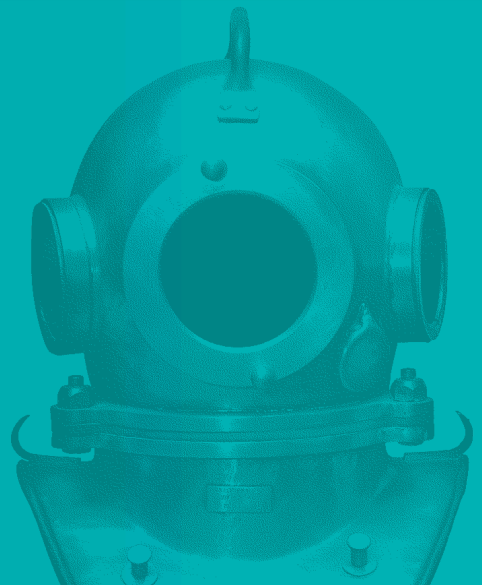
Detekce volumetrických útoků a jejich mitigace v ISP

Flowmon DDoS Defender a F5 řešení

Roman Tomášek
roman.tomasek@alef.com

ALEF



Partnerství a certifikace

- **Cisco Value Added Distributor**
- **Cisco Gold Certified Partner**
  - Advanced Collaboration Architecture
  - Advanced Data Center Architecture
  - Advanced Enterprise Networking Architecture
  - Advanced Security Architecture
  - Advanced Service Provider Architecture
- **Cisco Learning Partner**
- **F5 Distributor**
- **F5 Authorized Training Centre**
- **NetApp Value Added Distributor**
- **Microsoft Gold Technology Partner**
- **Flowmon Silver Partner**
- ISO 9001:2008
- ISO 27001:2013

ALEF

ALEF

cisco Distribution Partner

f5

Gold Microsoft Partner

Microsoft

NetApp

Distribution Partner

Flowmon

thycotic

A jiní

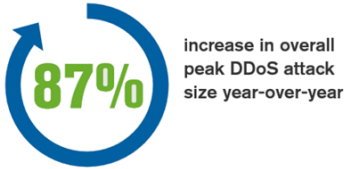
Kam kráčí telekomunikační sítě?

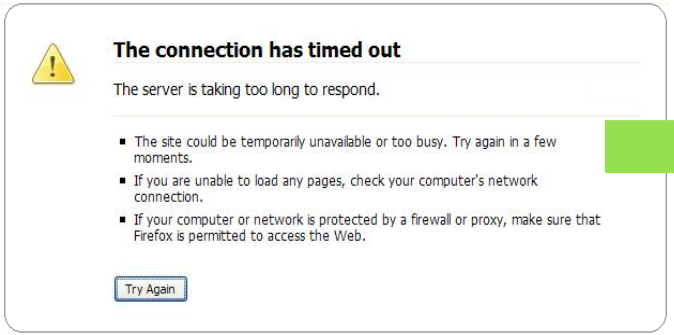
- Směrem k bezpečnosti!!
  - Ochrana citlivých dat
  - Ochrana aplikací
  - Ochrana sítě a zákazníku

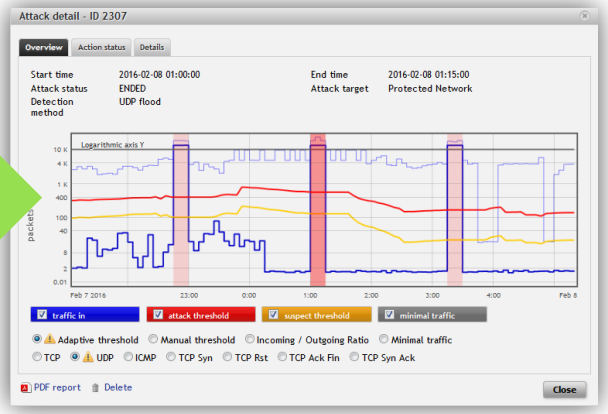
ALEF

Fakta o DDoS útocích

- Průměrná cena 1 min výpadku je 22 000 USD.
- Průměrná doba nedostupnosti sítě pro jeden útok je 54 minut
- Ochrana vašeho obchodu a zákazníků
- Ujistěte se, že vaše služby jsou dostupné
- Neztraťte svoji reputaci



