

NETSCOUT®

Guardians of the Connected World

Arbor

Flowspec – Just do it ? History and Best Current Practices

LACNIC/29-FTL

Julio Arruda – Solutions Architect

Agenda

- Context
- Introduction to flowspec
- Use Case: DNS Amplification attacks mitigation
- IOT and customer x customer attacks
- Flowspec automation
- Conclusions

Context

Background considerations

The DDoS attack surface

Any part of your network or services that is vulnerable to an attack:

- The whole PI/PA IP range
- Network interfaces
- Infrastructure
- Firewall/IPS
- Servers
- Protocols
- Applications

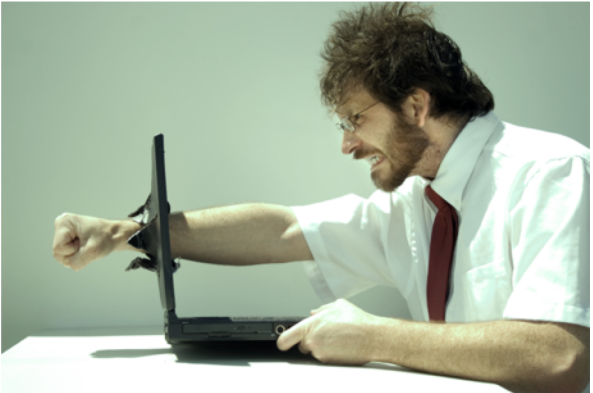


Attackers will find the weakness!

