IETF94 IDR WG

BGP Flowspec Interoperability Test @ Interop Tokyo 2015 ShowNet

ShowNet NOC Team member
Shuichi Ohkubo
Presenter :Cisco as ShowNet contributor

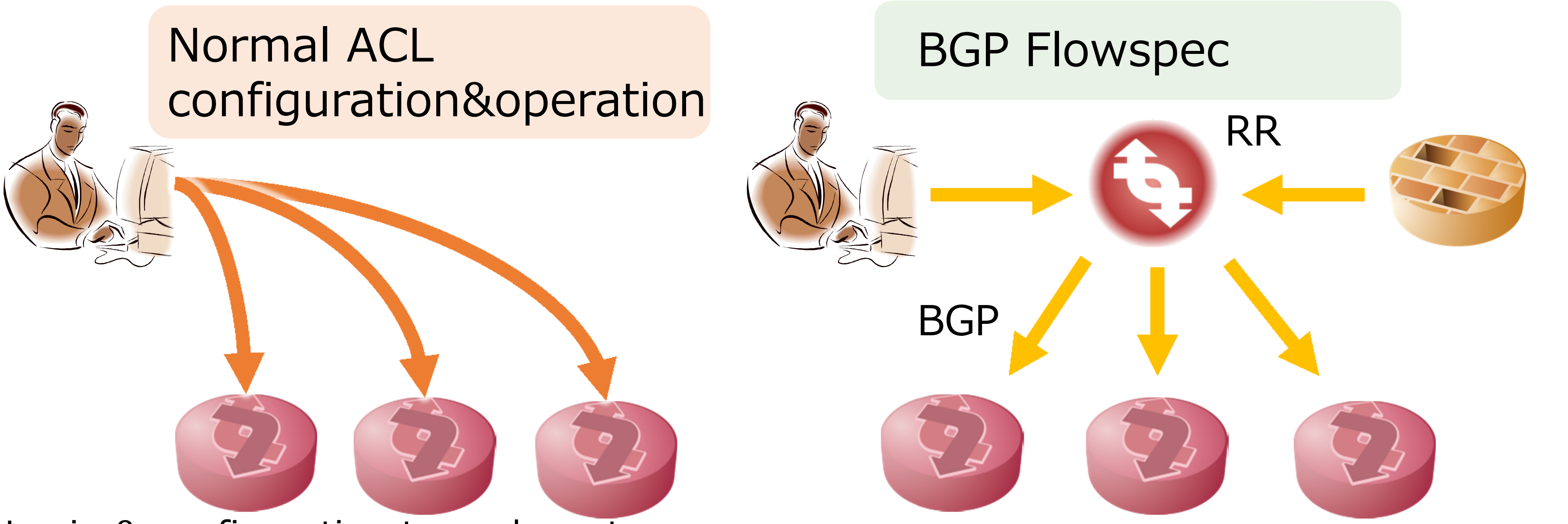
show net
Scratch and Re-build the Internet

Interop Tokyo 2015

- 8 th – 12 th June 2015
- The Number of Visitors:136,341
- Number of Exhibitors:486
- ShowNet: Interoperability test of hot topic (BGPflowspec,VXLAN/EVPN,RPKI,IEEE1588 and so on)

BGP Flowspec(RFC5575)