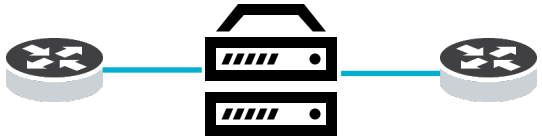




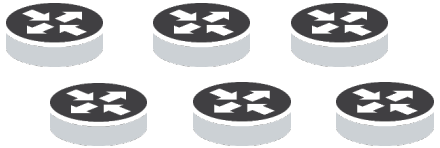
ALEF

Strategie ochrany vůči DDoS útokům

- In-line detekce a mitigace – vhodné pro enterprise sítě
  - Omezené množství linek k ISP
  - Zahrnuje i L7 útoky
  - Chrání před útoky až do kapacity linek



- SP/telco/datová centra potřebují řešení out-of-path
  - Zaměřeno na detekci volumetrických útoků
  - Velké množství uplinků a vysoká propustnost



ŘEŠENÍ?

Detekce volumetrických DDoS útoků kombinovaná s out-of-path mitigací.

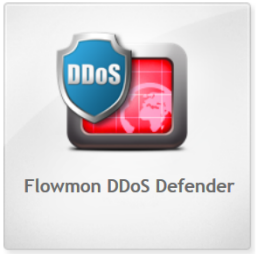
ALEF

NAŠE ŘEŠENÍ

ALEF

Flowmon a F5

- Flowmon DDoS Defender
  - detekce volumetrických DDoS útoků



- F5 AFM (Advanced Firewall Manager)
  - lokální čištění těchto útoků

ALEF

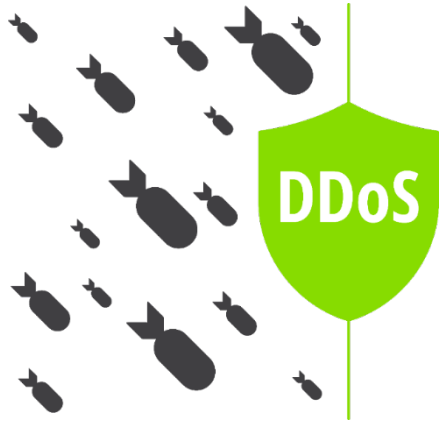
Flowmon DDoS Defender

- Detekce DDoS útoků
  - Zaměřeno na volumetrické útoky
  - Používá data o tocích z jakéhokoliv zdroje (směrovače, sondy…)
  - Předpovídá množství provozu použitím automatických/statických metod
  - Vytváří charakteristiky útoků a notifikace
- Podpora logické segmentace pro zákazníky, sítě, síťové segmenty, služby…
- Jednoduchý scénář nasazení

ALEF

Detekce útoků

- Detekce útoků se provádí pouze pro nadefinované segmenty – segmenty jsou určeny IP podsítěmi.
- Pro každý segment je ze sledovaného provozu naučena sada základních hodnot.
- Útok se zjistí, pokud aktuální provoz přesáhne stanovenou hranici.
- Výchozí hodnota je naučena pro:
  - TCP přenos s konkrétními příznaky
  - UDP přenos
  - ICMP provoz



