Packet Content Filter for BGP FlowSpec

Yong Cui, Yujia Gao

Tsinghua University, Beijing Zhongguancun Laboratory

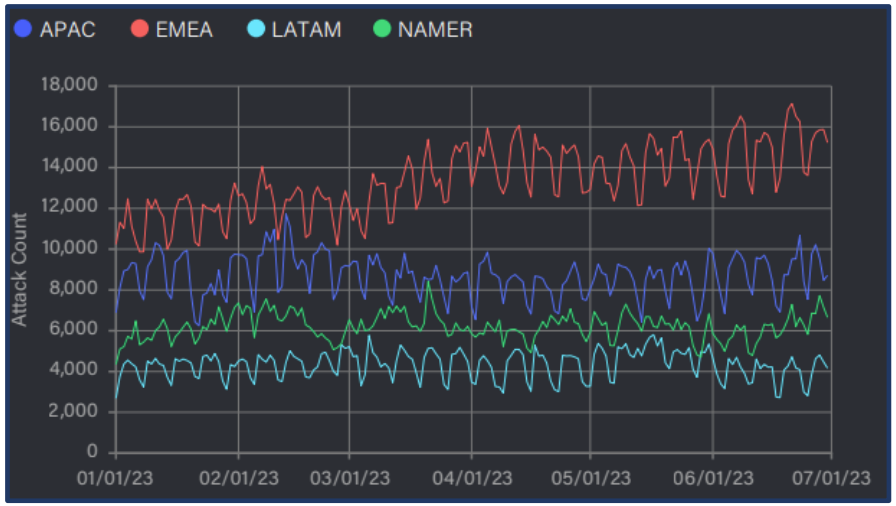
Background - DDoS Attack Trends

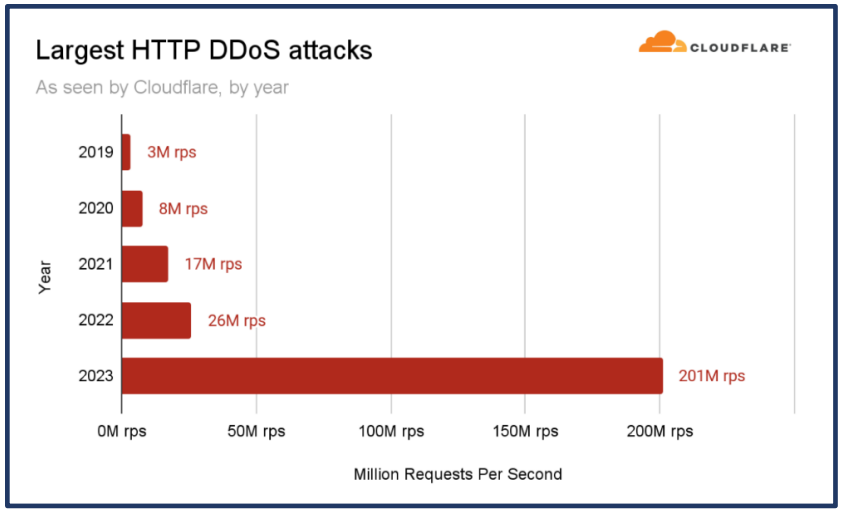
More Frequent

In the first six months of 2023, there are 7.9 million DDoS attacks happened. This represents a significant increase of 31% compared to the same period in the previous year.

Hyper-Volumetric

In 2023, the largest DDoS attack are recorded with an 201 million requests per second (rps). This attack did not just break the previous year's record —being nearly eight times larger than the largest attack observed in 2022.