- Distributes ACL configuration to network routers by BGP



Normal ACL configuration&operation

BGP Flowspec

RR

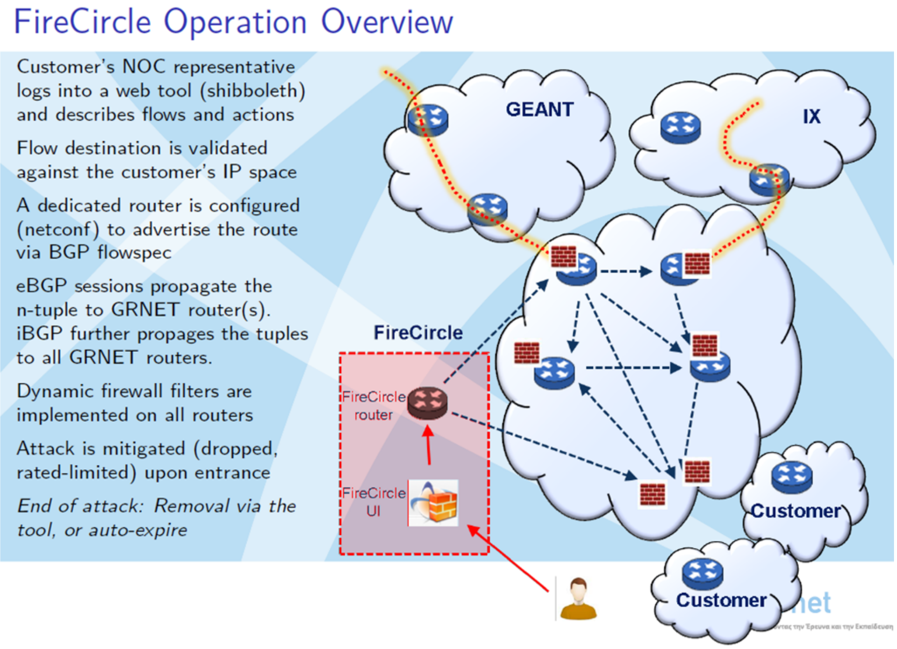
BGP

Login & configuration to each router
Too much work :(

Easy to work together with security appliance

Use case

GRNET



FireCircle Operation Overview

Customer's NOC representative logs into a web tool (shibboleth) and describes flows and actions

Flow destination is validated against the customer's IP space

A dedicated router is configured (netconf) to advertise the route via BGP flowspec

eBGP sessions propagate the n-tuple to GRNET router(s). iBGP further propages the tuples to all GRNET routers.

Dynamic firewall filters are implemented on all routers

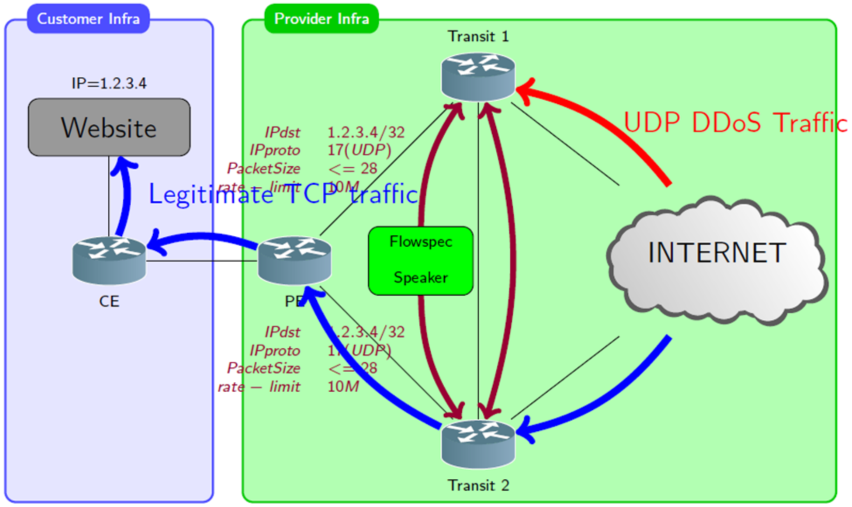
Attack is mitigated (dropped, rated-limited) upon entrance

