Flowmon DDoS Defender Models Specification

valid from 1.5.2017

Flowmon DDoS Defender	DDoS Defender 1 FC-DDOS-1	DDoS Defender 4 FC-DDOS-4	DDoS Defender 10 FC-DDOS-10	DDoS Defender 40 FC-DDOS-40	DDoS Defender 100 FC-DDOS-100	DDoS Defender 400 FC-DDOS-400	DDoS Defender 1000 FC-DDOS-1000
Throughput (Gbps)	1	4	10	40	100	400	1000
Recommended Collector	1TB+	1TB+	3TB+	3TB+	12TB+	12TB+	SSD
Traffic Diversion	PBR, BGP	PBR, BGP	PBR, BGP	PBR, BGP	PBR, BGP	PBR, BGP	PBR, BGP
Mitigation Techniques	RTBH, BGP Flowspec	RTBH, BGP Flowspec	RTBH, BGP Flowspec	RTBH, BGP Flowspec	RTBH, BGP Flowspec	RTBH, BGP Flowspec	RTBH, BGP Flowspec
3rd Party Mitigation Solutions Integration	YES	YES	YES	YES	YES	YES	YES

Attack Detection is done for every protected segment (network subnets, customer's networks) defined by user. Flowmon DDoS Defender support baseline (manual or adaptive threshold) and static (in/out ratio) methods for DDoS attack detection. Minimal traffic can be defined for triggering evaluation of detection methods or triggering attack detection.

Speed of Detection – Flowmon DDoS Defender uses 30 seconds flow data intervals and thus allows near real-time attack detection and reaction (from less than 30 seconds up to 60 seconds). Actual speed of attack detection depends on attack characteristics and timeouts settings of flow data export in the exporter (e.g. router, Flowmon Probe).

Throughput represents maximal network traffic volume in Gbps of legitimate traffic. License consumption is computed as summary of all baselines. Attack traffic is not counted into licensed throughput capacity.

Recommended Collectors refer to hardware Flowmon Collectors. Mentioned models differs in number of CPUs and RAM size. Flowmon DDoS Defender can be also deployed on virtual Flowmon Collectors with allocated sufficient amount of resources according to hardware collectors. For more information see Flowmon Collector specification document.

Traffic Diversion of network traffic can be done using PBR (Policy Based Routing, supported vendors: Alcatel-Lucent, Cisco, Juniper) or BGP (Border Gateway Protocol). Flowmon DDoS Defender support both external and internal BGP (eBGP & iBGP) and BGP Flowspec.

Mitigation Techniques RTBH (Remotely Triggered Black Hole) and BGP Flowspec are supported.

RTBH (Remotely Triggered Black Hole) can be configured using BGP or user-defined ACL (Access Control List) on supported routers (Alcatel-Lucent, Cisco, Juniper). Upon attack detection, Flowmon DDoS Defender sends ACL commands instruct routers to drop or redirect undesired traffic to black hole.

Flowmon Networks a.s.
info@flowmon.com

Flowmon DDoS Defender Models Specification

valid from 1.5.2017

BGP Flowspec can be used for DDoS attack mitigation on Flowspec enabled routers. Flowmon DDoS Defender creates dynamic signature of the attack and suggests appropriate Flowspec rule based on the signature. Flowspec rules for injection can be created for following items: destination and source network, destination and source port, L4 protocol. Flowmon DDoS Defender allows to configure Flowspec action for each of the rules. The action can be e.g.: accept, discard, rate-limit or redirect. For more information about BGP Flowspec see Flowmon DDoS Defender user-guide.

3rd Party Mitigation Solutions Integration – Flowmon DDoS Defender natively supports Radware DefensePro, Radware Vision, F5 BIG-IP or VIPRION and A10 Thunder TPS solutions for DDoS attacks mitigation.

Alerts can be done using email, syslog, SNMP trap or user-defined script can be triggered.

Multi-tenancy is supported.

Flowmon Networks a.s.
info@flowmon.com