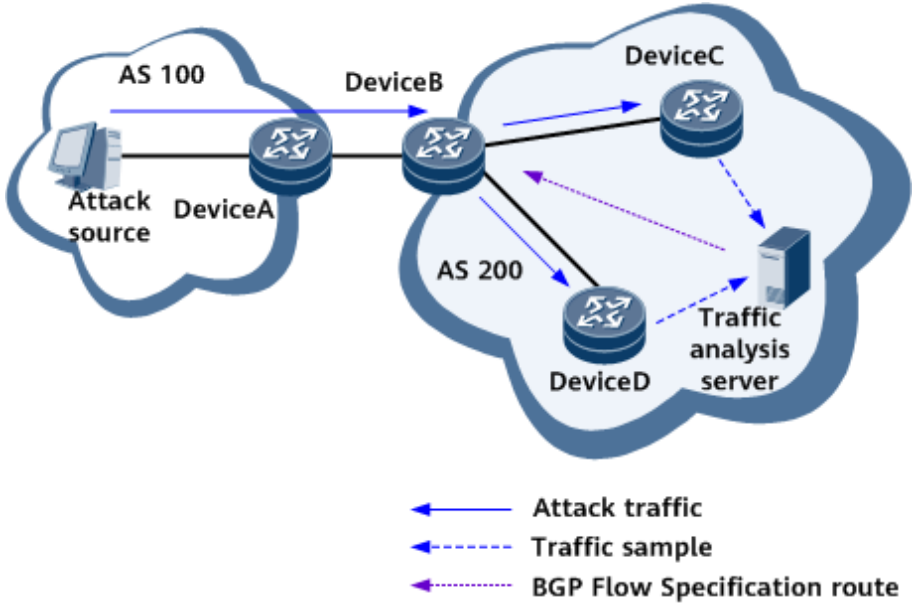


Why we use BGP flowspec?

Increased Attack Traffic and Cleanup Costs: Attack traffic is increasing but cleaning centers are costly to build. So we need to increase the filtering capability of the router to reduce the pressure in the cleaning center.

- ACL filtering: ACL is challenging due to the need for manual configuration, resulting in slow response times and the high risk of negative impact on business operations.
- BGP FlowSpec filtering: It enables the distribution of traffic filter policies (traffic filters and actions) via BGP. It can be used to rapidly spread filtering rules to mitigate DDoS attacks.

The flexibility of BGP flowspec makes it as an effective DDoS defense technology to responding to the evolving security threats.

