Flowmon DDoS Defender Models Specification

valid from 26.10.2020

Flowmon DDoS Defender		DDoS Defender 1 SUB-FC-DDOS-1	DDoS Defender 4 SUB-FC-DDOS-4	DDoS Defender 10 SUB-FC-DDOS-10	DDoS Defender 40 SUB-FC-DDOS-40	DDoS Defender 100 SUB-FC-DDOS-100	DDoS Defender 400 SUB-FC-DDOS-400	DDoS Defender 1000 SUB-FC-DDOS-1000
Throughput (Gbps)		1	4	10	40	100	400	1000
HW Requirements	**CPU**	2	4	8	12	16	24	32
	RAM*	8 GB (50 segments), 16GB (100 segments), 32 GB (200 segments), 64 GB (500 segments), 128 GB (1000 segments)						
Traffic Diversion		**PBR** (supported vendors: Alcatel-Lucent, Cisco, Juniper), **BGP** (eBGP and iBGP support), **BGP Flowspec**						
Mitigation Techniques		**RTBH** (BGP, ACL supported vendors: Alcatel-Lucent, Cisco, Juniper), **BGP Flowspec**						
3rd Party Mitigation Solutions Integration		**Radware DefensePro, Radware Vision, F5 BIG-IP, F5 VIPRION, A10 Thunder TPS**						

* Memory requirements depend on the system configuration and attack structure. The memory requirement is declared for the specific number of protected segments and corresponds to a scenario where up to 10% of protected segments is under the attack at the time, maximum of 5 traffic types under the attack (exceeded baselines) and maximum of 100 target (IP addresses) per attack. Required memory refers to memory consumed by DDoS Defender only. It is recommended that the total memory of the Flowmon appliance is double the one from DDoS Defender. Insufficient memory allocated to DDoS Defender lowers the number of segments processed and protected against the DDoS attacks.

Key features:

- **Volumetric DDoS attack detection**
- **Near real-time detection speed**
- **Mitigation Techniques**
- **Whitelisting of IP ranges and ASNs**

Volumetric DDoS Attack Detection is done for every protected segment (network subnets, customer's networks) defined by user. Flowmon DDoS Defender supports baseline (manual or adaptive threshold) and static (in/out ratio) methods for DDoS attack detection. Baseline methods use continuous and weekday baseline which are calculated for both

Flowmon Networks a.s.
info@flowmon.com

packets per second and bits per second. User can define own baselines using port(s) and protocol pairs. Minimal traffic can be defined for triggering evaluation of detection methods or triggering attack detection.

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.

Near real-time detection speed – Flowmon DDoS Defender processes flow data in stream allowing to detect DDoS attacks in near real-time. User is able to select the length of the traffic anomaly (10 - 90 seconds) before it is reported as an attack. Detection speed also depends on timeout settings of flow data export in the exporter (e.g. router, Flowmon Probe).

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.
- **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.

Mitigation tiering allows to use different mitigation tactics based on the attack volume (e.g. local scrubbing up to specific traffic volume and when exceeded, redirection to the cloud scrubbing). User is able to configure thresholds and additional BGP community for each defined protected segment and router. Once the volume of redirected traffic is exceeding the defined threshold, additional BGP community is used for the route. Thresholds for router and protected segment can be evaluated independently and continuously.

Whitelisting of IP ranges and ASNs allows user to mark regular traffic using defined filter. Whitelist are defined using IP ranges or ASNs, are valid for defined time period and can be assigned for specific protected segment or group of segments and traffic types.

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

Multi-tenancy is supported on a level of protected segments or group of protected segments.