

Flowmon + NBIP NaWas

Carrier-grade DDoS Protection

Configuration Guide

Overview

This document is intended to be a companion document to the **Flowmon + NBIP NaWas - Carrier-grade DDoS Protection** whitepaper. It provides a configuration example for setting up NBIP NaWas as a mitigation solution in Flowmon DDoS Defender. The following instructions should be adjusted based on local router configuration and network topology. For details on how to configure detection rules, baselines, and alerting, please refer to the official Flowmon DDoS Defender documentation.

Configuration

In order to set up Flowmon DDoS Defender to utilize NBIP NaWas for DDoS attack mitigation, you have to configure a local, BGP-capable router connected to the *Clean Path* provided by NBIP NaWas and define protected segments.

Configuration / Routers / New Router

Configure Flowmon DDoS Defender to act as an iBGP neighbor to your router, for BGP route injection. The injected route must advertise your AS number via the *Clean Path* port provided by NBIP NaWas on your local IX.

New router

Name: ISP Router

Method: ACL BGP

BGP neighbor IPv4: 172.16.1.1 Router IP address visible to Flowmon

BGP neighbor IPv6:

BGP injector: DDoS Defender

BGP mode: iBGP

Network interface: auto

Flowspec: Enable BGP Flowspec

Community: | [SHOW HELP](#)

AS: 65541 IP address of the router interface connected to the Clean Path port

Next-hop IPv4: 192.168.1.1

Next-hop IPv6:

Tiering:

SAVE **SAVE AND TEST** **CLOSE**

Segments / New Group

Create a group for segment(s) protected by NBIP NaWas.

Add new group

Name

Comment

SAVE **CLOSE**

Segments / New Segment

Create a new segment and assign it to the group created in the previous step. Provide information about flow sources and subnet ranges belonging to the segment. Configure detection with an infinite termination timeout and mitigation via redirection. Redirection will be performed via your BGP-capable router, in the *Route announcement* mode.

New segment


- Basic info
- Segment definition
- Detection
- Mitigation
- Mitigation redirection
- Scrubbing center
- Alerting
- Summary

Name

Group **+ ADD NEW GROUP**

Note

PREV **NEXT** **SAVE** **CLOSE**

 **New segment**
✕

- Basic info
- Segment definition
- Detection
- Mitigation
- Mitigation redirection
- Scrubbing center
- Alerting
- Summary

Flow sources

All sources Selected sources (2)

127.0.0.1 (defender-demo.flowmon.com, p9996) ✕


127.0.0.1 (defender-demo.flowmon.com, p3000) ✕

Subnets

CIDR notation AS numbers

10.0.0.0/24

PREV
NEXT
SAVE
CLOSE

 **New segment**
✕

- Basic info
- Segment definition
- Detection
- Mitigation
- Mitigation redirection
- Scrubbing center
- Alerting
- Summary

Rule

Adaptive threshold all ▾ Always ON

Termination timeout

Infinity

Custom


minutes

Maximal bandwidth

Automatic

Custom

PREV
NEXT
SAVE
CLOSE

 **New segment**
✕

- Basic info
- Segment definition
- Detection
- Mitigation
- Mitigation redirection
- Scrubbing center
- Alerting
- Summary

Mitigate

Mitigation target

Subnets

Preferred subnets

Autodetect subnets

Suspect

Manually

Automatically

Attack


Manually

Automatically

Redirection

Scrubbing center

PREV
NEXT
SAVE
CLOSE


 **New segment**
✕

- Basic info
- Segment definition
- Detection
- Mitigation
- Mitigation redirection
- Scrubbing center
- Alerting
- Summary

Flowspec
discard ▾

	NAME	COMMUNITY	MODE	TIERING
<input type="checkbox"/>	Cisco acl4			
<input checked="" type="checkbox"/>	ISP Router	<input type="text"/>	Route announcement ▾	<input type="checkbox"/> Add community when threshold is exceeded

PREV
NEXT
SAVE
CLOSE

 **New segment**
✕

- Basic info
- Segment definition
- Detection
- Mitigation
- Mitigation redirection
- Scrubbing center
- Alerting
- Summary

