# Flowmon & FlowGuard
# Komplexní ochrana před DDoS útoky pro podnikové sítě, ISP a datová centra

Ve světě závislém na informačních technologiích a dostupnosti aplikací představují DDoS útoky jednu z nejnebezpečnějších forem kyberteroristických útoků. Útok na libovolný cíl si může totiž objednat prakticky kdokoliv, ať již je to konkurenční firma či nespokojený zákazník a cena za provedení útoku se pohybuje již od řádu několika stokorun. Nelze se tedy divit, že počet i intenzita DDoS útoků neustále stoupá. Pokud poskytujete datovou konektivitu, provozujete podnikovou síť nebo datové centrum, je vaší základní potřebou zajistit neustálou dostupnost kriticky důležité síťové infrastruktury.

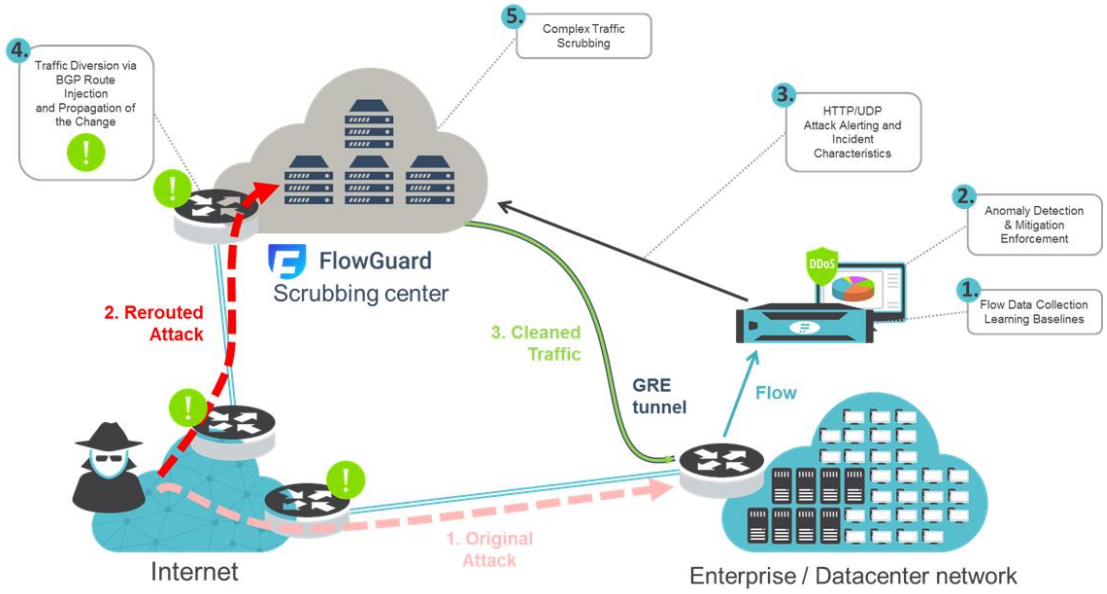
Základním předpokladem pro obranu před DDoS útoky je zvýšení odolnosti vaší síťové infrastruktury nasazením systémů pro jejich rychlou detekci a zastavení. K tomu slouží pokročilá řešení využívající permanentní analýzu statistik o síťovém provozu na bázi datových toků (NetFlow/IPFIX), a to zároveň prvky umělé inteligence, která se analýzou síťového provozu učí tyto útoky rozpoznávat. Ve spolupráci s cloudovým scrubbing centrem je pak zajištěna jejich eliminace.

## Společné řešení pro rychlou detekci a precizní vyčištění provozu

Jedinečná integrace mezi řešením Flowmon a cloudové služby čištění provozu FlowGuard představuje efektivní řešení ochrany před DDoS útoky pro podnikové sítě a datová centra. Řešení sestává z následujících komponent:

- **Flowmon kolektor** opatřený softwarovým modulem **Flowmon DDoS Defender** je nasazený v síti zákazníka (ve formě fyzického či virtuálního zařízení), kde sbírá a analyzuje statistiky o síťovém provozu ve formě datových toků (IPFIX/NetFlow). S využitím baseliningu a strojového učení sleduje charakteristiku provozu pro jednotlivé chráněné segmenty sítě, pro něž vytváří adaptivní prahy indikující útok. V případě detekovaného útoku automaticky informuje službu cloudovou službu FlowGuard poskytovanou společností ComSource. FlowGuard následně přesměruje provoz pomocí BGP (Border Gateway Protocol).

- **FlowGuard** představuje cloudovou službu, která dokáže eliminovat masivní volumetrické DDoS útoky tím, že je rozloží pomocí sítě svých bezpečnostních center vybudovaných na principu distribuované architektury. Vzhledem k neustálé aktualizaci znalostních databází jsou je služba FlowGuard schopna reagovat prakticky na libovolný DDoS útok s tím, že do síťové infrastruktury chráněného subjektu propustí pouze legitimní provoz. O přesměrování útoku do služby FlowGuard je uživatel okamžitě informován a průběh čištění datového toku může sledovat prostřednictvím webového uživatelského rozhraní.




*Obrázek 1: Architektura společného řešení*

Společné řešení v případě DDoS útoku proaktivně zabrání zahlcení datových linek tím, že závadný provoz téměř okamžitě přesměruje do cloudové služby, která zajistí jeho precizní vyčištění. Nedojde tak k výpadku dostupnosti vašich služeb nebo konektivity.

Společné řešení Flowmon a FlowGuard cloud pro mitigaci DDoS útoků vám přináší:

- Ochranu i před těmi nejsilnějšími volumetrickými DDoS útoky
- Plně automatizované propojení systému detekce a cloudové mitigace útoků
- Kompletní sadu nástrojů pro měření výkonností sítě
- Monitorovací aplikaci poskytující neustálý přehled o stavu čištění síťového provozu
- Jednoduché ovládání nevyžadující hluboké odborné znalosti
- Podporu FlowGuard v nepřetržitém režimu 24/7, a to v českém jazyce

**ComSource s.r.o.**
Nad Vršovskou horou 1423/10
101 00 Praha 10
Česká republika
www.comsource.cz

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