Ochrana před DDoS útoky – proč a jak to dělá UPC

1. Trocha chlubení
2. DDoS teorie
3. Jak to děláme v UPC?
4. Další nezodpovězené otázky
5. Poděkování závěrem

1. Trocha chlubení

TROCHA CHLUBENÍ

o skupině LGI a postavení UPC v ní

Největší celosvětový poskytovatel TV a broadband služeb

Přední poskytovatel v Evropě

Významný hráč v Latinské Americe a Karibiku

Celkem na trzích v 30 zemích po celém světě

Výnosy 2016: $17.7 mld

41,000 zaměstnanců

50.1 millionů HP

24.8 millionů zákazníků

50.4 millionů RGU

10.0 millionů mobilních zákazníků, 7 millionů WiFi AP

800 000 km optických sítí

TROCHA CHLUBENÍ

o skupině LGI v Evropě

Výnosy 2016: $ 14,1 mld

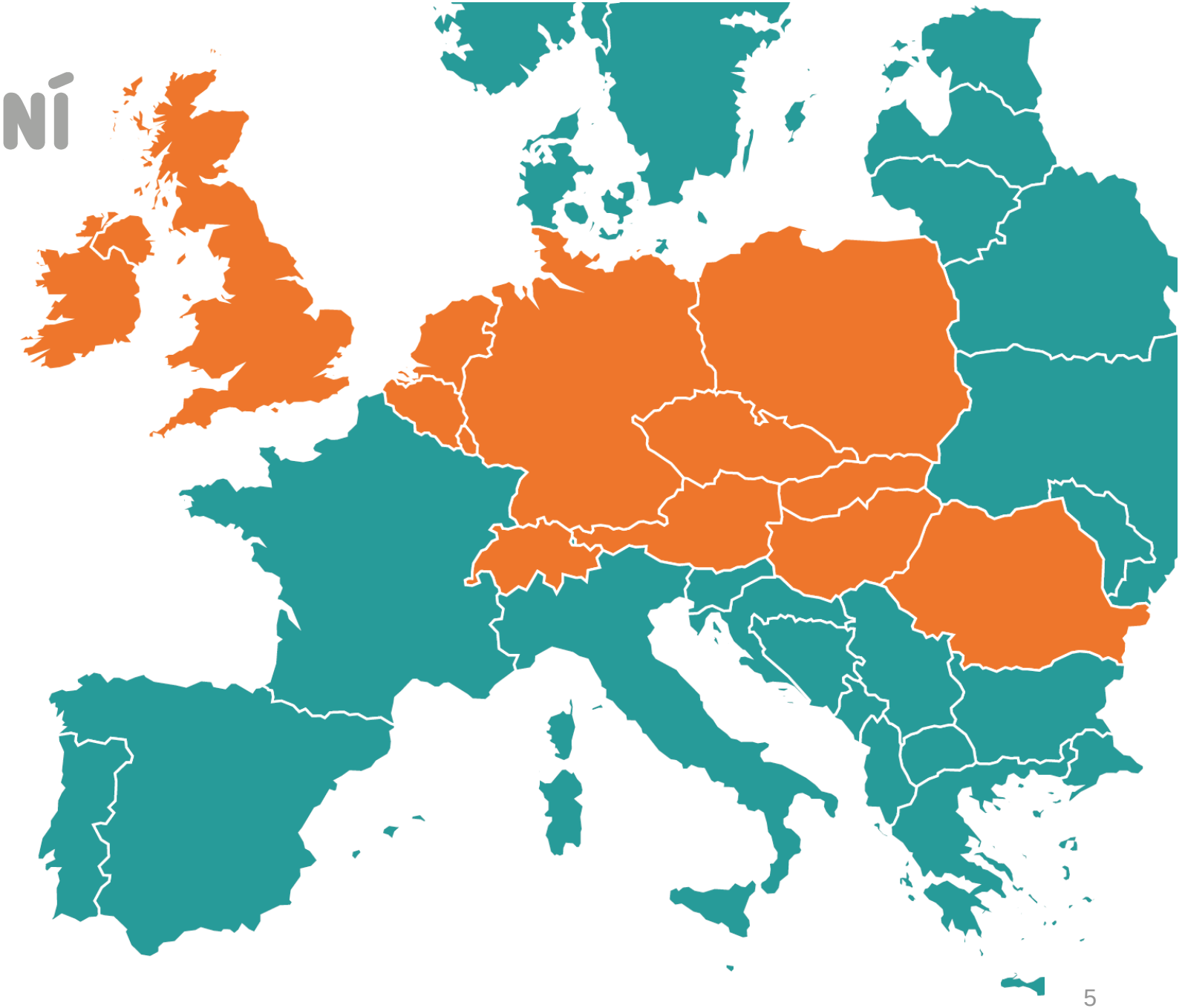
44,2 milionů HP

22 milionů zákazníků

45,1 milionů RGU

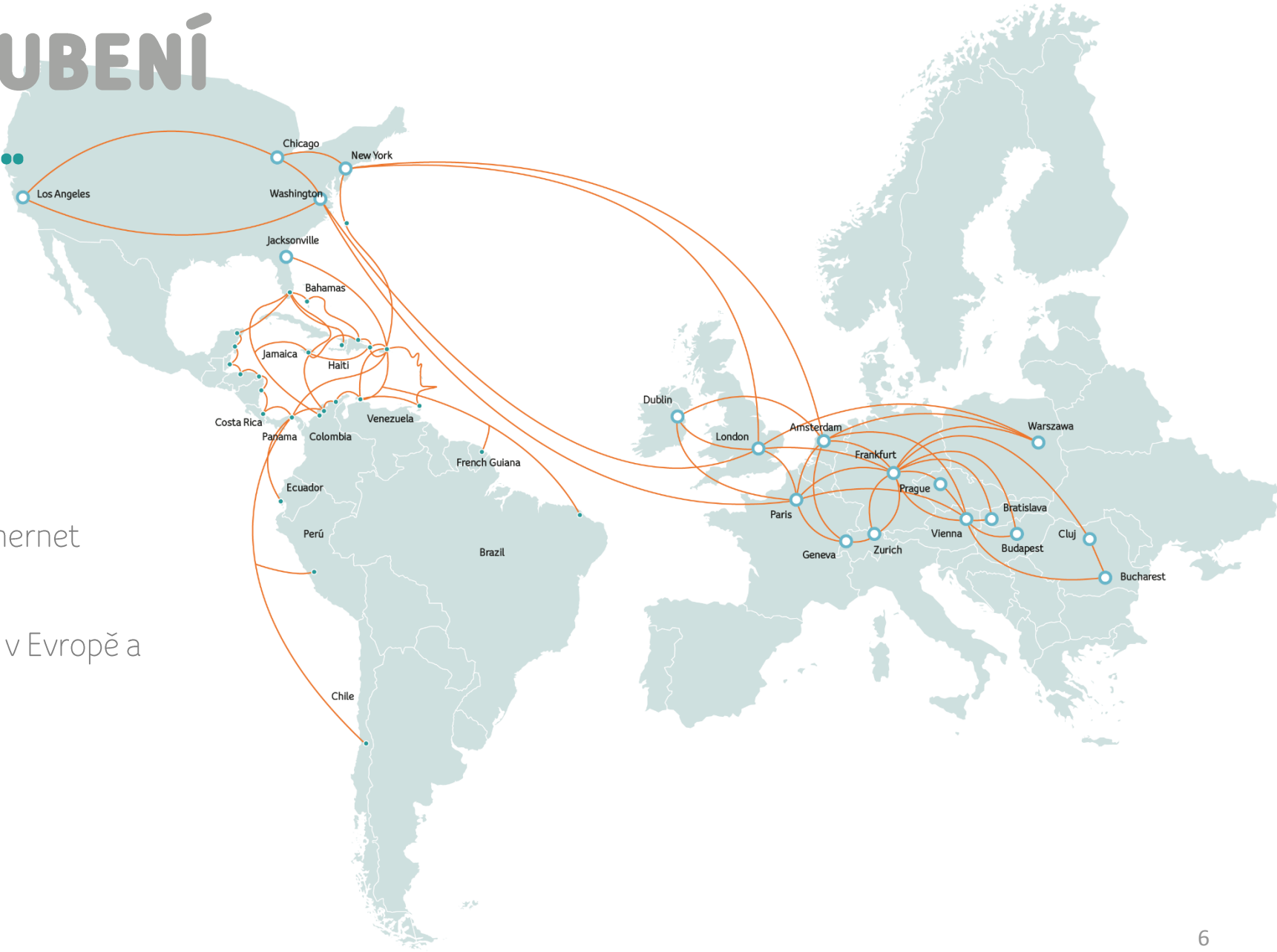
6,4 milionu mobilních uživatelů

11 + 1 zemí v pokrytí



TROCHA CHLUBENÍ

o naší síti po světě...