End of attack: Removal via the tool, or auto-expire

https://tnc2012.terena.org/core/presentation/41

NEO TELECOMS

Real life architecture

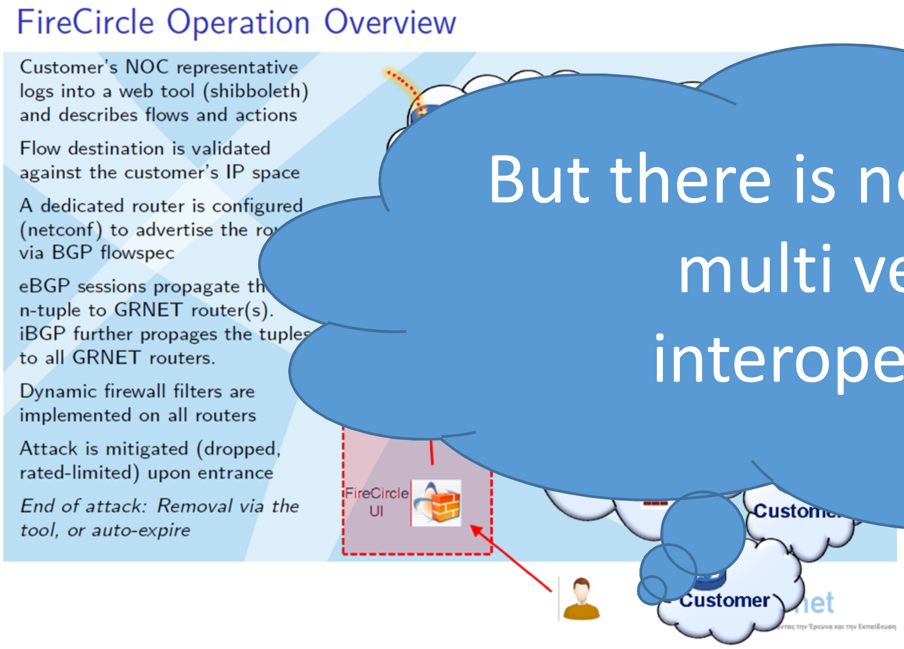


http://media.frnog.org/FRnOG_18/FRnOG_18-6.pdf

show.net
Scratch and Re-build the Internet

Use case

GRNET



FireCircle Operation Overview

Customer's NOC representative logs into a web tool (shibboleth) and describes flows and actions

Flow destination is validated against the customer's IP space

A dedicated router is configured (netconf) to advertise the ro via BGP flowspec

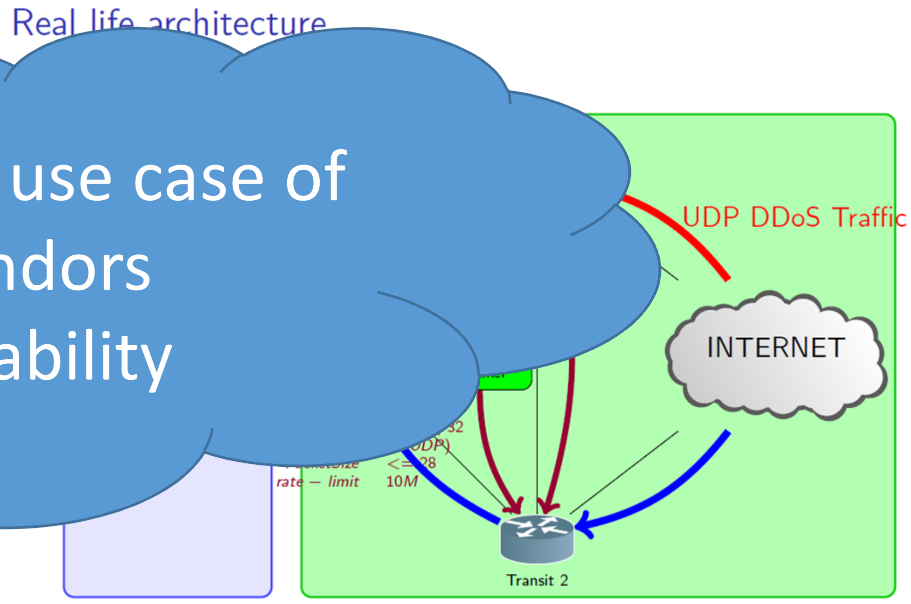
eBGP sessions propagate th n-tuple to GRNET router(s). iBGP further propages the tuples to all GRNET routers.

