Contribution ID : **32** Type : **not specified**

Adaptive mitigation of DDoS attacks using BGP Flowspec

Wednesday, 29 May 2019 09:30 (30)

Prupose of the presentation is to demonstrate capabilities of BGP Flowspec implemented on routers to mitigate volumetric DDoS attacks while adapting on continuously changing attack pattern. Attack detection is based on flow (NetFlow/IPFIX) technology that enable to identify attack pattern that is automatically converted into set of BGP Flowspec rules and pushed to routers for attack mitigation. Continuous monitoring of attack characteristics enables to update mitigation rules automatically when deviation from current attack pattern is detected. As part of the presentation we would like to explain flow data and show what value it brings for network operators in broader context than just DDoS protection.

Primary author(s) : MINAŘÍK, Pavel (Flowmon Networks a.s.); Mr KNAPEK, Jiří (Flowmon Networks a.s.)

Session Classification : CSNOG2

Track Classification : CSNOG 2019