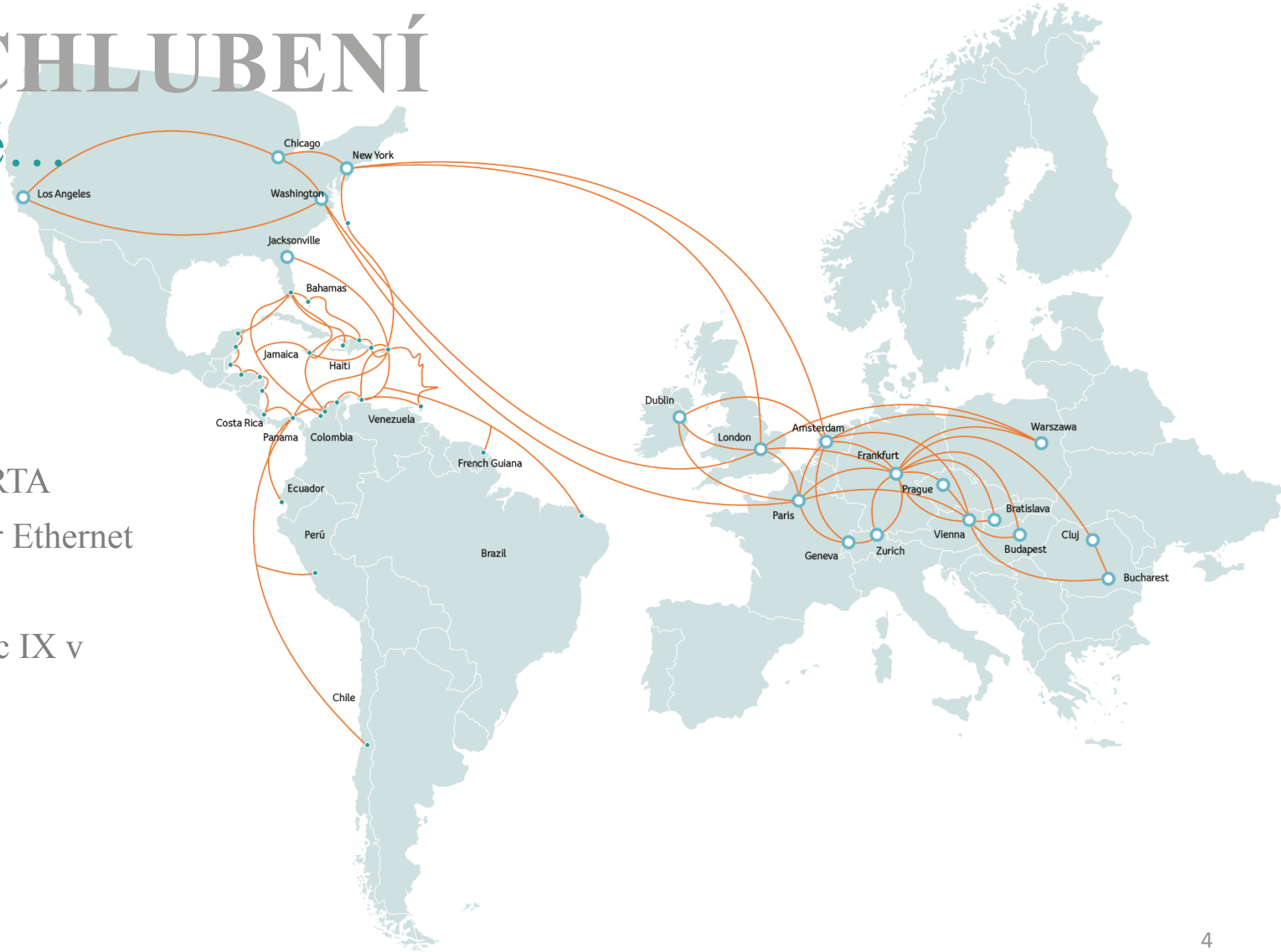
Ochrana před DDoS útoky – proč a jak to dělá UPC