Send alert

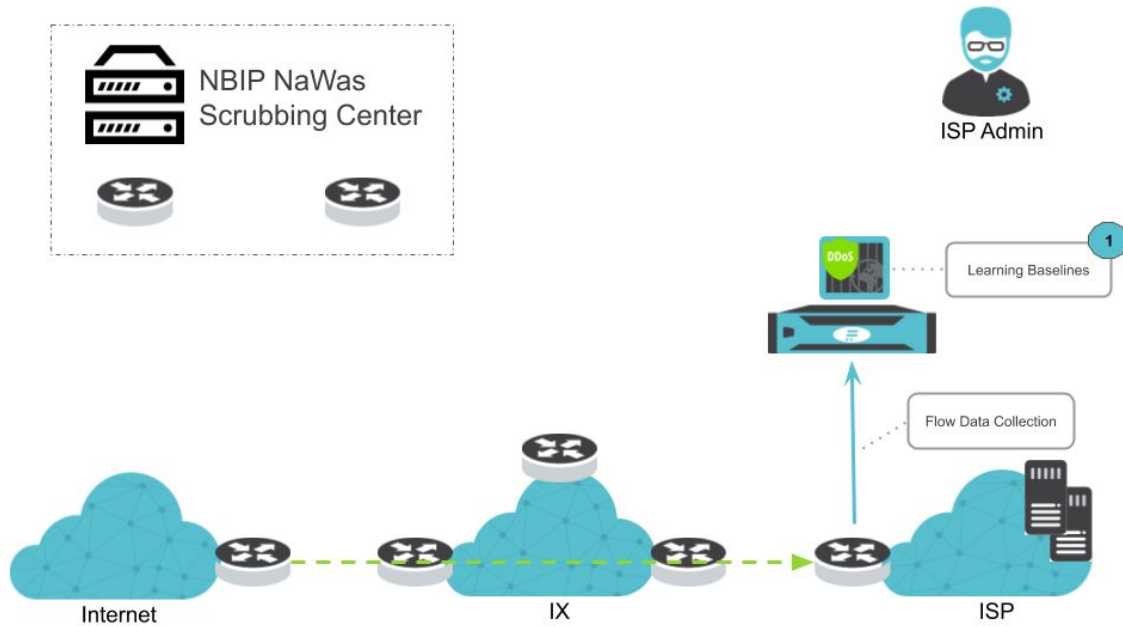
Alert

 Default alert ▾
 + NEW ALERT

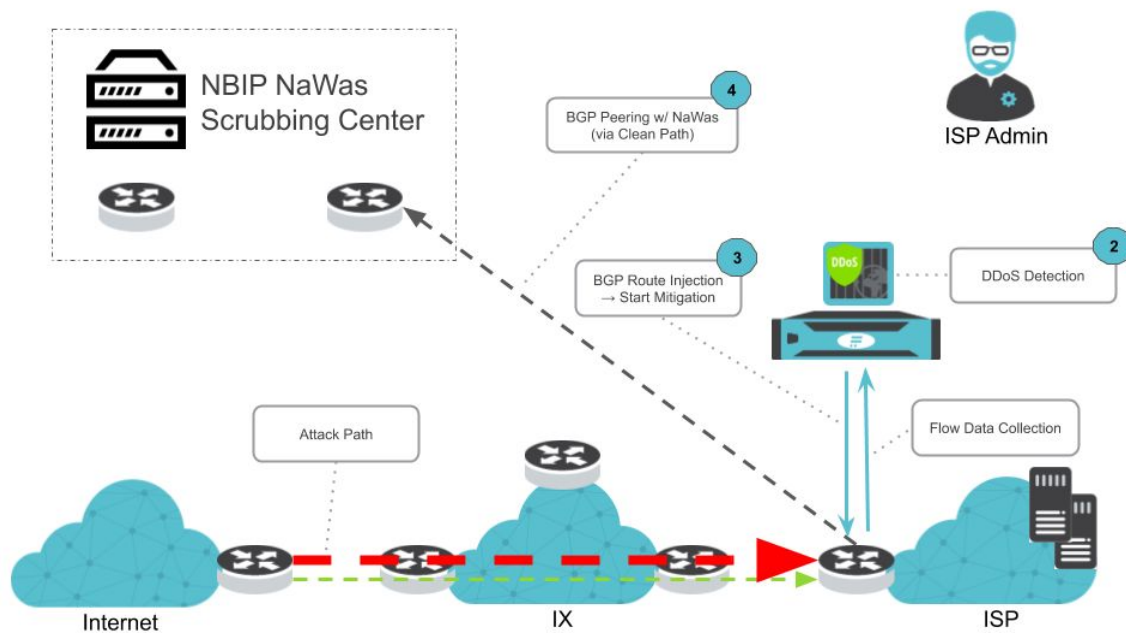
PREV
NEXT
SAVE
CLOSE

For any other configuration details, please refer to the official Flowmon DDoS Defender documentation.

