



Ochrana před DDoS útoky – proč a jak to dělá UPC



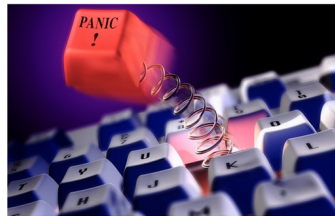
Hlavní stránka » Internet a PC » Bezpečnost » Podrubriky: Hardware Software Testy Hry a herní systémy Mobil Bezpečnost

Obří DDoS útok byl jen špička ledovce. Hackeři dostali detailní návod

Mimulý týden byl odhalen jeden z největších DDoS útoků v celé historii internetu. Zodpovědná za něj byla síť zotročených zařízení internetu věci, tedy například nejruznější kamery, které se mohou připojovat k internetu. Bezpečnostní experti však nyní upozorňují, že šlo jen o špičku ledovce. Předpokládají dramatický nárůst podobných útoků.



Internet mimo provoz? DDoS útok lze koupit za pár korun



Největší DDoS útok o síle 1 TB byl veden z napadených chytrých zařízení

SDILET: [Facebook](#) [Twitter](#) [Google+](#) [LinkedIn](#)

SecurityWorld Hardware Internet a komunikace Software E-knihy Vývoj Analýzy a studie

DDoS útoky se dostaly na své maximum

DDoS útoky zaznamenaly v posledních třech měsících roku 2016 značný pokrok – novým trendem jsou ataky spuštěné prostřednictvím velkého počtu botnetů tvořených zranitelnými zařízeními internetu věci (IoT).

autor Pavel Louča | SecurityWorld | 10.02.2017

Související články

- Spolku mobilních systémů zaří přicházející IoT i nositelná elektronika
- Během zářahu na DDoS služby zadržela policie desítky sítí, vyslechla mnoho dalších
- Oracle kupuje Dyn, chce dočít na hybridní cloud
- DDoS pod kapou: Co skutečně stojí za jedním z



o vedeného DDoS útoku v historii, stá je, že se na tomto útoky ihytrá zařízení, která jsou stále více tphony, chytré televize, ledničky, IP na tato zařízení, která tvoří tzv. Internet věcí (Internet of Things – IoT) se staly součástí obrovské sítě botnetů, kde každé z nich generovalo určitý datový tok, který se spojil v nevidanou sílu. Francouzská společnost OVH, která poskytuje hostingové služby, byla jednou z obětí tohoto distribuovaného útoku, která právě reportovala útok o rekordní síle až 1 TB.

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 naší síti po světě...