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 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

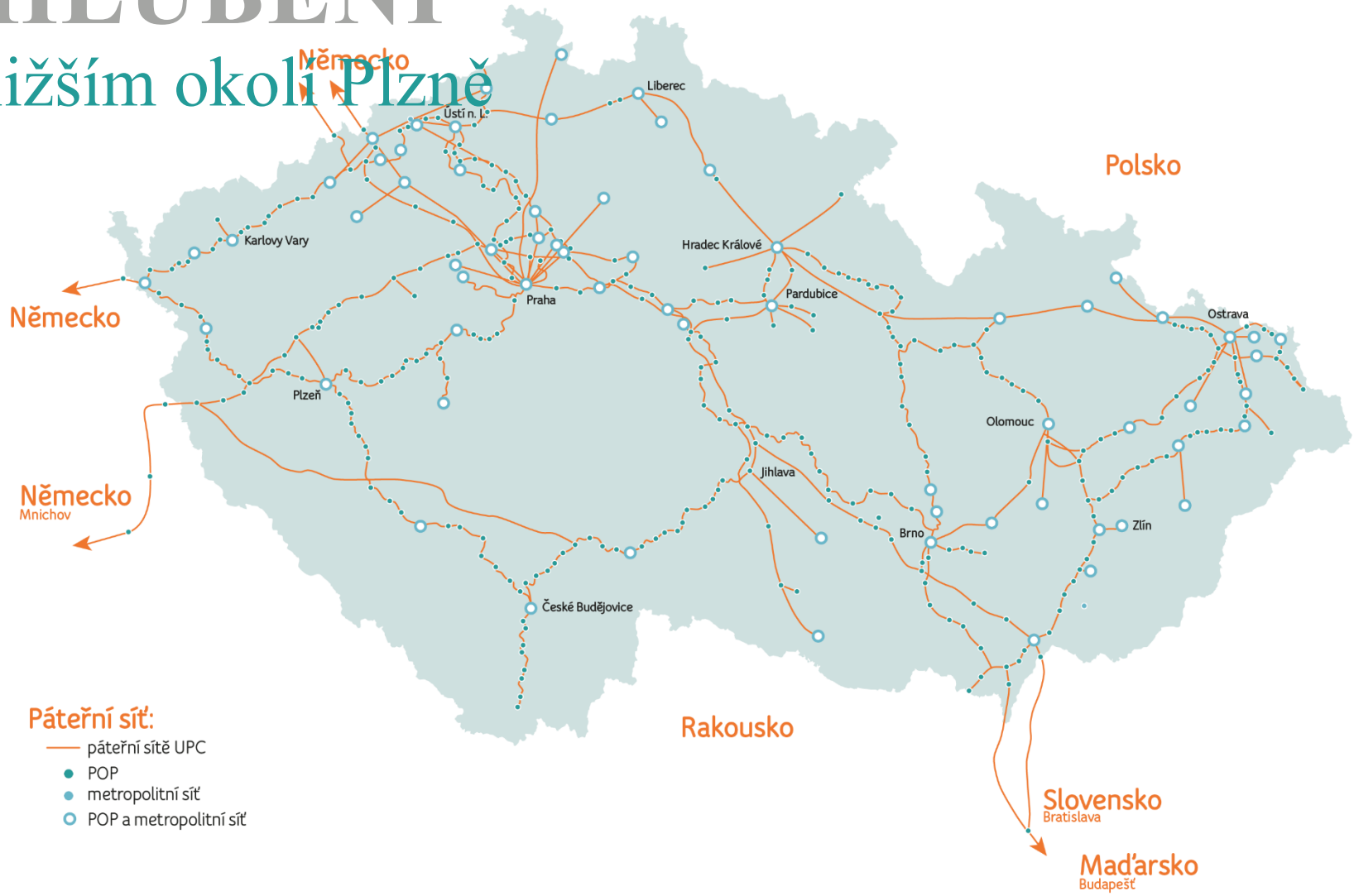
Mimo DF pokrytí LL realizovány radiovými spoji