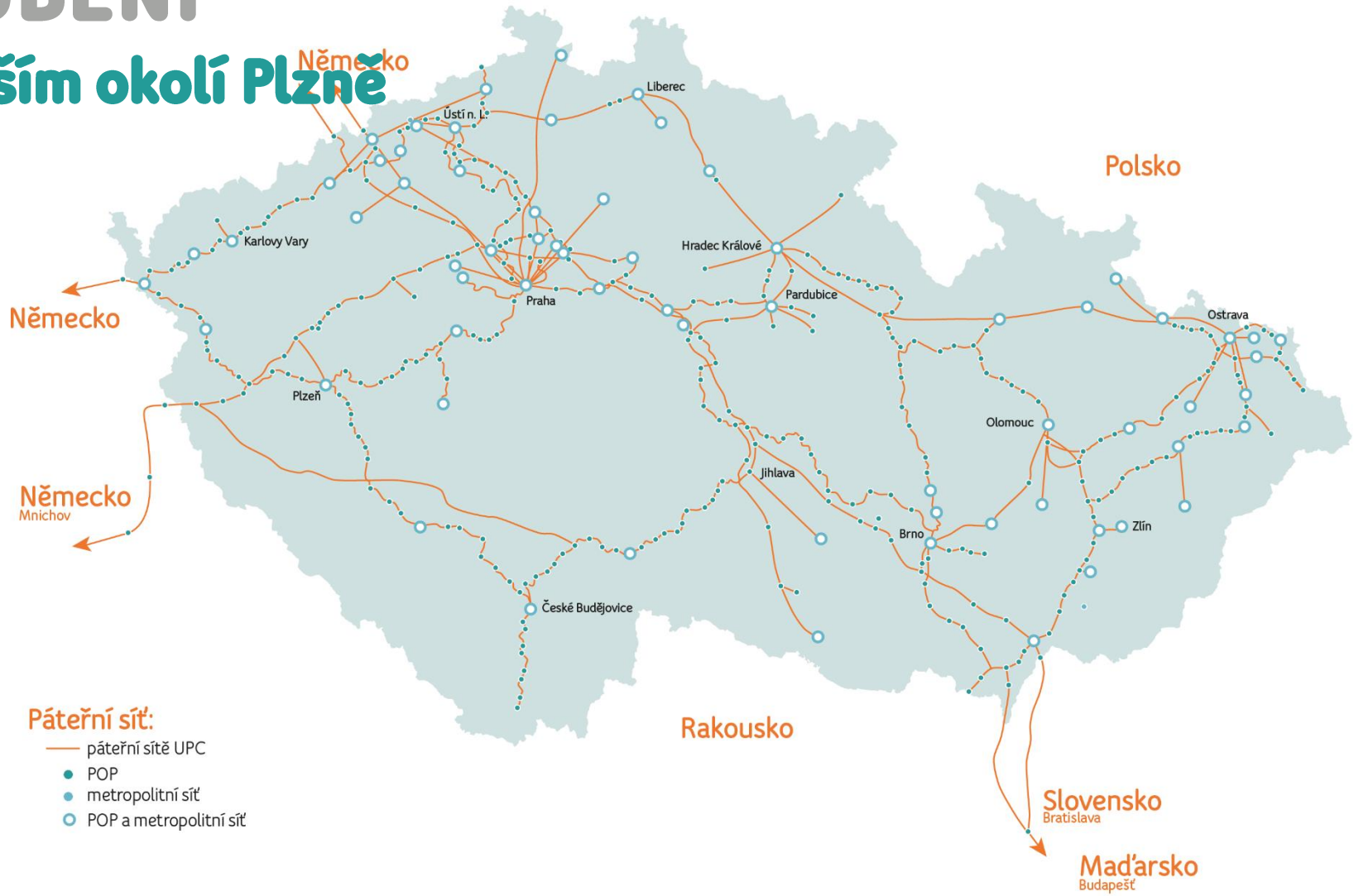


- Celosvětová páteřní síť – AORTA
- MEF 2.0 certifikovaný Carrier Ethernet
- Tier 1 IP Transit poskytovatel
- Peering ve významných Public IX v Evropě a zámoří
- Páteřní kapacity n x 100G

