cesnet

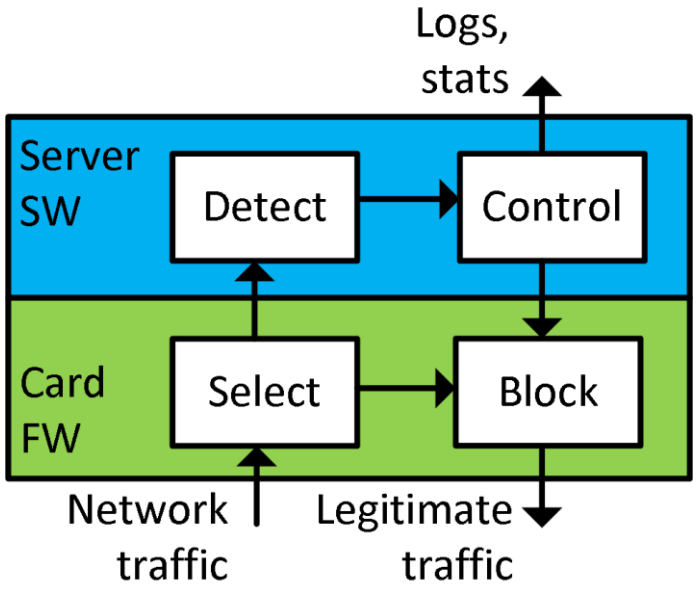
DDOS PROTECTOR: ALGORITMY A VÝZVY

Martin Žádník
CESNET

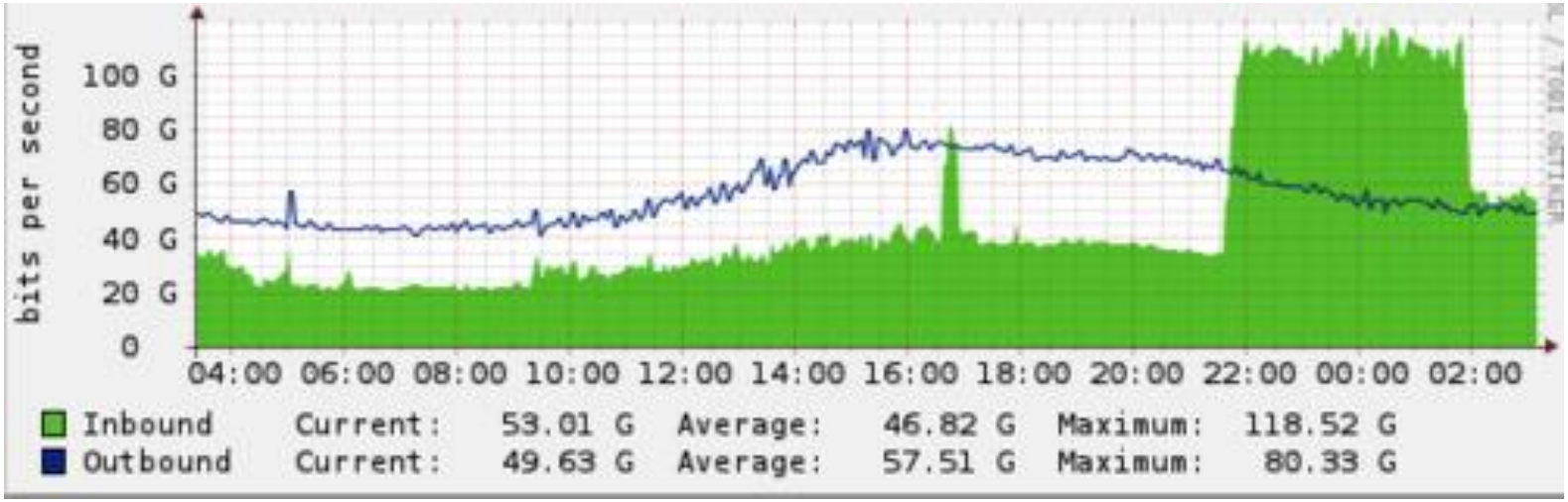
3. generace ochrany – DDoS Protector

- Vývoj vlastní DDoS čističky
- Implementace vlastního čištění
- Řádově levnější než podobná řešení
- Funkcionalita na míru