Páteřní kapacity n x 10G

Páteřní technologie:

Cisco, Ciena

Transmode, ECI

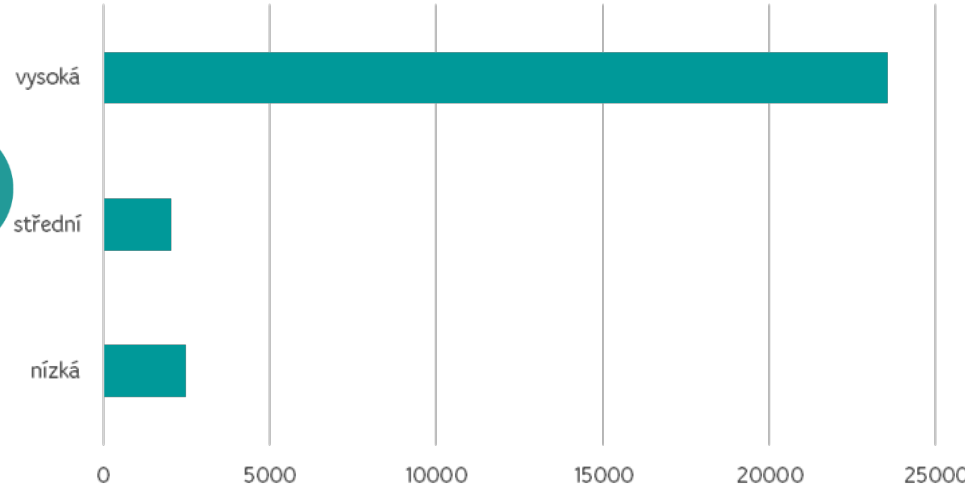


2. DDoS co se děje u nás

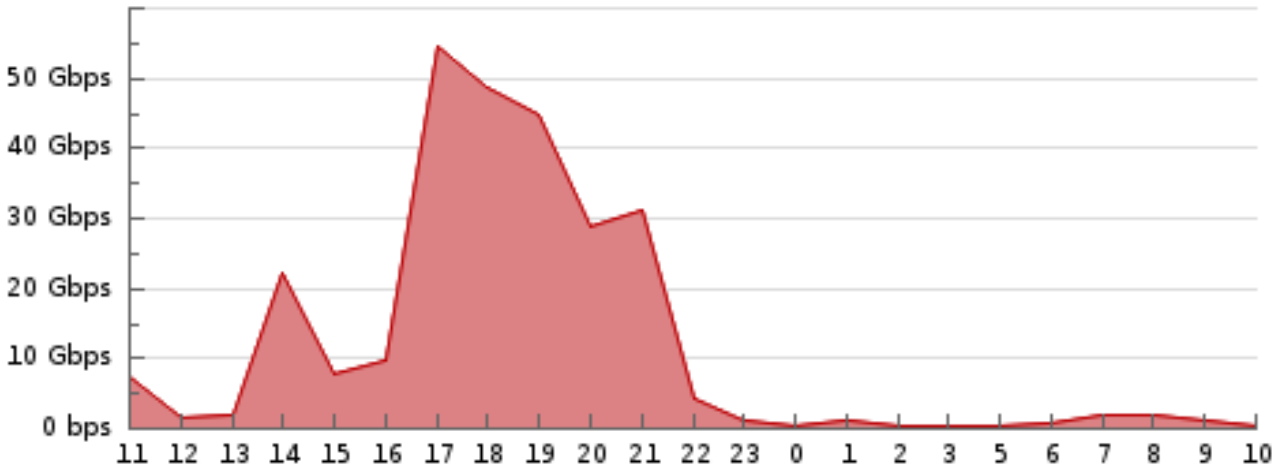
JAK TO VYPADÁ U NÁS V SÍTI

pohled z perspektivy LGI

Počet útoků na síť LGI podle kritičnosti

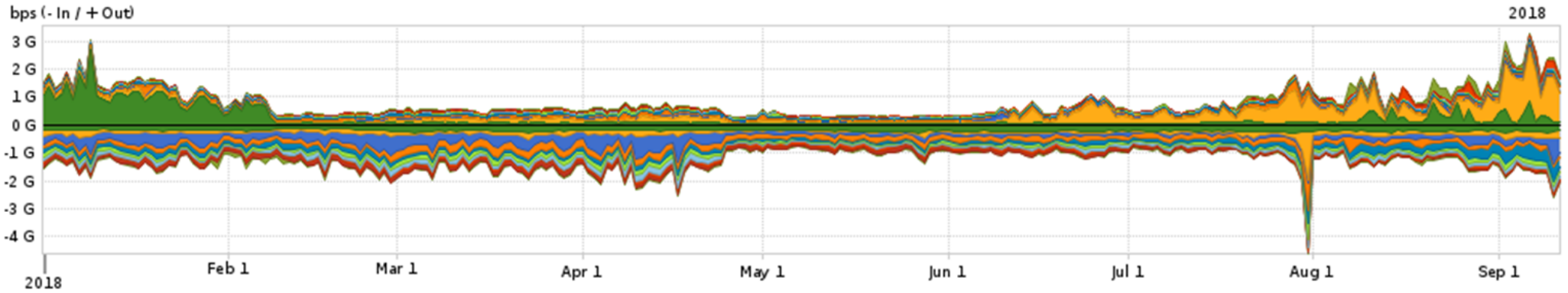


24 hodinová statistika útoků (12.9.)



