat-pool POOL
  user-quota icmp 128
  user-quota udp 1024 reserve 512
  user-quota tcp 1024 reserve 512
```

# A10 Harmony Controller



Centralizovaný management všech instancí Thunder. Běží v datovém centru nebo v cloudu.

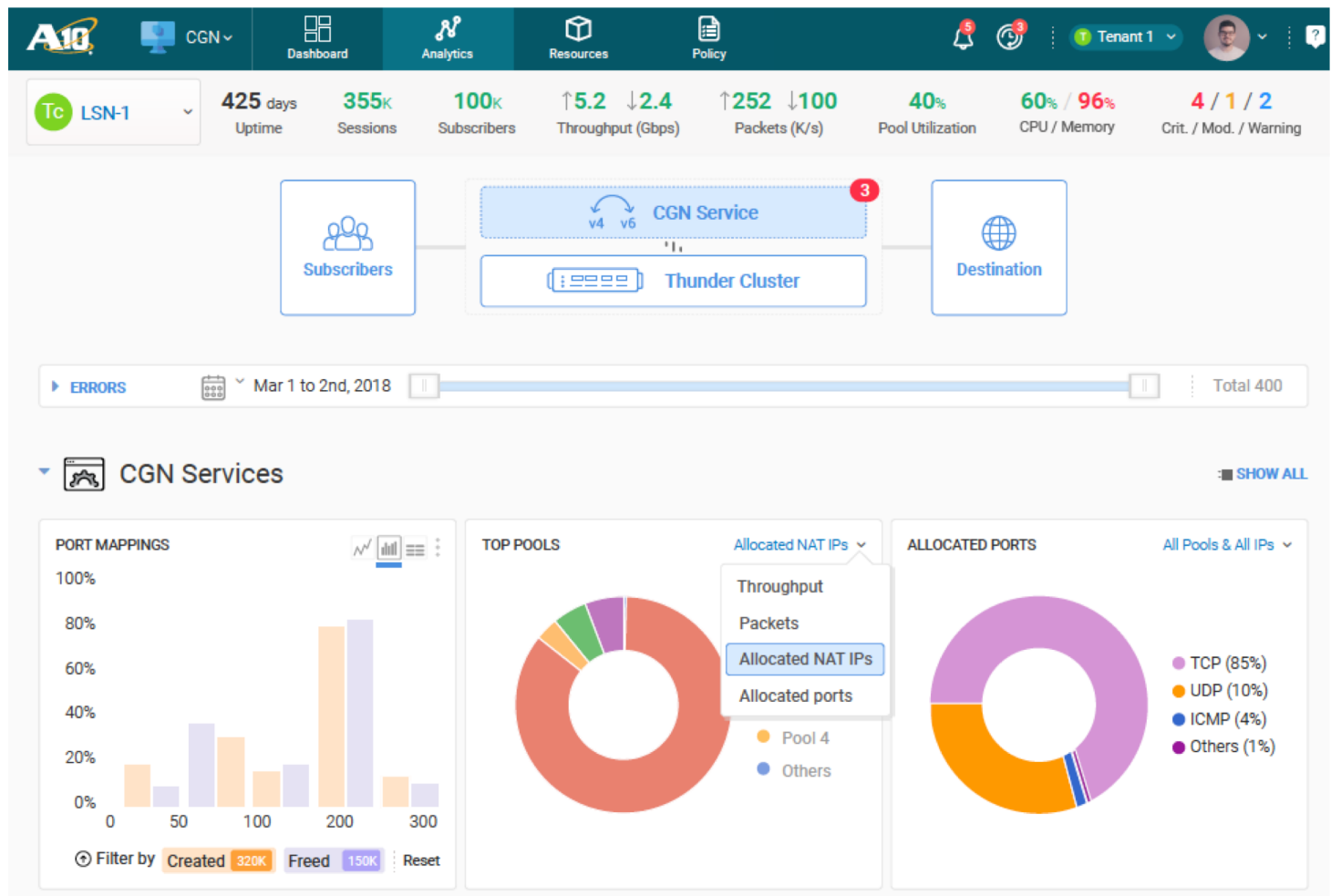


Automatizace a otevřená API



Analytika pro proaktivní management a řešení problémů

# Analytika v HC – Dashboard CGN



## UŽIVATELÉ

- Celková propustnost a upozornění na kvóty uživatelů