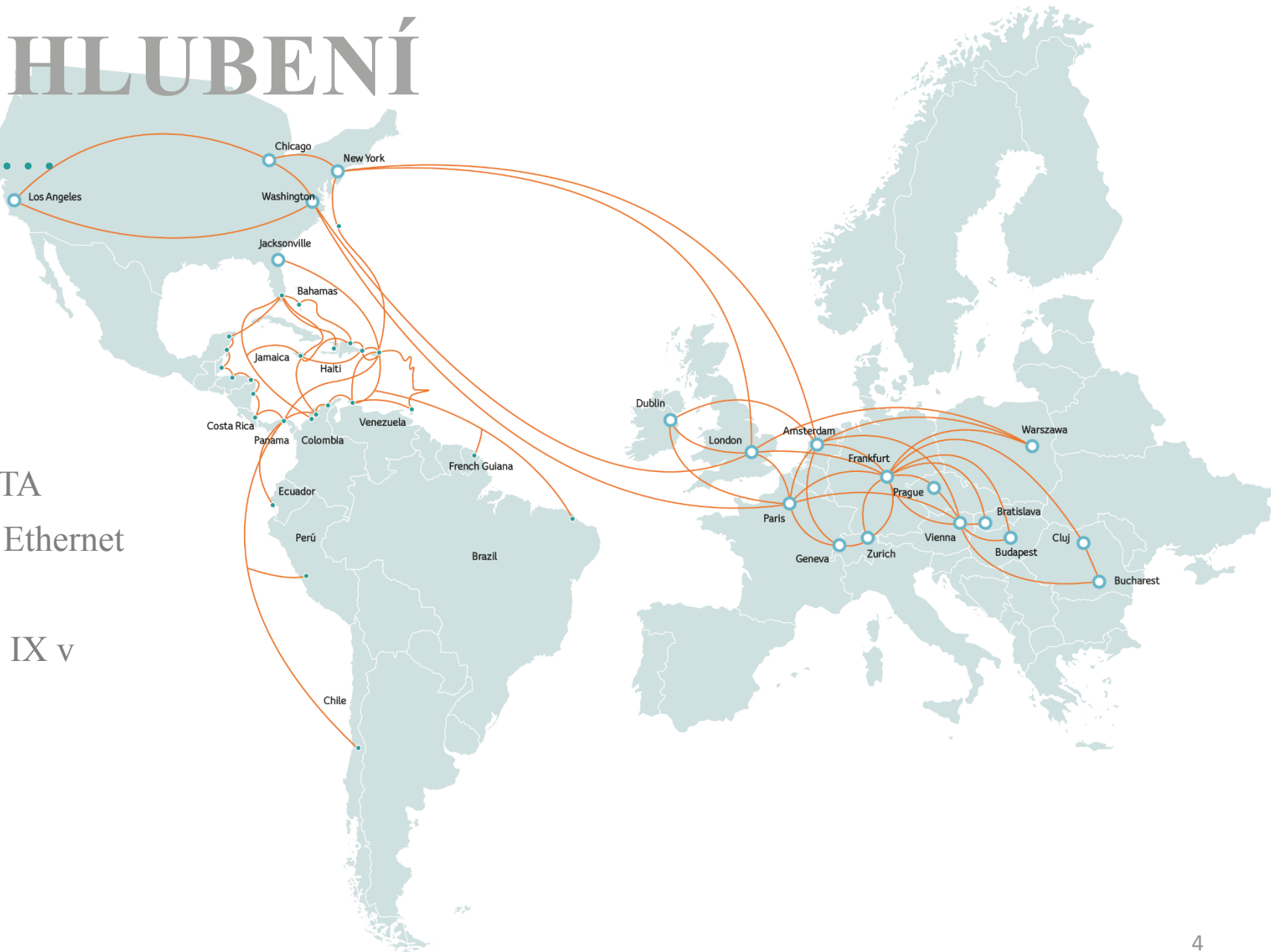
Celosvětová páteřní síť – AORTA

MEF 2.0 certifikovaný Carrier Ethernet

Tier 1 IP Transit poskytovatel

Peering ve významných Public IX v Evropě a zámorí

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 síť v městech, kde jsou
rezidentní aktivity UPC + síť našich
partnerů