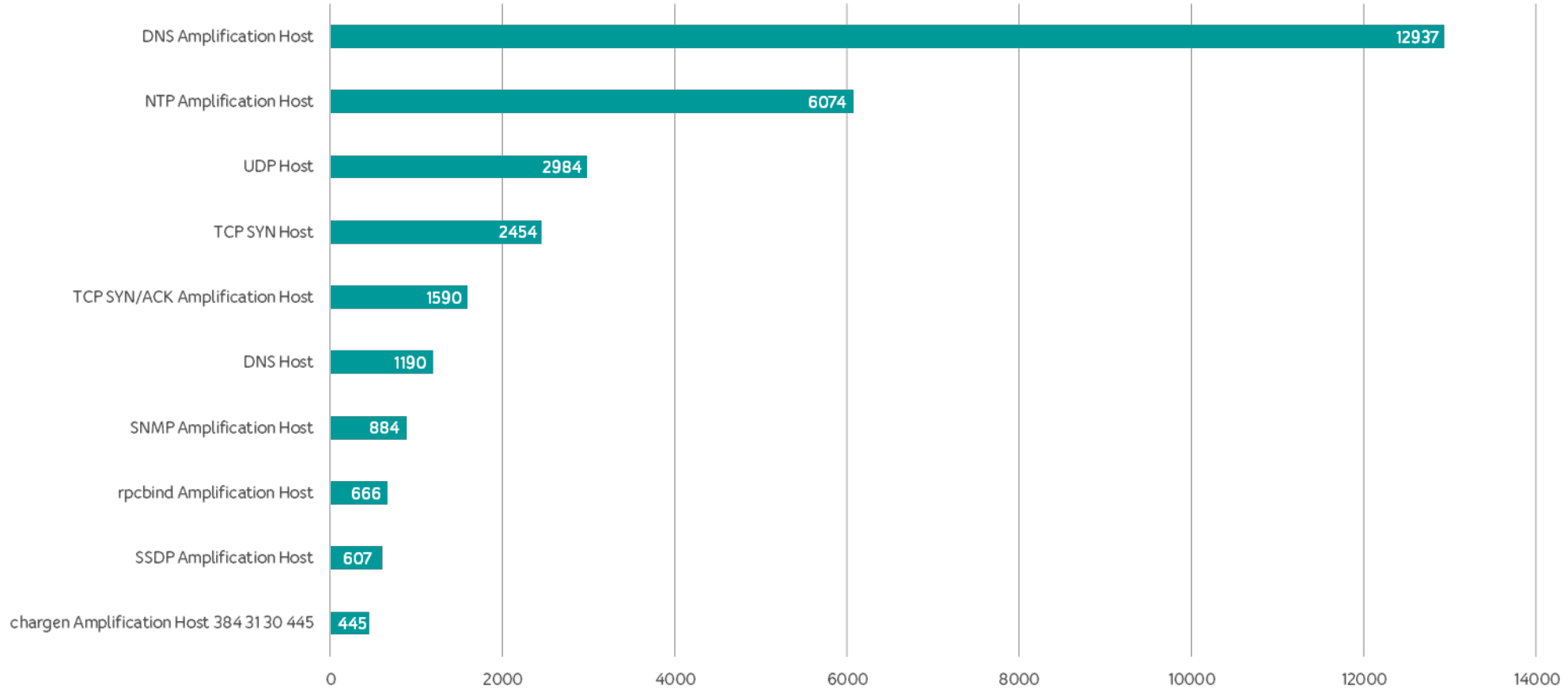
JAK TO VYPADÁ U NÁS V SÍTI

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