TROCHA CHLUBENÍ

...o naší síti v nejbližším okolí Plzně

- Optická páteř
- více než 6 000 km DF
- 3 000 PoPů
- Přítomnost ve všech významných Datových centrech v ČR
- Metropolitní sítě v městech, kde jsou rezidentní aktivity UPC + sítě našich partnerů
- Technologie metropolitních sítí Optika + Koax
- Mimo DF pokrytí LL realizovány radiovými spoji
- Páteřní kapacity n x 10G
- Páteřní technologie:
  - Cisco, Ciena
  - Transmode, ECI



2. DDoS teorie

TEORIE O DDOS

trocha statistiky

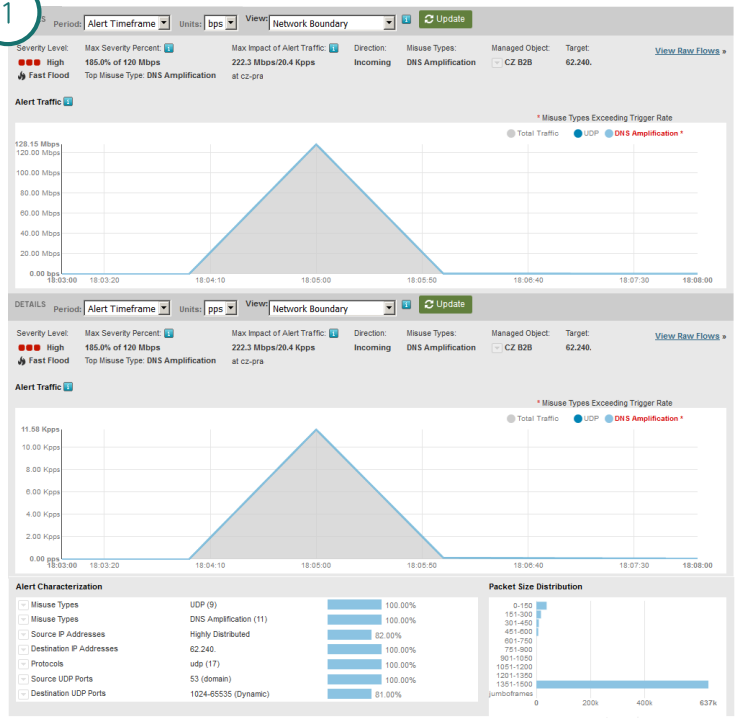
$150
je průměrná cena týdenního DDoS útoku na černém trhu

2 000
je průměrný počet útoku na celém světě zjištěných v síti Arbor Networks

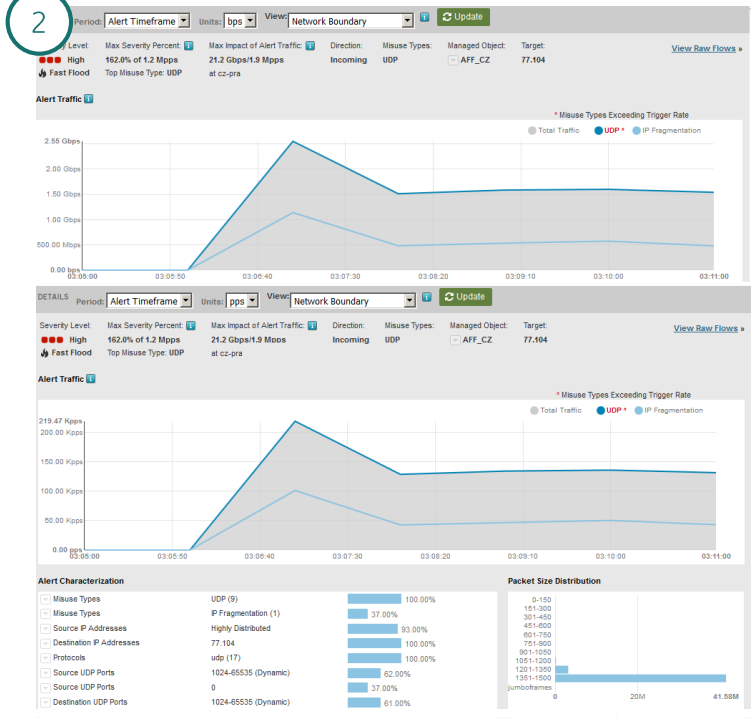
1/3
všech výpadků je způsobena DDoS útoky

