Flowmon DDoS Defender & F5® BIG-IP® AFM Integration

Implementation Guide

Introduction

This document provides a step-by-step guide how to deploy flow-based DDoS detection of volumetric attacks with an out-of-band mitigation solution. The benefits of this solution are:

- Leveraging flow-export capabilities from already deployed infrastructure
- Sharing resources of mitigation solution for several uplinks
- Cost efficient multi-layer mitigation combining RTBH, Flowspec and out-of-band mitigation
- Deep insight into network traffic, including history
- Baselining of normal traffic and fast mitigation enforcement
- Automated DDoS detection and attack redirection for mitigation for further analysis and cleaning of the traffic

Flowmon DDoS Solution detects volumetric DDoS attacks using flow statistics. Flow statistics can be generated from various sources (including routers, switches and firewalls, or Flowmon Probes) in various quality (sampled or non-sampled flow statistics) and exported to Flowmon Collector for flow statistics analysis.

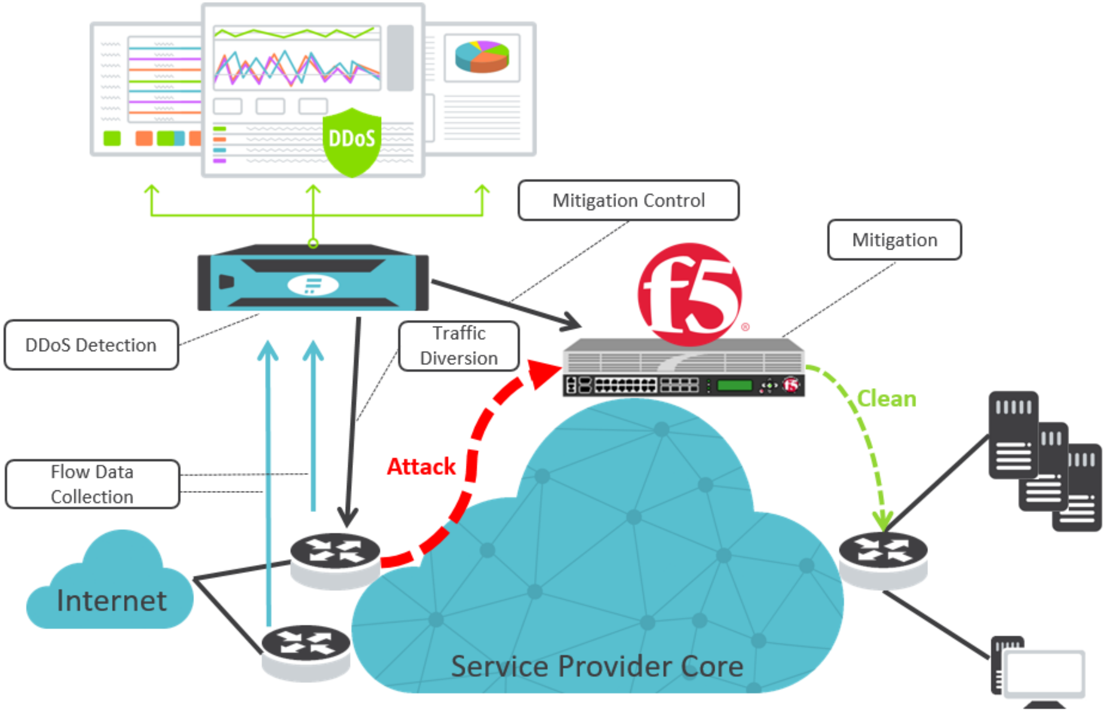


Figure 2: Joint F5 & Flowmon solution for fast DDoS detection and mitigation

Integrated Products

Flowmon DDoS Defender - flow-based solution for detection of volumetric attacks comprises:

- Flowmon Collector – storage and analysis of flow statistics in all major industrial formats (NetFlow v5/v9, IPFIX, sFlow and other technologies compatible with NetFlow) from thousands of flow sources. Available in the form of a physical and virtual appliance.
- Flowmon DDoS Defender – scalable multi-tenant DDoS detection module for Flowmon Collector (software module) using dynamic baselines to detect various types of volumetric attacks and bandwidth consumption.