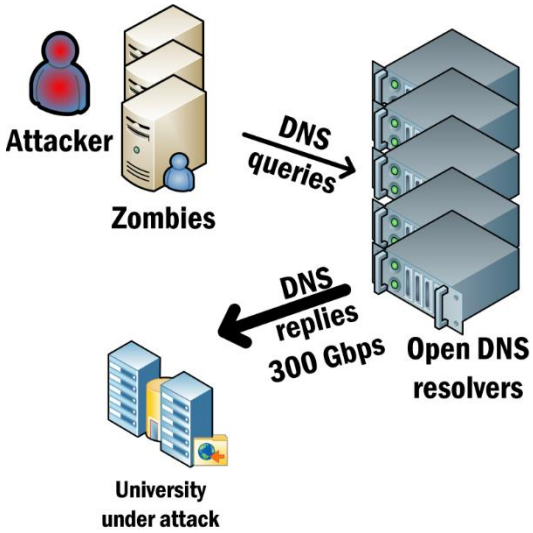
- Čistička se skládá ze serveru se síťovou akcelerační kartou COMBO-100G
- Programovatelné FPGA
- Vlastní firmware



- Primárně zaměřeno na ochranu konektivity
- Cílem je dostat objem provozu pro cílovou organizaci na zpracovatelnou úroveň



- **Velké útoky hrubou silou pomocí odrazu**
  - DNS
  - NTP
  - LDAP
  - SSDP
  - SNMP
  - CharGEN



- **TCP SYN flood útoky s podvrženou zdrojovou IP adresou**

PŘÍKLAD MITIGAČNÍ HEURISTIKY

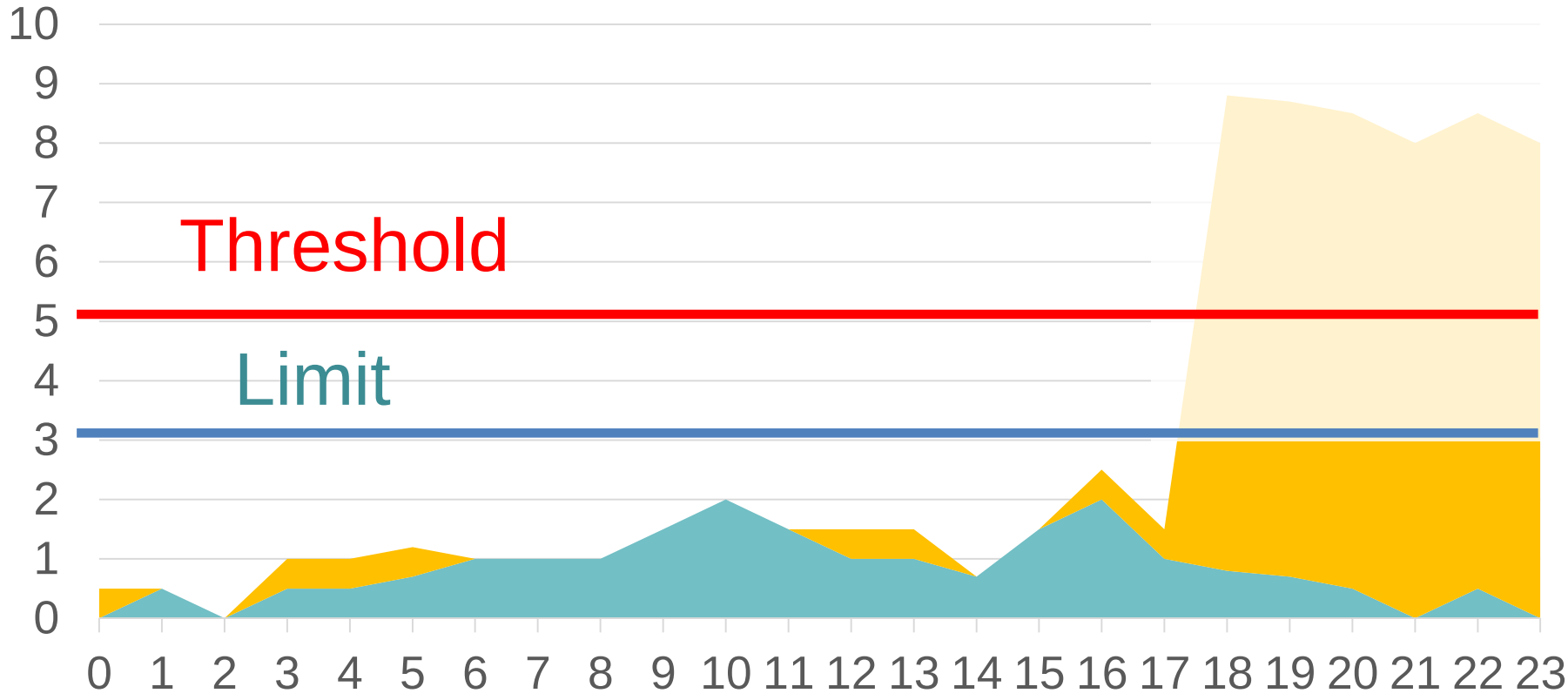
- Čistička hlídá překročení prahů pro zadané IP adresy/podsítě
- Volitelné časové rozlišení (s)
- Jednoduchá pravidla nastavená dle historické zkušenosti správcem