V síti UPC CZ jsme v týdnu od 4. – 10. 9 registrovali **57 útoků**, níže 3 příklady:

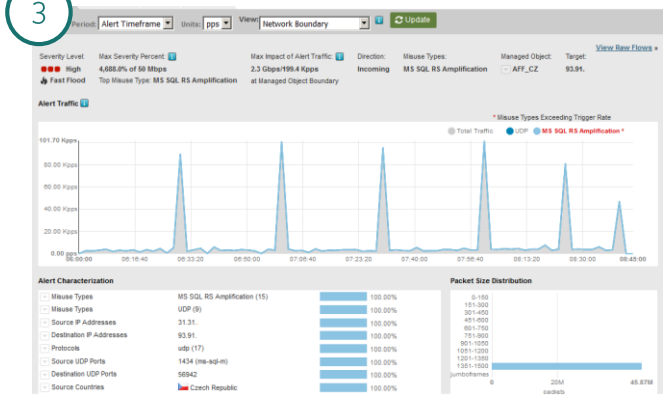
1



2



3



1. Malý útok, 222 Mbps / 20,4 kpps
2. Velký útok, 21,2 Gbps / 1,9 Mpps
3. Opakovaný útok 2,3 Gbps / 199 kpps

TEORIE O DDOS

způsoby odstranění / eliminace

Firewall

- hardwarový komponent,
- nutná uživatelská aktualizace bezpečnostních politik,
- chrání část sítě za FW, ne před
- zastaví neoprávněné pokusy o přístup, pomáhá blokovat nežádoucí datový tok, ale není jeho účelem odrazit hromadný paketový útok,
- vynucuje politiku založenou na statické množině pravidel, obvykle pouze na úrovni 3.vrstvy

Blackholing

- výbava CPE - nastavení nulového směrování
- při bránění útoku na jeden subjekt v síti jsou ovlivněny i další subjekty v síti
- je volbou pro organizace, které nemají jiné prostředky k zablokování útoku
- poškození dobrého jména
- ztráta produktivity
- podvod - útoky DDoS jsou často spuštěny, aby odvrátily pozornost a zdroje, takže jiné útoky nemohou být odhaleny

Anti-DDoS

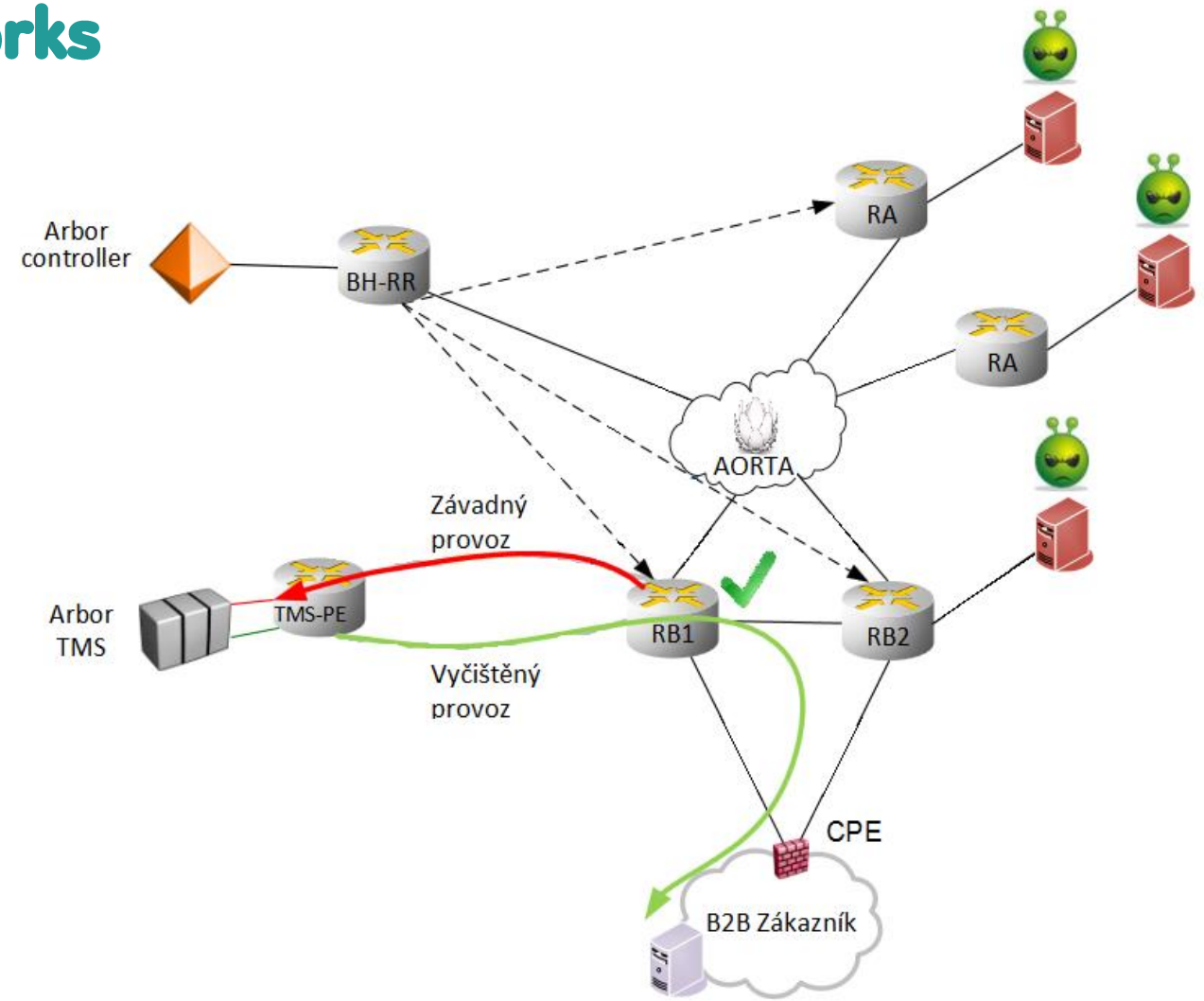
- služba Anti-DDoS zabraňuje nadměrným oprávněným pokusům o přístup.
- nabízí např. funkce hloubkové inspekce paketů (do 7.vrstvy) a analýzy chování, které mohou dynamicky detekovat útoky

