Содержание

Description of tools and architecture

VAS Experts offers a solution to protect telecom operators and their infrastructure from DDoS attacks that may prevent the operator from serving subscribers. As a result, this can lead to massive subscriber churn, financial losses, and reputational damage.

VAS Experts offers several DDoS protection options:

1. Using only SSG with the built-in automatic protection against SYN Flood, UDP Flood, and HTTP Flood. Requires SSG with the DDoS auto-protection option (**ddos**).
2. Using a combination of SSG and QoE to detect any type of DDoS attack with the ability to fully block incoming traffic (**blackhole**) and perform traffic scrubbing on SSG. Requires SSG with the IPFIX statistics collection and export option (**ipfix**) and QoE with the BotNet and DDoS detection and mitigation option (**blackhole and flowspec**) (**antiddos**). For traffic scrubbing, existing SSG versions can be used (available in: BASE, BRAS with **mark** and **channels** options, COMPLETE). A dedicated SSG BASE server can also be deployed to process part of the traffic.

Licensing of the AntiDDoS option within SSG and QoE is described here.

Requirements:

- Latest versions of QoE and GUI. Any QoE license is suitable; AntiDDoS is purchased as a separate option.
- SSG licenses BASE / COMPLETE / BRAS with additional options mark and channels
- QoE must be installed on a separate server or VM, **NOT on the SSG server**
- 8.4 GB of storage is required per 1 Gbps of peak incoming traffic for statistics retention

Most common types of attacks on telecom operators

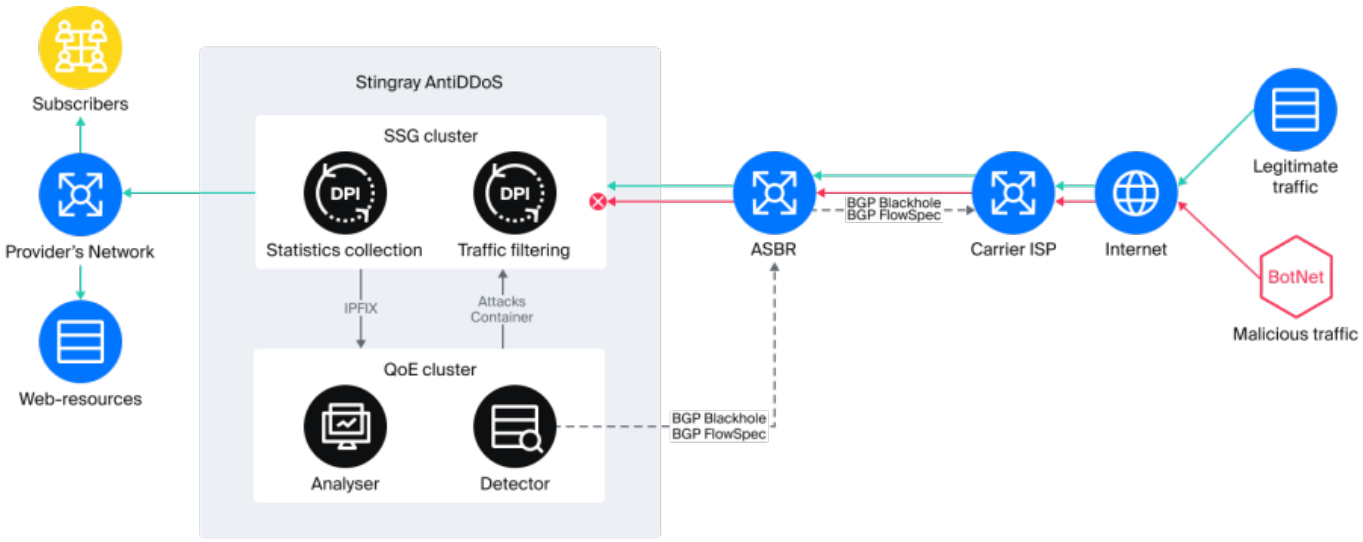
1. Saturation of inbound links
   - Amplification attacks (DNS, NTP, UDP flood, and others)
     Protection: blackhole for attacked addresses or applying flowspec on the uplink channel; other protection methods are ineffective.
   - BotNet attacks — each bot generates relatively small traffic similar to legitimate traffic, but in total the traffic exceeds the capacity of the operator's inbound links; source IP spoofing is not used (see also section 2)
     Complication: the attack target is often not a single IP address but up to thousands of addresses
     Protection: blackhole for attacked addresses, flowspec on the uplink channel (for certain traffic types), creation of a BotNet address list and blocking them on SSG (for certain traffic types)
2. High PPS attacks:
   - Flood, SYN flood, usually with source IP spoofing
     Protection: use source IP anti-spoofing mechanisms: IP source guard and Traffic Filtering.

Enable traffic redirection to SSG for filtering or activate blackhole for attacked addresses.

