DDoS Protector aneb čistička

Martin Žádník

Popularita

- DDoS útoky
  - Motivace
  - Cíl
  - Prostředky

- DDoS útoky jako služba
- DDoS-for-hire industry
- Booters/Stresser service
- Mirai

Statistiky

- AKAMAI
  - Několik stovek DDoS ročně
  - Největší od 2015
    - 363 Gbps
    - 600 Gbps
    - 1,1 Tbps

- CESNET
  - Podobné množství
  - Řádově nižší síla útoků
  - Testovací hřiště

Ukázka

- UDP - 23 mil. paketů za 5min.:

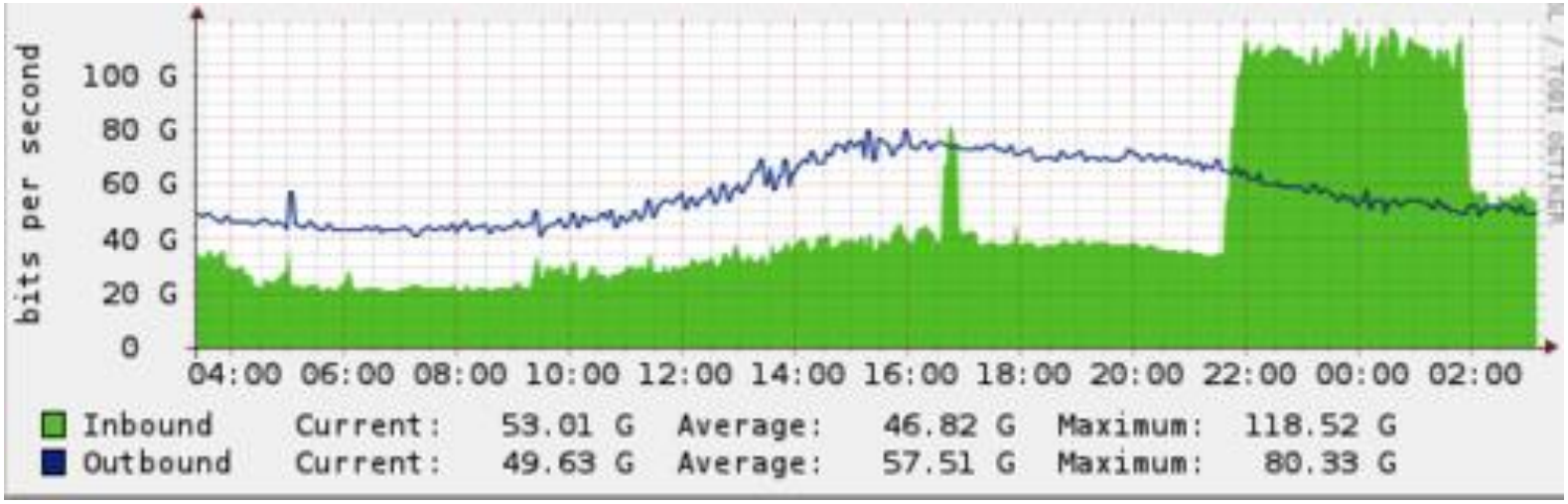
Src IP	Dst IP	Pkts	Bytes
194.228.x.x:53	194.160.x.x:4444	3	4163
182.52.x.x:53	194.160.x.x:4444	1	1453
54.39.x.x:53	194.160.x.x:4444	3	4163
182.52.x.x:53	194.160.x.x:4444	1	1453
192.48.x.x:53	194.160.x.x:4444	3	4163
71.230.x.x:53	194.160.x.x:4444	3	4163
200.229.x.x:53	194.160.x.x:4444	3	4163

DDoS mitigace

- Rate limiting na routerech
  - Hrubý filtr
  - Potenciální riziko blokování legitimního provozu
- DDoS Protector
  - Vývoj vlastní DDoS čističky
  - Detailnější čištění
  - Řádově levnější než podobná řešení
  - Funkcionalita na míru

