Jak přežít DDoS

Aspekty DDoS útoků v prostředí infrastruktury ISP

Petr Kadlec
ComSource s.r.o.


Com
Source


juniper
NETWORKS


FLOWGUARD


BriefCam


Flowmon
Networks

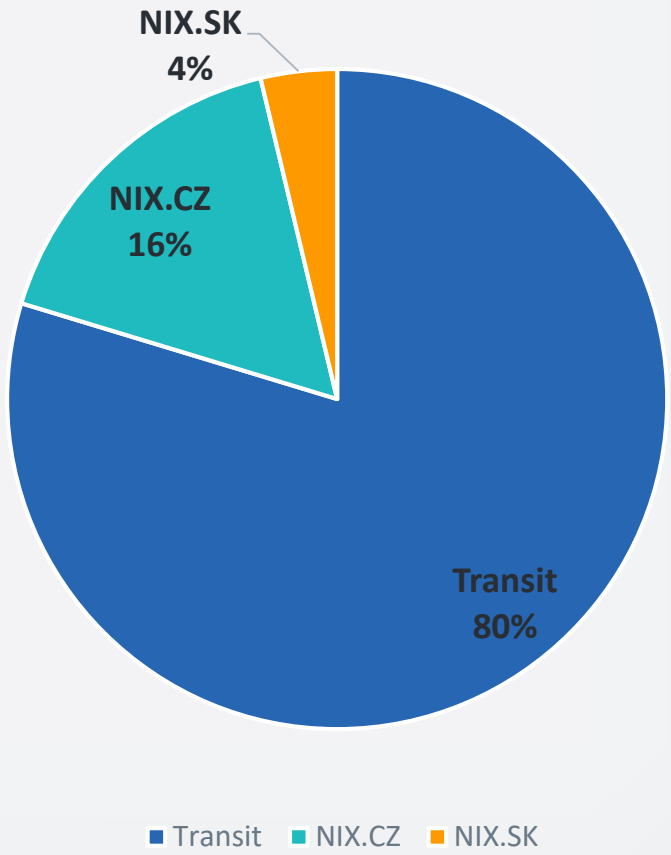

CISCO


FORCEPOINT

Zdroj: FlowGuard

Proti čemu stojíme?

- Červenec 2019, doba trvání cca 16 minut
- Datový přenos cca 94 Gbps @9.32 Mpps
- 2 400 000 unikátních zdrojových IP adres ze 42 000 AS
- Cílem útoku jediná IP adresa
- Více vektorový útok:
  - UDP flood na HTTP, fragmentovaný (velké packety)
  - TCP SYN flood na HTTPS (malé packety)
  - ICMP flood
- Z nuly na 9 Mpps za necelých 10 sekund ☺



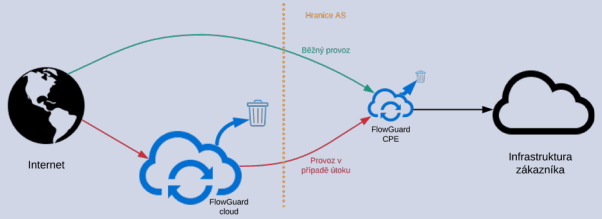
Možnosti obrany

Prevence

- Robustní infrastruktura
- Minimální terč
- Výkon a propustnost
- Limitace systémových prostředků
- Krizové plány

Záchrana

- Filtrace v cloudu
- Specializované zařízení pro filtraci
- Hybridní filtrace



Obětování

- Blokace (RTBH, Flowspec)
- Jeden za všechny je lepší než všichni za jednoho

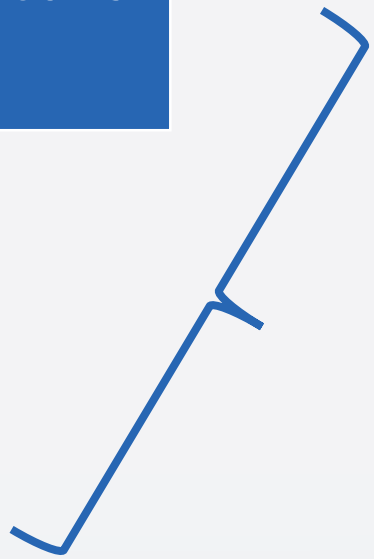
Dopady útoku

Kdo je útokem postižen?