- Navázaná/ukončená spojení na uživatele
- Top uživatelé podle propustnosti/spojení

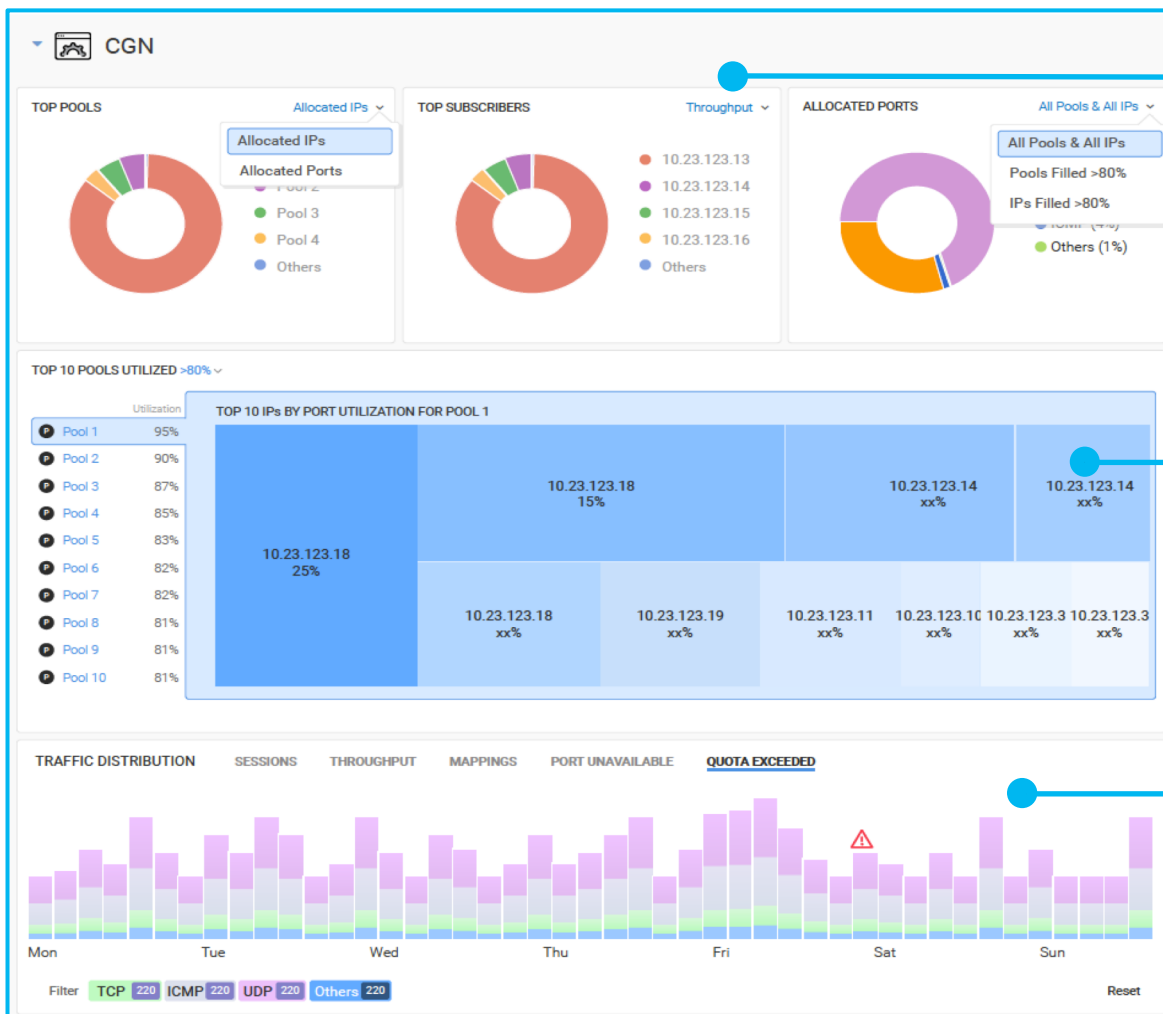
## CGN SLUŽBY

- Stav alokací a chybové stavy - kvóty
- Alokace portů podle protokolu
- Statistiky Top poolu podle počtu spojení
- Využití Full Cone Session a další

## DESTINACE

- Celkový počet paketů podle protokolů
- Analytika fragmentovaného provozu
- Průměrná velikost paketů, atd.