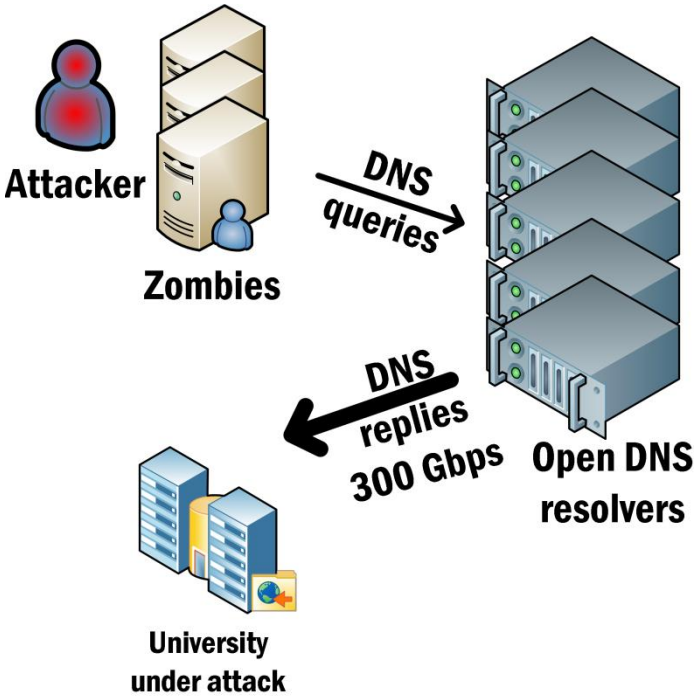
Cíl

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



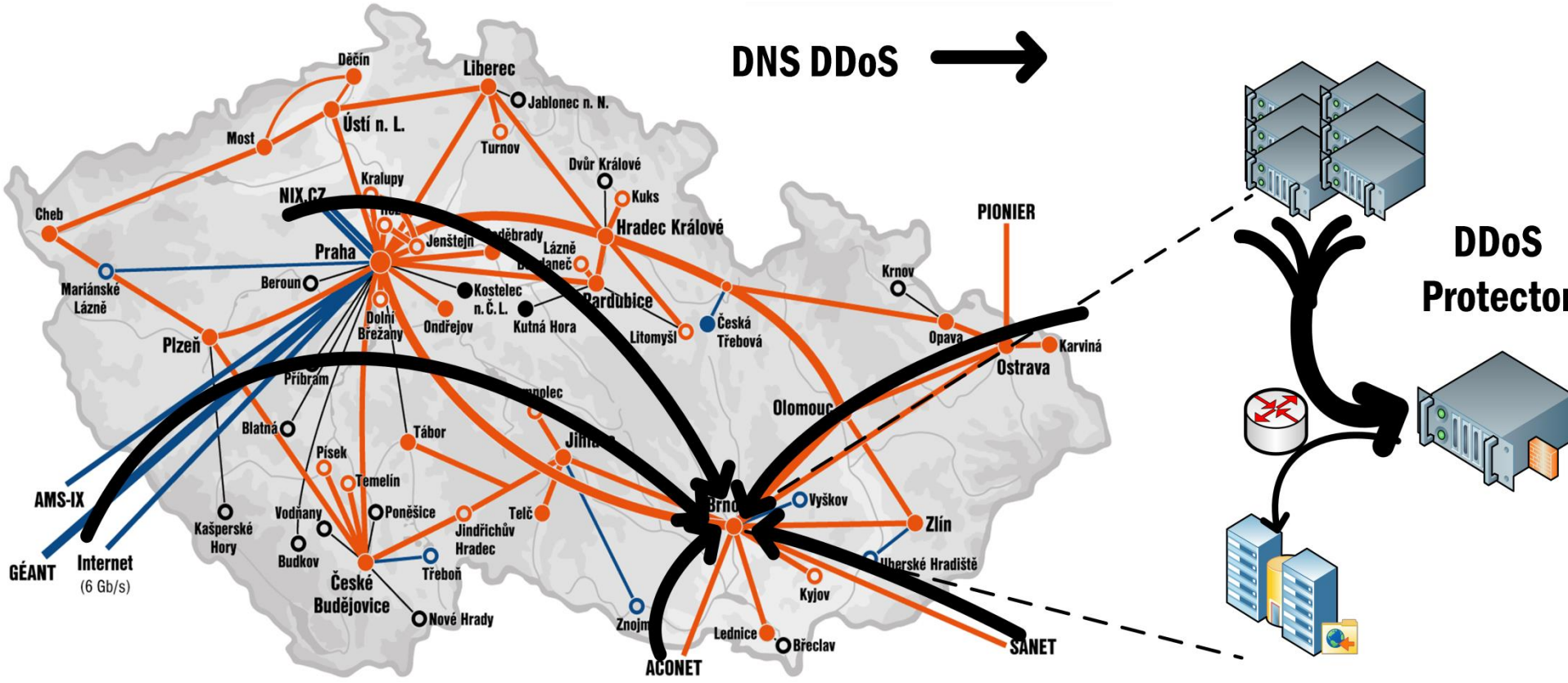
Útoky

