*Flowmon Networks and NBIP introduce a cost-effective, carrier-grade DDoS protection consisting of flow-based volumetric DDoS attack detection and on-demand cloud mitigation.*

## CHALLENGE

Distributed denial-of-service (DDoS) attacks have been a major threat for service providers and their customers during the last decade. Attacks have been continuously increasing year over year, and negatively affecting the entire service provider business. The principle of a DDoS attack is simple: a large number of geographically distributed bots generate requests to saturate the victim's resources. The attack is powered by consuming the network's processing capacity, thus interrupting network connectivity. As a result, both the target and the service provider's network infrastructure are impacted.

Many service providers have been unable to defend themselves against DDoS attacks, as the cost of deploying robust enterprise-class DDoS protection is too high. Launching an attack, on the other hand, is extremely cheap and easy, often offered as a service. These considerations result in a resigned approach when a DDoS attack strikes: an ISP usually just drops all traffic to the target, which effectively accomplishes the attacker's goal. Without functional DDoS protection, however, there are not many other options for the ISP to avoid collateral damage – a large DDoS attack floods the whole ISP's network, so all customers get affected even if only one site is under attack.

## FLOWMON & NAWAS SOLUTION

Fighting DDoS attacks in carrier-grade networks requires deep network visibility, fast traffic analysis, attack detection, and reliable attack mitigation. Network traffic statistics collected from routers or dedicated network probes make it possible to detect attacks and understand their characteristics to start successful mitigation. A cloud mitigation service with direct access to the most used autonomous systems ensures attack mitigation as close to the source of the attack as possible.

To use the described cloud mitigation, service providers in the WEMEA region can join the non-profit NaWas cloud-based mitigation service provided by NBIP. Flowmon Networks and NBIP have joined forces to bring cost-effective, high-performance, carrier-grade DDoS mitigation with centralized control. The solution combines flow-based DDoS attack detection with traffic redirection to the NaWas cloud for cleaning.

## BENEFITS

### Automation

*Cost-effective DDoS detection with automated on-demand cloud mitigation*

### NPMD tools

*Network Performance Monitoring and Diagnostics tools for IT operations, an out-of-the-box functionality of Flowmon solution available to all users*

### Security extensions

*Optional extension module for Network Behavior Analysis to reveal malicious activities in the network*

> ***“Flowmon solution not only allows us to improve our visibility into the network, it also makes it possible to rapidly deploy multiple defense strategies against DDoS attacks. Above that, it enables us to resolve security incidents from within our network. We appreciate the flexibility of the tooling and applaud the technical support.”***

**Tjebbe de Winter**

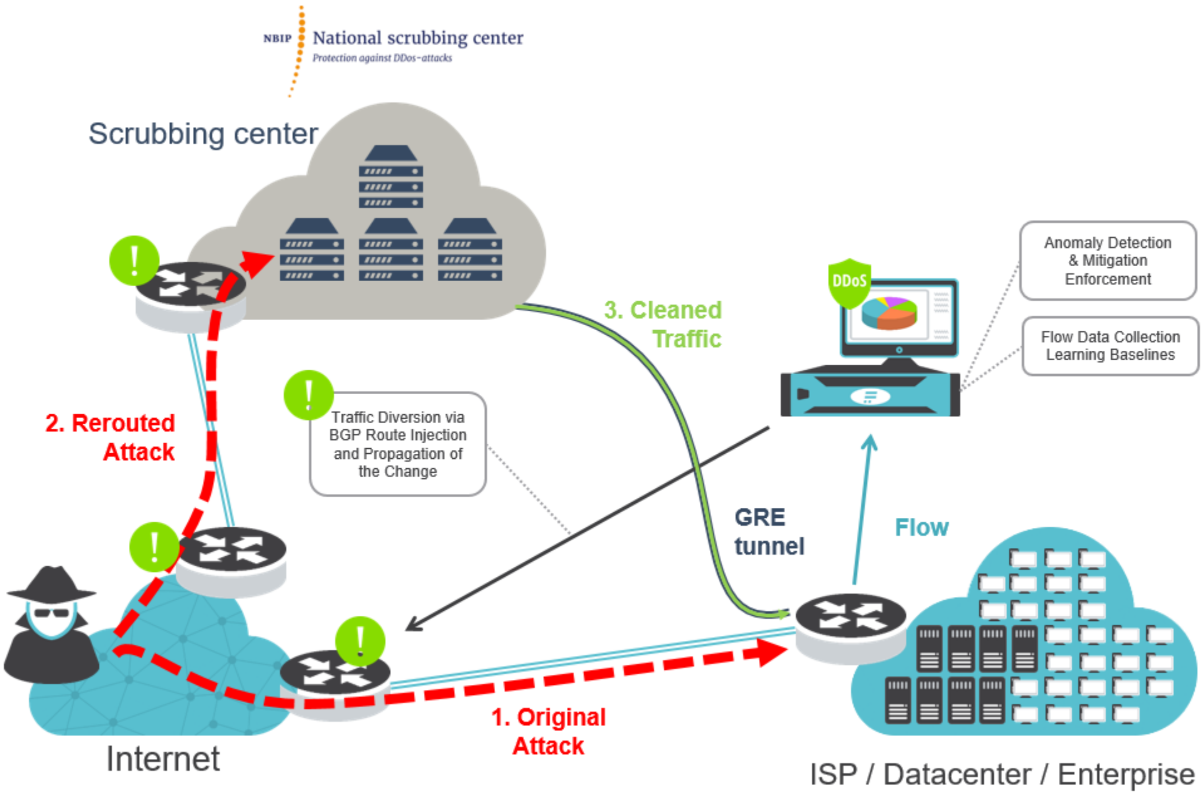
**Technical Director at Cyso, Flowmon & NBIP solution user**

