Flowmon & FlowGuard
Comprehensive protection against DDoS attacks for corporate networks, ISPs and data centers

In a world dependent on information technology with the ready availability of applications, DDoS attacks are one of the most dangerous forms of cyber-terrorism attacks. An attack on any target can be ordered by virtually anyone, no matter it is a competitive business or unsatisfied customer, and the price for conducting an attack varies from a few tens of dollars. It is no wonder then that the number and intensity of DDoS attacks is constantly rising. If you provide data connectivity, run a corporate network or data center, it is a fundamental need to ensure the constant availability of crucial network infrastructure.

A basic condition for defense against DDoS attacks is to increase the resilience of your network infrastructure by deploying systems for the rapid detection and stopping of DDoS attacks. To do this, advanced solutions permanently analyze statistics about network traffic based on data flows (NetFlow/IPFIX), and at the same time incorporate artificial intelligence to learn how to recognize these attacks through analyzing network traffic. In cooperation with a cloud scrubbing center, elimination of DDoS attacks is guaranteed.

A joint solution for fast detection and precise cleanup of traffic

The unique integration between the Flowmon solution and FlowGuard cloud service of cleaning traffic is an effective solution to protect against DDoS attacks for enterprise networks and data centers. The solution comprises the following components:

- **Flowmon collector,** equipped with the **Flowmon DDoS Defender** software module, is deployed on a customer's network (in the form of a physical or virtual device) to collect and analyze IPFIX / NetFlow network traffic statistics. Using baselining and machine learning, it monitors traffic characteristics for each protected network segment, for which it creates adaptive thresholds indicating an attack. With an attack detected, the FlowGuard cloud service is automatically provided by ComSource. FlowGuard then redirects traffic using BGP (Border Gateway Protocol).
- **FlowGuard** is a cloud service that can eliminate massive volumetric DDoS attacks by spreading them through a network of security centers built on the principle of distributed architecture. Due to the constant updating of knowledge databases, FlowGuard can respond practically to any DDoS attack by allowing only the legitimate traffic to the network infrastructure of the protected entity. The user is immediately informed about the FlowGuard attack redirection, and the flow of data can be tracked through the web user interface.

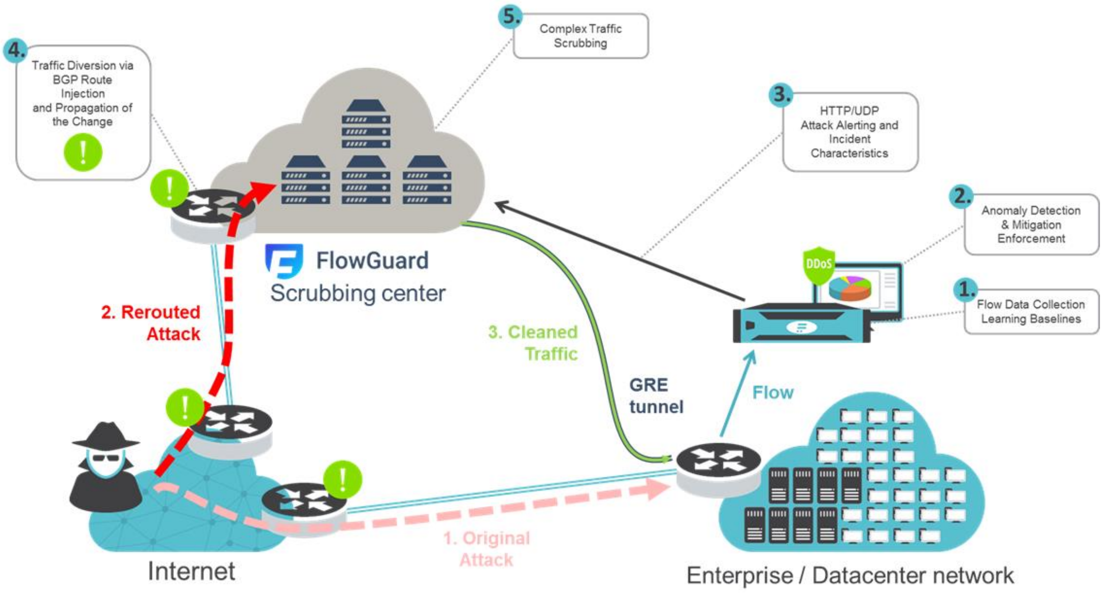
4. Traffic Diversion via BGP Route Injection and Propagation of the Change
5. Complex Traffic Scrubbing
3. HTTP/UDP Attack Alerting and Incident Characteristics
2. Anomaly Detection & Mitigation Enforcement
1. Flow Data Collection Learning Baselines
FlowGuard
Scrubbing center
2. Rerouted Attack
3. Cleaned Traffic
GRE tunnel
Flow
DDoS
Internet
1. Original Attack
Enterprise / Datacenter network

Diagram 1: Architecture of the joint solution

The common solution for DDoS attack proactively prevents congestion of data links by shifting the malicious traffic almost instantly into a cloud service that ensures its precise cleanup. There will be no loss of availability of your services or connectivity.

The joint Flowmon and FlowGuard cloud solution to mitigate DDoS attacks brings you:

- Protection even against the most powerful volumetric DDoS attacks
- Fully automated link detection and cloud mitigation from attacks
- A complete set of tools for measuring network performance
- A monitoring application that provides a consistent overview of the state of network traffic cleaning
- Simple operation requiring no deep expertise
- FlowGuard non-stop support 24/7

ComSource s.r.o.
Nad Vršovskou horou 1423/10
101 00 Praha 10
Czech Republic
www.comsource.cz

Flowmon Networks a.s.
Sochorova 3232/34
616 00 Brno
Czech Republic
www.flowmon.com