# Analytika v HC – CGN pohled



## VHLED DO SPOJENÍ PŘEDPLATITELŮ

- Míry navázání/ukončení spojení - behaviorální ukazatele potenciálního DDoS útoku
- Předplatitelé spotřebovávající nejvíce šířky pásma/toků – ukazatele potenciálního zneužití sítě

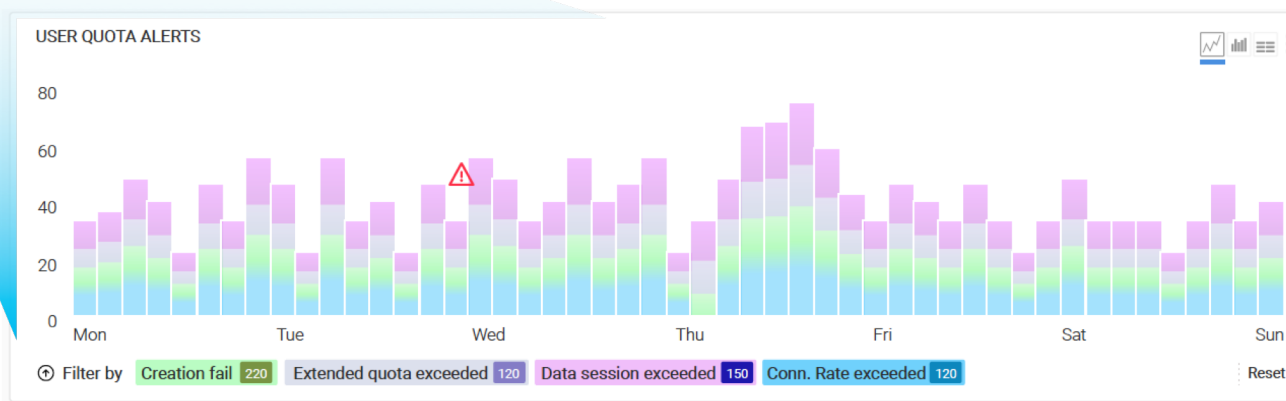
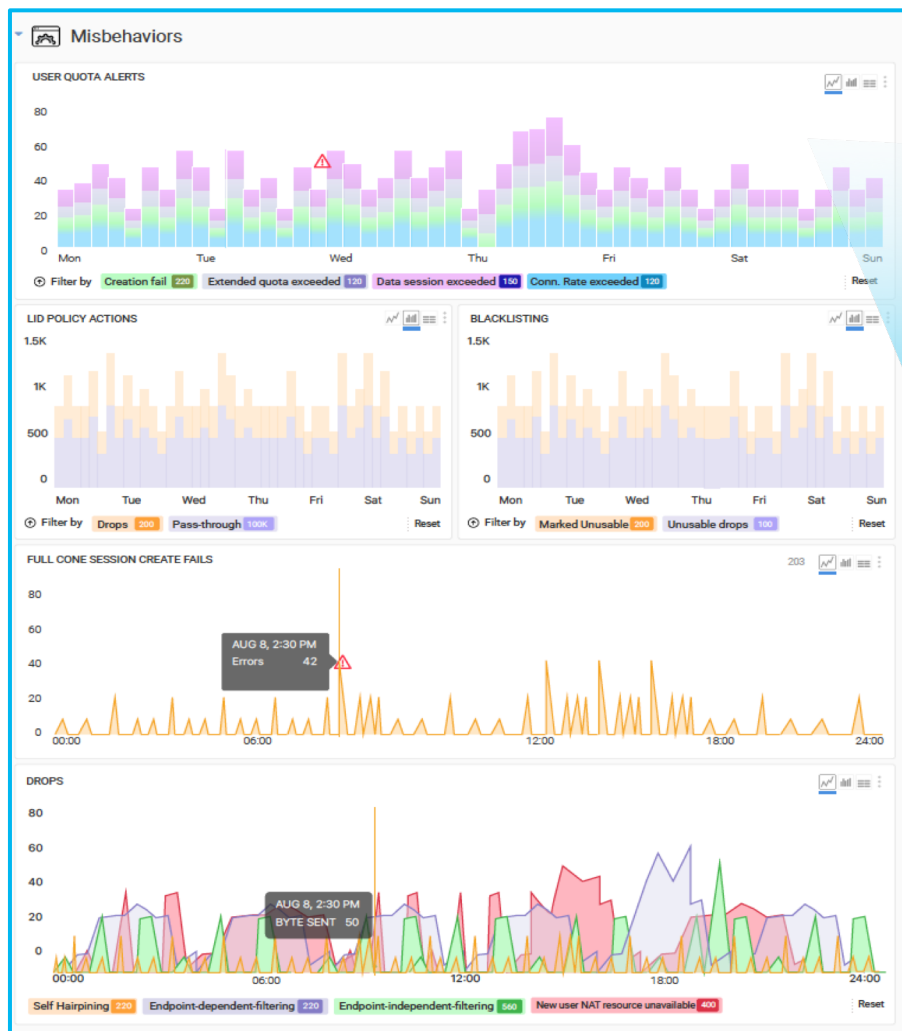
## SLEDOVÁNÍ ZDROJŮ CGN

- Mapování per protokol a technologii – behaviorální ukazatele potenciálního botnet DDoS útoku
- Využití NAT IP poolu – ukazatele útoků na NAT IP pooly

## UPOZORNĚNÍ NA ROZLOŽENÍ PROVOZU

- Upozornění na uživatelské kvóty předplatitelů – může upozornit na využití aplikací pro sdílení dat nebo na DDoS útok.

