Flowmon & Radware DDoS Integration Guide

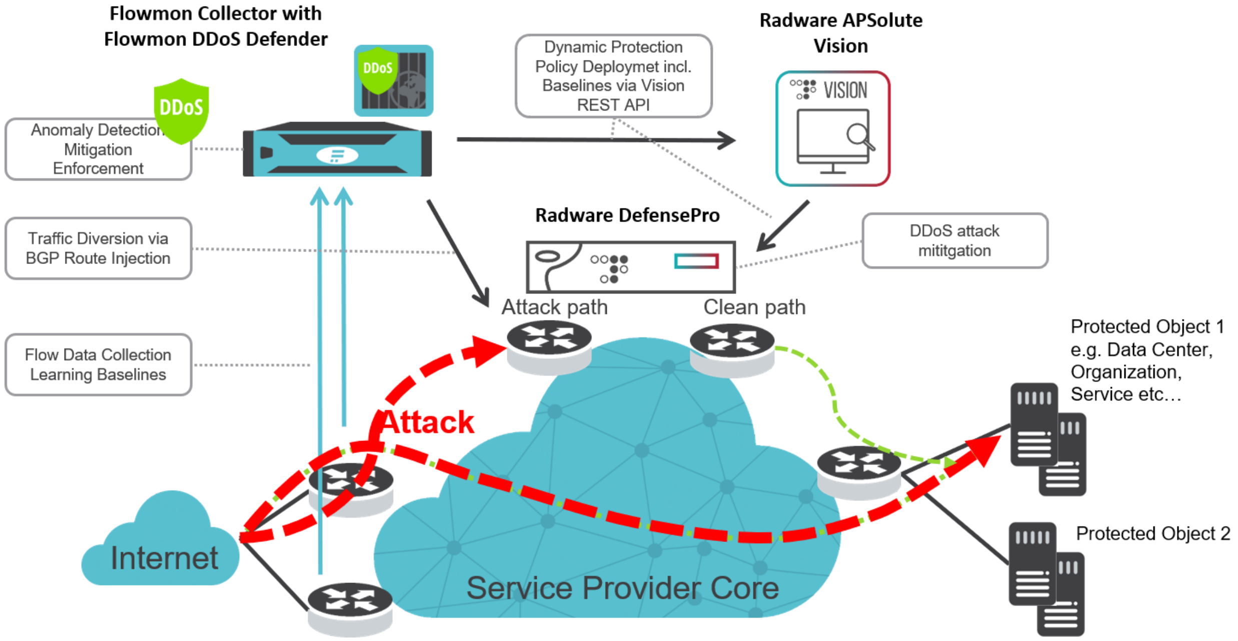
Purpose of this document is to describe integration steps for Flowmon DDoS Defender with Radware DefensePro and Radware APSolute Vision. Guide is valid for Flowmon DDoS Defender version 4.x and higher.

Joint solution description

Flowmon Collector with the DDoS Defender module, Radware APSolute Vision and the DefensePro appliance together form a DDoS protection ecosystem suited to protect even the largest infrastructures and internet backbones.

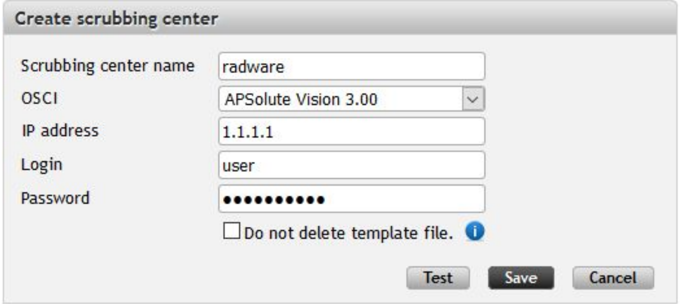
- **Flowmon Collector** aggregates and stores flow data in all major industrial formats from an unlimited number of sources. Collector provides advanced tools for reporting and analysis of network and application traffic.
- **Flowmon DDoS Defender** is a scalable multi-tenant DDoS detection module for Flowmon Collector. It uses dynamic baselines to detect various types of volumetric attacks and bandwidth consumption.
- **Radware APSolute Vision** network management tool that consolidates the monitoring and configuration of up to 1,000 devices across multiple data centers
- **Radware DefensePro** is a network attack mitigation device that can be used both in-line and out-of-band to protect IT infrastructure against network and application downtime.

Flowmon DDoS Defender together with Radware DefensePro appliance and Vision management appliance represent DDoS protection ecosystem designed to protect largest infrastructures and internet backbones. Native integration of DDoS Defender with Vision via RESTful API enables to manage multiple DefensePro appliances via standard management interface and dynamically configure network protection profiles while providing to DefensePro details about the attack and baselines of standard network traffic. Traffic diversion capabilities of DDoS Defender include policy based routing for local ISPs and BGP support for Tier 1 networks, Telcos and transit operators to divert the traffic to DefensePro DDoS mitigation appliance deployed out-of-band.



Flowmon DDoS Defender Configuration

1) Configure scrubbing center – choose supported version of APSolute Vision and enter other information.



Create scrubbing center

Scrubbing center name	radware
OSCI	APSolute Vision 3.00
IP address	1.1.1.1
Login	user
Password	●●●●●●●●●●●

□ Do not delete template file.

2) Configure Router for traffic redirection via scrubbing center – please refer to Flowmon DDoS Defender user guide, chapter 4 for more information about BGP injection configuration and scenarios.