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



Čištění útoku

- Přesměrování útoku na DDoS Protector
- Vrácení čistého provozu do cílové organizace



Detekce

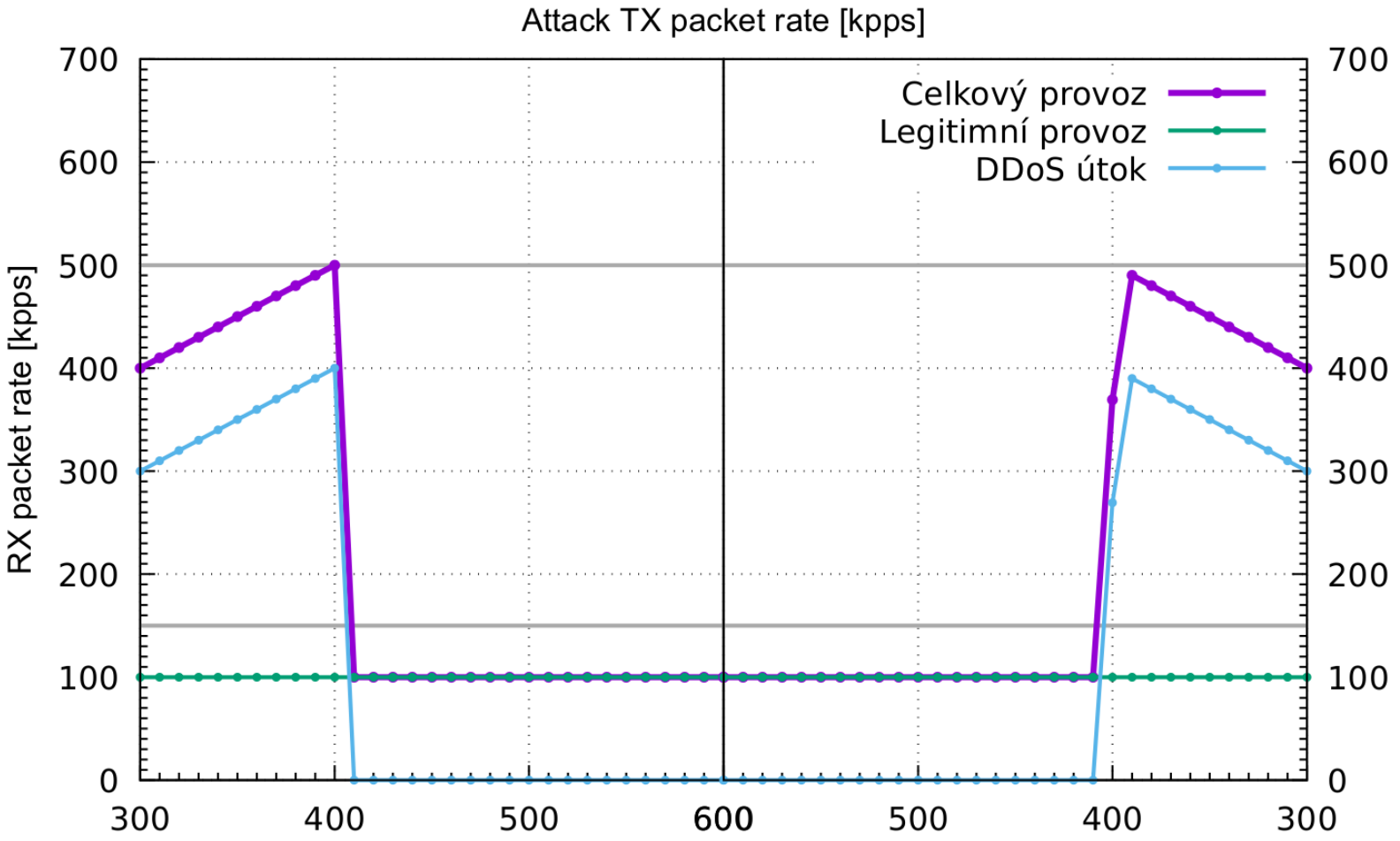
- Čistička hlídá překročení prahů pro zadané IP adresy/podsítě
- Volitelné časové rozlišení (s)
- Jednoduchá pravidla nastavená dle historické zkušenosti správcem