Technologie metropolitních sítí Optika +
Koax

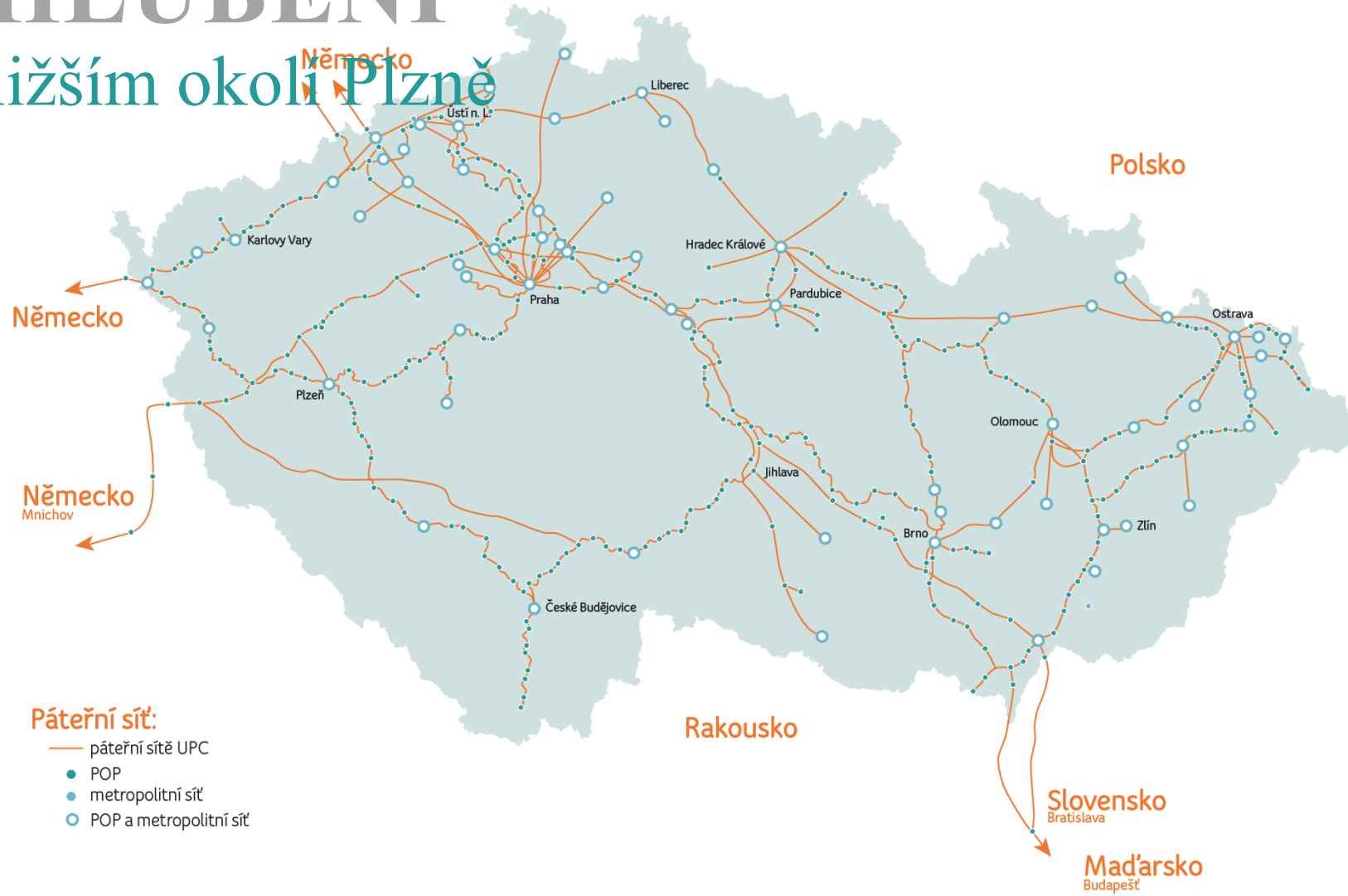
Mimo DF pokrytí LL realizovány
radiovémi spoji

Páteřní kapacity n x 10G

Páteřní technologie:

Cisco, Ciena

Transmode, ECI

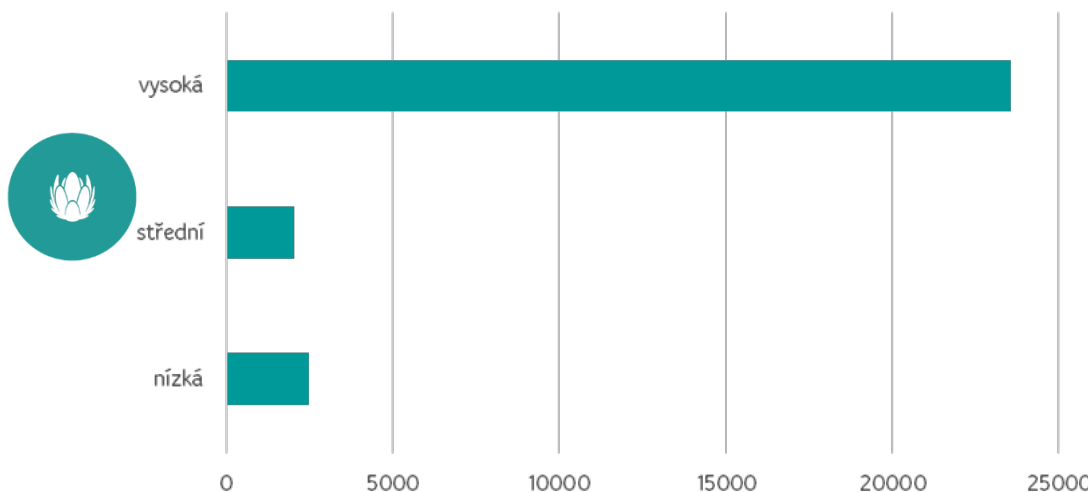


2. DDoS co se děje u nás

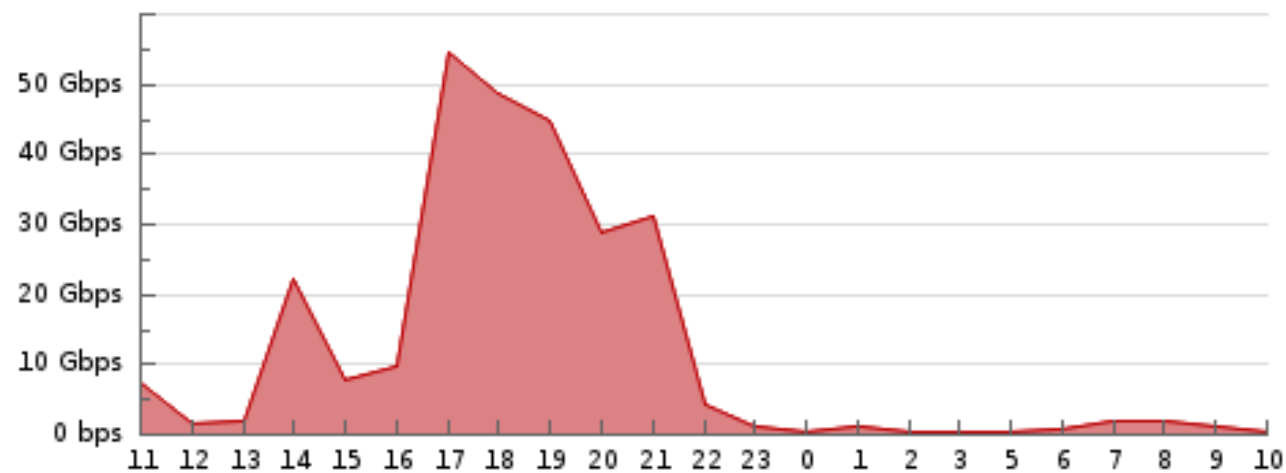
JAK TO VYPADÁ U NÁS V SÍTI

pohled z perspektivy LGI

Počet útoků na síť LGI podle kritičnosti

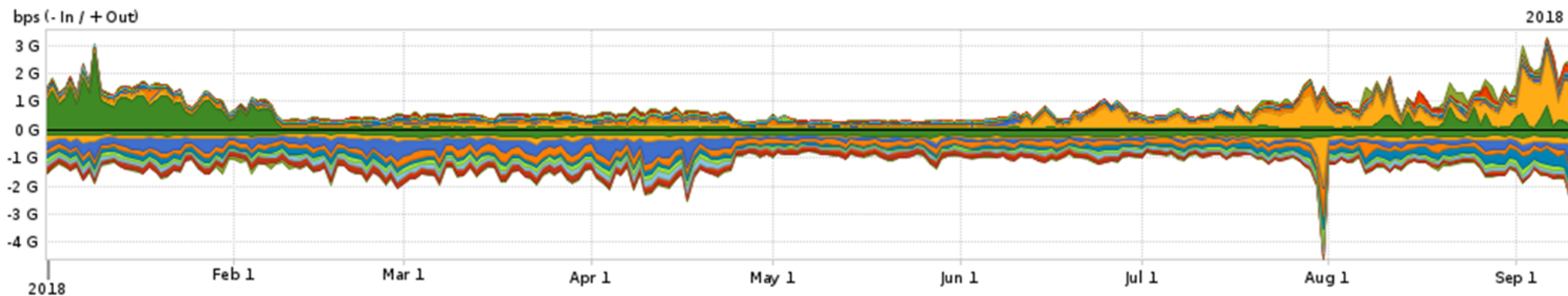


24 hodinová statistika útoků (12.9.)