ALEF

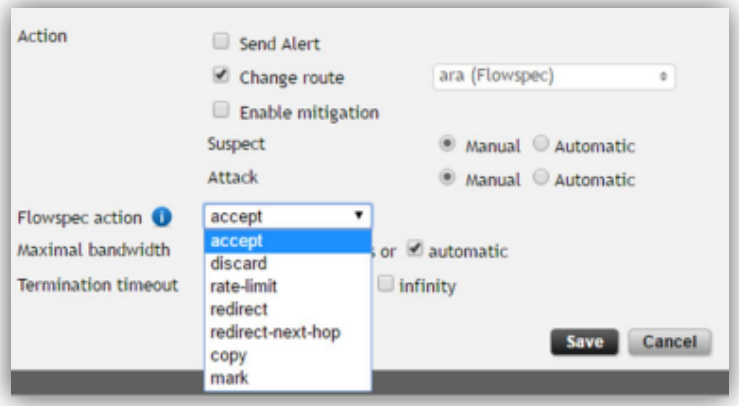
Odpovědi na útok

- Upozornění
  - E-mail, Syslog, SNMP trap
- Změna směrování
  - PBR (Policy Based Routing)
  - BGP (Border Gateway Protocol),
  - BGP Flowspec
  - RTBH (Remotely-Triggered Black Hole)
- Uživatelsky definované skripty
- Automatická mitigace
  - Lokální zařízení na čištění provozu
  - Scrubbing centra

ALEF

Podpora BGP Flowspec

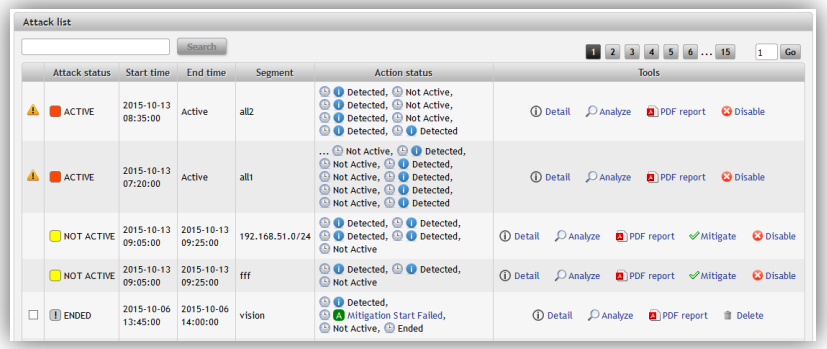
- Standardizovaná metoda pro pokročilé filtrování provozu na routeru pro mitigaci DDoS útoků
- Používá dynamický popis útoku (dynamic signature)
- Poskytuje konkrétní akce, které je třeba provést s příslušným síťovým provozem
- Pravidla Flowspec jsou založena na
  - Cílový IP prefix
  - Zdrojový IP prefix
  - IP protokol
  - Cílový port
  - Typ ICMP
  - Kód ICMP

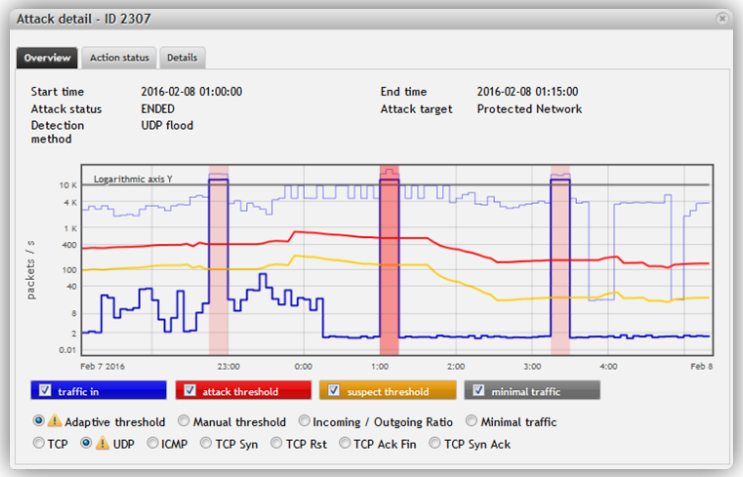


ALEF

Informace o útoku

- Začátek a konec útoku
- Cíl útoku
- Typ a stav útoku
- Objemy dat během útoku a mimo něj
- Detaily útoku





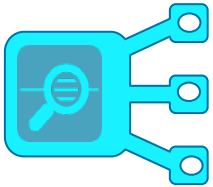
ALEF

Produktová řada DDoS Defenderu

DDoS Defender	1	4	10	40	100	400
Propustnost (Gbps)	1	4	10	40	100	400
Doporučený kolektor	1TB+	1TB+	3TB+	3TB+	12TB+	12TB+
Přesměrování provozu	PBR, BGP	PBR, BGP	PBR, BGP	PBR, BGP	PBR, BGP	PBR, BGP

