



Packet Content Filter for BGP FlowSpec

draft-cui-idr-content-filter-flowspec-05

Yong Cui, Tsinghua University

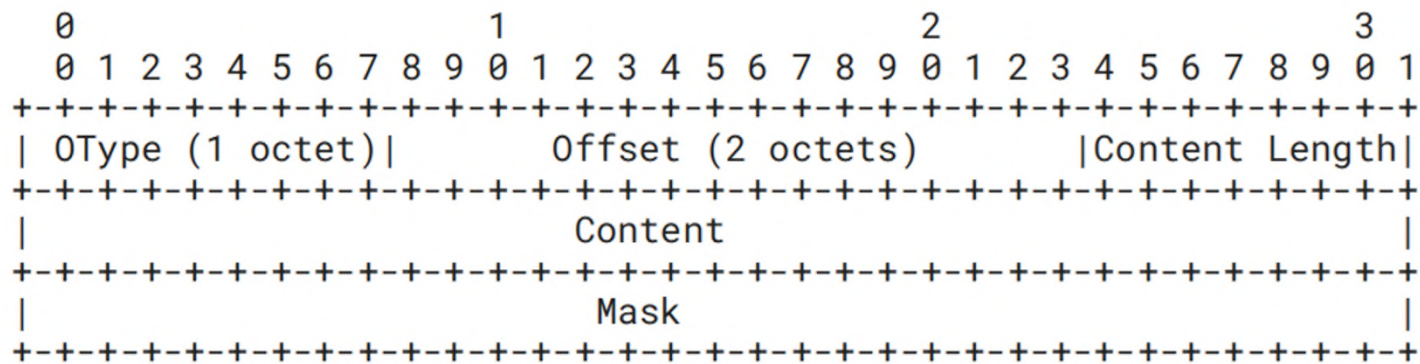
Yujia Gao, Zhongguancun Laboratory

Susan Hares, Hickory Hill Consulting

Oct 26th, 2026

Updated Filter Component Encoding

- Component Sub-TLV Encoding



- The Filter Family Type is 1000 for IPv4 Basic and 1100 for IPv6 Basic.
- The Packet Content Filter Component Type is 3000.

Problem Statement

- DDoS attack intensity has surged, with a record peak of **31.4 Tbps**, far beyond scrubbing centers' defense capability
- Some real world attacks captured in operator networks show fixed payload (e.g., ACK flood, SSDP attack [1])

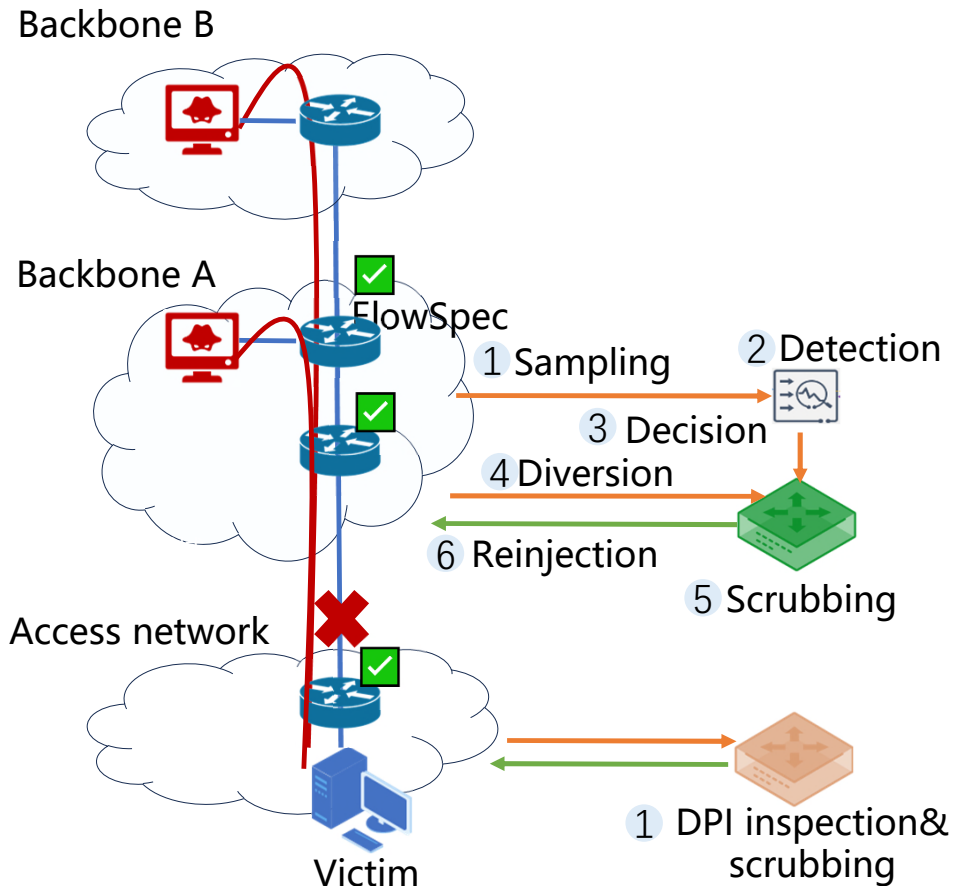
[illegible]