3. Jak to děláme v UPC

NAŠE ŘEŠENÍ

globální řešení Arbor Networks

- plně automatický provoz 24/7/365 support
- customizované nastavení ve spolupráci s účastníkem (typ provozu, akce,…)
- vysoká a stále se navyšující kapacita filtrování (v tuto chvíli max 240 Gb)
- jeden kontakt na všechny služby – NOC UPC
- bez rizika problému s HW
- bez CAPEXových nákladů
- čištění provozu probíhá nad IP konektivitou dodávanou UPC Česká republika



NAŠE ŘEŠENÍ

globální řešení Arbor Networks

Parametr	Hodnota
Reakční doba v případě útoku	méně než 60 sekund
Garantovaná roční dostupnost služeb (platforma Arbor)	99,99 %
Dopad na latenci, jitter a ztrátu paketů v internetové službě během čištění provozu	Při útoku je provoz přesměrován skrz čistící centrum - dopad na reakční dobu v případě zmírňování dopadů útoku: < 100ms *(na základě dosavadních zkušeností 3 – 6 ms)*
Maximální doba čištění provozu po skončení útoku DDoS	5 minut
Maximální provozní kapacita scrubing centra	3 x 80Gbps = 240Gbps

NAŠE ŘEŠENÍ

kolik za to?

Konektivita (Mbit/s)	Název služby	cena měsíčně	akční cena
0-100	AntiDDoS 100M	Kč	Kč
101-200	AntiDDoS 200M	Kč	Kč
201-300	AntiDDoS 300M	Kč	Kč
301-400	AntiDDoS 400M	Kč	Kč
401-500	AntiDDoS 500M	Kč	Kč
501-750	AntiDDoS 750M	Kč	Kč
750-1 000	AntiDDoS 1G	Kč	Kč
1 001-2 000	AntiDDoS 2G	Kč	Kč
2 001-4 000	AntiDDoS 4G	Kč	Kč
4 001-10 000	AntiDDoS 10G	Kč	Kč
nad 10 000	AntiDDoS Max	Kč	Kč

4. Další nezodopovězené otázky?

DĚKUJEM' PĚKNĚ!

TOMÁŠ STOJAN, WS Senior Manager
tomas.stojan@upc.cz, +420 778 525 689

JIŘÍ PŘEVRÁTIL, Data Network Administrator
jiri.prevratil@upc.cz