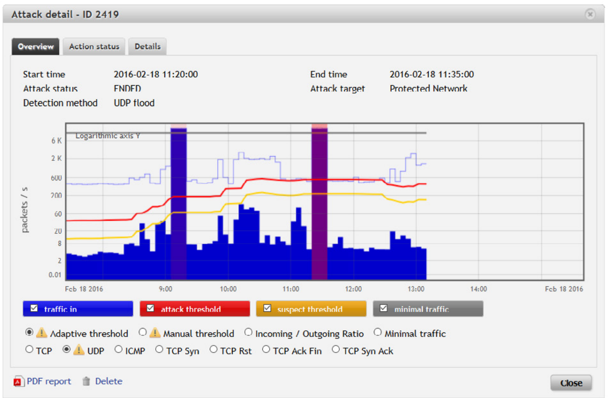
Flowmon DDoS Defender

DDoS Attack Detection and Mitigation Module

Product Brief

INTRODUCTION

Flowmon DDoS Defender is a solution for detection and mitigation of volumetric attacks – DoS (Denial of Service) or DDoS (Distributed Denial of Service). Without any configuration changes, topology changes or any additional investments in the network components, it is possible to detect the volumetric attacks led against the IT infrastructure, servers, critical systems or applications in real time. Deployment is a matter of minutes thanks to the universal architecture and the extensive integration capabilities with network equipment or DDoS mitigation appliances.


Attack detail - ID 2419

Start time	2016-02-18 11:20:00	End time	2016-02-18 11:35:00
Attack status	ENDED	Attack target	Protected Network
Detection method	UDP flood		

☑ traffic in ☑ attack threshold ☑ suspect threshold ☑ minimal traffic

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

○ TCP ● UDP ○ ICMP ○ TCP Syn ○ TCP Rst ○ TCP Ack Fin ○ TCP Syn Ack

UNIVERSAL DEPLOYMENT

Flowmon DDoS Defender can be deployed in heterogeneous environments collecting common flow statistics from the active network components in various formats and/or processing of highly accurate flow statistics gained through the Flowmon Probes. Thanks to the robust and versatile architecture, it is possible to deploy standalone DDoS Defender as well as in combination with specialized out-of-band solutions for DDoS attack elimination or together with attack mitigation services provided by Scrubbing centers. The integration with network components is supported via PBR (Policy Based Routing) or BGP (Border Gateway Protocol) or you can possibly use the RTBH (Remotely Triggered Black Hole) mechanism as a simple method of attack mitigation.

FEATURES AND BENEFITS

- **Real-time DoS and DDoS attack detection**
- **Significant attack response time acceleration**
- **Dynamic baselining of traffic volumes and characteristics**
- **Attacks characteristic visualisation**
- **Notifications via e-mail, syslog, SNMP trap**
- **Support for standard methods of traffic diversion (PBR, BGP, RTBH)**
- **Advanced options of immediate reaction (script initiation, mitigation)**
- **Independent configurations for different customers, services, network segments, etc.**
- **Module for Flowmon solution, simple installation and quick time-to-value**

ADVANCED METHODS OF DETECTION

Flowmon DDoS Defender monitors the traffic volume characteristics of secured infrastructure (defined profiles) and responds to the increasing volumes in traffic based on defined rules and dynamic baselines. In order to define such a profile, IP address range, port- and protocol-defined services or VLAN numbers and MPLS tags, etc. can be used. A combination of static rule and percentage deviation from dynamically created and continuously updated baseline is a way how to easily configure rules of attack detection. Based on the detected DDoS attack, the following actions can be performed:

- **Alert (e-mail, syslog, SNMP trap)**
- **Traffic diversion (PBR, BGP, RTBH)**
- **User-defined script initiation**
- **Attack elimination (mitigation) in collaboration with Scrubbing center or a specialized out-of-band solution**

ORDERING INFORMATION

Distributed by

NEOX NETWORKS

sales@neox-networks.com
+49 6103 37 215 910
www.neox-networks.com

Flowmon Networks

Flowmon Networks, a. s.
U Vodárny 2965/2
616 00 Brno

+420 511 205 250
info@flowmon.com
www.flowmon.com