Traditional DDoS Mitigation



BGP Blackhole



S/RTBH
Source-based /
Remotely Triggered Blackhole

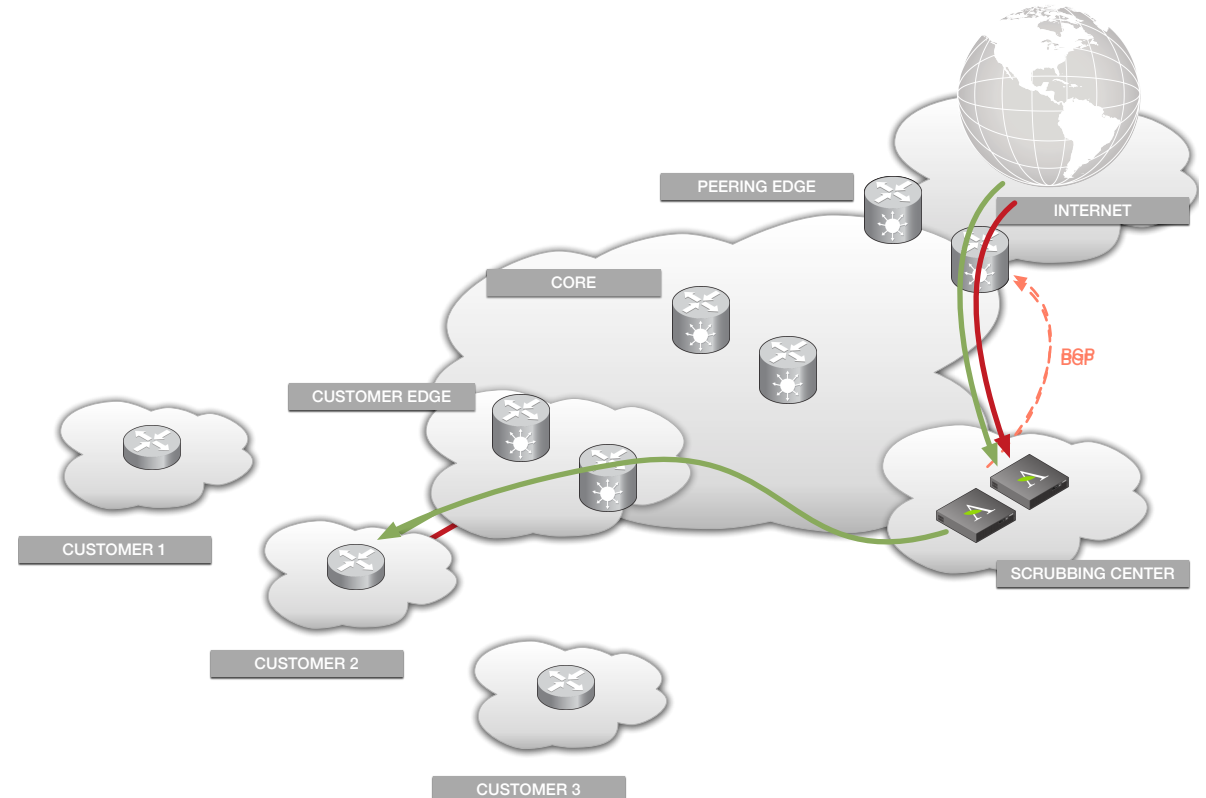


IDMS
Intelligent DDoS
Mitigation System

Traditional diversion to IDMS

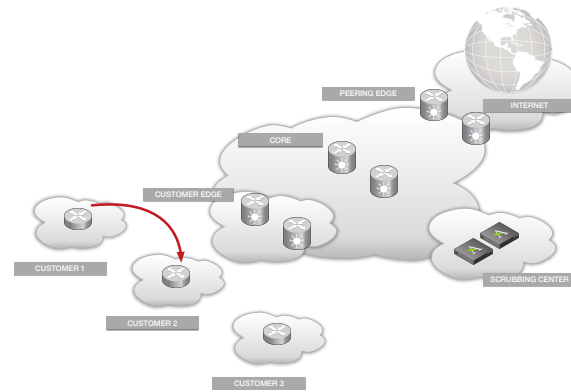
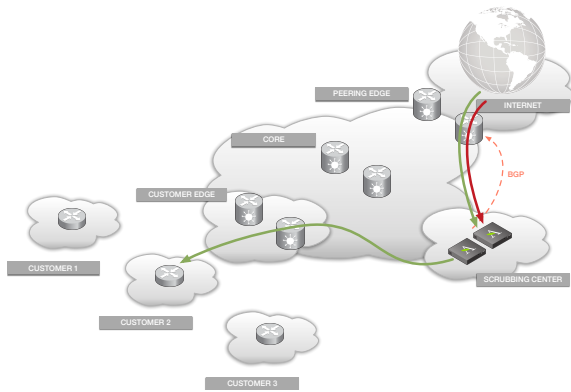
Based on BGP

- Legitimate and attack traffic received from Internet towards customer.
- BGP announcement is triggered pointing nexthop to a scrubbing device.
- Victim traffic is diverted to scrubbing center to identify and filter malicious traffic
- Clean traffic then gets returned to the victim via GRE, VRF or other method.



Limitations of traditional approach

There's always room for improvement



Protection Prefixes
10.245.26.14/32



Good for North >
South attacks

Not simple for East >
West attacks

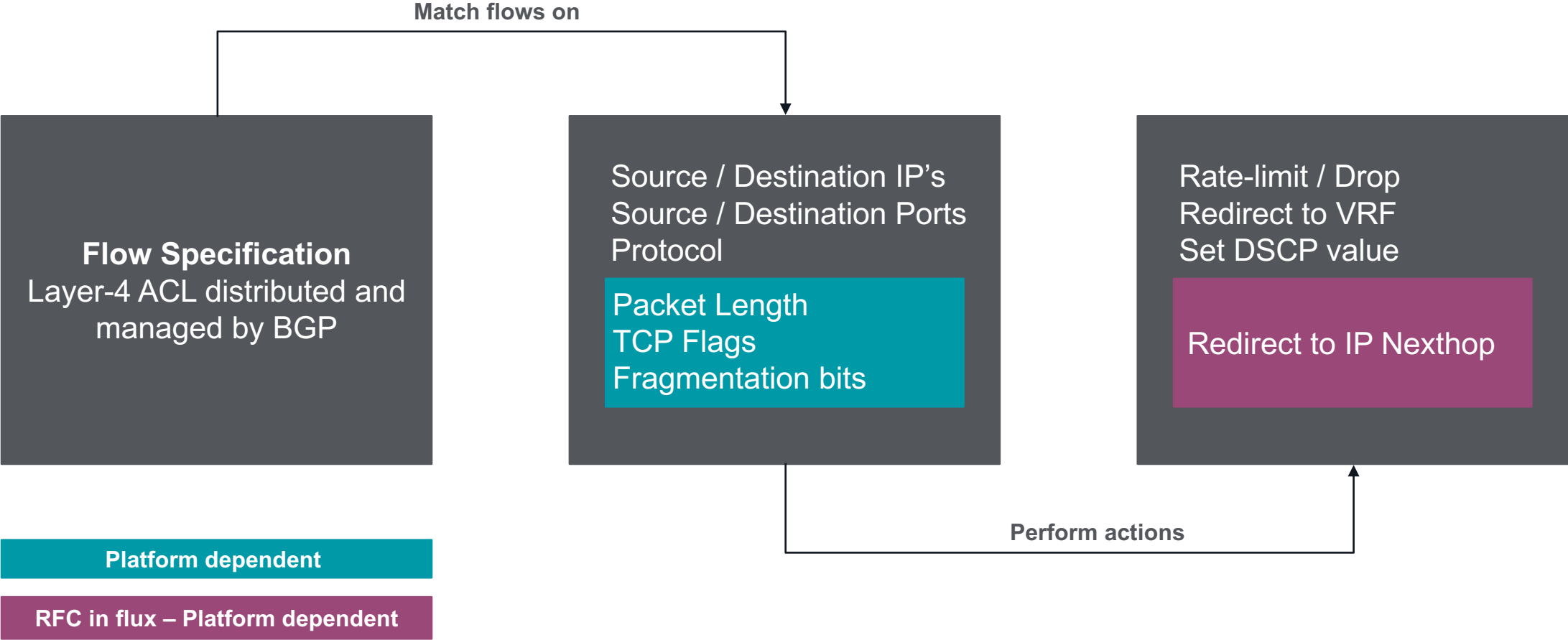
All or nothing
(based on hosts)

