Содержание

Description of Tools and Architecture

VAS Experts offers a solution to combat DDoS attacks on telecom operators and their infrastructure, which can result in the operator being unable to serve its subscribers. Consequences include mass subscriber churn, financial and reputational losses.

VAS Experts provides several options for DDoS protection:

1. Using SSG only with auto-protection against SYN Flood, UDP Flood, and HTTP Flood. Requires SSG with the Anti-DDoS Auto-protection option (**ddos**). **More about configuring DDoS protection using SSG DPI**
2. Using a combination of SSG and QoE to detect all types of DDoS attacks with the ability to fully block incoming traffic (**blackhole**) and clean it on SSG. Requires SSG with the option to collect and export protocol and direction statistics in IPFIX format (**ipfix**) and QoE with the option Traffic detection and cleaning (**blackhole and flowspec**) from BotNet and DDoS attacks (**antiddos**). For traffic cleaning, existing SSGs can be used (available in versions: BASE, BNG with mark and channels options, COMPLETE), or a dedicated SSG BASE server can be deployed to handle part of the traffic. **More about configuring DDoS and BotNet detection based on QoE**

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

Requirements:

- QoE and GUI latest version. QoE license — any, AntiDDoS purchased as a separate option
- SSG license BASE / COMPLETE / BNG with additional options mark and channels
- QoE installed on a separate server or VM, **NOT on the SSG server**
- For 1Gb/s peak incoming traffic, 8.4 GB is required for statistics storage

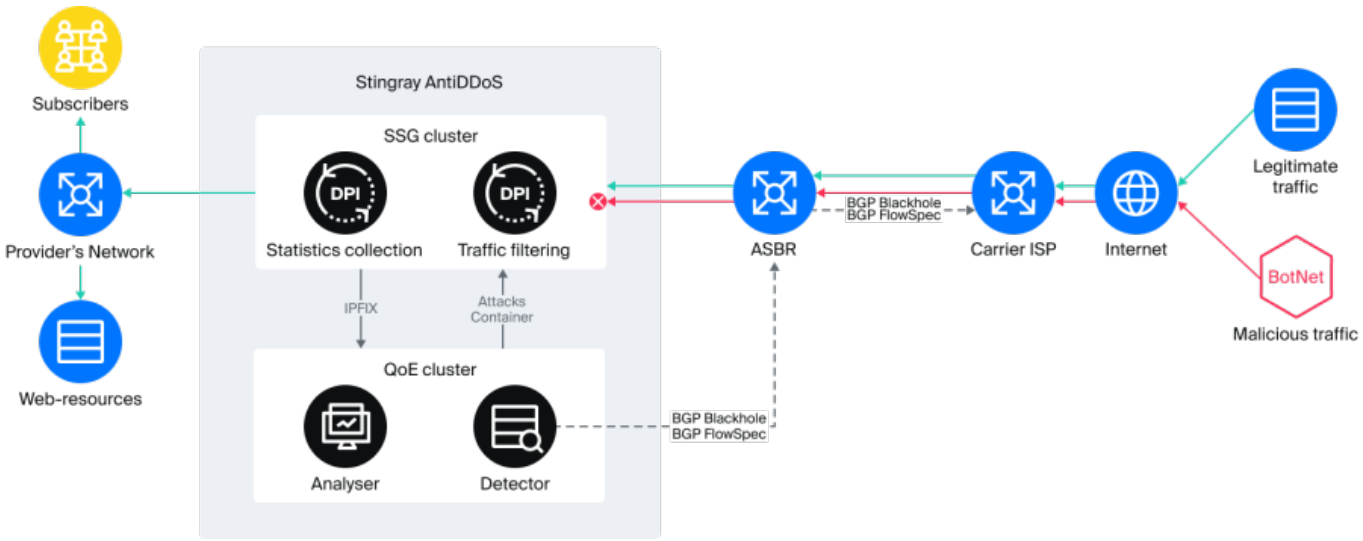
Most Common Forms of Attacks on Telecom Operators

1. Input channel saturation
   - Amplification attacks (DNS, NTP, UDP flood, etc.)
     Protection: blackhole the targeted addresses or use flowspec on the uplink channel; other protection methods are ineffective.
   - BotNet attacks — each bot generates relatively small traffic similar to legitimate traffic, but cumulatively the traffic exceeds operator input channel capacity; source address spoofing is not performed (see also item 2)
     Challenge: often up to a thousand IPs are targeted, not just one
     Protection: blackhole targeted addresses, flowspec on uplink channel (for some traffic types), create BotNet address list and block them on SSG (for some traffic types)
2. High PPS attack:
   - Flood, SYN flood, usually with source IP spoofing
     Protection: use source IP spoofing protection mechanisms: IP source guard and Traffic Filtering. Redirect traffic to SSG for filtering or enable blackhole for targeted addresses