F5 BIG-IP AFM - out-of-path mitigation device:

- F5 BIG-IP Advanced Firewall Manager™ (AFM) software runs on BIG-IP or VIPRION® hardware or as a virtual edition on a client server. Hardware offers the greatest scalability, while virtual editions offer added deployment flexibility.

Terminology

- Virtual server - group of IPs, subnets, services (ports), matches our understanding of what a protected segment is. Can be defined even to match a specific Flowspec rule. You can have multiple virtual server definitions.
- DDoS Profile - set of rules how to handle DDoS attacks, includes thresholds and actions you want to take. You can have multiple DDoS profiles defined.
- Device profile - similar to DDoS Profile but only one per appliance, global settings how to handle traffic of the whole network.

Integration Principle

Flowmon DDoS Defender uses the F5 BIG-IP iControl® REST API for integration with F5 BIG-IP AFM. The purpose of the integration is to set a communication interface between Flowmon DDoS Defender and F5 BIG-IP AFM. The interface allows a way to automatically configure the virtual server (network segment under the attack) and DDoS profile (set of rules and thresholds how to mitigate the attack) based on attack baselines, volume and signature created by DDoS Defender.

How the Integrated Solution Works

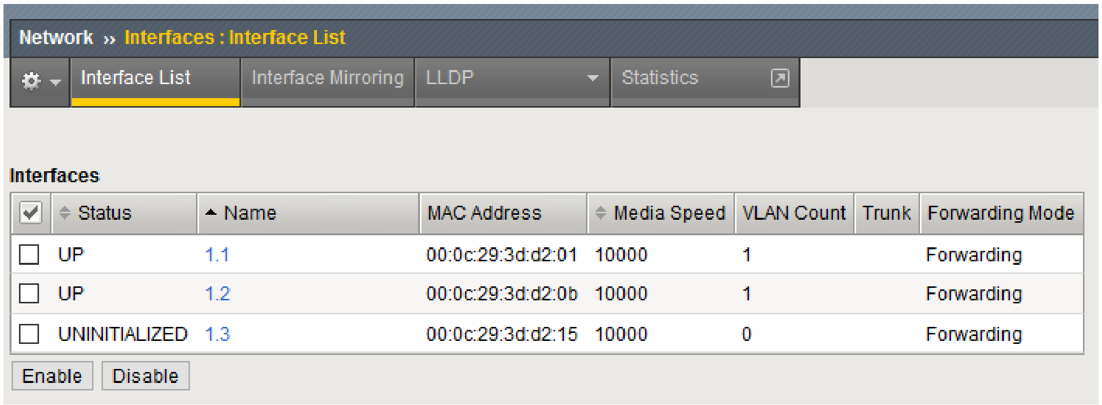
1. Flowmon DDoS Defender detects an attack in a specific protected segment.
2. Flowmon DDoS Defender extracts the attack signature to mitigate the attack.
3. Based on the signature Flowmon DDoS Defender creates a “Virtual server” and “DDoS Profile” on F5 BIG-IP AFM.
4. DDoS Defender diverts traffic to F5 BIG-IP AFM using the existing mechanisms of PBR or BGP.
5. F5 BIG-IP AFM mitigates the DDoS attack.
6. When the attack is over, F5 BIG-IP AFM informs Flowmon DDoS Defender that the attack is over.
7. Flowmon changes the routing back to normal and cleans the configuration on F5 BIG-IP AFM.

Integration Settings

The following steps will provide the proper settings for full integration of both the Flowmon and F5 solutions.

