IETF Hackathon - Extending BGP FlowSpec with Packet Content Matching

Yujia Gao, Zhongguancun Lab
Guangchen Song, China Mobile
Mingzhe Xing, Zhongguancun Lab

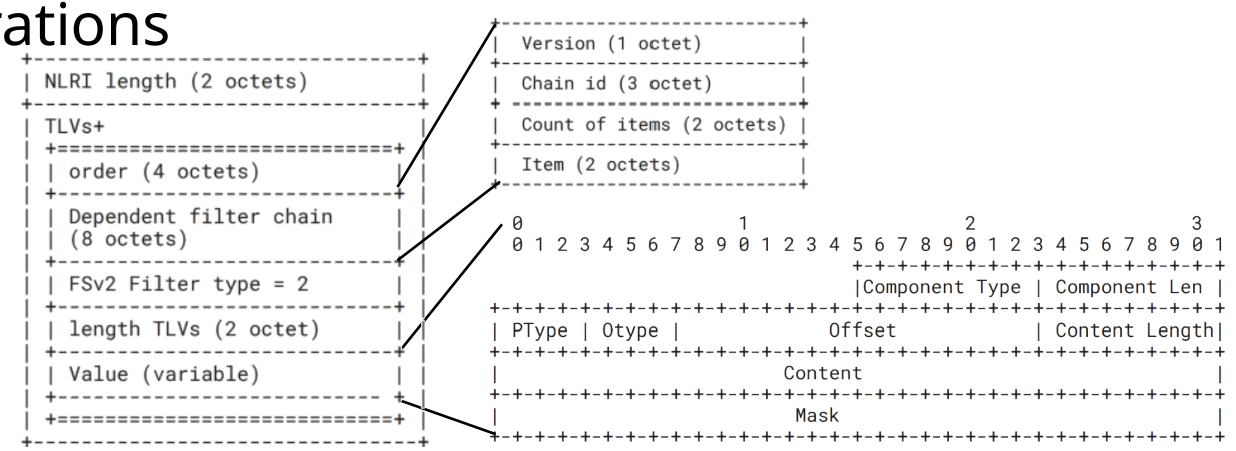
IETF 125
Shenzhen, China

Hackathon Plan

- Background
  - Packet content matching is increasingly needed in practice
  - Current FlowSpec only supports header-based matching
  - Aligns with exploring FSv2 in IDR WG
- Objective
  - Implement the packet content matching on network devices
  - Demonstrate feasibility and deployability
- Relevant drafts
  - draft-cui-idr-content-filter-flowspec

