Flowmon Networks

Driving Network Visibility

Specifikace modulu Flowmon DDoS Defender

platné od 1.5.2017

Flowmon DDoS Defender	DDoS Defender 1 FC-DDOS-1	DDoS Defender 4 FC-DDOS-4	DDoS Defender 10 FC-DDOS-10	DDoS Defender 40 FC-DDOS-40	DDoS Defender 100 FC-DDOS-100	DDoS Defender 400 FC-DDOS-400	DDoS Defender 1000 FC-DDOS-1000
Propustnost (Gb/s)	1	4	10	40	100	400	1000
Doporučený kolektor	1TB+	1TB+	3TB+	3TB+	12TB+	12TB+	SSD
Přesměrování provozu	PBR, BGP	PBR, BGP	PBR, BGP	PBR, BGP	PBR, BGP	PBR, BGP	PBG, BGP
Mitigace útoků	RTBH, BGP Flowspec	RTBH, BGP Flowspec	RTBH, BGP Flowspec	RTBH, BGP Flowspec	RTBH, BGP Flowspec	RTBH, BGP Flowspec	RTBH, BGP Flowspec
Integrace s mitigačními zařízeními třetích stran	ANO	ANO	ANO	ANO	ANO	ANO	ANO

Detekce útoků je prováděna pro každý uživatelem definovaný chráněný segment (části sítě, sítě zákazníků). Pro detekci DDoS útoků Flowmon DDoS Defender používá baseline metody (manuální a adaptivní práh) a statické (in/out ratio) metody. Dále je možné definovat úroveň minimálního provozu, jejímž překročením se buď vždy detekuje útok, nebo se začne vyhodnocovat síťový provoz podle definované baseline či statické metody.

Rychlost detekce – Flowmon DDoS Defender zpracovává 30-ti sekundové intervaly flow dat a tím umožňuje detekci a reakci na útok v téměř reálném čase (v intervalu pod 30 sekund až maximálně 60 sekund). Skutečná rychlost detekce je závislá na charakteristice útoku a nastavení exportérů (nastavení timeoutů pro export flow dat).

Propustnost představuje maximální velikost legitimního provozu v Gb/s pro veškeré chráněné profily, tj. součet všech baseline. Do licencované propustnosti se nezapočítává velikost a provoz DDoS útoků.

Doporučené kolektory – hardwarové Flowmon kolektory se liší v počtu procesorů a velikosti operační paměti. Flowmon DDoS Defender může být nasazen i na virtuálních kolektorech, kterým je alokováno dostatečné množství prostředků odpovídající specifikaci hardwarového kolektoru. Pro více informací viz specifikační dokument Flowmon kolektorů.

Přesměrování provozu je možné provést pomocí PBR (Policy Based Routing, podporovaní výrobci: Alcatel-Lucent, Cisco, Juniper) nebo BGP (Border Gateway Protocol). Flowmon DDoS Defender podporuje externí i interní BGP (eBGP & iBGP) a BGP Flowspec.

Mitigace útoků může být provedena pomocí RTBH (Remotely Triggered Black Hole) a BGP Flowspec.

Multi-tenance je podporována.

Flowmon Networks a.s.
info@flowmon.com

Specifikace modulu Flowmon DDoS Defender

platné od 1.5.2017

RTBH (Remotely Triggered Black Hole) techniku pro mitigaci útoků je možné využít pomocí BGP nebo uživatelsky definovaných ACL (Access Control List) na podporovaných routerech (Alcatel-Lucent, Cisco, Juniper). Flowmon DDoS Defender při detekci útoku posílá ACL příkazy routerům s instrukcemi pro zahození nebo přesměrování nežádoucího provozu do černé díry.

BGP Flowspec je možné použít pro mitigaci DDoS útoků na routerech s podporou BGP Flowspec. Flowmon DDoS Defender stanoví dynamickou signaturu útoku a podle toho navrhne vhodné Flowspec pravidlo. Pro injektovaná Flowspec pravidla je možné použít následující parametry: cílová a zdrojová síť, cílový a zdrojový port, L4 protokol. Flowmon DDoS Defender umožňuje nastavit různé Flowspec akce pro každé Flowspec pravidlo. Dostupné akce jsou například: přijmout (accept), zahodit (discard), omezit (rate-limit) nebo přesměrovat (redirect). Pro více informaci o BGP Flowspec viz uživatelskou příručku modulu Flowmon DDoS Defender

Integrace s mitigačními zařízeními třetích stran – Flowmon DDoS Defender nativně podporuje Radware DefensePro a Radware Vision, F5 BIG-IP nebo VIPRION a A10 Thunder TPS zařízení pro mitigaci DDoS útoků.

Alerty je možné zaslat pomocí emailu, syslog zprávy nebo SNMP trap. Dále je možné spustit uživatelem definovaný skript.

Flowmon Networks a.s.
info@flowmon.com