F5 BIG-IP AFM Settings

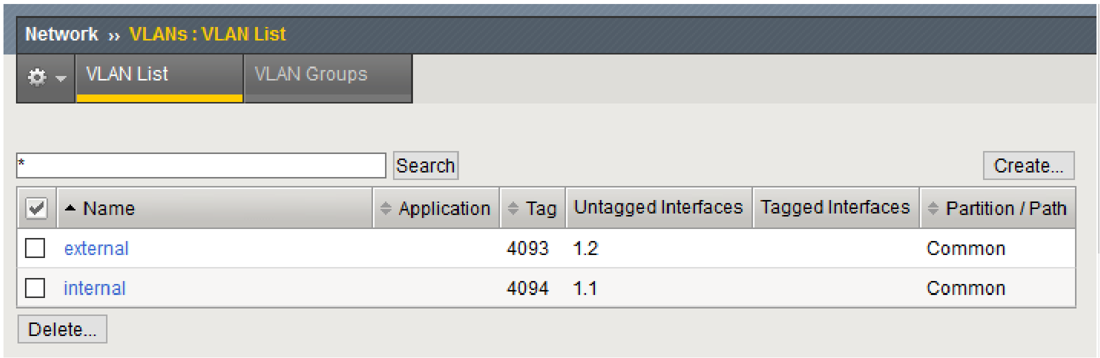
1. It is necessary to run config and set IP for management after the F5 BIG-IP AFM deployment.
2. Set interfaces in Network > Interfaces:



Interfaces

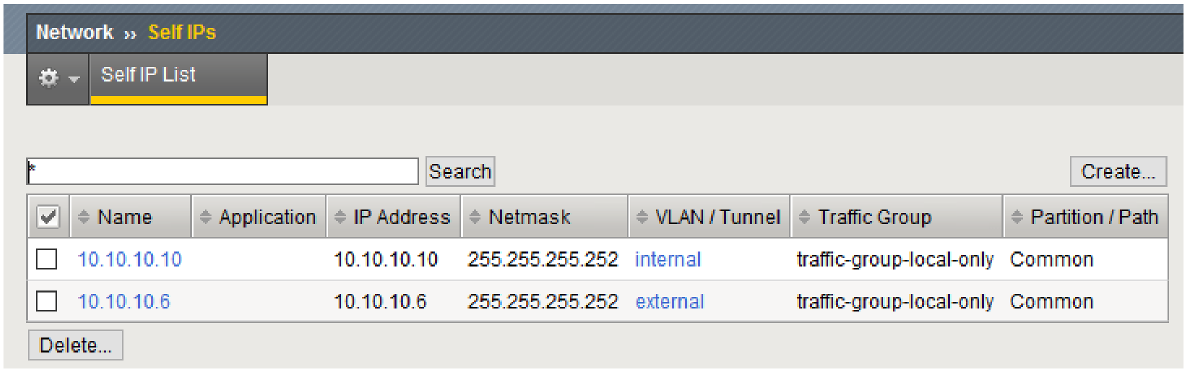
☑	Status	Name	MAC Address	Media Speed	VLAN Count	Trunk	Forwarding Mode
□	UP	1.1	00:0c:29:3d:d2:01	10000	1		Forwarding
□	UP	1.2	00:0c:29:3d:d2:0b	10000	1		Forwarding
□	UNINITIALIZED	1.3	00:0c:29:3d:d2:15	10000	0		Forwarding

3. Set VLANs in Network > VLANs:



☑	Name	Application	Tag	Untagged Interfaces	Tagged Interfaces	Partition / Path
□	external		4093	1.2		Common
□	internal		4094	1.1		Common

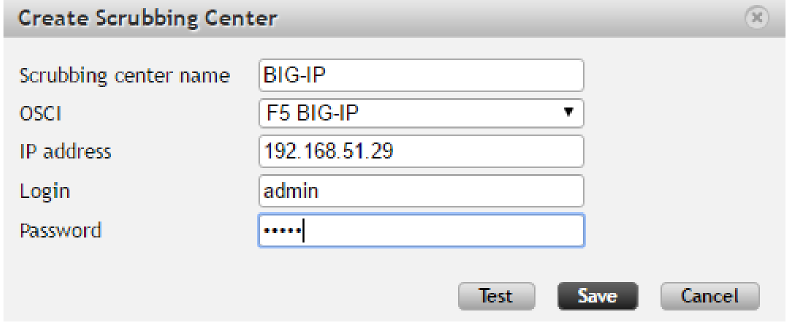
4. Set self IPs in Network > Self IPs:



☑	Name	Application	IP Address	Netmask	VLAN / Tunnel	Traffic Group	Partition / Path
□	10.10.10.10		10.10.10.10	255.255.255.252	internal	traffic-group-local-only	Common
□	10.10.10.6		10.10.10.6	255.255.255.252	external	traffic-group-local-only	Common

