Flowmon + NBIP NaWas
Carrier-grade DDoS Protection

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

Benefits

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

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

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

▪ CHALLENGE ▪

Distributed denial-of-service (DDoS) attacks have been a major threat to service providers and their customers for the last decade. Attacks have been 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 consumes 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, even offered as a service. This is why the victims often meet DDoS attacks with resignation; an ISP usually just drops all traffic to the target, which effectively accomplishes the attacker's goal. Without functional DDoS protection, however, there are few other options for the ISP to avoid collateral damage – a large DDoS attack floods the ISP's whole network, so all customers get affected even if only one site is under attack.

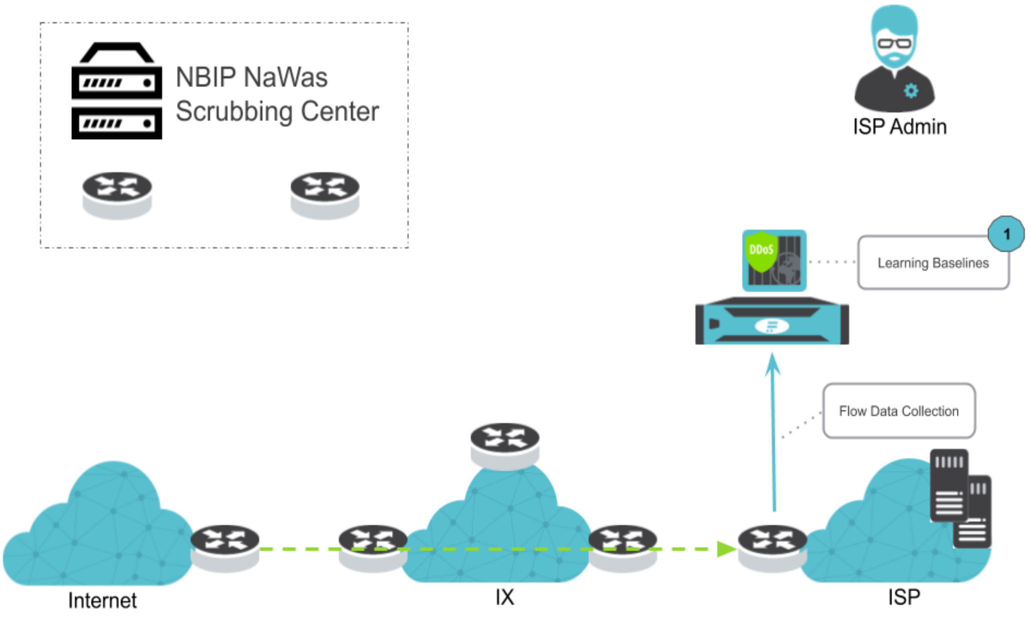
▪ FLOWMON & NAWAS SOLUTION ▪

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 commonly used autonomous systems ensures attack mitigation as close to the source of the attack as possible.

