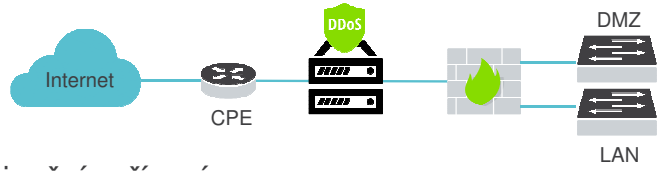
Partnerské školení

Flowmon DDoS Defender

Flowmon
Driving Network Visibility

Strategie ochrany podniků

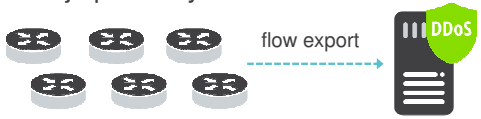
- Schéma perimetru podniků
  - Omezené množství linek a jejich omezená kapacita



- In-line DDoS mitigační zařízení
  - All-in-one detekce & mitigace stačí zapojit
  - Pokrytí volumetrických a aplikačních (L3/L4/L7) útoků
  - Nejvýše však do kapacity linek!

Strategie ochrany páteřní sítě

- Specifikace perimetru páteřní sítě
  - Více peering uzlů – routery & linky
  - Velká přenosová kapacita – snadno desítky gigabytů
  - In-line ochrana je prakticky nemožná!



1. Sběr flow dat
2. Detekce DDoS
3. Řízení přesměrování
4. Řízení mitigace

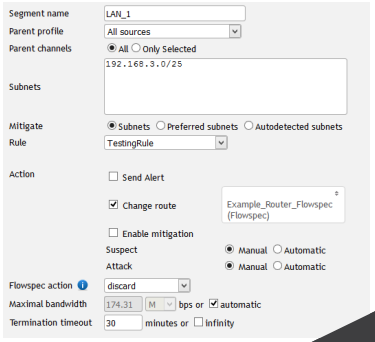
- Detekce založená na flow datech a out-of-path mitigace
  - Snadné a cenově výhodné k nasazení v páteřních sítích/ISP
  - Znemožňuje volumetrickým DDoS útokům dosáhnout perimetru podniků

DDoS ochrana založená na flow datech

1. Definice zákazníků = chráněné segmenty
   - Většinou pomocí podsítí
2. Nastavení pravidel pro DDoS detekci
   - Několik typů baseline pro každý chráněný segment
3. Nastavení alertů
   - Upozornění na útoky
4. Konfigurace přesměrování provozu
   - Přesměrujte provoz a mitigujte DDoS útok
5. Konfigurace řízení mitigace = scrubbing
   - Integrace se scrubbing zařízeními a službami

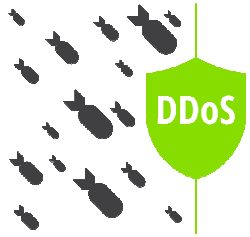
Definice tenantů

- Uživatelem definované chráněné segmenty k detekci a reakci na DDoS útoky
  - Na zákazníka, služby nebo obecně libovolné IP segmenty
- Definovány pomocí podsítě
- Rozsah mitigace
- Pravidlo pro detekci
- Akce



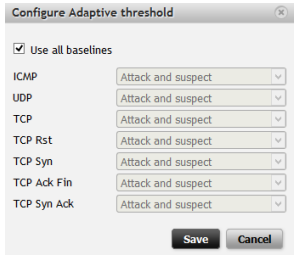
Detekce útoku

- Detekce prováděna pro všechny chráněné segmenty
  - Podsítěmi definované segmenty
- Sada **baseline** naučena podle síťového provozu pro každý segment. Útok je detekován v případě, kdy aktuální provoz překročí stanovenou hranici.
- Základní úrovně jsou naučeny pro:
  - Provoz TCP se specifickými příznaky
  - Provoz UDP
  - Provoz ICMP