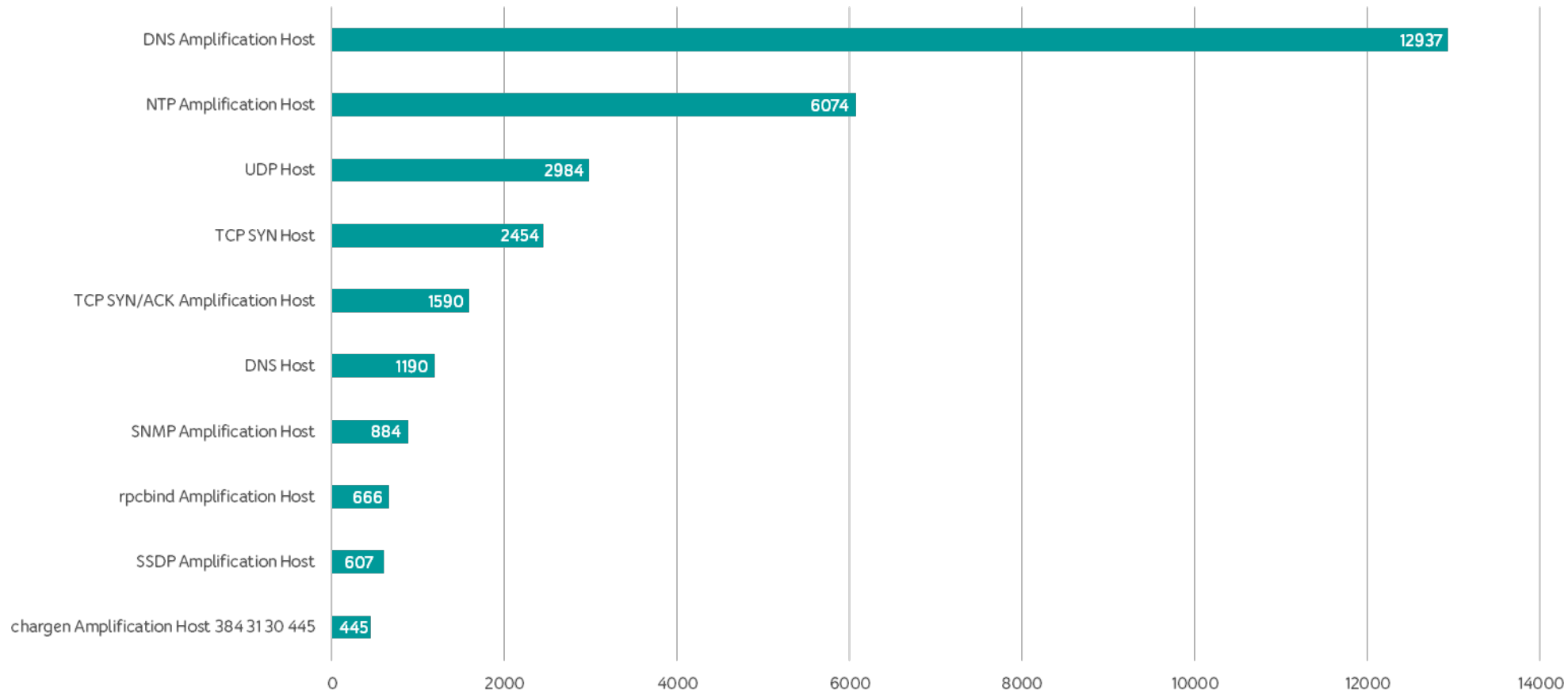
JAK TO VYPADÁ U NÁS V SÍTI

žádoucí a nežádoucí provoz DNS v rámci LGI Evropa



JAK TO VYPADÁ U NÁS V SÍTI

typy útoků na naši síť – statistika za poslední rok



JAK TO VYPADÁ U NÁS V SÍTI

CZ statistika za poslední týden událostí na naší síti