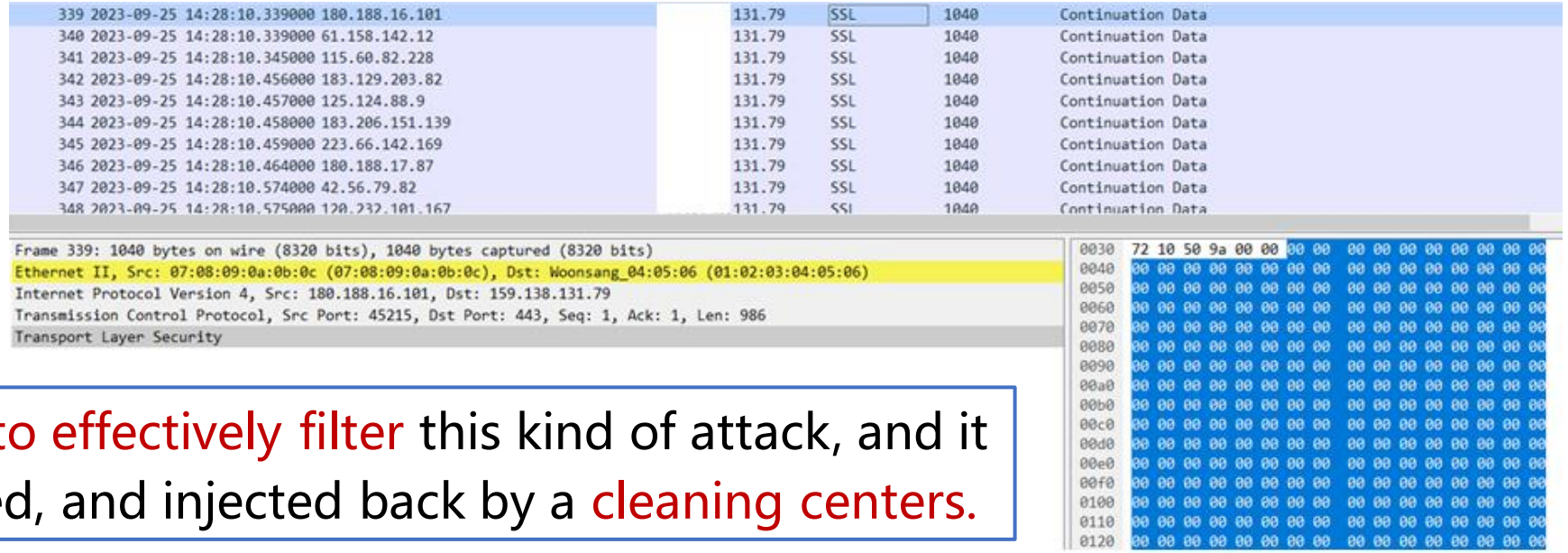


Problem Statement

Although BGP flowspec can provide the ability to filter traffic through n-tuples, in pre-defined fields such as IP protocol, IP prefix and port number, etc, it still cannot filter traffic well in the face of some types of volumetric DDoS.

Example：An ACK Flood carpet bombing attack captured on the operation network.

- It is characterized by a large packet and the destination port is 443, the packet payload content has a fixed characteristic (all zeros).



Existing flowspec is unable to effectively filter this kind of attack, and it can only be diverted, cleaned, and injected back by a cleaning centers.

Problem Statement

It is necessary to add a new flowspec filters for traffic with constant packet content.

Some Surveys:

- The latest enhancements in IP router forwarding plane filter implementations support matching at any location within the packet header or content. This capability allows for the precise matching of attack traffic signatures and can be combined with traditional n-tuple filtering criteria to effectively mitigate DDoS attacks and minimize false positives.
- An existing draft: draft-khare-idr-bgp-flowspec-payload-match-08
  - 2018.7-2021.9
  - Make some more router friendly changes
  - Give continuous adaptation with FSv2

BGP FlowSpec Packet Content Filter

New Flowspec Component：Packet Content Filter，Type TBD

Encoding: <type (1 octet), [value]+>

- value: < offset-type (4 bits), offset-value(2 octets), content-length, content-value >

Offset value from corresponding type

Value	Description of Offset Type
0	IP Header
1	IP Header Data
2	Data within TCP/UDP

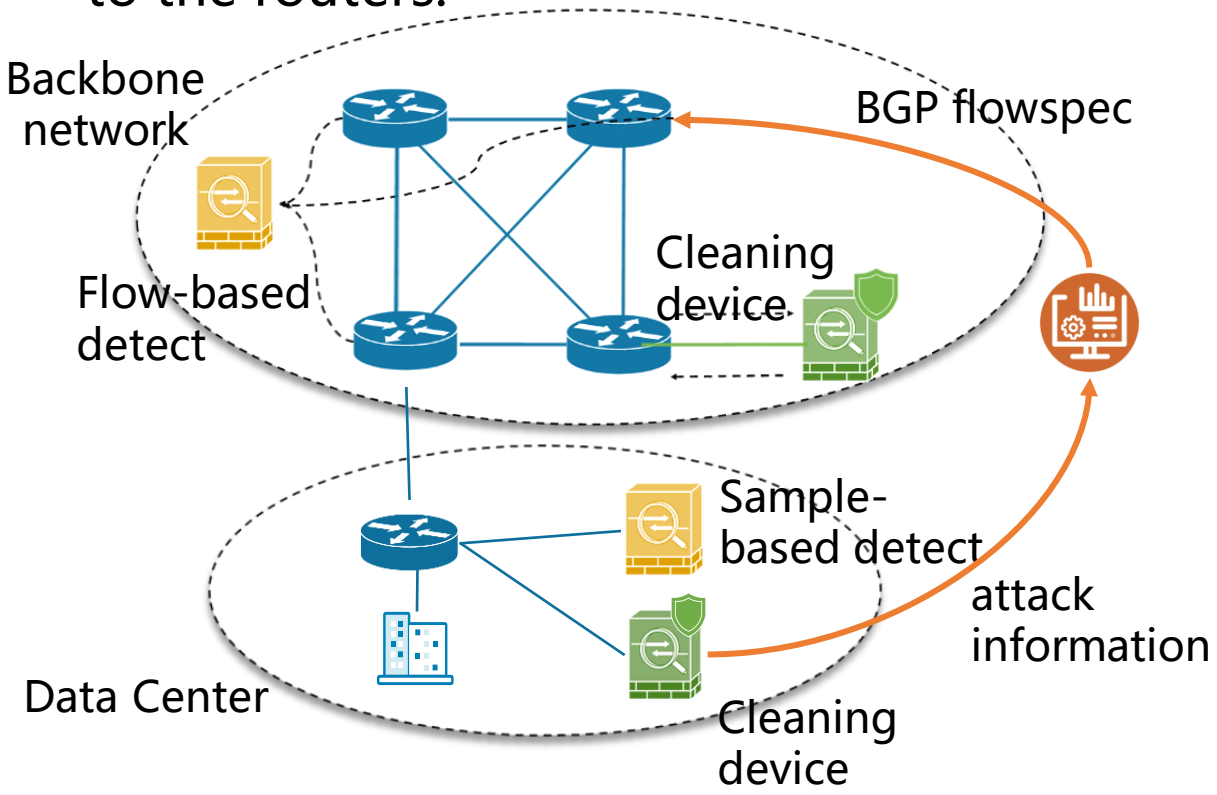
Example：Match IP packets containing the string '10101100' starting 100 bytes after the TCP header.