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

Čištění

- Zahoď provoz ze zdrojových IP adres, které nejvíce přispěli 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

Ukázka


Attack TX packet rate [kpps]
RX packet rate [kpps]
Celkový provoz
Legitimní provoz
DDoS útok
700
600
500
400
300
200
100
0
300
400
500
600
500
400
300

Algoritmus

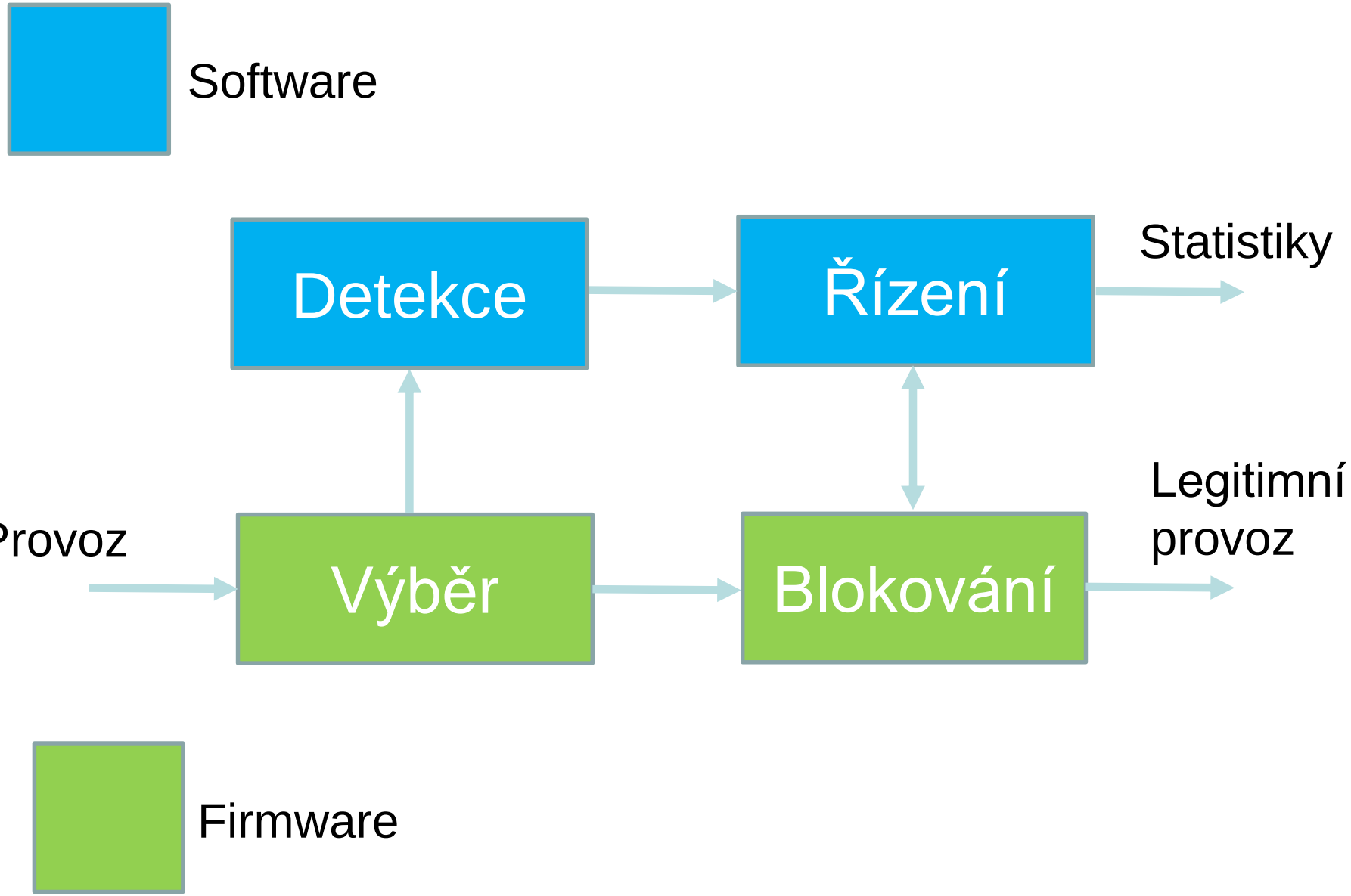
Při příchodu paketu

1. Najdi všechna odpovídající pravidla
2. U každého pravidla aktualizuj zdrojové IP adresy a statistiky
3. Je zdrojová IP adresa již blokována?
   - Ano, zahoď paket, aktualizuj statistiky
   - Ne, edituj paket a přepošli
4. Na konci časového intervalu zkontroluj překročení limitů pravidel
5. Vytvoř seznam top N zdrojových IP adres k blokování