# Analytika v HC – sledování uživatelů z pohledu kvót

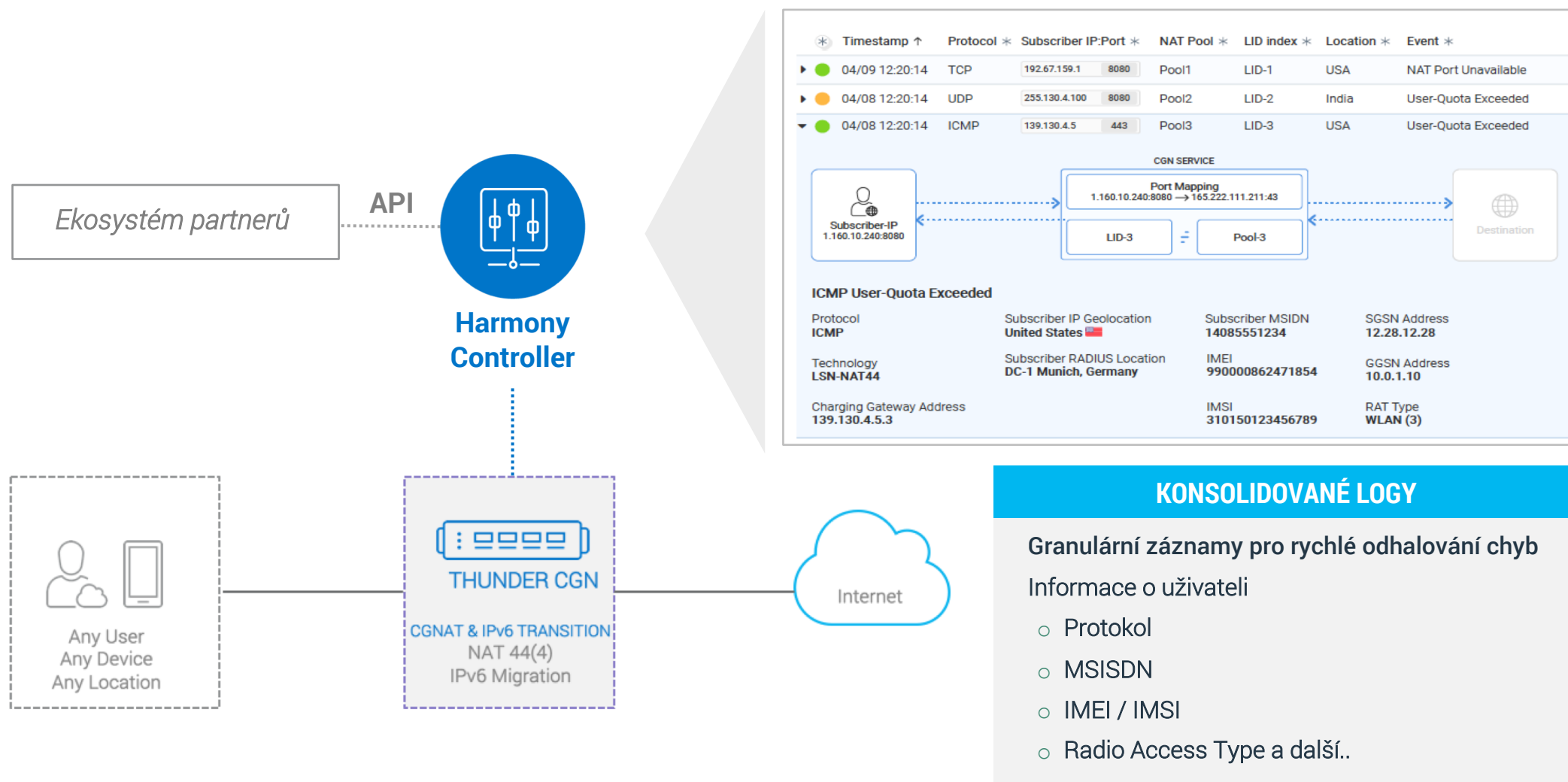


## ŠPATNÉ CHOVÁNÍ

- Upozornění na uživatelské kvóty – překročení počtu
- Selhání navázání spojení
- Hair pinning, selhání EIM/EIF



# Analytika v HC – konsolidované logy z CGN



# Typické problémy? Existuje řešení

|                                                                                     |                              |                                                 |
|-------------------------------------------------------------------------------------|------------------------------|-------------------------------------------------|
|    | <i>Špatná škálovatelnost</i> | <i>Až 220 Gb/s a 256 mil. spojení v 1U</i> ✓    |
|    | <i>Funkcionalita</i>         | <i>Kompletní NAT, ALG, logování</i> ✓           |
|    | <i>Bezpečnost</i>            | <i>AntiDDoS, ADC/WAF součástí licence</i> ✓     |
|   | <i>Složitá konfigurace</i>   | <i>Cisco-like CLI, GUI, API</i> ✓               |
|  | <i>Minimální analytika</i>   | <i>Detailní analytika o CGN i uživatelích</i> ✓ |



# Reference A10 Networks



+ mnoho dalších v Evropě, na Středním východě, Americe a Asii

## DALŠÍ REFERENCE ADC / WAF



# *DĚKUJEME*