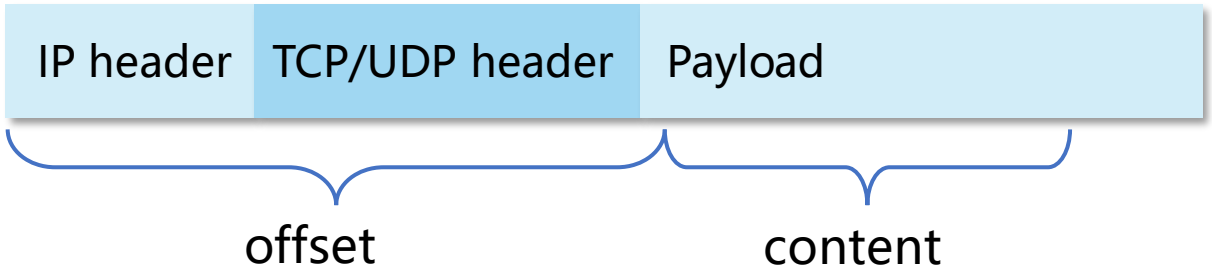
- value：<01, 64, 08， {ac ,ff}>

Use Case

A data center in backbone network suffered an ACK flood attack with many packets containing identical content characteristics.

The cleaning device generate flowspec filter rules based on the attack information (type 1, offset 0, packet content 01010000, and mask 00000000) and send BGP flowspec instructions to the routers.





BGP flowspec can significantly reduce cleaning center overheads.

Future Work - FSv1 & FSv2

In this draft, we have designed the filter only for FSv1, and we welcome suggestions for further modifications.

In the future work, we will try to combine the packet content filter with FSv2.

Table 2 IP SubTLV Types for IP Filters

SubTLV -type	Definition	DDOS support	
1	IP Destination prefix		FSv1
2	IP Source prefix		
3	IPv4 Protocol / IPv6 Upper Layer Protocol		
4	Port		
5	Destination Port		
6	Source Port		
7	ICMPv4 type / ICMPv6 type		
8	ICMPv4 code / ICPv6 code		
9	TCP Flags		
10	Packet length		
11	DSCP		
12	Fragment		
13	Flow Label		FSv2
14	TTL		
15-63	reserved for IP Extensions (standards action)		

IPv4 Extended Communities (Type 0x80) 2 byte AS,

Value	Description	Name	Reference
0x01	Flow Spec Action Chain	ACO	[This document]
0x06	Flow spec traffic-rate-byte	TRB	[RFC8955]
0x07	Flow spec traffic-action	TAIS	[RFC8955]
0x08	Flow spec rt-redirect AS-2 octet format	RDIP	[RFC8955]
0x09	Flow spec traffic-remarking	TM	[RFC8955]
0x0C	Flow Spec Traffic-rate-packets	TRP	[RFC8955]

FSv1：12 match conditions；5 actions

FSv2：14 match conditions（Flow Label、TTL）；6 actions

Thanks!

Contact information: gaoyj@zgclab.edu.cn