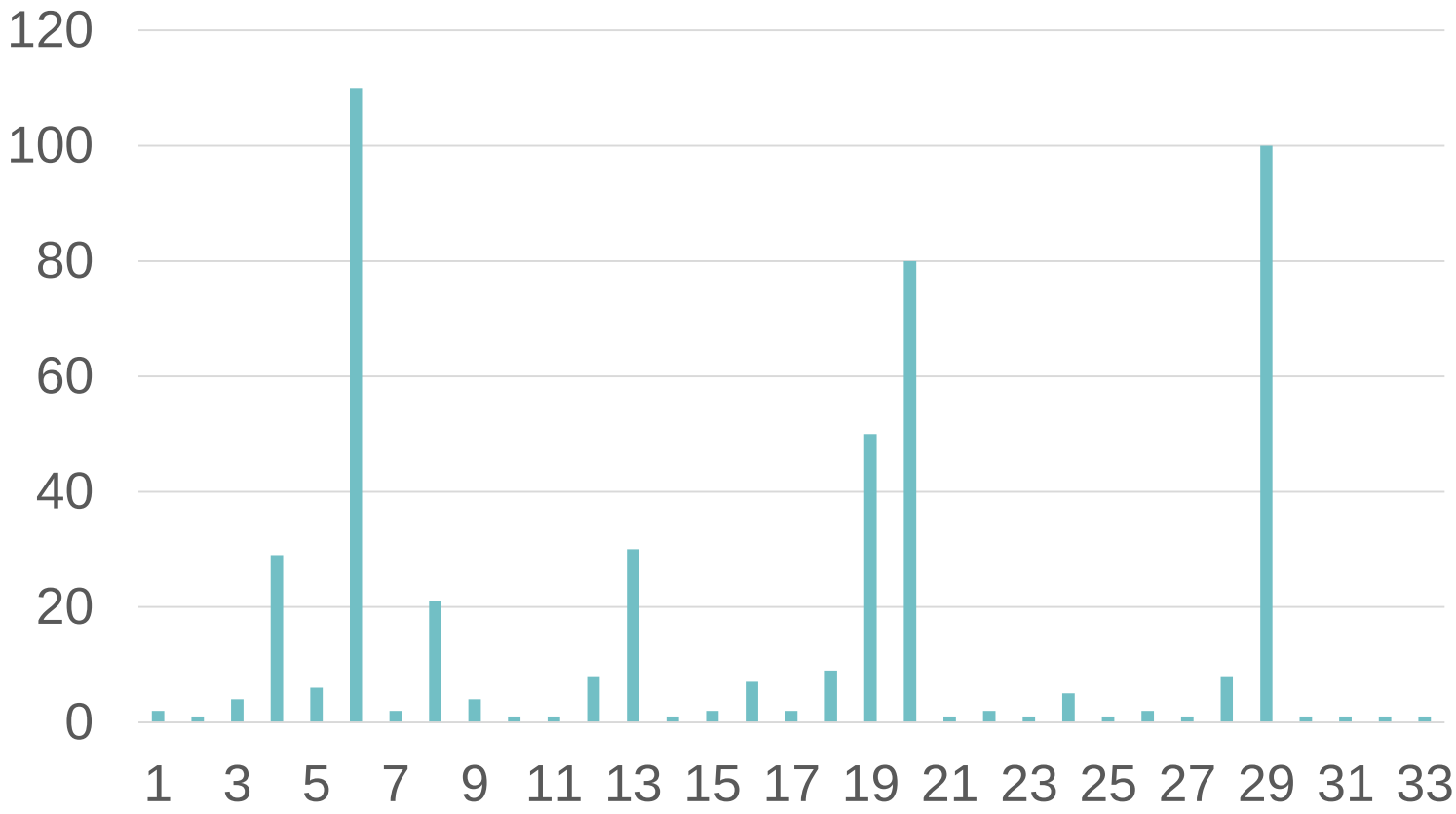
„VUT UDP“ dst net 147.229.0.0/16 protocol 17 src port 53 threshold 1 Gbps limit 100 Mbps