Dynamic firewall filters are implemented on all routers

Attack is mitigated (dropped, rated-limited) upon entrance

End of attack: Removal via the tool, or auto-expire

NEO TELECOM



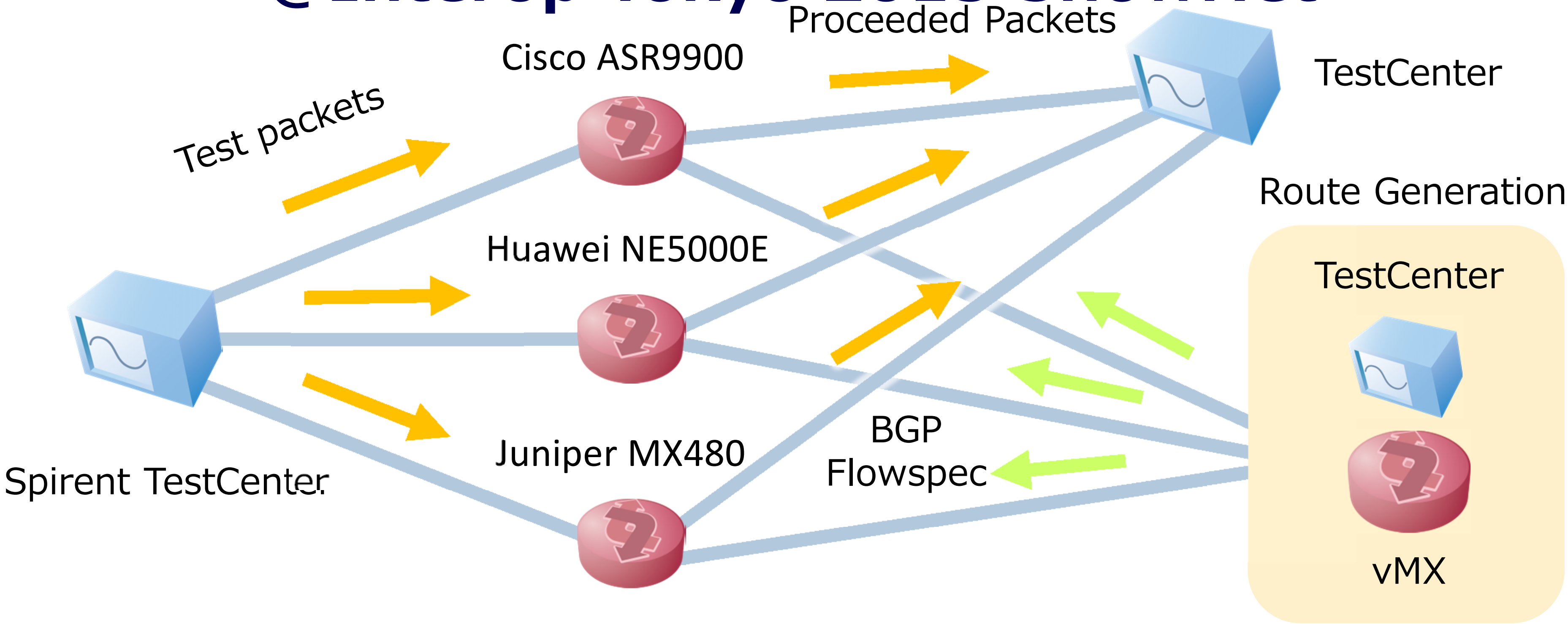
Real life architecture

But there is no use case of multi vendors interoperability

https://tnc2012.terena.org/core/presentation/41

http://media.frnog.org/FRnOG_18/FRnOG_18-6.pdf

Interoperability test topology @Interop Tokyo 2015 ShowNet

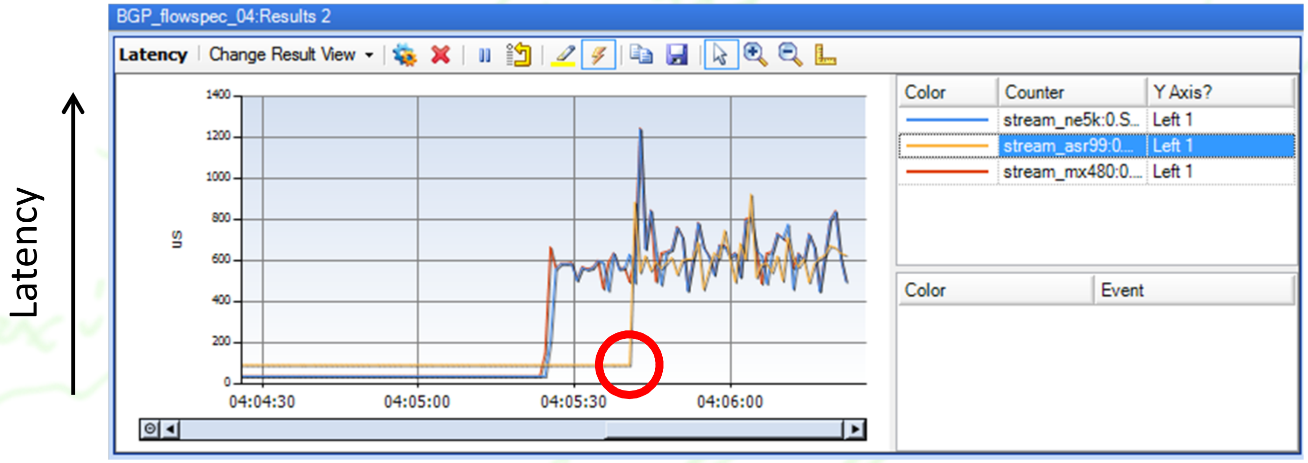


Test result BGP Flowspec Action rule

Test Item	NE5000E	ASR9900	MX480
Drop	○	○	○
Rate-limit	○	○	○
VRF Redirect	○	○	○

- Configure rate-limit=0 for Drop action
- Rate-limit: Confirmed by measuring the receiving rate to limit 100Mbps against sending 1Gbps traffic from TestCenter.
- Redirect :confirm interface counter on 3 routers and monitor latency for received packets by Spirent TestCenter