Protocol	Length	Acknowledgment number (raw)	Identification	Info	
UDP	434		0x0000 (0)	54452 + 3703	Len=388
UDP	379		0xe694 (5902)	47558 + 3703	Len=333
UDP	446		0x0000 (0)	38607 + 3703	Len=400
UDP	497		0xe77f (2828)	39866 + 3703	Len=451
UDP	434		0xc702 (5094)	37332 + 3703	Len=388
ICMP	164		0x05cc (1484)	Destination	nreachable
UDP	536		0x0000 (0)	52468 + 3703	Len=490
ICMP	164		0xf54c (6279)	Destination	nreachable
ICMP	164		0x1cf7 (7415)	Destination	nreachable
UDP	368		0x0000 (0)	43325 + 3703	Len=322
ICMP	164		0xc742 (5101)	Destination	nreachable
UDP	369		0x5179 (2085)	58526 + 3703	Len=323
UDP	382		0x0000 (0)	57379 + 3703	Len=336
UDP	550		0x87ab (3473)	32948 + 3703	Len=504
ICMP	164		0x8cb0 (3601)	Destination	nreachable
ICMP	164		0x5f6f (2443)	Destination	nreachable
ICMP	164		0x3ce1 (1558)	Destination	nreachable
UDP	474		0x0000 (0)	39775 + 3703	Len=428
UDP	483		0x0000 (0)	39775 + 3703	Len=437
UDP	322		0xad65 (1981)	53867 + 3703	Len=276
UDP	328		0xa466 (1081)	52967 + 3703	Len=283

A packet-content filter enables FlowSpec to match **stable, visible** payload patterns.

[1] <https://nsfocusglobal.com/wp-content/uploads/2023/03/2022-Global-DDoS-Attack-Landscape-Report.pdf>

Use Case



- Carpet-bombing DDoS targets changing destination IPs, making mitigation difficult and congesting access links.
- Traffic analysis finds a stable payload pattern in attack packets.
- Upstream routers use a FlowSpec content filter to block matching traffic, reducing link congestion and scrubbing load.

Considerations

- Operational considerations
 - Deploy payload filtering only at controlled locations
 - Enable only on devices that support content parsing and sufficient rule scale
 - Match on the decapsulated inner IP packet to avoid offset ambiguity with MPLS or tunnels
- **Security considerations**
 - Accept rules only from trusted peers and restrict their propagation scope
 - Combine payload filter with other conditions to reduce false positives
 - Ignore unsupported rules locally and limit update rates to keep BGP stable
 - Apply local policy at each receiving device to authorize rule installation
- Scalability considerations
 - Limit rules to a small set of high-value entries
 - Use FSv2 rule ordering to limit the scope of traffic inspected
 - Restrict propagation scope to avoid inter-domain scale issues

Thanks!

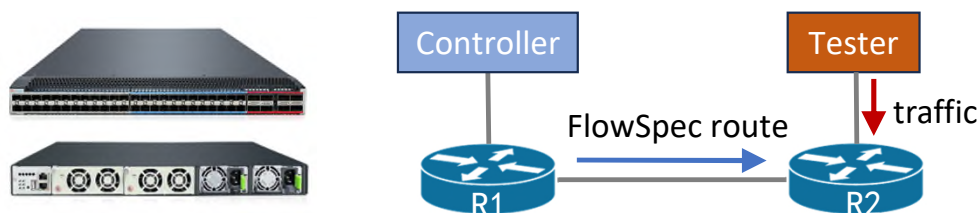
Contact information: gaoyj@zgclab.edu.cn

Current Draft Status

- 2024/3 first proposed packet content filter @IETF 119
- 2024/5 join FSv2 design team work
- 2024/6 conduct software router function development and testbed validation
- 2024/7-2025/10 introduce the latest work @IETF 120/121/124
- 2026/2 update scaling, operational, security considerations @Interim meeting
- 2026/5 Update draft @Interim meeting
- 2026/10 Update draft and adoption call @Interim meeting

Hardware Deployment

- Testbed: Sino SR3600 switch by ASIC switching chips



```

SR3600#diagnose
Enter diagnose mode, please input password:
%Warning: Executing certain commands may cause abnormal or traffic crash.
If you need to execute such kinds of commands, please contact
the technical engineer, and use it carefully under the guidance
of the technical engineer.
SR3600(diagnose)#
SR3600(diagnose)#task she
SR3600(diagnose)#task shell srosdriver

**** enter srosdriver shell ****
use "help" for help information

# show_bgp_flow_acl
rule_id desc dir group_id entry_id pri valid_flag
-----
2119 bgp-flowspec Ingress 2 2119 500000 valid
Rule used total: 1
return value = 0x1aa5f98
#
  
