On the Potential of BGP Flowspec for DDoS Mitigation at Two Sources: ISP and IXP

Nico Hinze[1], Marcin Nawrocki[1], Mattijs Jonker[2],
Alberto Dainotti[3], Thomas C. Schmidt[4], Matthias Wählisch[1]
[1]Freie Universität Berlin, [2]University of Twente, [3]CAIDA, [4]HAW Hamburg
givenname.surname@fu-berlin.de,m.jonker@utwente.nl,alberto@caida.org,t.schmidt@haw-hamburg.de

CCS CONCEPTS

• **Security and privacy → Denial-of-service attacks**;

ACM Reference Format:
N. Hinze, M. Nawrocki, M. Jonker, A. Dainotti, T.C. Schmidt, M. Wählisch. 2018. On the Potential of BGP Flowspec for DDoS Mitigation at Two Sources: ISP and IXP. In *ACM SIGCOMM 2018 Conference Posters and Demos, August 20–25, 2018, Budapest, Hungary*. ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/3234200.3234209

1 INTRODUCTION

Distributed Denial of Service (DDoS) attacks are a major threat to the Internet ecosystem. DDoS cannot only exhaust resources of end systems but also of provider uplinks. Ideally, DDoS attacks are mitigated close to the attacker, and mitigation only affects malicious traffic.

Mitigation on inter-domain level is commonly implemented with remotely triggered blackholing (RTBH). Blackholing enables the victim domain to mark the (usually /32) IP prefix under attack using BGP communities. Based on this tagging, adjacent peers can filter traffic to the victim to prevent overload. Although RTBH is an easy to implement, cost-efficient and effective mitigation solution, it faces a significant drawback: since *all* traffic to the victim is discarded, the victim becomes completely unreachable. A more fine-grained filtering is provided in BGP Flowspec [3], which supports filtering rules – exchanged through BGP – for 12 different components (*e.g.,* source and destination address, TCP flags).

SIGCOMM'18, August 21-23, 2018, Budapest, Hungary

ACM ISBN 978-1-4503-5915-3/18/08…$15.00
https://doi.org/10.1145/3234200.3234209

In this poster, we aim for a better understanding of DDoS traffic from an inter-domain perspective. We analyze malicious traffic based on passive measurements from a national Internet Service Provider and from a large regional Internet Exchange Point. In contrast to previous work (*e.g.,* [2]), we try to characterize collateral damage that occurs while blackholing DDoS traffic, compared to the benefits of deploying Flowspec. Our ongoing analysis shows that (*i*) current blackholing drops significant portion of valid traffic whereas BGP Flowspec requires very little additional information to improve the situation, (*ii*) an IXP is a good vantage point to deploy Flowspec close to the attacker.

2 RESULTS

2.1 ISP Lens

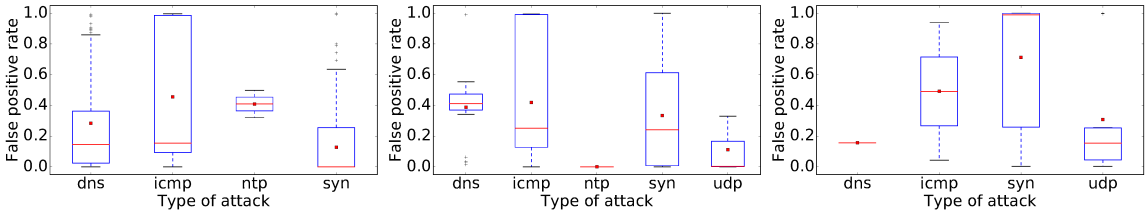
Data set. We look at the *MAWI* data set, which contains full packet captures from a transpacific Internet link between Japan and the United States. Each trace represents a 15 minute snapshot per day. The data explicitly annotates DDoS events and includes traffic features that characterize each attack [1]. We map these attack traffic features to Flowspec components and create Flowspec rules [3] which would protect each victim IP address.

Complexity of BGP Flowspec rules. For each attack in the MAWI data set, we quantify the average number of components that describe the attack (see Table 1). The IP destination address as well as the transport layer type are always required. Depending on the attack, the source port (DNS, NTP) or the ICMP type are necessary as well. Syn flooding attacks are more complex, as they do not only require TCP flags but also destination ports and (sometimes) IP source addresses to identify distributed attacks. Rarely (< 5%) TCP source or UDP destination ports are used.

False positives introduced by Blackholing. Blackholing filters all traffic to the victim, including DDoS *and* legitimate data. We define false positives as those packets to the victim that do not match the corresponding Flowspec rule but would be filtered by blackholing. Figure 1 presents the statistical distribution of false positives rates per attack. On average, the ratio of false positives ranges between 20% and

Table 1: Average number of BGP Flowspec components required to specify exact filter rules per attack.