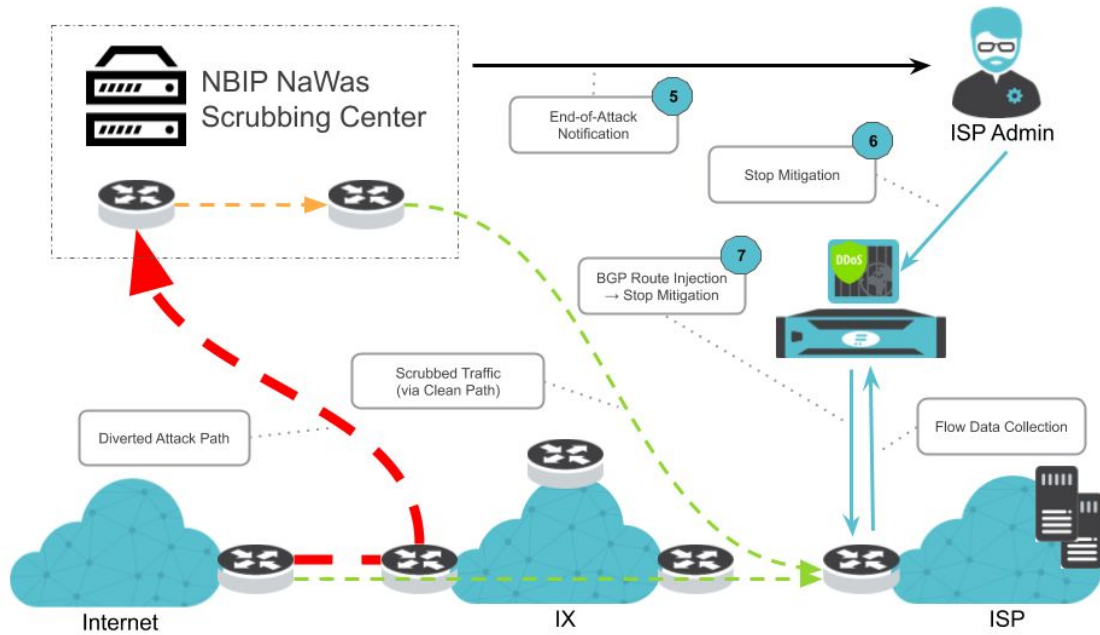
Attack Mitigation



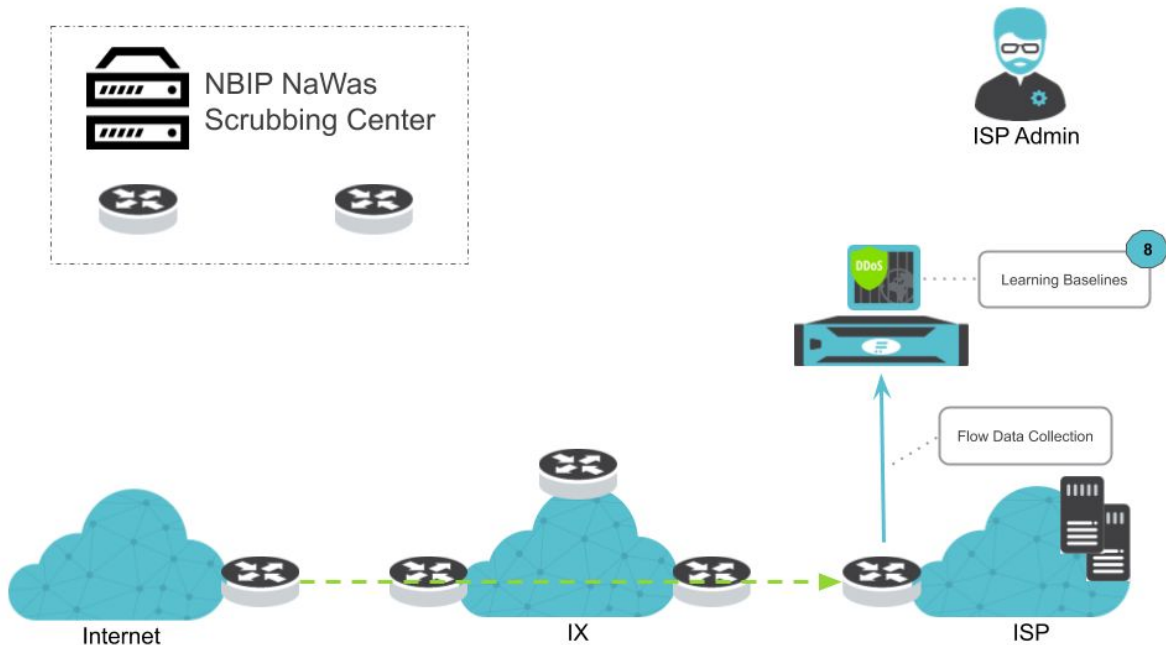
Flow data from routers at the border of the protected infrastructure is collected by Flowmon Collector with Flowmon DDoS Defender (1). Depending on Flowmon DDoS Defender configuration and detected baselines, the detection of a DDoS attack triggers a series of predefined steps to alert and/or mitigate (2).



All traffic designated for the affected segment is diverted to NaWas by BGP Route Injection (3). The BGP Route Injection is performed on a local BGP-capable router and advertised to NaWas via BGP Peering over the Clean Path (4). 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.



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 (6). Subsequently, Flowmon DDoS Defender stops the local BGP-capable router from advertising the diversion to its peers (7). 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.