Содержание

General Description

VAS Experts offers a solution to deal with DDoS attacks targeting telecom operators and their infrastructure, which lead to the operator's inability to serve its subscribers. Consequently, this results in mass subscriber churn, financial losses, and reputational damage.

VAS Experts offers two options for protection against DDoS attacks:

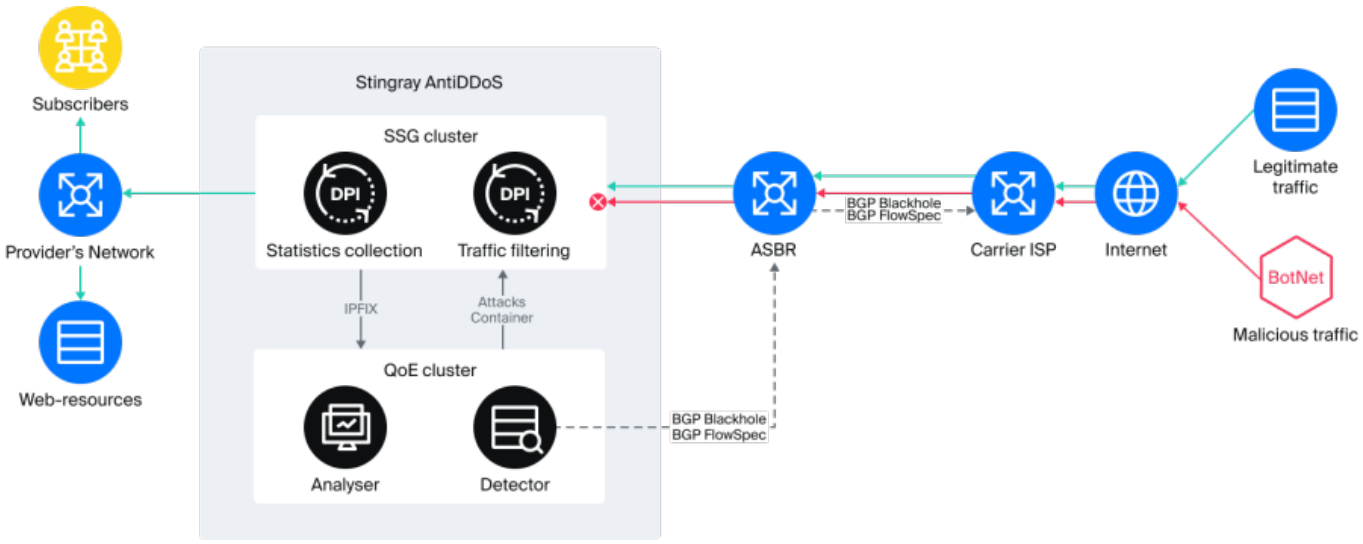
1. Using only SSG with the auto-protection function against SYN Flood, UDP Flood, and HTTP Flood. Requires SSG with the DDoS Auto-Protection option (option **ddos**).
2. Using a combination of SSG and QoE to detect and mitigate all types of DDoS attacks with complete inbound traffic blocking (**blackhole**) and scrubbing on SSG. Requires SSG with the option for Collection and export of protocol and direction statistics in IPFIX format (option **ipfix**) and QoE with the option for Traffic detection and scrubbing (**blackhole and flowspec**) against BotNet and DDoS attacks (option **antiddos**). For scrubbing, SSG version BASE is required.

Most Common Forms of Attacks on Telecom Operators

1. Inbound Channel Overflow
    - Amplification attacks (DNS, NTP, UDP flood, and others)
      Protection: blackholing attacked addresses or applying flowspec on the uplink channel; other protection methods are ineffective.
    - BotNet attacks — each bot generates relatively small traffic resembling legitimate traffic, but the aggregate traffic exceeds the capacity of the operator's ingress channels; source address spoofing is not performed (see also item 2)
      Complication: the target IP for the attack often involves not one address, but up to a thousand addresses
      Protection: blackholing attacked addresses, flowspec on the uplink channel (for certain traffic types), creating a list of BotNet network addresses and blocking them on SSG (for certain traffic types)
2. High PPS Attack:
    - Flood, SYN flood, usually with source IP spoofing
      Protection: redirecting traffic to SSG for filtering or blackholing attacked addresses
3. Compromise of Operator's Network Elements: detected by the presence of SSH and other sessions from the operator's service addresses, which are pre-configured and the addresses are not in the whitelist
   Protection: detecting such sessions and blocking them by external address

AntiDDoS Solution Architecture Based on SSG and QoE

FastMitigator is an intelligent network attack protection system. It is a distributed traffic analysis module that provides real-time detection and blocking of a wide range of cyber threats.



Operation Principle

1. Deep Traffic Analysis (DPI) and Statistics Export
    - All traffic passes through DPI (SSG), operating in-line or on a traffic mirror.
    - Full NetFlow in IPFIX format is sent to the QoE system for detailed analysis.
2. Statistics Analysis and Baseline Formation
    - The analyzer processes Full NetFlow and creates a "normal profile" — a baseline of "healthy" traffic (without attacks and botnet activity).
    - The profile is stored in QoE's distributed tables for fast access.
3. Anomaly Detection
    - A detector based on neural networks and machine learning algorithms identifies deviations, classifies threats, and determines their sources.
4. Traffic Scrubbing Based on Dynamic Rules
    - Upon attack detection, QoE forms an Attacks container containing:
        - IP addresses of attacking hosts
        - Ports used for attacks
    - The container is transmitted to the SSG DPI, where special Attacks protocols (or protocol groups) are created for each threat type. It is recommended to use a dedicated SSG in in-line mode, which constantly passes all traffic or receives only a portion of traffic for scrubbing.
    - Protection profiles are pre-configured on DPI (e.g., via "18. Session Policing"), where for Attack protocols, the following actions are applied if the operator's channel capacity is not exhausted:
        - Drop (complete blocking)
        - Policing (bandwidth limiting)
    - The Attacks container is updated in real-time: if an attack stops, IP hosts are removed from the list.
5. Protection via BGP using Blackhole and Flowspec
    - In cases where the operator's channel capacity is exhausted, the Attacks container can be passed to a special script that automatically adds subscriber IPs to a blackhole, ensuring the maximum level of protection for the operator's infrastructure. Inbound traffic to these subscribers is dropped at the Uplink channel.
    - To allow subscribers on blocked public IP addresses to continue accessing the internet, it is necessary to temporarily change their IP address — enable the CG-NAT service on SSG (use a previously announced public address pool). Thus, there is no need to change the IP address on the subscriber's device during the attack; the subscriber will temporarily

access the internet via a different public IP address, and when the attack ends, the original IP address is restored — disable the CG-NAT service on SSG.

Advantages of FastMitigator

1. Distributed architecture — high fault tolerance
2. Adaptive protection — automatic rule updates
3. Deep analytics — neural network algorithms + DPI
4. Flexibility — support for various blocking scenarios

Organic AntiDDoS System

The evolution of the DDoS protection solution aims to filter malicious traffic even before it enters the internet. Deploying SSG AntiDDoS complexes at multiple telecom operators will allow stopping BotNet traffic inside the operator's network. Centralized management via VAS Cloud will enable lightning-fast response to any attacks and leave the transport channels between operators, IXs, and Data Centers untouched. If an attack is detected on any resource protected by SSG AntiDDoS, it is possible to transmit filtering parameters to the operator from which the illegitimate traffic originates.