Zákazník

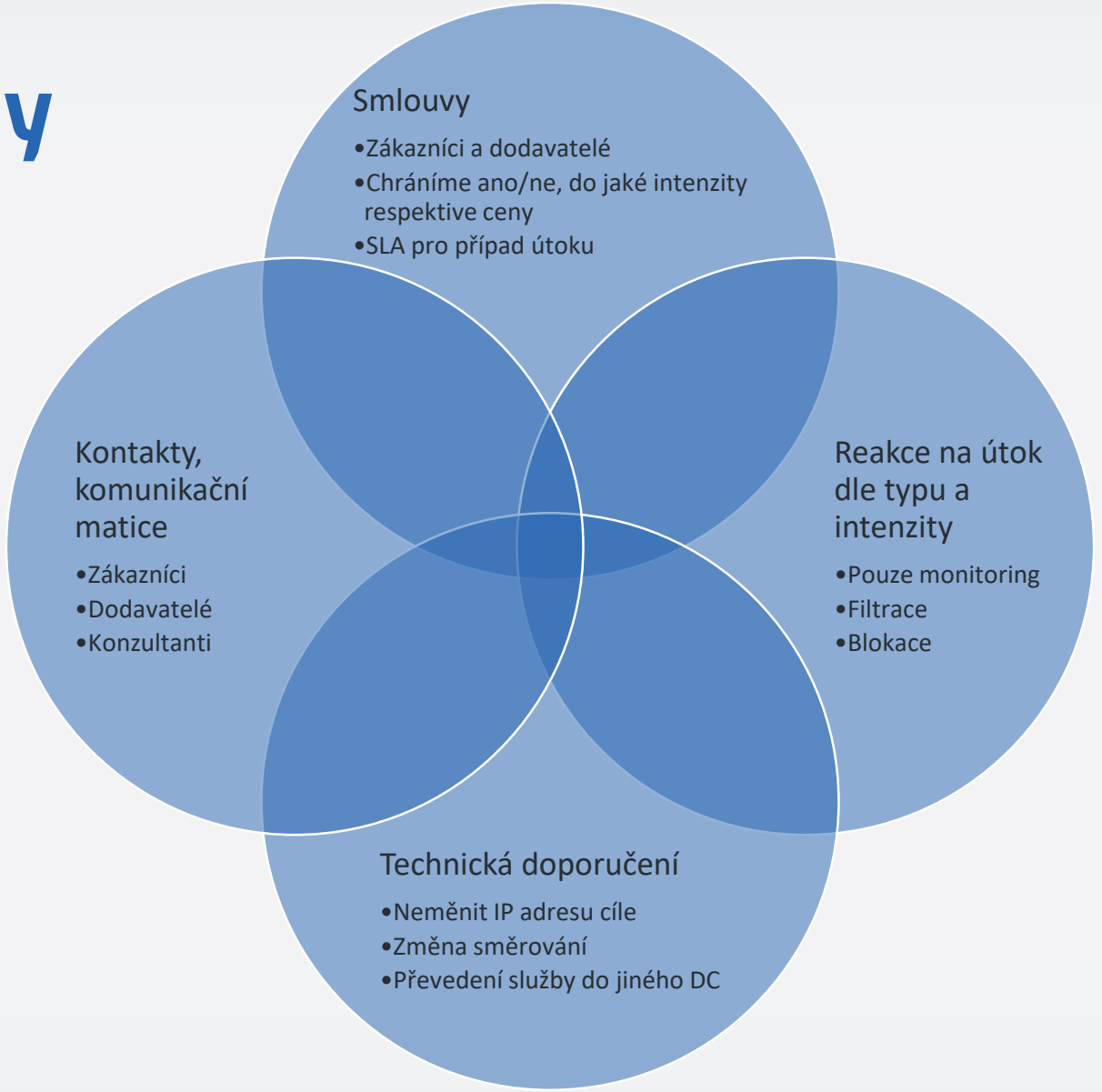
Infrastruktura

Zákazník + infrastruktura

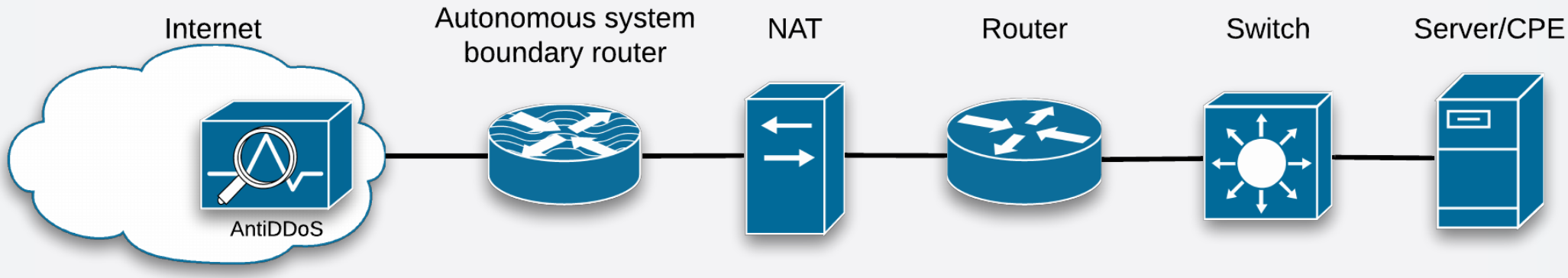


Vedlejší oběti

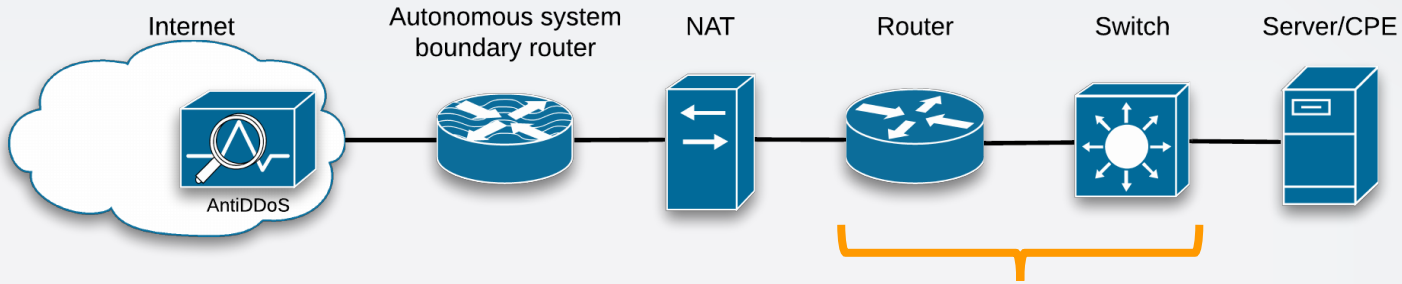
Krizové plány



Infrastruktura

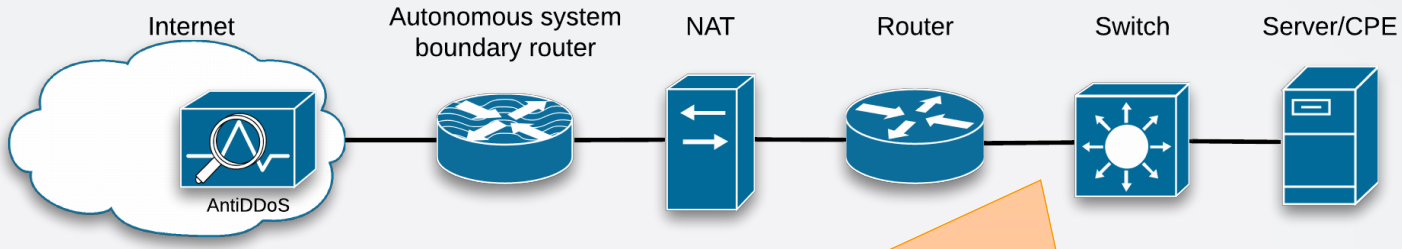


Routing & Switching