77

DDoS
útoků na naše
zákazníky

16,2

Gb

celková kapacita
útoků za poslední
týden

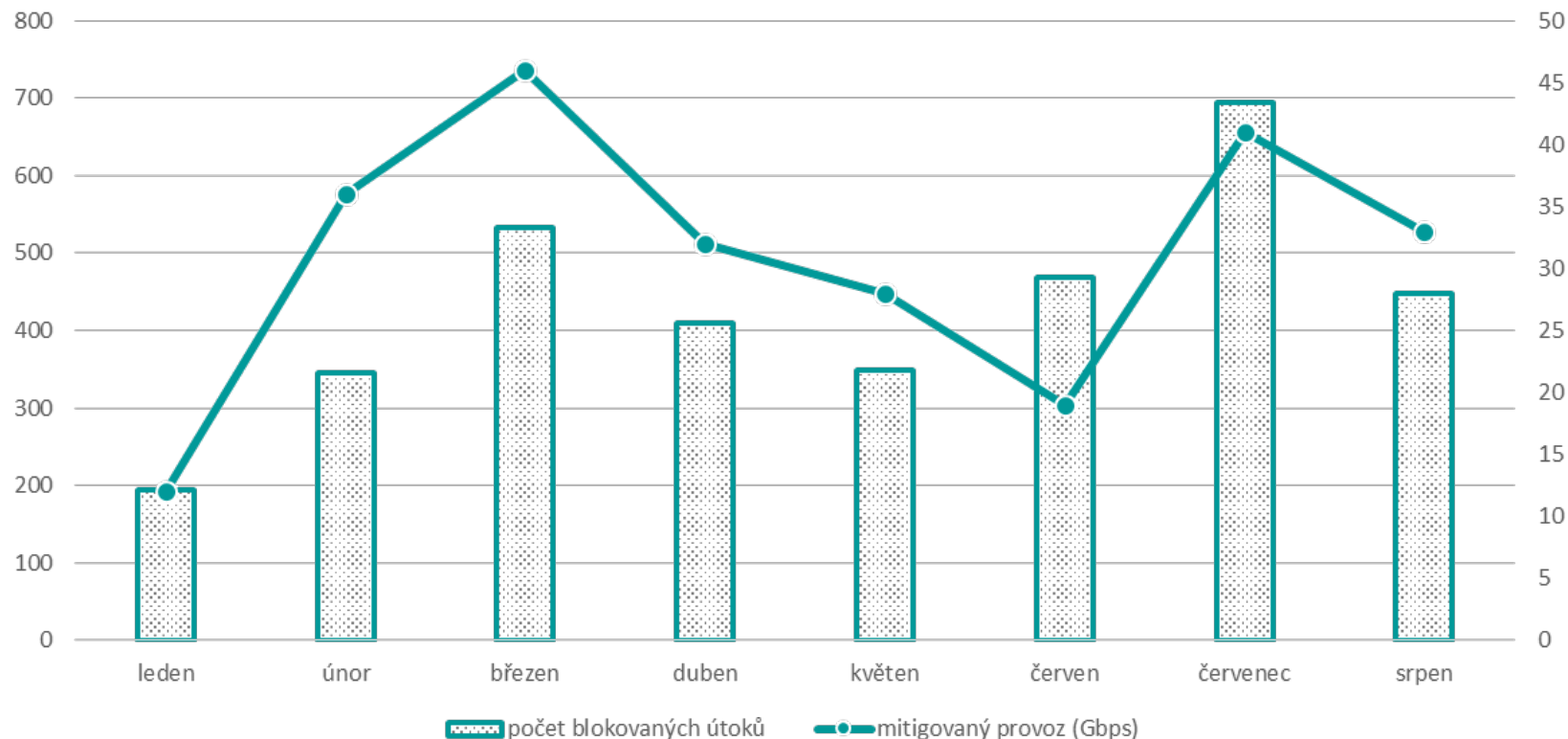
0

[nula]

otevřených TT na
našem NOC

JAK TO VYPADÁ U NÁS V SÍTI

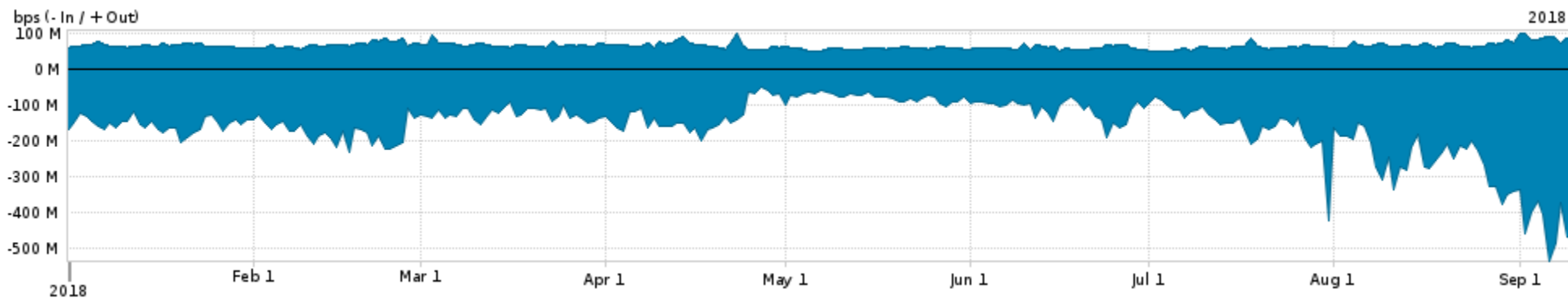
CZ statistika za poslední rok, co jsme se neviděli