3. Compromise of operator network elements: detected by the presence of SSH and other sessions from operator service addresses that are preconfigured and not included in the whitelist
   Protection: detection of such sessions and blocking 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 ensures real-time detection and mitigation of a wide range of cyber threats.



Operating principle

1. Deep traffic inspection (DPI) and statistics export
   - All traffic passes through DPI (SSG), operating in-line or via traffic mirroring.
   - Full NetFlow in IPFIX format is sent to the QoE system for detailed analysis.
2. Statistics analysis and baseline creation
   - The analyzer processes Full NetFlow and creates a “normal profile” — a baseline of “healthy” traffic (without attacks or botnet activity).
   - The profile is stored in distributed QoE 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 using dynamic rules
   - When an attack is detected, an Attacks container is generated in QoE containing:
     - IP addresses of attacking hosts
     - Ports used for attacks
   - The container is transmitted to 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 that continuously passes all traffic or receives only part of the traffic for scrubbing.
   - Protection profiles are preconfigured on DPI (for example, via “18. Session policing”), where for Attack protocols the following actions are applied if channel capacity is not exhausted:
     - Drop (complete blocking)

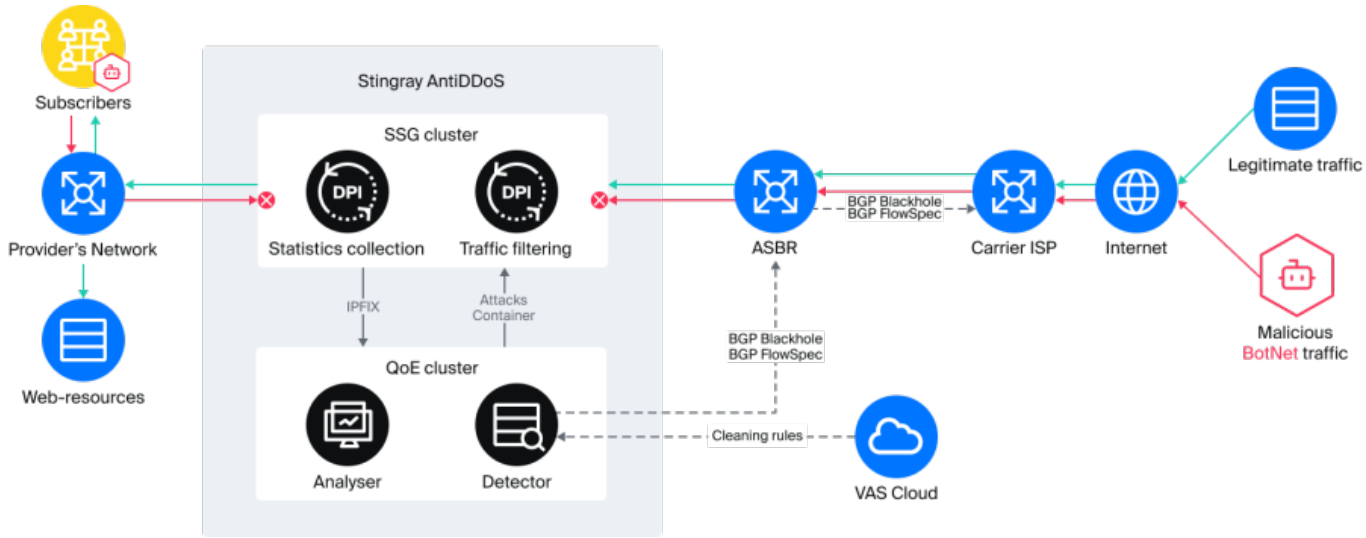
        - Policing (bandwidth limitation)
    - The Attacks container is updated in real time: if the attack stops, host IPs are removed from the list.
5. Protection via BGP using blackhole and flowspec
    - If the operator’s channel capacity is exhausted, the Attacks container can be passed to a special script that automatically adds subscriber IPs to blackhole, ensuring maximum infrastructure protection. Incoming traffic to these subscribers is dropped at the uplink channel.
    - To ensure subscribers with blocked public IP addresses continue to access the Internet, their IP address must be temporarily substituted — enable the CG-NAT service on SSG (using a previously announced public IP pool). This eliminates the need to change the IP address on the subscriber’s device during the attack. The subscriber temporarily receives Internet access via another public IP address, and after the attack ends, the original IP address is restored — disable the CG-NAT service on SSG.

FastMitigator advantages

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

Organic AntiDDoS System

Further development of the DDoS protection solution is aimed at scrubbing traffic before it reaches the Internet network. Deployment of SSG AntiDDoS systems across multiple telecom operators allows BotNet traffic to be stopped within the operator’s network. Centralized management via VAS Cloud enables rapid response to any attack while keeping even transport links between operators, IX, and data centers unaffected. If an attack is detected on any resource protected by SSG, scrubbing parameters can be transmitted to the operator from which the illegitimate traffic originates.



Solution usage scenarios