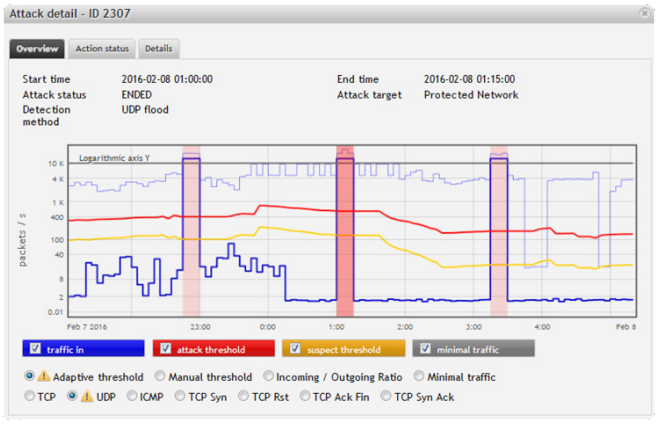
Flowmon
DDoS Defender

Plugin pro detekci a mitigaci DDoS útoků

Product Brief

ÚVOD

Flowmon DDoS Defender je řešení pro detekci a mitigaci útoků typu odepření služby – DoS (Denial of Service) nebo DDoS (Distributed Denial of Service). Bez jakýchkoliv změn konfigurace, topologie datové sítě nebo dodatečných investic do síťových komponent je možné v reálném čase odhalovat volumetrické útoky vedené proti IT infrastruktuře, serverům, kritickým systémům nebo aplikacím. Navíc ve spolupráci se službou tzv. Scrubbing centra nebo specializovaným řešením pro eliminaci DDoS útoků nasazeného tzv. out-of-band je možné tento útok efektivně automaticky zablokovat. Flowmon DDoS Defender je možné nasadit v řádu minut díky univerzální architektuře a rozsáhlým možnostem integrace s aktivními prvky.



UNIVERZÁLNÍ NASAZENÍ

Flowmon DDoS Defender je možné nasadit v heterogenním prostředí se sběrem běžných flow statistik z aktivních prvků v různých formátech a/nebo sběrem velmi přesných flow statistik získávaných prostřednictvím Flowmon sond. Díky robustní a univerzální architektuře je možné nasadit DDoS Defender samostatně, v kombinaci se specializovaným out-of-band řešením pro eliminaci DDoS útoků nebo službou Scrubbing centra. Integrace s aktivními prvky je možná metodami PBR (Policy Based Routing) nebo BGP (Border Gateway Protocol), případně je možné využít mechanismu RTBH (Remotelly Triggered Black Hole) pro jednoduchou eliminaci útoku, nebo BGP Flowspec pro přesnější eliminaci útoku.

PŘÍNOSY A VÝHODY

- **Detekce útoků typu DoS a DDoS v reálném čase**
- **Významné zrychlení reakční doby na útok**
- **Dynamické baselinování objemů a charakteristik provozu**
- **Vizualizace charakteristických znaků útoku**
- **Notifikace prostřednictvím e-mailu, syslogu, SNMP trap**
- **Podpora pro standardní metody změny směrování provozu (PBR, BGP, RTBH)**
- **Pokročilé možnosti okamžité reakce (BGP Flowspec, spuštění skriptu, mitigace)**
- **Nezávislá konfigurace ochrany pro různé zákazníky, služby, segmenty sítě, ...**
- **Plugin pro řešení Flowmon, jednoduchá instalace a zhodnocení stávajících investic**

POKROČILÉ METODY DETEKCE DDOS ÚTOKŮ

Flowmon DDoS Defender sleduje objemové charakteristiky provozu pro chráněnou infrastrukturu (definované profily) a reaguje na zvýšení objemu provozu na základě definovaných pravidel. Pro definici profilu je možné využít IP adresní rozsahy, služby definované pomocí portů a protokolů, čísla VLAN, MPLS značky apod. K nastavení pravidel detekce útoků slouží kombinace statického pravidla a procentuální odchylky od dynamicky vytvořené a kontinuálně aktualizované baseline. Na základě detekovaného DDoS útoku je možné provést následující akce:

- **Alert (e-mail, syslog, SNMP trap)**
- **Změna směrování provozu (PBR, BGP, RTBH)**
- **Spuštění uživatelsky definovaného skriptu**
- **Eliminace útoku použitím BGP Flowspec, ve spolupráci se Scrubbing centrem nebo specializovaným řešením nasazeným tzv. out-of-band**

JAK ZÍSKAT PRODUKTY FLOWMON?

Obraťte se na svého systémového integrátora či přímo na nás. Rádi Vám řešení předvedeme, provedeme analýzu či navrhneme projekt monitorování Vaší sítě.

www.flowmon.com

Flowmon Networks

Flowmon Networks, a. s.
U Vodárny 2965/2
616 00 Brno

+420 511 205 250
info@flowmon.com
www.flowmon.com