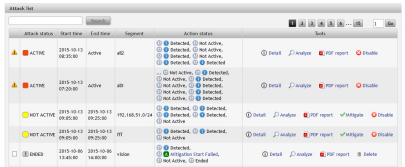
Metoda adaptivního prahu

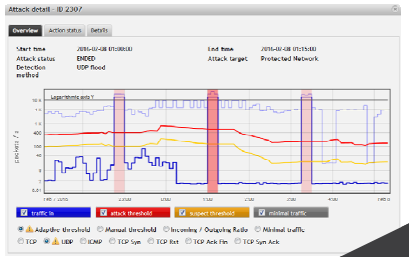
- Plně automatizovaný přístup k nastavení baseline bez nutnosti manuálních vstupů
- Dvě úrovně citlivosti
  - Detekce útok nebo podezření na útok
- Jednoduchá konfigurace
- Nastavitelná doba učení
  - Průběžné aktualizace baseline
- Ladění false positives
  - Pro každý útok



Report útoku

- Čas začátku/konce
- Cíl útoku
- Typ a stav útoku
- Objem provozu při útoku/klidovém stavu
- Cíle útoků (top 10 dst IPs, zdroje podsítí, L4 protokoly, TCP příznaky…)



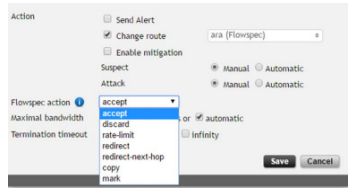


Reakce na útok

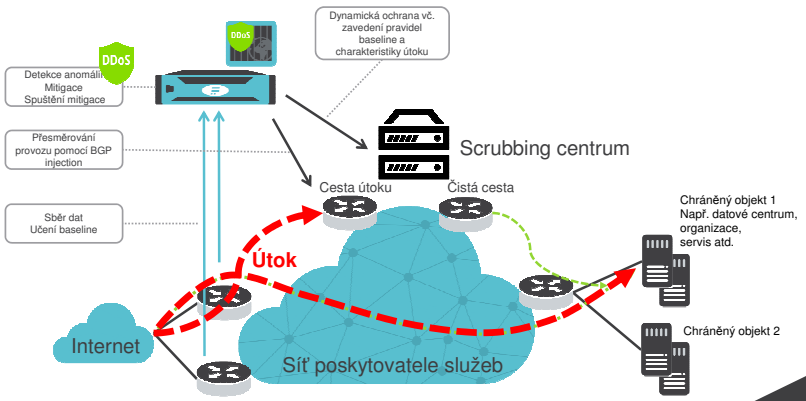
- Oznámení
  - E-mail, Syslog, SNMP trap
- Přesměrování provozu
  - PBR (Policy Based Routing)
  - BGP (Border Gateway Protocol),
  - BGP Flowspec
  - RTBH (Remotely-Triggered Black Hole)
- Uživatelem definované skripty
- Automatická mitigace
  - V Out-of-Band mitigačních zařízeních
  - Pomocí služeb scrubbing centra