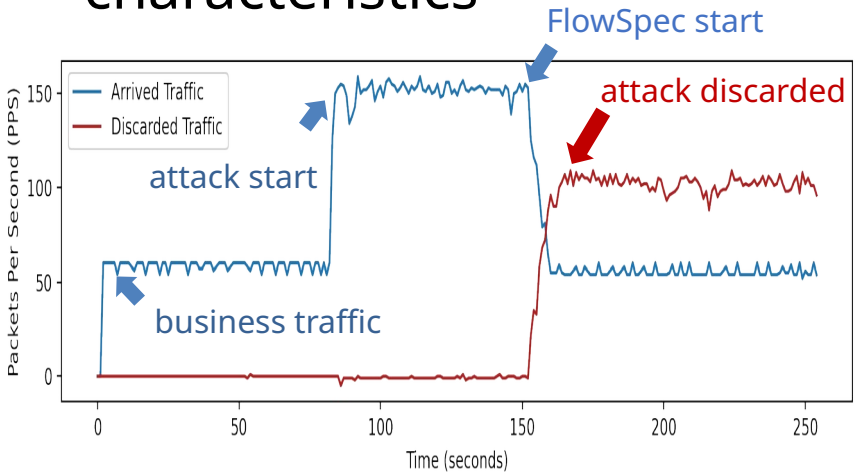
What got done

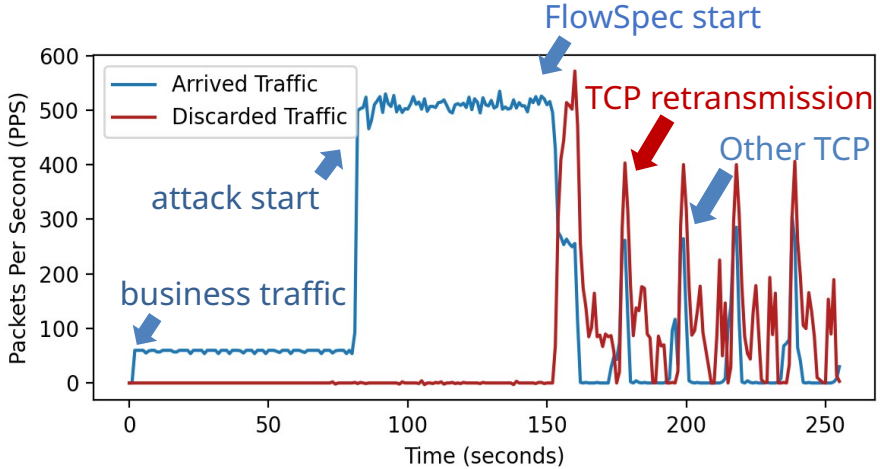
- Defined Filter encoding and ordering
- Implemented and validated in open-source software
- Deployed on commercial hardware
- Summarized operational, scalability, and security considerations



Implementation

- Testbed: OpenBGPD-8.3-portable, FRRouting-10.2-dev
- Scenario: Defend DDoS attacks with specific payload characteristics

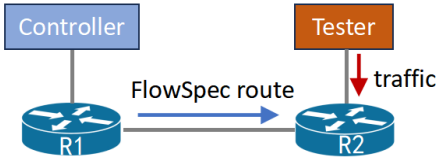




https://github.com/Flowspec-extension/Packet-Content-Filter-Demo

Hardware Deployment

- Testbed： Sino SR3600 switch by ASIC switching



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

```
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

#
```

```
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:
 --DsProgrammingAclTcam2            :1280
 --DsAcl2Ingress                    :1280
 --DsProgrammingAclTcam3            :1280
 --DsAcl3Ingress                    :1280

Key:
-----------------------------------
UDF               : 000102030405000000000000000000000/FFFFFFFFFFFF00000000000000000000
L3-TYPE           : 2/0xF
IP-PROTOCOL       : 6/0xFF

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

```
25gigaethernet 1/0/44       Down   Full/25G      0.00%   0.00%   0          0
25gigaethernet 1/0/45       Up     Full/10G      10.03%  0.00%   0          0
25gigaethernet 1/0/46       Down   Full/25G      0.00%   0.00%   0          0
25gigaethernet 1/0/47       Up     Full/10G      0.00%   0.00%   0          0
25gigaethernet 1/0/48       Down   Full/25G      0.00%   0.00%   0          0
100gigaethernet 1/1/1       Down   Full/100G     0.00%   0.00%   0          0
100gigaethernet 1/1/2       Down   Full/100G     0.00%   0.00%   0          0
100gigaethernet 1/1/3       Down   Full/100G     0.00%   0.00%   0          0
```

What we learned

- Reduce traffic processing cost, but requires careful deployment
- Only can be deployed on devices with payload parsing capability
- UDF and TCAM resources may limit rule scale
- More guidance is needed on encoding, ordering, and operational practices
- Further multi-device interoperability validation is still needed

Wrap Up

Team members:

Yujia Gao, Zhongguancun Lab

Guangchen Song, China Mobile

Mingzhe Xing, Zhongguancun Lab

First timers @ IETF/Hackathon

Contact:
gaoyj@zgclab.edu.cn

GitHub Demo

https://github.com/Flowspec-extension/Packet-Content-Filter-Demo

Related Drafts

draft-cui-idr-content-filter-flowspec
draft-hares-idr-fsv2-more-ip-filters