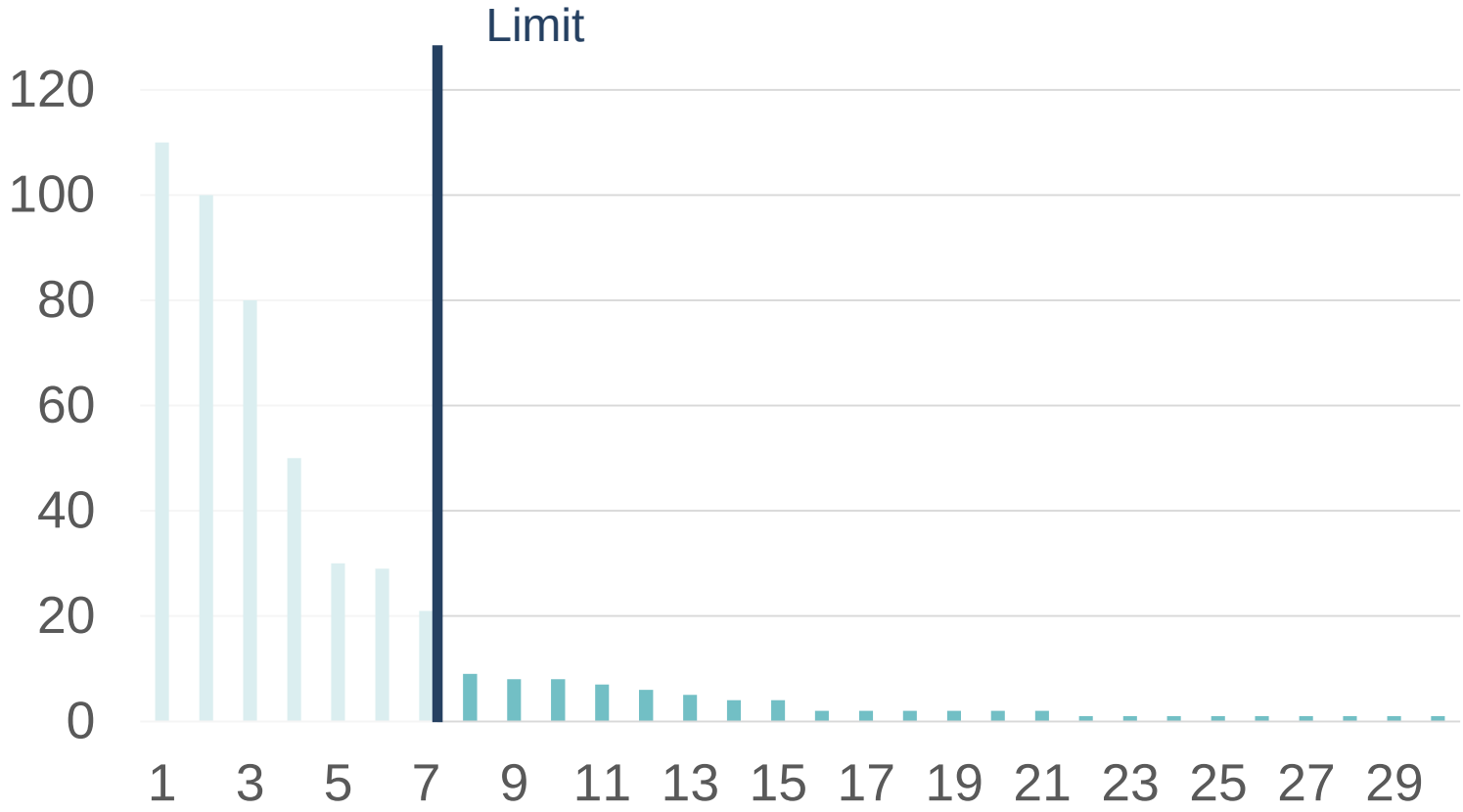
cesnet

ČIŠTĚNÍ AMPLIFIKACE

- Zahoď provoz ze zdrojových IP adres, které nejvíce přispěly k překročení limitu pravidla
- Ke každému pravidlu sleduj množství provozu pro zdrojové IP adresy