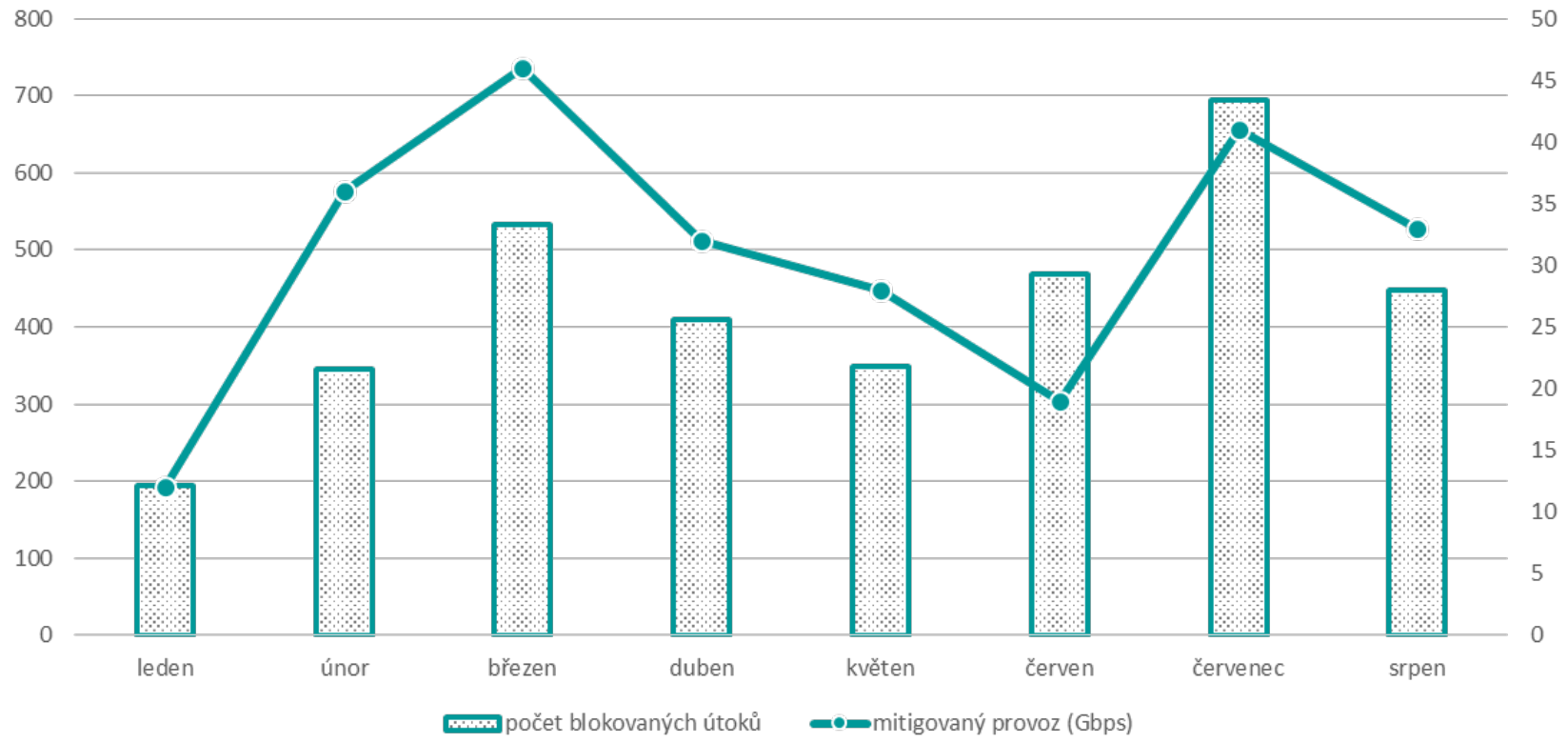
celková kapacita útoků za poslední týden

