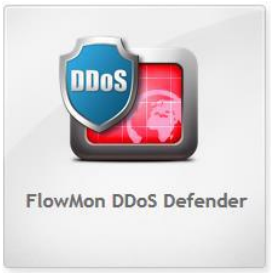
FlowMon DDoS Defender

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 řešení 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. Samplování při generování flow statistik rovněž nepředstavuje žádný problém nebo omezení.



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. Spuštění předem připraveného skriptu umožňuje reagovat na útoky i v prostředí, kde není možné využít standardní metody pro změnu směrování provozu nebo notifikace útoku.

Přínosy a výhody

- Detekce útoků typu DoS a DDoS v reálném čase
- Významné zrychlení reakční doby na útok
- Dynamické baselineování objemů a charakteristik provozu
- Získání charakteristických znaků útoku a prezentace uživateli
- Notifikace prostřednictvím e-mailu, syslogu, SNMP trap
- Pokročilé možnosti okamžité reakce (spuštění skriptu, mitigace)
- Podpora pro standardní metody změny směrování provozu – PBR, BGP, RTBH
- Nezávislá konfigurace ochrany různé zákazníky, služby, segmenty sítě, …
- Plug-in pro řešení FlowMon, jednoduchá instalace a zhodnocení stávajících investic
- Postačuje základní kvalita flow dat z běžných aktivních prvků, NetFlow v5/v9, IPFIX, jFlow, NetStream, sFlow, samplované i nesamplované statistiky

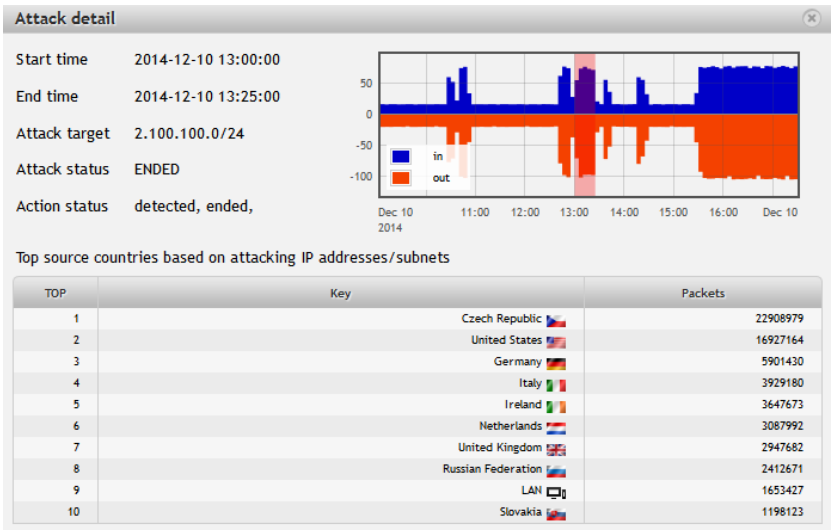
Pokročilé metody detekce volumetrických DDoS útoků

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 (mitigace) ve spolupráci se Scrubbing centrem nebo specializovaným řešením out-of-band

Pro všechny detekované útoky typu DDoS zobrazuje FlowMon DDoS Defender informace o objemech normálního provozu a velikosti útoku, časové značky, aktuální stav útoku a pokročilou charakteristiku útoku, která zahrnuje:

- Top 10 cílových IP adres
- Top 10 zdrojových autonomních systémů
- Top 10 síťových segmentů s maskami /8 a /16
- Top 10 L4 protokolů (TCP, UDP, ICMP, atd.)
- Top 10 zdrojových zemí (dle geolokace IP adres)
- Top 10 rozhraní směrovačů (zdrojů dat) – IP adresa a číslo rozhraní



TOP	Key	Packets
1	Czech Republic	22908979
2	United States	16927164
3	Germany	5901430
4	Italy	3929180
5	Ireland	3647673
6	Netherlands	3087992
7	United Kingdom	2947682
8	Russian Federation	2412671
9	LAN	1653427
10	Slovakia	1198123