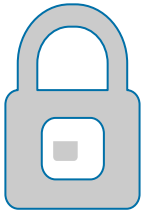
ALEF

F5 Advanced Firewall Manager (AFM)



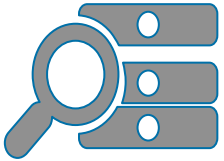
Zaměření na aplikace

- Kontrola přístupu na aplikace
- Jednoduchá správa politik
- Rozšiřitelné pomocí iRules



DoS ochrana

- Ochrana proti L3-L4 D/DOS útokům
- 120+ DoS vektorů & HW DoS ochrana
- Dynamická IP inteligence & Blacklisting
- RTBH & akcelerovaný auto-blacklisting
- Ochrana proti zneužití portů



Správa a viditelnost

- Vysokorychlostní FW logy/syslogy
- Detailní reporty o útocích
- Centrální správa pomocí BIG-IQ
- Kompilace pravidel na vyžádání
- Automatické nastavení DDoS prahových hodnot
- Zjednodušené NAT/PAT toky

ALEF

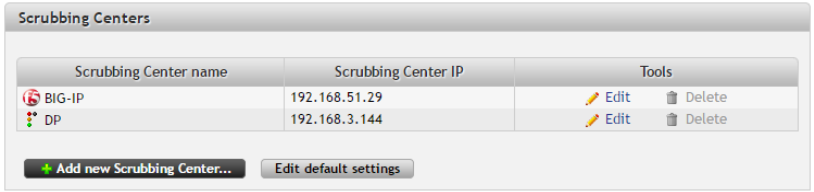
Pokročilá detekce a čištění DDoS

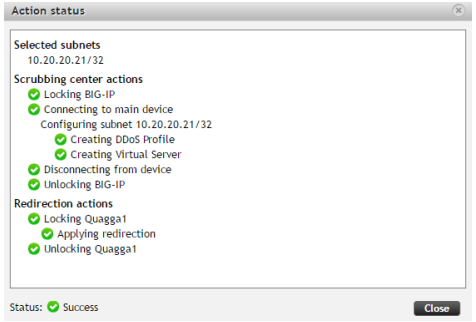
- Podpora více jak 100 DDoS vektorů z toho 84 je podporováno v HW
- Detekce špatného a podezřelého chování a volumetrických útoků
- Zabránění útokům způsobujícím přetečení tabulky toků
- Limity detekce a čištění – na globální úrovni, na úrovni routovací domény a na úrovní virtuálního serveru

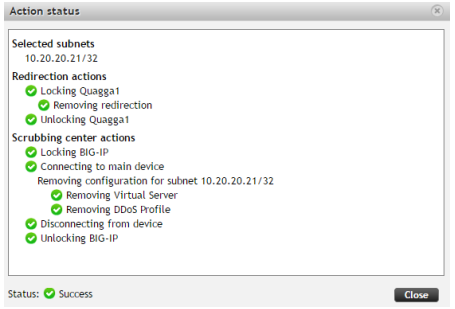
ALEF

Integrace Flowmon s F5

- Integrace s F5 BIG-IP a VIPRION
  - Nativní podpora
  - Integrace použitím API
  - Od verze TMOS 13.0
- Plně automatické nastavení čištění
  - Přesměrování a nastavení konfigurace na F5
  - Automatické odstranění konfigurace po skončení útoku