- Pokud je překročen limit pravidla vyber tolik top zdrojových IP adres, aby bylo dosaženo snížení objemu provozu na požadovanou úroveň

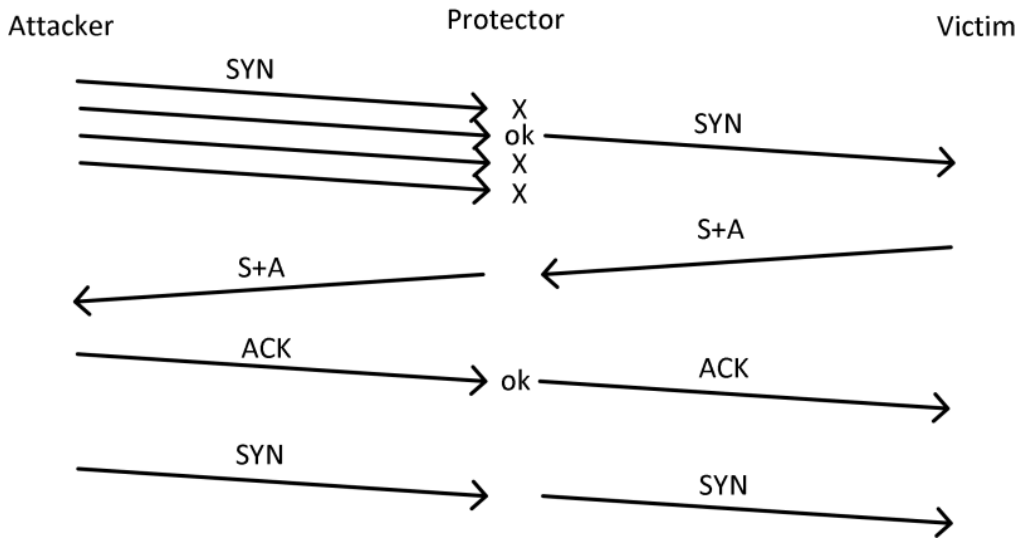

10
9
8
7
6
5
4
3
2
1
0
Threshold
Limit
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23