Radware DefensePro Preparation

1) Install the latest signature file on the DefensePro and enable the signature protection

dp signatures-protection dos-shield global status set enable

2) Enable Out-of-state protection

dp out-of-state global-parameters op-state set on

3) Enable BDoS Protection

dp behavioral-DoS global status set enable

4) Enable SYN Protection

dp syn-protection status set enable

5) Enable the HTTP Mitigator

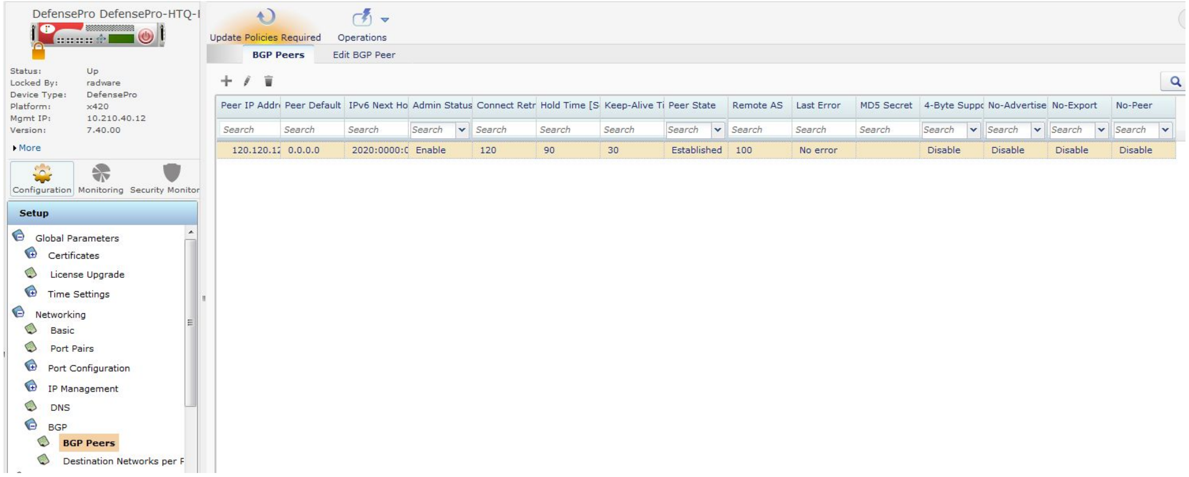
dp http-mitigator global status

Utilize DefensePro for BGP injection (IP Operation Mode)

1) Enable SSH Access

manage ssh status set enable

2) Establish a BGP peer connection



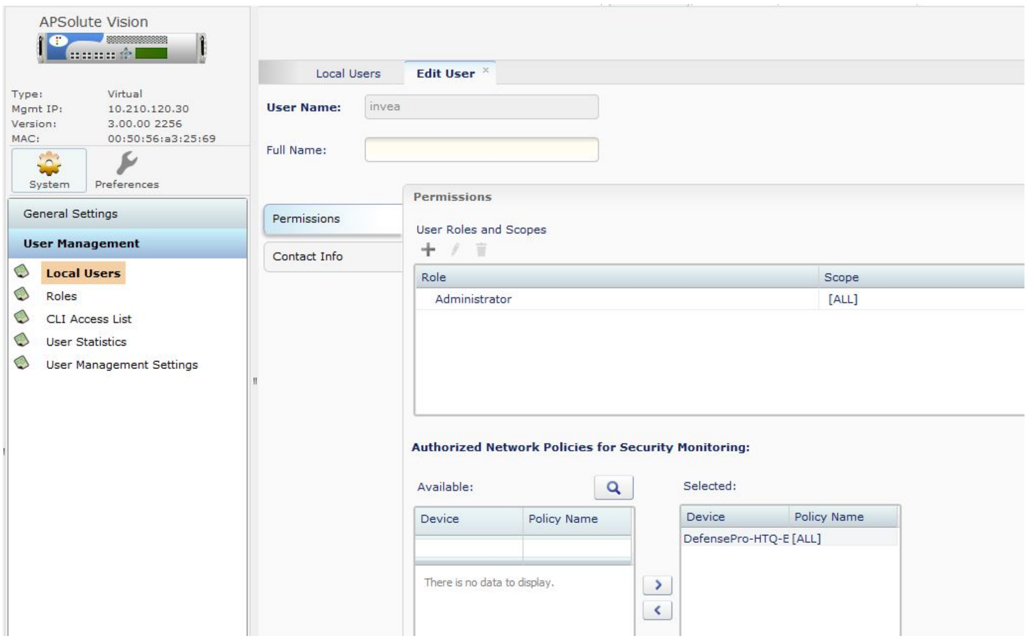
DefensePro DefensePro-HTQ-I

Status:	Up
Locked By:	radware
Device Type:	DefensePro
Platform:	x420
Mgmt IP:	10.210.40.12
Version:	7.40.00

Peer IP Addr	Peer Default	IPv6 Next Ho	Admin Status	Connect Retr	Hold Time [S	Keep-Alive Ti	Peer State	Remote AS	Last Error	MD5 Secret	4-Byte Suppc	No-Advertise	No-Export	No-Peer
Search	Search	Search	Search	Search	Search	Search	Search	Search	Search	Search	Search	Search	Search	Search
120.120.12	0.0.0.0	2020:0000:C	Enable	120	90	30	Established	100	No error		Disable	Disable	Disable	Disable

Radware APSolute Vision Configuration

Add a new and dedicated user on Vision with administrator permissions



Type: Virtual
Mgmt IP: 10.210.120.30
Version: 3.00.00 2256
MAC: 00:50:56:a3:25:69

User Name: invea

Full Name:

Role	Scope
Administrator	[ALL]

Available:

Device	Policy Name

Selected:

Device	Policy Name
DefensePro-HTQ-E	[ALL]