VRF Redirect

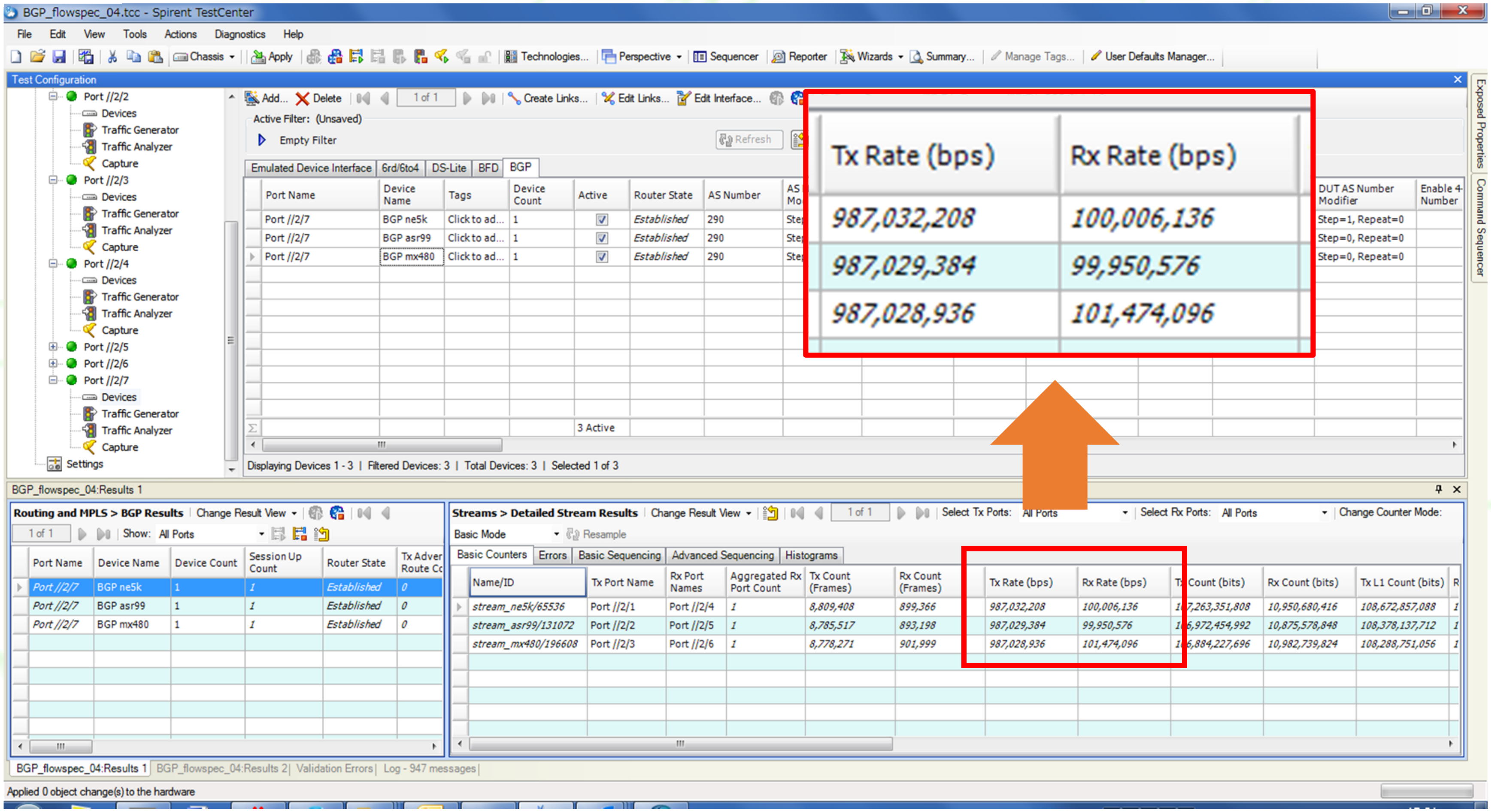


Color	Counter	Y Axis?
🟦	stream_ne5k:0.S...	Left 1
🟨	stream_asr99:0....	Left 1
🟥	stream_mx480:0....	Left 1

Color	Event

- Confirmed by measuring packets latency after redirecting (it’s not caused by degradation of forwarding functionality of the router)
- ASR99xx took about 10 sec for processing after Redirection action rule injection. In case of withdrawn, the change was immediately reflected to the forwarding process.
- It depends on BGP Next-hop Scan Timer(configurable)