Flowmon DDoS Defender Settings

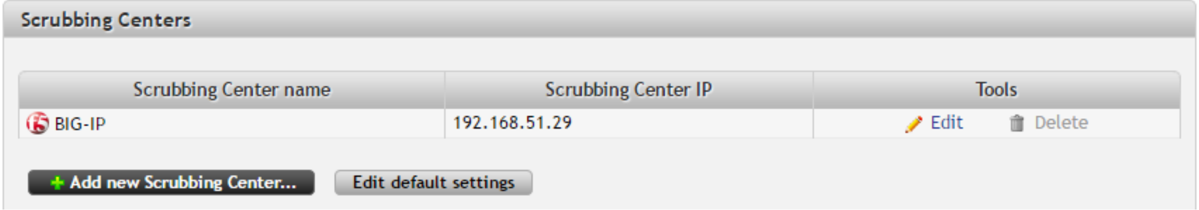
1. In Flowmon DDoS Defender Configuration, click Add New Scrubbing Center.
   a. Enter Scrubbing center name.
   b. Choose F5 BIG-IP from dropdown menu.
   c. Enter IP address of mitigation device and credentials.



Create Scrubbing Center

Scrubbing center name	BIG-IP
OSCI	F5 BIG-IP ▾
IP address	192.168.51.29
Login	admin
Password	•••••

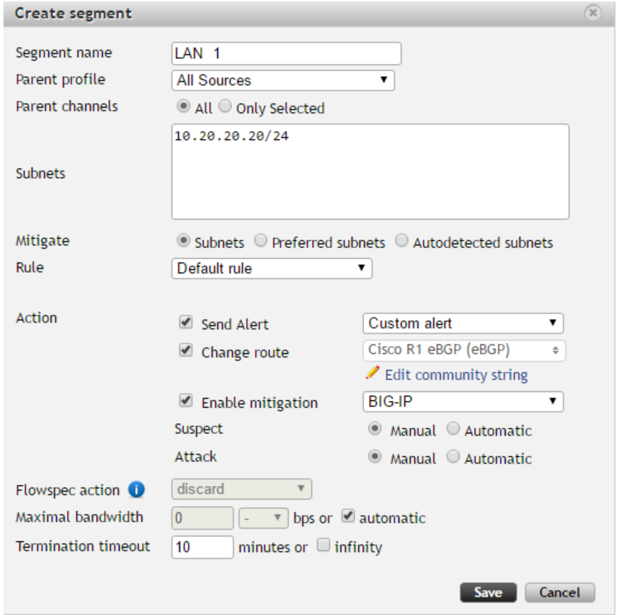
2. The Scrubbing Center will appear in the list and you can edit it later by clicking Edit.



Scrubbing Centers

Scrubbing Center name	Scrubbing Center IP	Tools
BIG-IP	192.168.51.29	Edit Delete

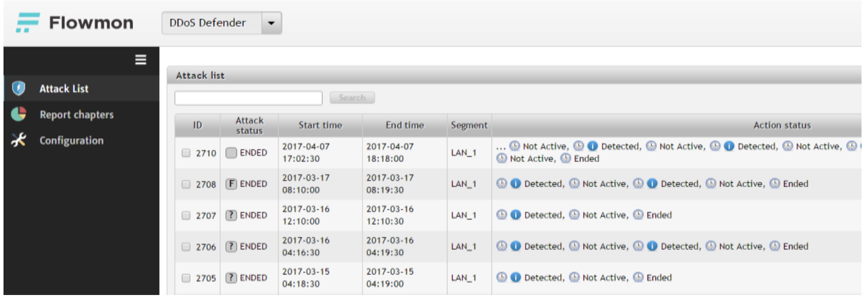
3. Having specified Scrubbing Center, we can set up a protected segment and attack mitigation using this Scrubbing Center. Click “Create segment”.