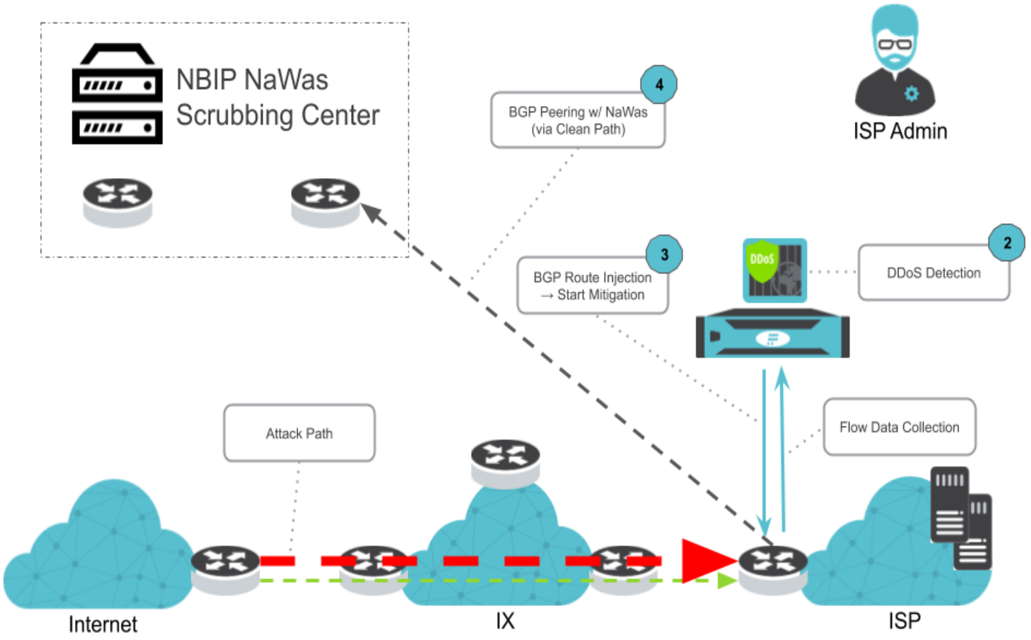
To use this cloud mitigation, service providers in the WEMEA region can join the non-profit NaWas cloud-based mitigation service provided by the NBIP. Flowmon Networks and the NBIP have joined forces to bring cost-effective, high-performance, carrier-grade DDoS mitigation with centralized control. The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

DEPLOYMENT

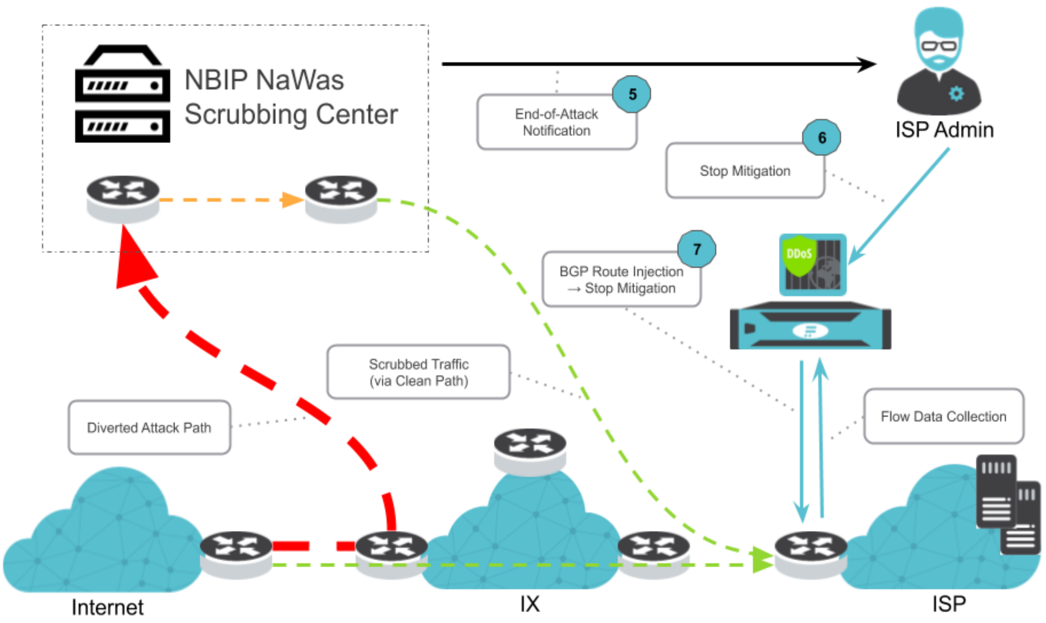
The integrated Flowmon & NaWas solution uses IP flow records from existing service provider infrastructure (routers, switches). There is no need to install a DDoS mitigation device at every peering link. Typically, only Flowmon Collector as a virtual or hardware appliance needs to be deployed in the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