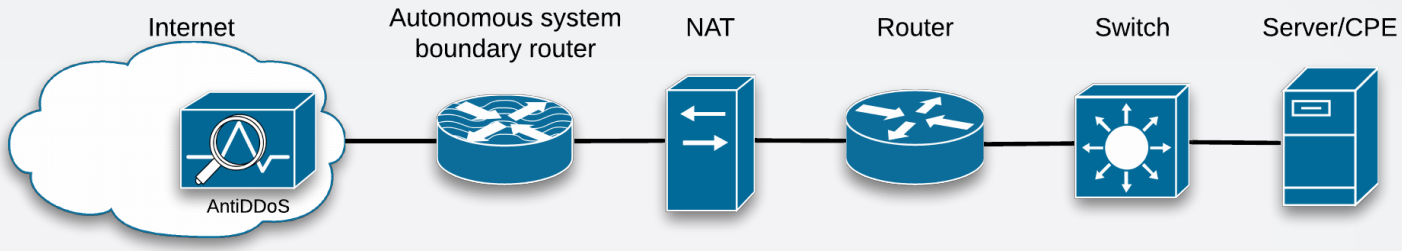
- L3 interfacy, ACL
- Oddělený data plane a control plane v samostatném HW
- Control Plane Policing
- Dimenzování prvků pro malé i velké packety (IMIX je v případě útoku nefungující teorie)
- Expirace ARP vs. MAC
- Pozor na softwarová řešení (Mikrotik, některé L3 switche)