0 [nula]

otevřených TT na našem NOC

JAK TO VYPADÁ U NÁS V SÍTI

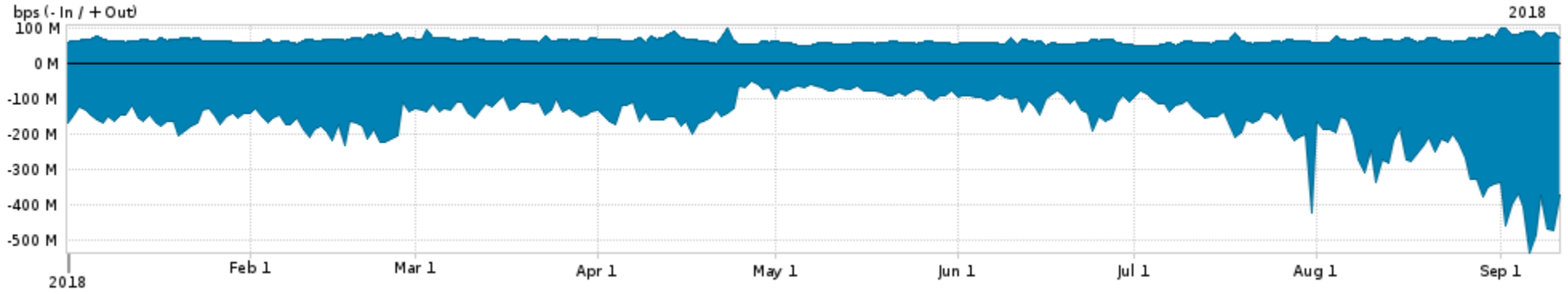
CZ statistika za poslední rok, co jsme se neviděli