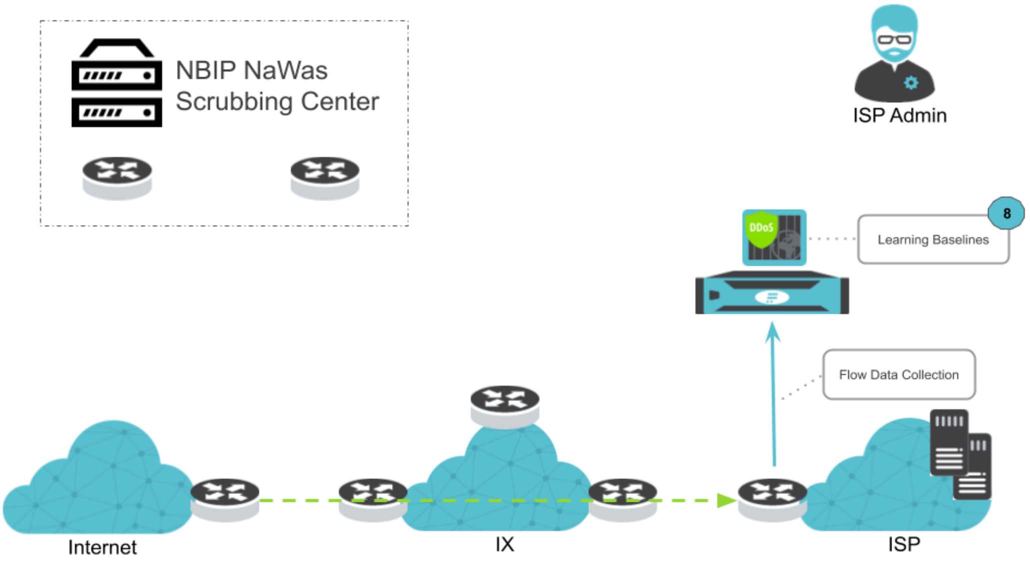
Flow data from routers at the border of the protected infrastructure is collected by Flowmon Collector with Flowmon DDoS Defender. Depending on Flowmon DDoS Defender configuration and detected baselines, the detection of a DDoS attack triggers a series of predefined steps to alert and/or mitigate.


NBIP NaWas Scrubbing Center
BGP Peering w/ NaWas (via Clean Path)
4
ISP Admin
BGP Route Injection → Start Mitigation
3
DDoS
DDoS Detection
2
Flow Data Collection
Attack Path
Internet
IX
ISP

All traffic designated for the affected segment is diverted to NaWas by BGP Route Injection. The BGP Route Injection is performed on a local BGP-capable router and advertised to NaWas via BGP Peering over the Clean Path. After scrubbing, the clean traffic is returned to the border of the protected infrastructure via the Clean Path in the form of a port, dedicated or virtual, provided by the Internet Exchange. The initial BGP Route Injection can be triggered automatically by Flowmon DDoS Defender.



Once the NBIP NaWas concludes that the DDoS attack has ended (i.e., when a drop in the volumetric profile of the affected traffic is detected), changes to the routing configuration need to be reversed manually by stopping the ongoing mitigation in Flowmon DDoS Defender. Subsequently, Flowmon DDoS Defender stops the local BGP-capable router from advertising the diversion to its peers.



In time, all traffic designated for the affected segment is routed directly to the border of the protected infrastructure.

Reports about the specifics of the mitigated DDoS attack are generated and provided by the NBIP NaWas.

BENEFITS

Apart from BGP traffic diversion, Flowmon DDoS Defender can perform other configurable actions that include alerting (e-mail, syslog, SNMP trap) and the execution of scripts. Protected segments can be defined based on IP ranges, subnets or AS numbers, and different mitigation strategies can be applied to each of them. The NBIP NaWas keeps detailed logs and generates reports on the mitigated attacks.

Tjebbe de Winter, *Technical Director at Cyso*

“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.”

NBIP

The Dutch National Internet Providers Management Organization (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

In a world where technology exists for the benefit of people, secure and healthy digital environments are essential. That’s why Flowmon develops an actionable network intelligence solution that enables businesses to ensure their services are running well and securely, and their workforce is productive. Driven by a passion for technology, we have earned the trust of customers who rely on our solution to maintain control over their networks, keep order and overcome uncertainty.

www.flowmon.com

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