Create segment

Segment name	LAN 1
Parent profile	All Sources
Parent channels	● All ○ Only Selected
Subnets	10.20.20.20/24
Mitigate	● Subnets ○ Preferred subnets ○ Autodetected subnets
Rule	Default rule
Action	☑ Send Alert — Custom alert ☑ Change route — Cisco R1 eBGP (eBGP) Edit community string ☑ Enable mitigation — BIG-IP Suspect ● Manual ○ Automatic Attack ● Manual ○ Automatic
Flowspec action	discard
Maximal bandwidth	0 - bps or ☑ automatic
Termination timeout	10 minutes or □ infinity

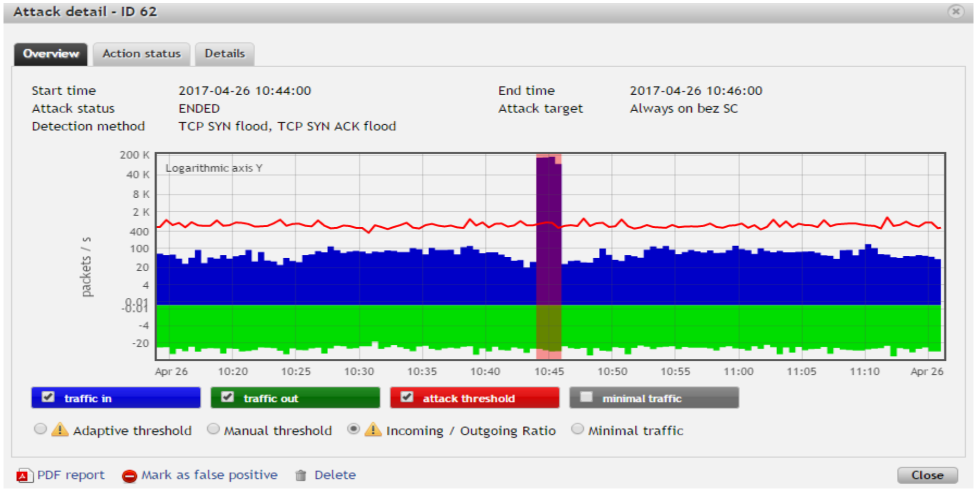
4. Now the integration is set and you can find attacks and their mitigation status in the list of detected attacks in Flowmon DDoS Defender.



Attack list

ID	Attack status	Start time	End time	Segment	Action status
□ 2710	ENDED	2017-04-07 17:02:30	2017-04-07 18:18:00	LAN_1	... Not Active, Detected, Not Active, Detected, Not Active, Not Active, Ended
□ 2708	F ENDED	2017-03-17 08:10:00	2017-03-17 08:19:30	LAN_1	Detected, Not Active, Detected, Not Active, Ended
□ 2707	? ENDED	2017-03-16 12:10:00	2017-03-16 12:10:30	LAN_1	Detected, Not Active, Ended
□ 2706	? ENDED	2017-03-16 04:16:30	2017-03-16 04:19:30	LAN_1	Detected, Not Active, Detected, Not Active, Ended
□ 2705	? ENDED	2017-03-15 04:18:30	2017-03-15 04:19:00	LAN_1	Detected, Not Active, Ended

5. You can click on details of the detected attack.



Attack detail - ID 62

Start time	2017-04-26 10:44:00	End time	2017-04-26 10:46:00
Attack status	ENDED	Attack target	Always on bez SC
Detection method	TCP SYN flood, TCP SYN ACK flood		

○ Adaptive threshold ○ Manual threshold ● Incoming / Outgoing Ratio ○ Minimal traffic

Flowmon DDoS Simulator

You can use Flowmon DDoS Simulator (traffic generator) to confirm proper functionality of integration. Flowmon DDoS Simulator is available at Flowmon Support Portal: https://support.flowmon.com/download.php?did=1586

Additional Sources

- Flowmon Collector - Product Brief, Specification
- Flowmon DDoS Defender - Product Brief, Specification

Feel free to contact Flowmon Support team at support@flowmon.com for further assistance.

For more information, please contact your F5 Networks or Flowmon Networks partner.

F5 Networks, Inc.
401 Elliott Avenue
Seattle, WA 98119-4017
USA
www.f5.com

Flowmon Networks a.s.
U Vodárny 2965/2
616 00 Brno
Czech Republic
www.flowmon.com