HW akcelerace

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

Schéma

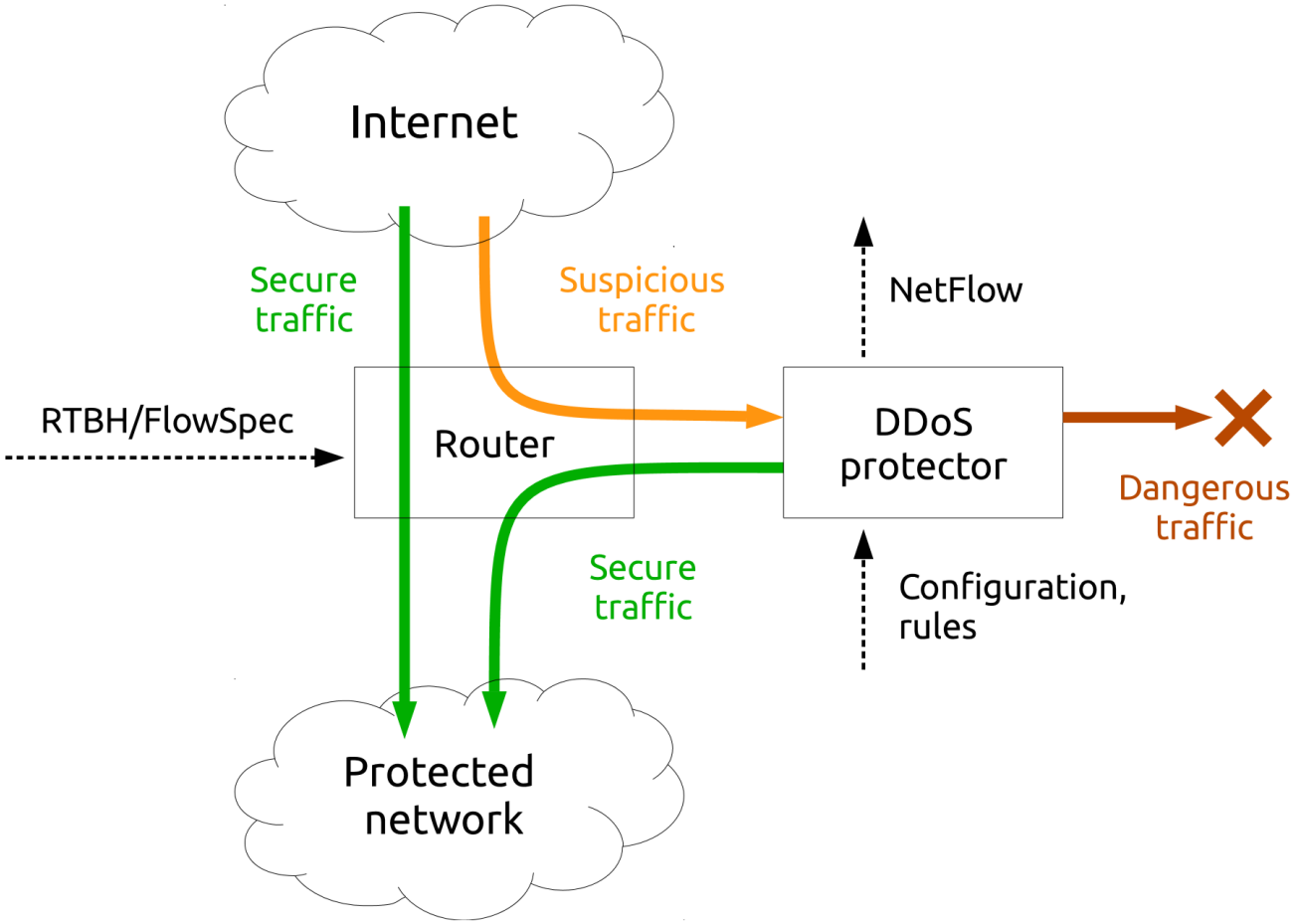

Software
Detekce
Řízení
Statistiky
Provoz
Výběr
Blokování
Legitimní
provoz
Firmware

Parametry

- Plná propustnost 100Gbps full duplex
- Extrémně nízká latence (mikrosekund)
- Podpora IPv6
- Podpora překladu VLAN
- Hlídání až 3 tis. pravidel
- Blokování 16 tis. zdrojových IP adres

Zapojení

- 10x 10Gbps
- 1x 100Gbps



Plány

- Heuristické blokování TCP Syn Flood útoků
- Blokování 100tis. zdroj. IP adres

- Podpora různých strategií blokování
  - TCP proxy
  - TCP proxy heuristika
  - Povolení zdrojových AS
  - Blokování cíle

- Rozšiřování konfiguračního rozhraní
  - Databáze
  - BGP Flowspec

Závěr

- Nasazeno v síti CESNET
- Přímočaré řešení s deterministickým chováním
- Čištění provozu za účelem ochrany infrastruktury
- Flexibilní platforma umožňuje rozšiřování dle aktuálních potřeb
- Vhodné pro ochranu českého kybernetického prostoru

Děkuji za pozornost.
Dotazy?