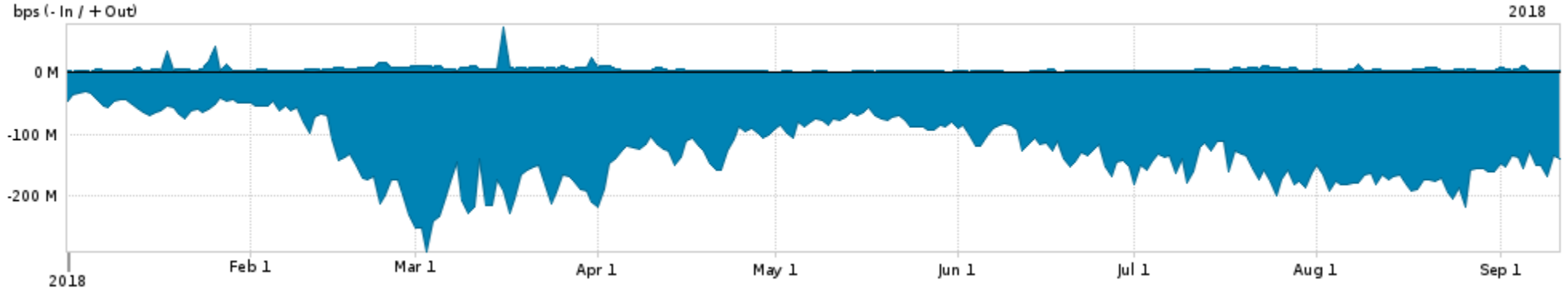
JAK TO VYPADÁ U NÁS V SÍTI

pohled z perspektivy CZ

Nežádoucí provoz DNS do ČR

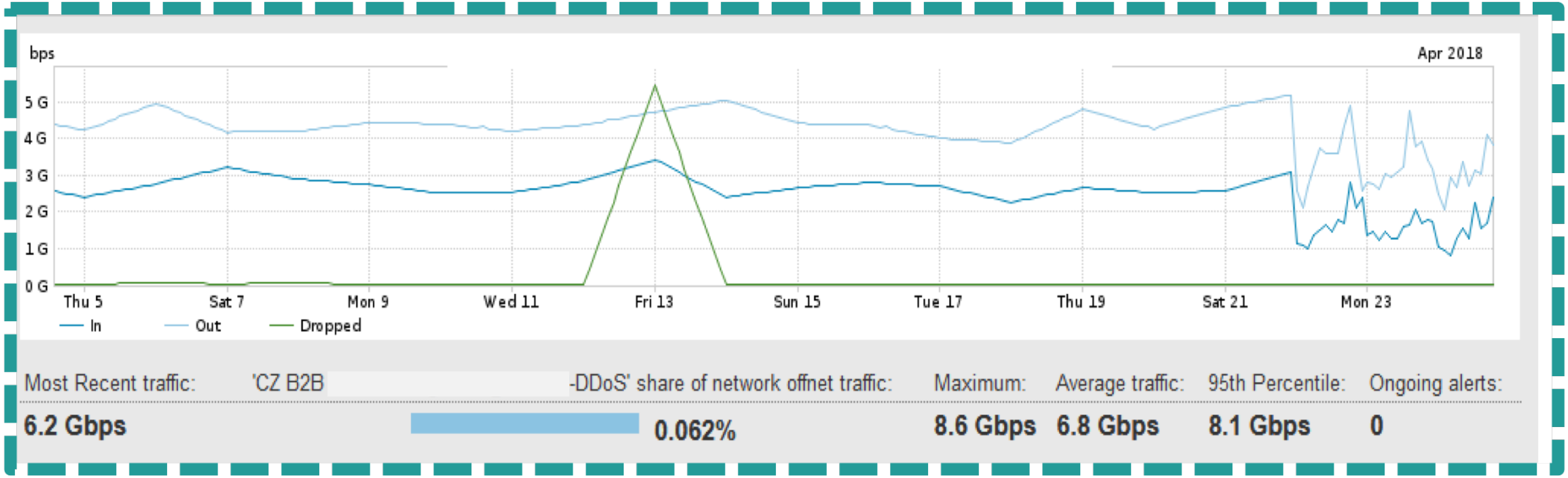


Nežádoucí provoz LDAP do ČR



JAK TO VYPADÁ U NÁS V SÍTI

“Pátek třináctého“ u našeho zákazníka XY

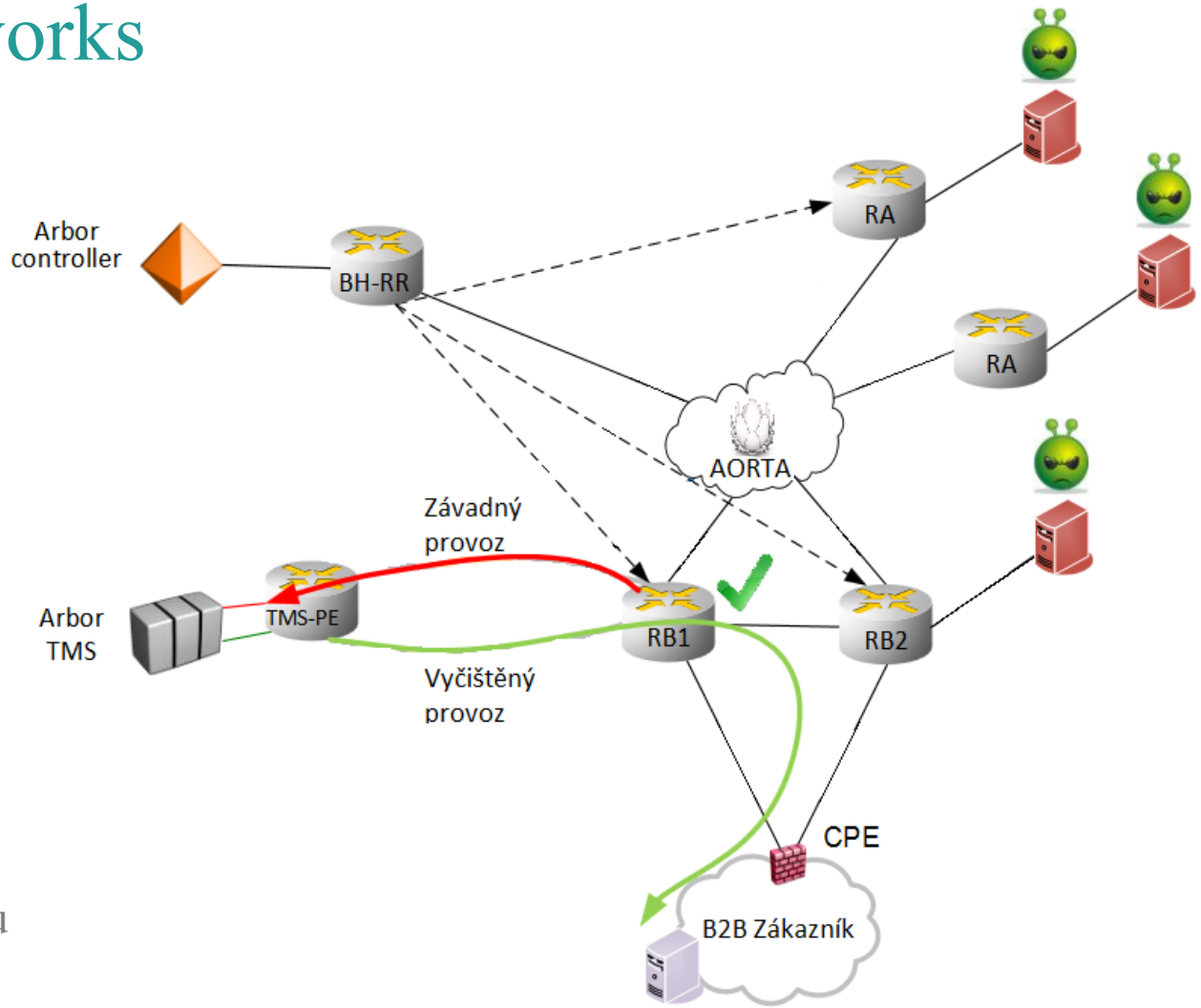


3. Jak to děláme v UPC

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 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

4. Další nezodopovězené otázky?

DĚKUJE M' PĚKNĚ!

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

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