3. Compromise of operator network elements: detected by the presence of SSH and other sessions from operator service addresses, which are pre-configured and not in the whitelist
   Protection: detect such sessions and block by external address

AntiDDoS Solution Architecture Based on SSG and QoE

FastMitigator — an intelligent network attack protection system. It is a distributed traffic analysis module providing real-time detection and mitigation 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 QoE for detailed analysis.
2. Statistical analysis and baseline creation
   - Analyzer processes Full NetFlow and creates a "normal profile" — a baseline of "healthy" traffic (without attacks or BotNet activity).
   - Profile is stored in distributed QoE tables for fast access.
3. Anomaly detection
   - Detector based on neural networks and machine learning algorithms identifies deviations, classifies threats, and determines their sources.
4. Traffic cleaning based on dynamic rules
   - When an attack is detected, QoE creates an Attacks container containing:
     - IP addresses of attacking hosts
     - Ports used for attacks
   - Container is sent to SSG DPI, where special Attack 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 part of it for cleaning.
   - DPI pre-configures protection profiles (e.g., via "18. Session Policing") where Attack protocols are applied if operator channel capacity is not exhausted:
     - Drop (full block)
     - Policing (bandwidth limitation)
   - Attacks container is updated in real-time: if the attack stops, IP hosts are removed from the list.

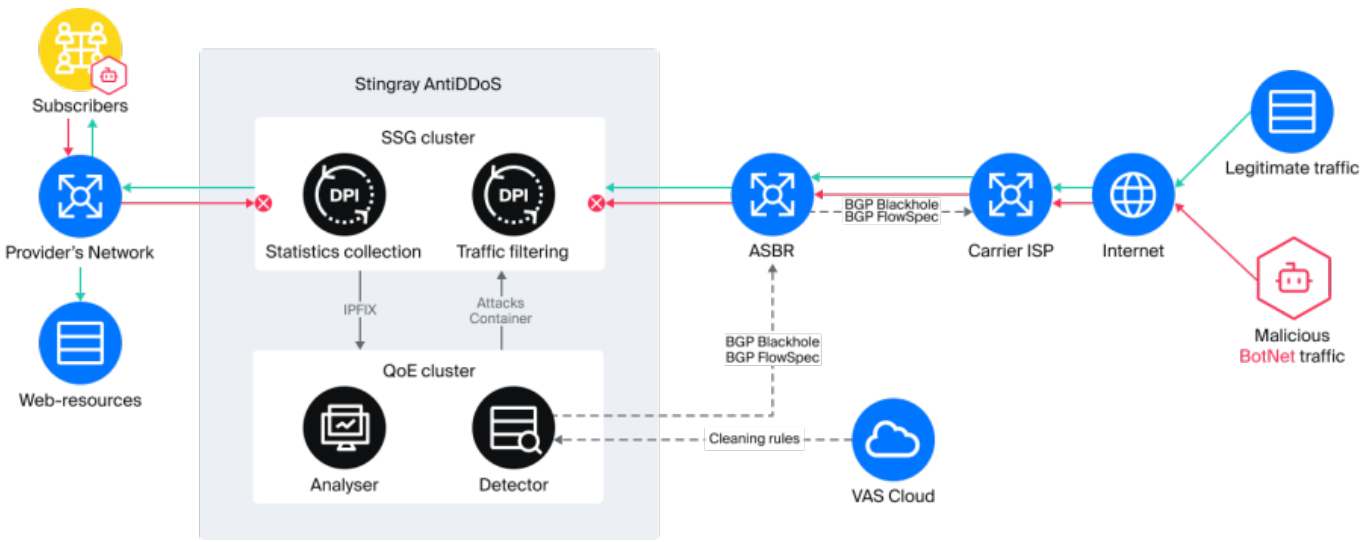
5. Protection via BGP using blackhole and flowspec
    - If operator channel capacity is exhausted, Attacks container can be sent to a special script that automatically adds subscriber IPs to blackhole, ensuring maximum infrastructure protection. Incoming traffic to these subscribers is dropped on the uplink channel.
    - To allow subscribers on blocked public IPs to access the internet, their IP can be temporarily replaced — enable CG-NAT on SSG (using the previously announced public IP pool). This avoids changing the subscriber device IP during the attack. Access is temporarily via a different public IP, and after the attack ends, the original IP is restored — disable CG-NAT 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 — supports different blocking scenarios

Organic AntiDDoS System

The development of DDoS protection aims to clean traffic before it reaches the internet. Deploying SSG AntiDDoS complexes across multiple operators will stop BotNet traffic inside the operator network. Centralized management via VAS Cloud allows lightning-fast reaction to any attacks while leaving transport channels between operators, IX, and data centers untouched. Upon detecting an attack on any resource with SSG, parameters for mitigation can be forwarded to the operator from which the illegitimate traffic originates.



Use cases of the solution