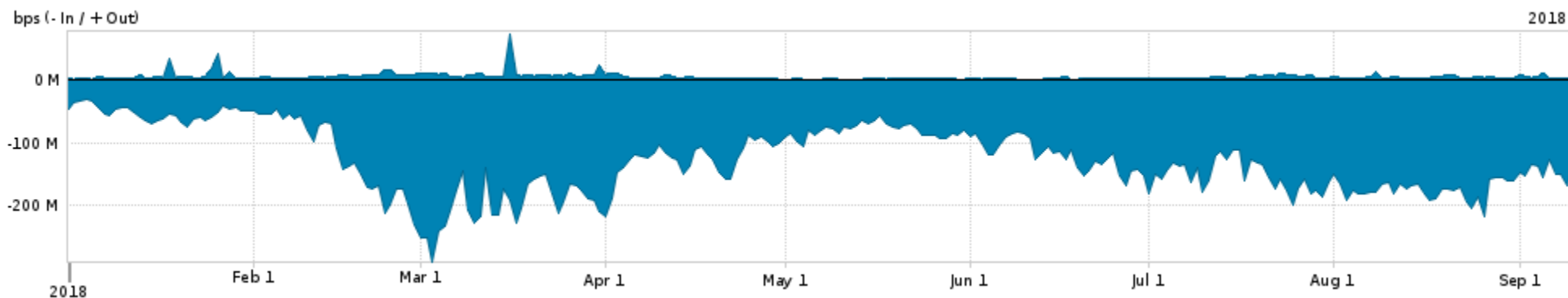
JAK TO VYPADÁ U NÁS V SÍTI

pohled z perspektivy CZ

Nežádoucí provoz DNS do ČR

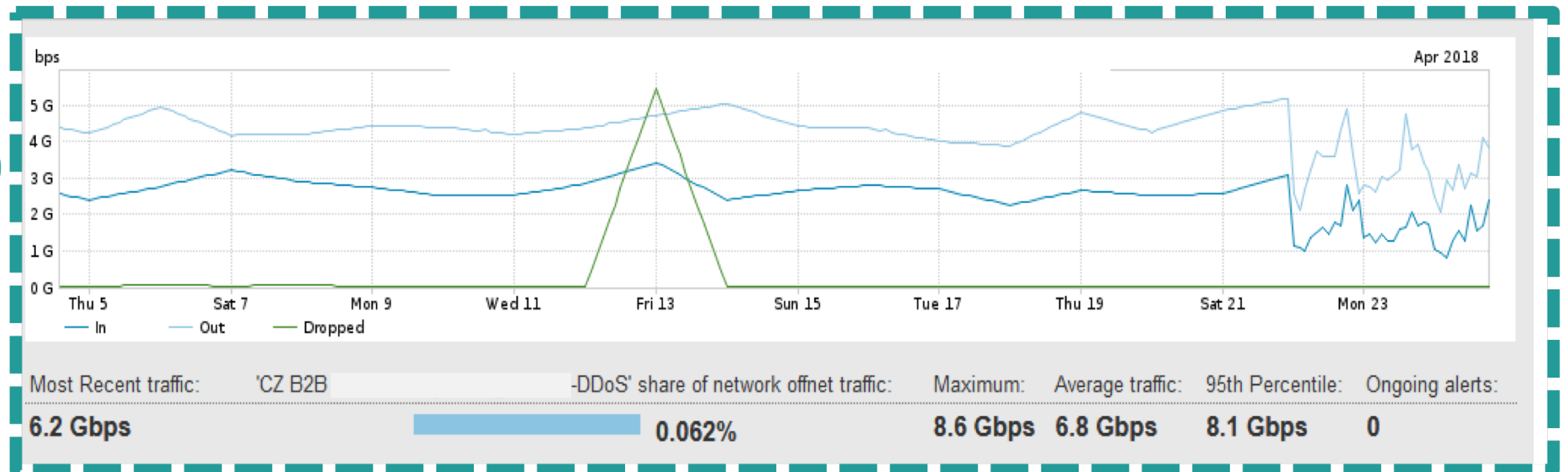


Nežádoucí provoz LDAP do ČR



JAK TO VYPADÁ U NÁS V SÍTI

“Pátek třináctého“ u našeho zákazníka XY

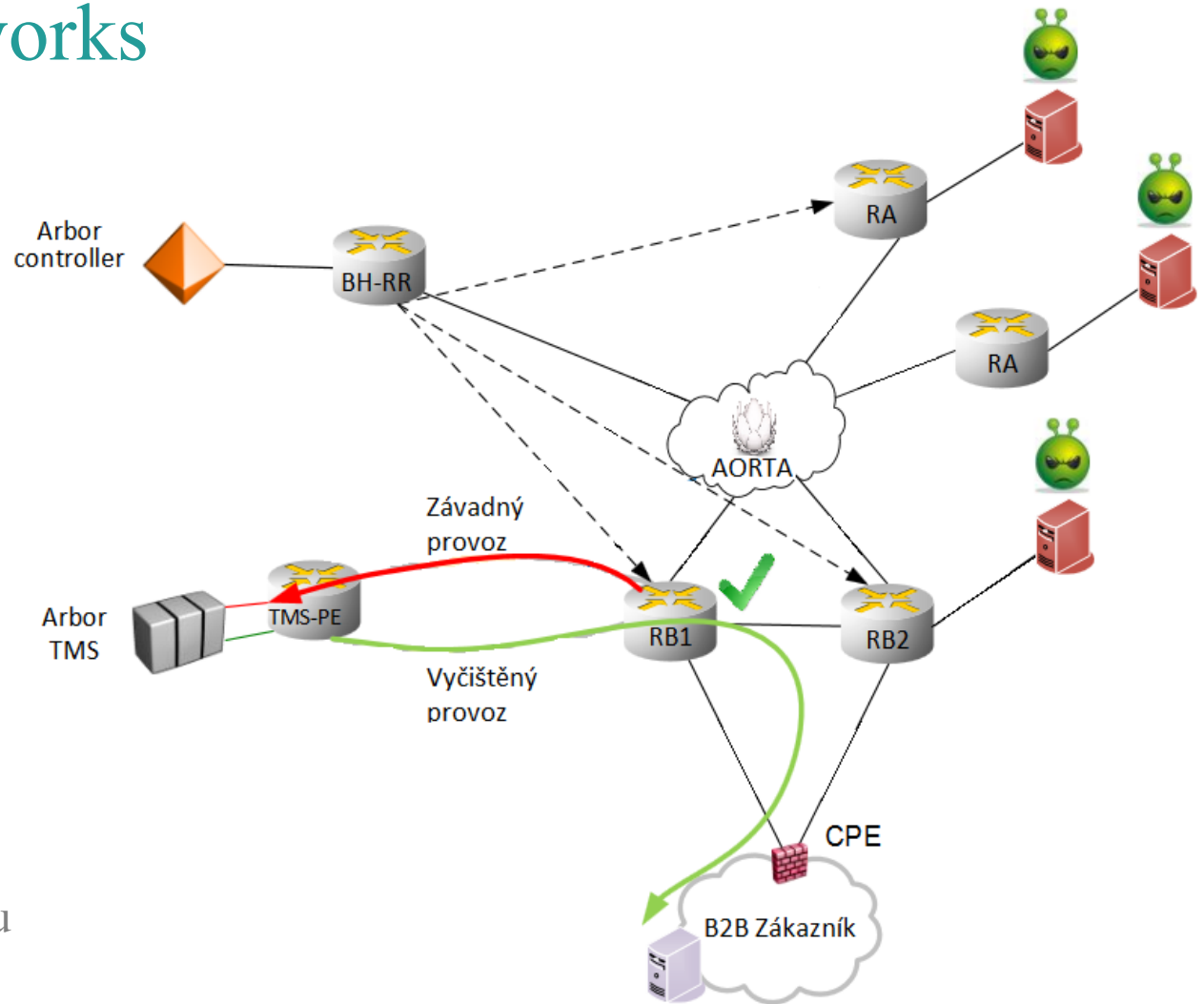


3. Jak to děláme v UPC

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 zmírnování dopadů útoku: < 100ms <i>(na základě dosavadních zkušeností 3 – 6 ms)</i>
Maximální doba čištění provozu po skončení útoku DDoS	5 minut
Maximální provozní kapacita scrubbing centra	3 x 80Gbps = 240Gbps

4. Další
nezodpovězené
otázky?



DĚKUJE
M'
PĚKNĚ!
TOMÁŠ STOJAN, WS Senior Manager
tomas.stojan@upc.cz, +420 778 525 689

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