## DEPLOYMENT

The integrated Flowmon & NaWas solution makes use of IP flow records from existing service provider infrastructure (routers, switches). There is no need to install a DDoS mitigation device at every peering link. Typically, only Flowmon Collector as a virtual or hardware appliance needs to be placed in the customer's network.

## DETECTION

Flowmon Collector equipped with the DDoS Defender module stores flow data from border routers, and continually analyzes volumetric characteristics of network traffic to create and maintain dynamic baselines. In case of an unexpected increase in network traffic, it performs traffic diversion via BGP injection or BGP Flowspec rule, and re-routes the attack traffic to NaWas to be cleaned.


NBIP National scrubbing center
Protection against DDos-attacks
Scrubbing center
2. Rerouted Attack
Traffic Diversion via BGP Route Injection and Propagation of the Change
3. Cleaned Traffic
DDoS
Anomaly Detection & Mitigation Enforcement
Flow Data Collection Learning Baselines
GRE tunnel
Flow
1. Original Attack
Internet
ISP / Datacenter / Enterprise

## MITIGATION

NaWas makes it possible for participating ISPs to redirect only the affected part of their targeted network (the /24 segment) to the Scrubbing Center, which means that the ISP's network is available immediately again, and the targeted site is cleaned very fast. The exact cleaning time depends on how the traffic is sent to NaWas. Flowmon DDoS Defender enables automatic BGP reroute of the attack to NaWas, so the anti-DDoS function takes effect within minutes. If needed, NaWas provides professional assistance by a NBIP engineer.

## BENEFITS

Apart from the traffic diversion options (PBR, BGP, RTBH), Flowmon DDoS Defender can perform other configurable actions that include alerting (e-mail, syslog, SNMP trap) and execution of scripts. Protected segments can be defined based on IP ranges, subnets or AS numbers, and different mitigation strategies applied to each of them. The attack log includes detailed attack characteristics such as top source 10 IP addresses, subnets, autonomy systems and countries, L4 protocols and interfaces.

## NBIP

The Dutch National Internet Providers Management Organisation (Nationale Beheersorganisatie Internet Providers, **NBIP**) provides supporting services to Internet providers. Among other things, it operates **NaWas**, the National Anti-DDoS Scrubbing Center, specialized in mitigating large volume DDoS attacks launched at ISPs and hosting providers. NaWas is an independent, non-profit and cooperative initiative that was launched in less than three months. It brought together rivalling companies to solve a problem that all faced: large scale botnet attacks resulting in serious downtime, angry customers and high mitigation costs. NaWas offers an on-demand DDoS protection to its participants.

www.nbip.nl/en/nawas

NBIP
PO Box 628
6710 Ede
Netherlands

## FLOWMON NETWORKS

Flowmon Networks enables businesses to manage and secure their computer networks confidently. Flowmon's unique monitoring technology and behavior analytics offer perfect network traffic visibility, which helps enhance network and application performance and deal with modern cyber threats. Flowmon's NetFlow/IPFIX network monitoring is high performing, scalable, and easy to use. The world's largest businesses, internet service providers, government entities and even small and midsize companies rely on Flowmon, making it one of the fastest growing companies in the industry.
The Flowmon solution is recognized by Gartner and recommended by Cisco, Check Point, and IBM.

www.flowmon.com

Flowmon Networks, a. s.
Sochorova 3232/34
616 00 Brno
Czech Republic