Rate-limit


BGP_flowspec_04.tcc - Spirent TestCenter
File Edit View Tools Actions Diagnostics Help
Chassis Apply Technologies... Perspective Sequencer Reporter Wizards Summary... Manage Tags... User Defaults Manager...
Test Configuration
Port //2/2
Devices
Traffic Generator
Traffic Analyzer
Capture
Port //2/3
Devices
Traffic Generator
Traffic Analyzer
Capture
Port //2/4
Devices
Traffic Generator
Traffic Analyzer
Capture
Port //2/5
Port //2/6
Port //2/7
Devices
Traffic Generator
Traffic Analyzer
Capture
Settings
Add... Delete 1 of 1 Create Links... Edit Links... Edit Interface...
Refresh
Emulated Device Interface 6rd/6to4 DS-Lite BFD BGP
Exposed Properties
Command Sequencer

Active Filter: (Unsaved)

Empty Filter

Port Name	Device Name	Tags	Device Count	Active	Router State	AS Number	AS Mo	DUT AS Number Modifier	Enable 4-Number
Port //2/7	BGP ne5k	Click to ad...	1	☑	*Established*	290	Ste	Step=1, Repeat=0	
Port //2/7	BGP asr99	Click to ad...	1	☑	*Established*	290	Ste	Step=0, Repeat=0	
Port //2/7	BGP mx480	Click to ad...	1	☑	*Established*	290	Ste	Step=0, Repeat=0	
				3 Active					

Displaying Devices 1 - 3 | Filtered Devices: 3 | Total Devices: 3 | Selected 1 of 3

Tx Rate (bps)	Rx Rate (bps)
987,032,208	*100,006,136*
987,029,384	*99,950,576*
987,028,936	*101,474,096*

BGP_flowspec_04:Results 1

Routing and MPLS > BGP Results | Change Result View

1 of 1 | Show: All Ports

Port Name	Device Name	Device Count	Session Up Count	Router State	Tx Adver Route Co
Port //2/7	BGP ne5k	1	*1*	*Established*	*0*
Port //2/7	BGP asr99	1	*1*	*Established*	*0*
Port //2/7	BGP mx480	1	*1*	*Established*	*0*

Streams > Detailed Stream Results | Change Result View | 1 of 1 | Select Tx Ports: All Ports | Select Rx Ports: All Ports | Change Counter Mode:

Basic Mode | Resample

Basic Counters | Errors | Basic Sequencing | Advanced Sequencing | Histograms

Name/ID	Tx Port Name	Rx Port Names	Aggregated Rx Port Count	Tx Count (Frames)	Rx Count (Frames)	Tx Rate (bps)	Rx Rate (bps)	Tx Count (bits)	Rx Count (bits)	Tx L1 Count (bits)	R
stream_ne5k/65536	Port //2/1	Port //2/4	*1*	*8,809,408*	*899,366*	*987,032,208*	*100,006,136*	*1[illegible]7,263,351,808*	*10,950,680,416*	*108,672,857,088*	*1*
stream_asr99/131072	Port //2/2	Port //2/5	*1*	*8,785,517*	*893,198*	*987,029,384*	*99,950,576*	*1[illegible]6,972,454,992*	*10,875,578,848*	*108,378,137,712*	*1*
stream_mx480/196608	Port //2/3	Port //2/6	*1*	*8,778,271*	*901,999*	*987,028,936*	*101,474,096*	*1[illegible]6,884,227,696*	*10,982,739,824*	*108,288,751,056*	*1*

BGP_flowspec_04:Results 1 | BGP_flowspec_04:Results 2 | Validation Errors | Log - 947 messages

Applied 0 object change(s) to the hardware

Test result by Flow type

Flow type	NE5000E	ASR9900	MX480
Type 1 - Destination Prefix	○	○	○
Type 2 - Source Prefix	○	○	○
Type 3 - IP Protocol	○	○	○
Type 4 - Port	ー	ー	ー
Type 5 - Destination port	○	○	○
Type 6 - Source port	○	○	○
Type 7 - ICMP type	○	○	○
Type 8 - ICMP code	○	○	○
Type 9 - TCP flags	○（Different NLRI）	○（Different NLRI）	○
Type 10 - Packet length	will support in Next release	○	○
Type 11 - DSCP	○	○	○
Type 12 - Fragment	ー（Different NLRI）	○	○

Difference in NLRI format
Type9. TCP Flags

Juniper

Configure syn+ack

	Dest	/32	45.0.2.54	Src	/32	45.0.2.42	TCP Flg.	op	Bit mask	op	Bit mask
0x	01	20	2d000236	02	20	2d00022a	09	00	02	80	10

0x02 SYN

0x10 ACK

Cisco

	Dest	/32	45.0.2.54	Src	/32	45.0.2.42	TCP Flg.	op	Bit mask
0x	01	20	2d000236	02	20	2d00022a	09	81	12

0x12
ACK-SYN

Difference NLRI format
Type9. TCP Flags

ASR receives NLRI but does not work as expected

Cisco provides special firmware during the Interop period
, confirmed work as expected
(It’s already integrated in 5.3.2 as CSCuu79956)

Difference in Match bit Type9. Type12.