```

- FlowSpec rules are installed as ACL entries
- Payload matching is implemented via UDF and TCAM in hardware
- Rules are implemented in ASIC
- Traffic statistics confirm effective packet dropping

```

CTC_CLI(ctc-sdk)# show acl entry-info entry 2119 detail
No. ENTRY_ID GROUP_ID HW E_PRI G_PRI TYPE INDEX ACTION SIZE
-----
1 2119 2 Y 500000 2 Tcam-Flex-100 1280 Discard 320

#ENTRY_ID: 2119 Table:
--DsProgrammingAc1Tcam2 :1280
--DsAc12Ingress :1280
--DsProgrammingAc1Tcam3 :1280
--DsAc13Ingress :1280

Key:
-----
UDF : 00010203040500000000000000000000/FFFFFFFF00000000000000000000
L3-TYPE : 2/0xFF
IP-PROTOCOL : 6/0xFF

Action:
-----
DISCARD : G Y R
  
```

Interface	Port	Line	Speed	Mode	FlowSpec	Drop	Discard	Size
25gigaethernet	1/0/44	Down	Full/25G	0.00%	0.00%	0	0	0
25gigaethernet	1/0/45	Up	Full/10G	10.03%	0.00%	0	0	0
25gigaethernet	1/0/46	Down	Full/25G	0.00%	0.00%	0	0	0
25gigaethernet	1/0/47	Up	Full/10G	0.00%	0.00%	0	0	0
25gigaethernet	1/0/48	Down	Full/25G	0.00%	0.00%	0	0	0
100gigaethernet	1/1/1	Down	Full/100G	0.00%	0.00%	0	0	0
100gigaethernet	1/1/2	Down	Full/100G	0.00%	0.00%	0	0	0
100gigaethernet	1/1/3	Down	Full/100G	0.00%	0.00%	0	0	0

Test Results and Device Features

- Sino SR3600 switch — ASIC-based content matching Forwarding Test
 - 100Gbps attack traffic
 - Average store-and-forward latency: 2.145 μ s

No.	Time	Source	Protocol	Length	Info
9	2026-08-17 09:11:41.744283572	62.1.1.2	UDP	256	62.1.1.2 → 61.1.1.2
10	2026-08-17 09:11:41.744283572	62.1.1.2	UDP	256	62.1.1.2 → 61.1.1.2
11	2026-08-17 09:11:41.744283572	62.1.1.2	UDP	256	62.1.1.2 → 61.1.1.2
12	2026-08-17 09:11:41.744283572	62.1.1.2	UDP	256	62.1.1.2 → 61.1.1.2
13	2026-08-17 09:11:41.744283572	62.1.1.2	UDP	256	62.1.1.2 → 61.1.1.2
14	2026-08-17 09:11:41.744283572	62.1.1.2	UDP	256	62.1.1.2 → 61.1.1.2

```
R2#show bgp ipv4 flowspec route
Total 1 route(s)

Instance: public_
Network      Neighbor      NextHop
>+ Proto=6, Content:1/2/0/cb427a3b73c4/ffffffffffff
4.4.4.4      0.0.0.0

R2#show bgp ipv4 flowspec route Proto=6, Content:1/2/0/cb427a3b73c4/fffff

Instance      : public_
Network       : Proto=6, Content:1/2/0/cb427a3b73c4/ffffffffffff
Neighbor      : 4.4.4.4 (4.4.4.4)
NextHop       : 0.0.0.0
Status        : Best
               : Selected
               : In system (0d:0h:1m:33s)
Origin        : IGP
Local preference : 100
MED           : 0
Preferred value : 0
AS-path       : as-seq<300>
Extended Community : Redirect-IP<47.1.1.1>
Advertised neighbors : None
```

Summary	Settings	Tracking and Latency	All
Rx L1 Rate (bps) 99,999,999,840.000			
Store-Forward Avg Latency (ns) 2,145			

- Nokia SR OS — supports payload matching on supported FP4-based line cards

- pattern conditional drop

Traffic can be dropped when it is based on a pattern found in the packet header or data payload. The pattern is defined by an expression, mask, offset type, and offset value match in the first 256 bytes of a packet.

The pattern expression is up to 8 bytes long. The **offset-type** command identifies the starting point for the offset value and the supported offset-type command options are:

- layer-3: layer 3 IP header
- layer-4: layer 4 protocol header
- data: data payload for TCP or UDP protocols
- dns-qtype: DNS request or response query type

[2] <https://documentation.nokia.com/sr/25-10/7x50-shared/router-configuration/filter-policies-router-configuration.html>