120
100
80
60
40
20
0
1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33


Limit
120
100
80
60
40
20
0
1
3
5
7
9
11
13
15
17
19
21
23
25
27
29

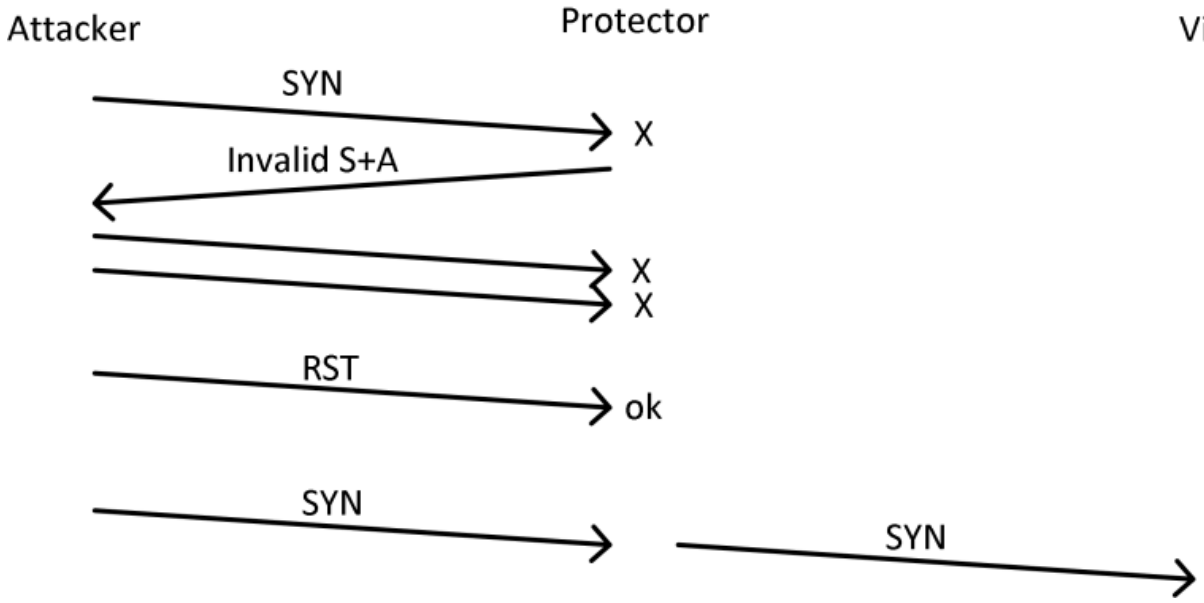
ČIŠTĚNÍ SYN FLOOD I.