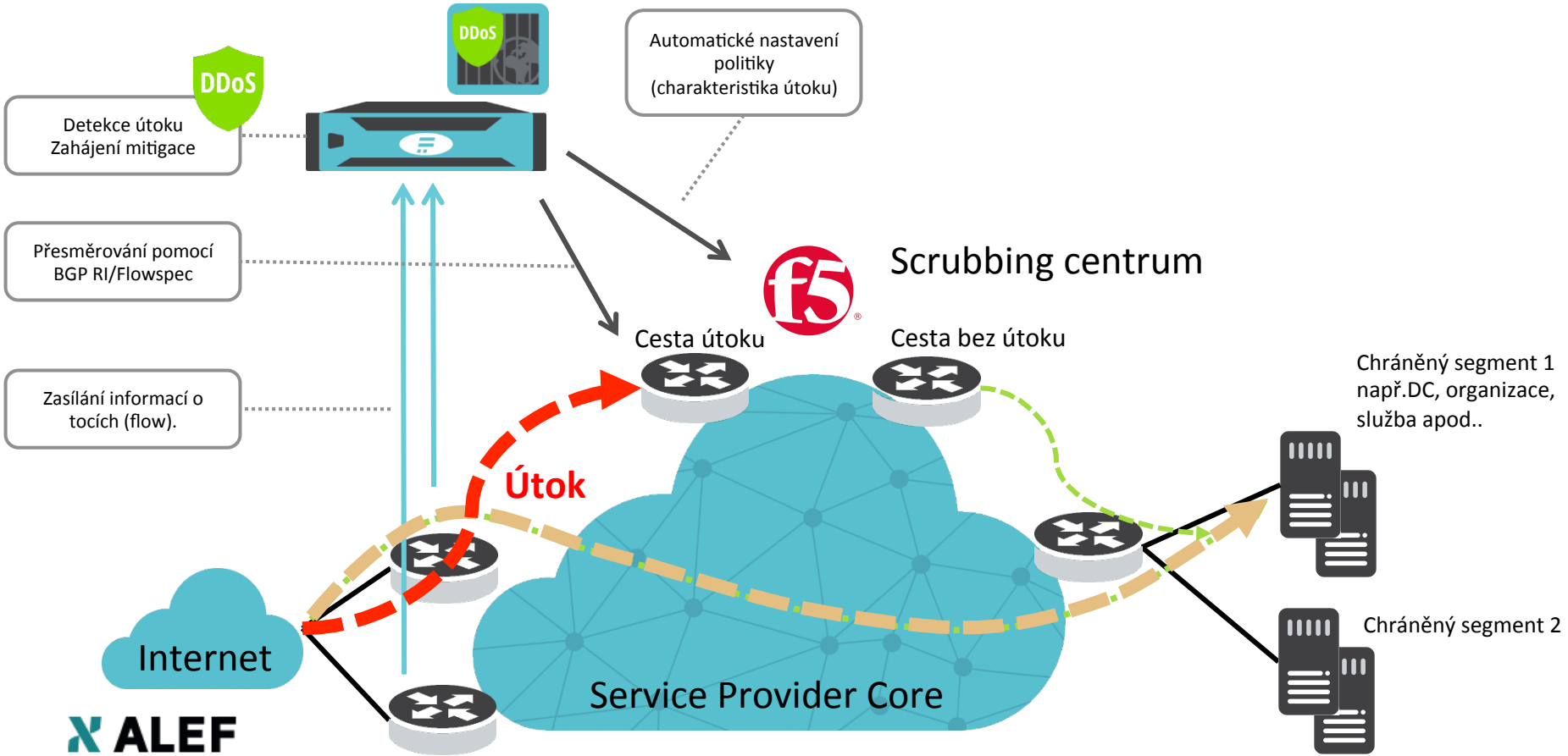






ALEF

Scénář použití



Popis řešení

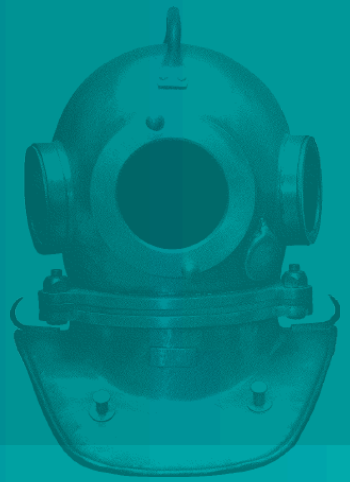
- Flowmon poskytuje:
  - Rychlou detekci DDoS útoku
  - Přesměrování na lokální zařízení/scrubbing centrum
  - Charakteristiku útoku pro čištění

- Lokální zařízení/Scrubbing centrum
  - Čištění datového provozu

ALEF

UKÁZKA

ALEF



Děkuji za pozornost

ALEF