Juniper

op=0x80

```
  0   1   2   3   4   5   6   7
+---+---+---+---+---+---+---+---+
| e | a |  len  | 0 | 0 |not| m |
+---+---+---+---+---+---+---+---+
  1   0   0   0   0   0   0   0
```

Cisco, Huawei

op=0x81

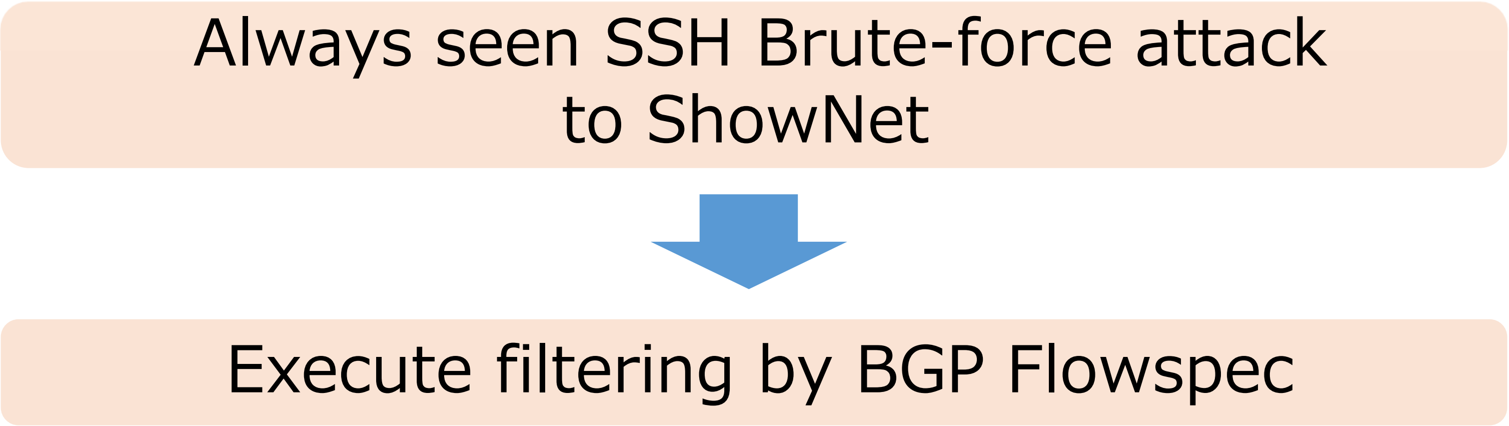
```
  0   1   2   3   4   5   6   7
+---+---+---+---+---+---+---+---+
| e | a |  len  | 0 | 0 |not| m |
+---+---+---+---+---+---+---+---+
  1   0   0   0   0   0   0   1
```

NE5000E treat as
Invalid m=0

↓

Huawei will support in
future
(support m=0)