Trasy



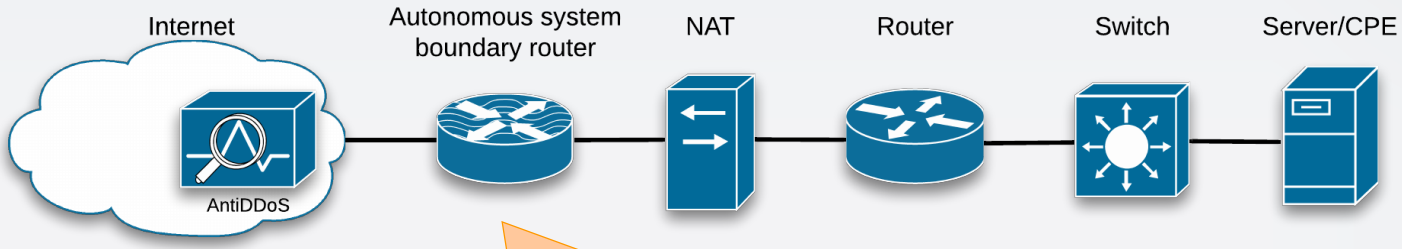
- Dostatečná rezerva propustnosti
- Implementace QoS
- Algoritmus balancování u link aggregation
- Saturace tras je důvodem pro blokaci

NAT



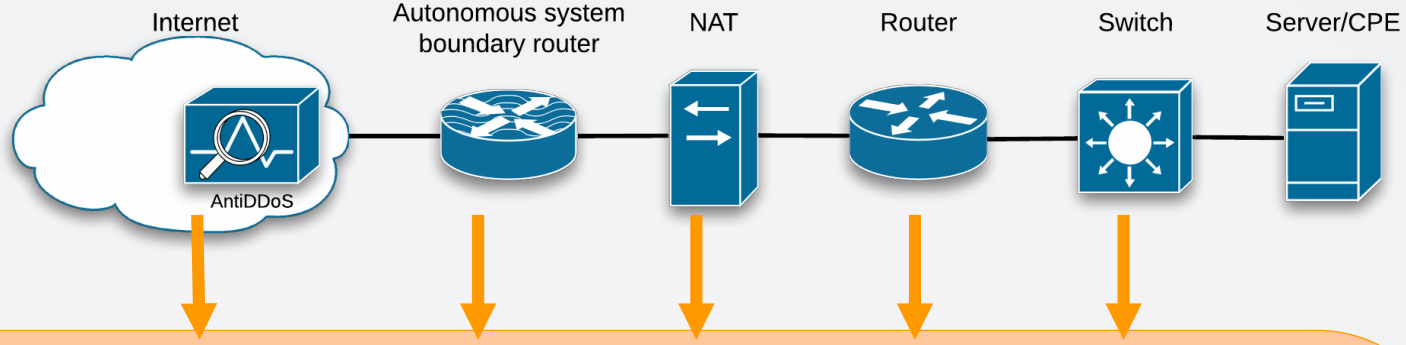
- Počet paralelních konexí
  - celkem
  - přírůstek za jednotku času
- Nejasný cíl, vedlejší oběti prakticky vždy
- Falešný billing u subscriberů

ASBR



- Výkon PPS, kapacita NetFlow
- Vstupní filtry
  - Anti-spoofing
  - Anti-bogon
  - Policery na specifický provoz (UDP frags, DNS, LDAP atd.)
- Výstupní filtry
- Implementace záchranné brzdy (RTBH, Flowspec)

Monitoring



- Měření všech interface
  - BPS
  - PPS
- NetFlow
  - cílové IP adresy dle poštu konexí, přenesených dat a packetů
  - počet unikátních zdrojových IP adres
  - počet unikátních zdrojových AS
  - průměrná velikost packetu dle protokolu
- Report útoků z filtrace

Štěstí přeje připraveným!

Email: petr.kadlec@comsource.cz
Tel: 774 744 725