	2015					2016					2017				
# Comp.	DNS	ICMP	NTP	UDP	SYN	DNS	ICMP	NTP	UDP	SYN	DNS	ICMP	NTP	UDP	SYN
2	0%	0%	0%	0%	0%	0%	0%	0%	33%	0%	0%	0%	0%	0%	0%
3	83%	56%	0%	0%	1%	96%	58%	100%	33%	0%	100%	50%	0%	78%	0%
4	17%	44%	100%	0%	74%	4%	42%	0%	33%	60%	0%	50%	0%	22%	58%
5	0%	0%	0%	0%	23%	0%	0%	0%	0%	40%	0%	0%	0%	0%	13%
6	0%	0%	0%	0%	2%	0%	0%	0%	0%	0%	0%	0%	0%	0%	29%



(a) 2015 (b) 2016 (c) 2017

Figure 1: Incorrectly filtered traffic because of /32 blackholing compared to fine-grained BGP Flowspec.

70%, indicating demand for more fine-grained filtering compared to blackholing. The distribution shows outliers for two reasons. First, ≈ 100% false positives may arise because of DDoS misclassification of the MAWI detection system. Second, high volumes of DDoS traffic block legitimate traffic which thus might not be visible in our snapshot. Our results show a lower bound. Improving the methodology towards historical traffic models is part of our on-going work.

2.2 IXP Lens

Data set. We analyze data from the switching fabric of a large regional Internet Exchange Point (IXP). The data includes full IP and transport headers but is sampled (*i.e.,* 1 out of every 10,000 packets). Based on this data set, we can better understand source and destination as well as transit of DDoS traffic between peers. To infer blackholing events, which indicate DDoS incidents, we analyze public BGP data, *i.e.,* from RIPE RIS and RouteViews. Our measurement is based on the methodology by Giotsas et al. [2] and uses the same dictionary of BGP communities known to be used for blackholing. From Oct. 2017 till March 2018 we detect 71 IP addresses that have been protected by blackholing and belong to one of the IXP members. For 18 of these IP addresses, we find in our sampled flow data traffic in the 30 minutes window preceding blackholing. We assume that such traffic is thus affected by the DDoS attack. For 4 IP addresses we also measured traffic before the DDoS incidents.

Traffic mix before and during DDoS attack. The attack traffic is mainly amplification traffic [4], and there is a clear distinction between traffic that is visible before and during the DDoS attack with respect to each victim IP address. In terms of volume, the traffic increases between two and four orders of magnitude. In terms of traffic type, any packet to a victim that was sampled before the corresponding DDoS attack exhibits a different transport and application protocol compared to any traffic during the attack. Such clear signatures enable fast, automatic filter rules based on the sampled flow data to allow legitimate traffic to pass. However, to assess false positives, it is worth noting that we do not see all packets because of sampling. This makes characterization of legitimate traffic challenging in contrast to the MAWI data, in particular in case of low-traffic IXP members.

Sources of DDoS traffic. To analyze the topological locations of the amplifiers, we measure the distances in AS hops from the AS that hosts the amplifiers to the IXP members that forwards malicious traffic to other peers. Our analysis is based on AS paths advertised by the IXP route server. Any path prepending is resolved.

39% of the traffic comes from amplifiers hosted in IXP member networks, 37% of the traffic is only one hop away and thus initiated within networks of direct customers of IXP members. Non-malicious traffic is slightly more local, 86% of traffic originates from a member or a direct customer of a member. We argue that this locality allows for social interaction to mitigate DDoS. In particular, when IXPs do not offer blackholing services, they could personally contact their members hosting an amplifier to setup immediate filters. On the other hand, when IXP members experience DDoS against one of their hosts, BGP Flowspec would enable them to request dropping invalid traffic close to the root of the attack, making IXPs a promising candidate for BGP Flowspec.

Next steps. We will work on an extended traffic model to assess the beneficial impact of BGP FlowSpec in more detail.

REFERENCES

[1] Romain Fontugne, Pierre Borgnat, Patrice Abry, and Kensuke Fukuda. 2010. MAWILab: Combining Diverse Anomaly Detectors for Automated Anomaly Labeling and Performance Benchmarking. In *Proceedings of ACM International Conference on emerging Networking EXperiments and Technologies (CoNEXT '10)*. ACM, New York, NY, USA, 8:1–8:12. https://doi.org/10.1145/1921168.1921179

[2] Vasileios Giotsas, Philipp Richter, Georgios Smaragdakis, Anja Feldmann, Christoph Dietzel, and Arthur Berger. 2017. Inferring BGP Blackholing Activity in the Internet. In *Proceedings of the 2017 Internet Measurement Conference (IMC '17)*. ACM, New York, NY, USA, 1–14. https://doi.org/10.1145/3131365.3131379

[3] P. Marques, N. Sheth, R. Raszuk, B. Greene, J. Mauch, and D. McPherson. 2009. *Dissemination of Flow Specification Rules.* RFC 5575. IETF.

[4] Fabrice J. Ryba, Matthew Orlinski, Matthias Wählisch, Christian Rossow, and Thomas C. Schmidt. 2015. *Amplification and DRDoS Attack Defense – A Survey and New Perspectives.* Technical Report arXiv:1505.07892. Open Archive: arXiv.org. http://arxiv.org/abs/1505.07892