Operation example on ShowNet



Always seen SSH Brute-force attack
to ShowNet

Execute filtering by BGP Flowspec

1. permit TCP Port 22 from specific server
2. drop 45.0.0.0/16 TCP Port 22,23

order of evaluation is important

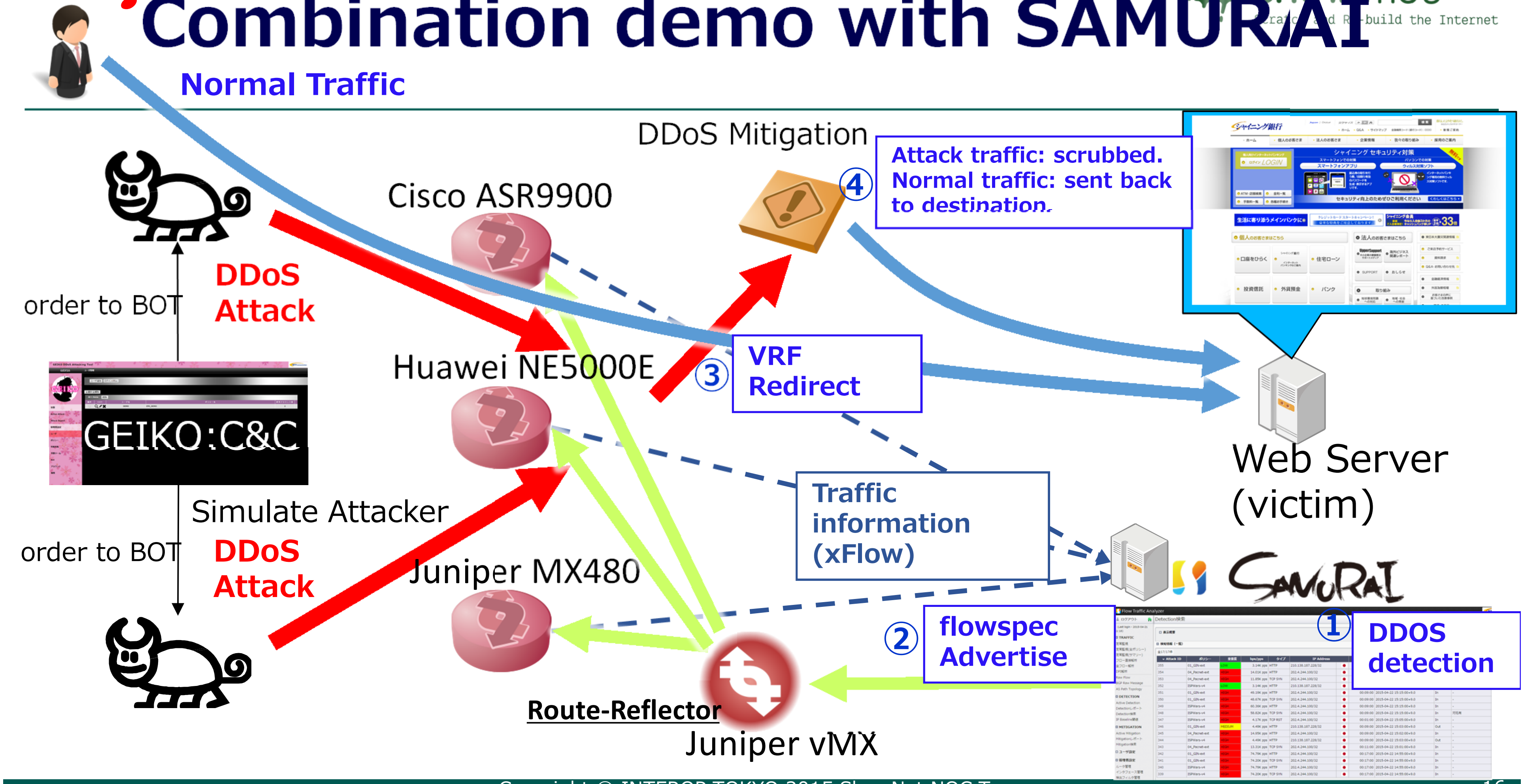
Need additional command for JUNOS

```
set routing-options flow term-order standard
```

http://www.juniper.net/documentation/en_US/junos14.2/topics/topic-map/bgp-flow-routes.html

> By default, the Junos OS uses the term-ordering algorithm defined in version 6 of the BGP flow specification draft. In Junos OS Release 10.0 and later, you can configure the router to comply with the term-ordering algorithm first defined in version 7 of the BGP flow specification and supported through RFC 5575, Dissemination of Flow Specification Routes.
>
> Best Practice: We recommend that you configure the Junos OS to use the term-ordering algorithm first defined in version 7 of the BGP flow specification draft. We also recommend that you configure the Junos OS to use the same term-ordering algorithm on all routing instances configured on a router.

♪Combination demo with SAMURAI



Normal Traffic

DDoS Mitigation

4 Attack traffic: scrubbed. Normal traffic: sent back to destination.

3 VRF Redirect

Traffic information (xFlow)

2 flowspec Advertise

1 DDOS detection

Summary

- Operator very interested in BGP flowspec
- Need more multi vendor interop report
- We confirmed 4 vendors(Cisco/Juniper/Huawei/Samurai) interoperability
- Implementation date is quite difference , therefore detail information would be needed.
- RFC5575 description sometimes heavy to understand, sample example is helpful. (m=0 is needed??)
- IETF implementation report would be welcomed.

Special Thanks

We appreciate a lot of support

TOYO Corporation

SPIRENT

CISCO

HUAWEI

NTT Communications

JUNIPER NETWORKS

show.net Scratch and Re-build the Internet

Appendix

show net
Scratch and Re-build the Internet

Software Version

- Huawei NE5000E 8.65
- Cisco ASR9900 IOS-XR 5.3.1
- Juniper MX480 Junos 15.1R1.8