Podpora BGP Flowspec

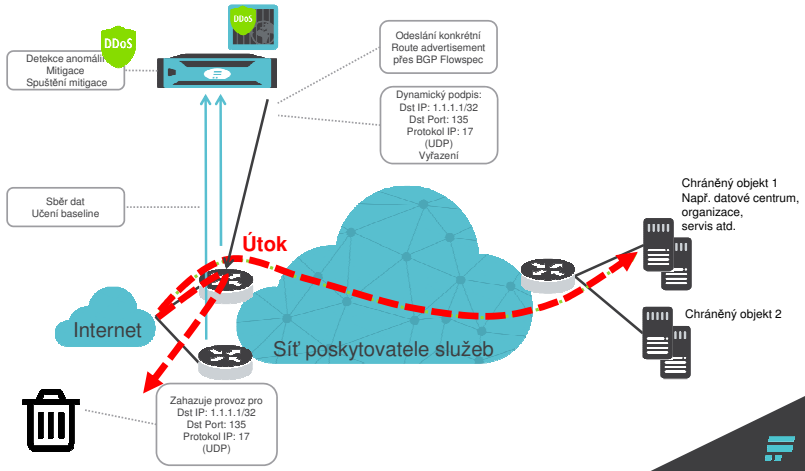
- Standardizovaná metoda pro pokročilé filtrování provozu na routeru pro mitigaci DDoS útoku
- Použití **dynamických charakteristik** útoku
- Provedení **vybrané akce** pro provoz odpovídající Flowspec pravidlu
- Pravidla Flowspec jsou založena na:
  - cílový prefix
  - zdrojový prefix
  - IP protokol
  - cílový port
  - ICMP typ
  - ICMP kód

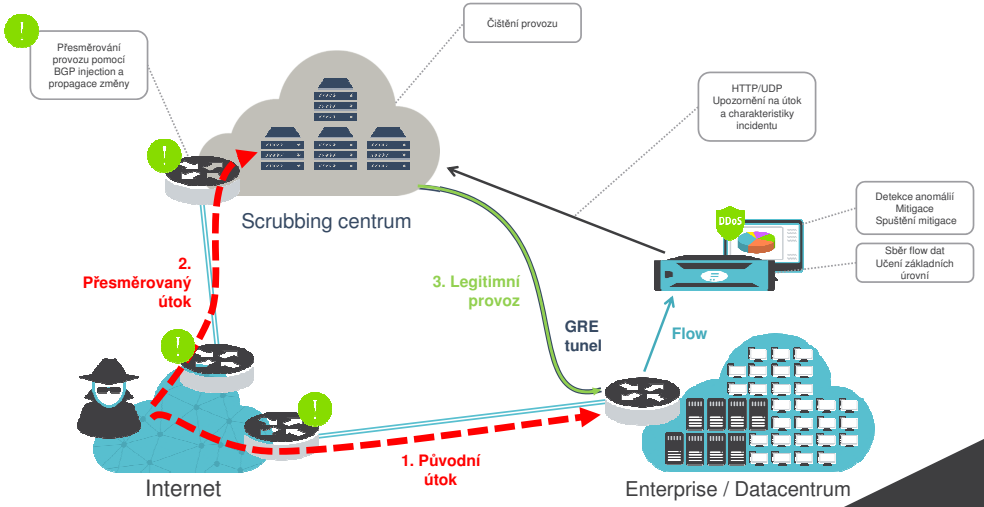


Scénář Out-of-Band mitigace



Scénář mitigace pomocí BGP Flowspec





DDoS Defender - modely

	1	4	10	40	100	400	1000
Propustnost (Gbps)	1	4	10	40	100	400	10000
Doporučený kolektor	1TB+	1TB+	3TB+	3TB+	12TB+	12TB+	SSD
Odklon provozu	PBR, BGP	PBR, BGP	PBR, BGP	PBR, BGP	PBR, BGP	PBR, BGP	PBR, BGP
Podpora BGP Flowspec	YES	YES	YES	YES	YES	YES	YES
Integrace třetích stran	YES	YES	YES	YES	YES	YES	YES

Shrnutí

- Využijte detekci DDoS založenou na flow datech kombinovanou s out-of-band mitigací
  - Využijte flow data z (routerů, sond, …) pro rychlou detekci DDoS
  - Chraňte všechny své zákazníky nebo rozšiřte svou nabídku MSSP služeb
  - Integrace s produkty třetích stran lokálně nebo s cloudovými službami

Děkuji za pozornost

Monitorování výkonu, viditelnost a bezpečnost s jediným řešením

Flowmon Networks a.s.
Sochorova 3232/34
616 00 Brno, Česká republika
www.flowmon.com

Flowmon
Driving Network Visibility