- Mitigace TCP SYN flood útoku
- SYN drop heuristika



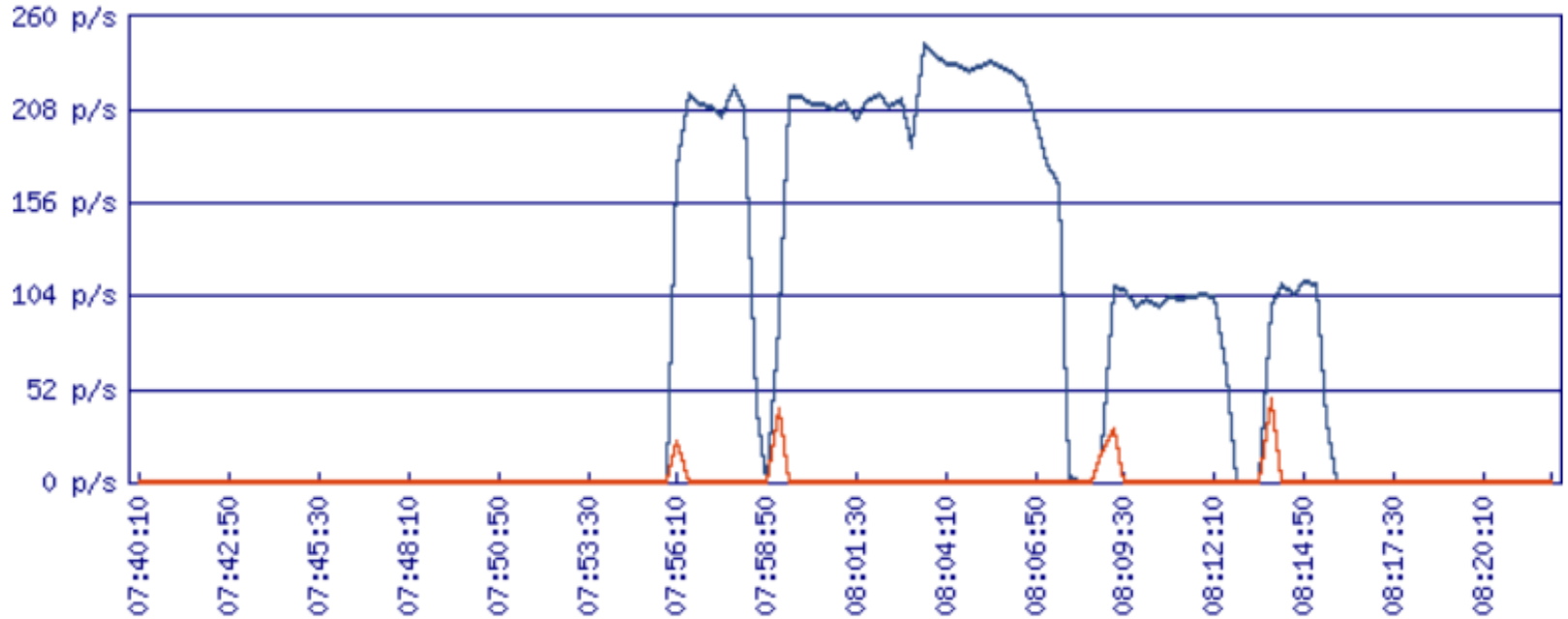
ČIŠTĚNÍ SYN FLOOD II.

- Alternativa k SYN drop heuristice
- Protector vygeneruje nevalidní odpověď
- Pokud potencionální útočník zašle RST, pak je whitelistován



Zneužití protokolu memcached

- Extrémní amplifikace i v reálných podmínkách i více jak 1:3000



Carpet bombing DDoS

- Obvykle reflektivní útok
- Mnoho zdrojů
- Mnoho cílů

Detekce založená na sledování per IP adresa nebude fungovat

- Příklad pro protokol memcached lze na základě pozorování nastavit práh pro IP adresu na 5 Mb/s. Pro prefix /16 souhrnný vygenerovaný provoz může být až 262 Gb/s.

Využití Simple Service Discovery Protocol (SSDP)

- Některá embedded a IOT zařízení generují náhodné číslo portu v odpovědi
- Není možné identifikovat provoz dle čísla portu
- Problematická selekce provozu

- “It turns out that about 2.4% of the IPs that respond to SSDP queries, do so from a weird port number! For example:“

- IP 192.168.1.75.50950 > 239.255.255.250.1900: UDP, length 95
- IP 192.168.1.71.1026 > 192.168.1.75.50950: UDP, length 249

- **Útočník si pronajme VM, kde zprovozní vlastní implementaci memcached s náhodným portem v odpovědi a zkombinuje s Carpet bombing.**

- **Multi-vector útok**
  - Ztížení obrany
  - Skrytí průniku za DDoS útok

- **DDoS útočící na DDoS ochranu**
- **DDoS zneužívající aplikačních protokolů**

BUDOUCNOST DDOS OBRANY

- **Vyšší míra automatizace**
  - Analytika nejen dodává prahy, ale podrobně určuje typy útoků
  - Automatizace derivace mitigačních pravidel
  - Automatizace řízení mitigace na základě zdrojů
  - Reakce na obcházení či útoky na obranu, např. variabilní hash funkce

- **Vysokorychlostní sledování aplikačních hlaviček případně vyhledávání v obsahu**
  - Heuristiky

cesnet

DĚKUJI ZA POZORNOST. DOTAZY?