There's a better
way...

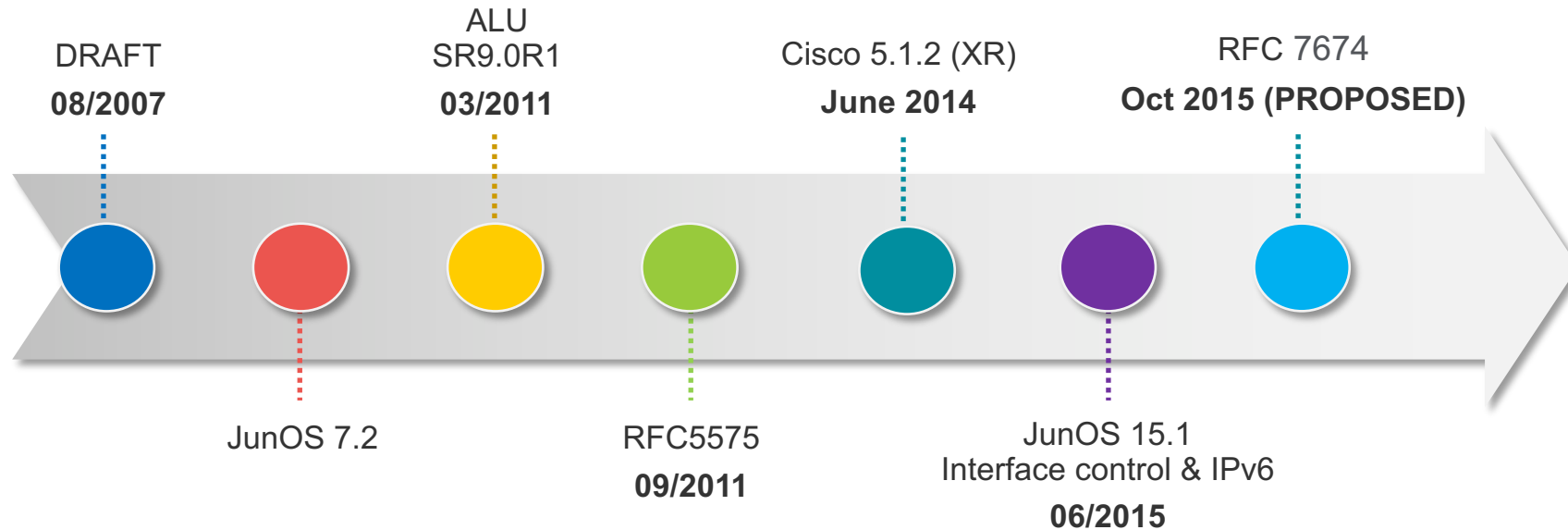
Introduction to Flowspec



What is flowspec?



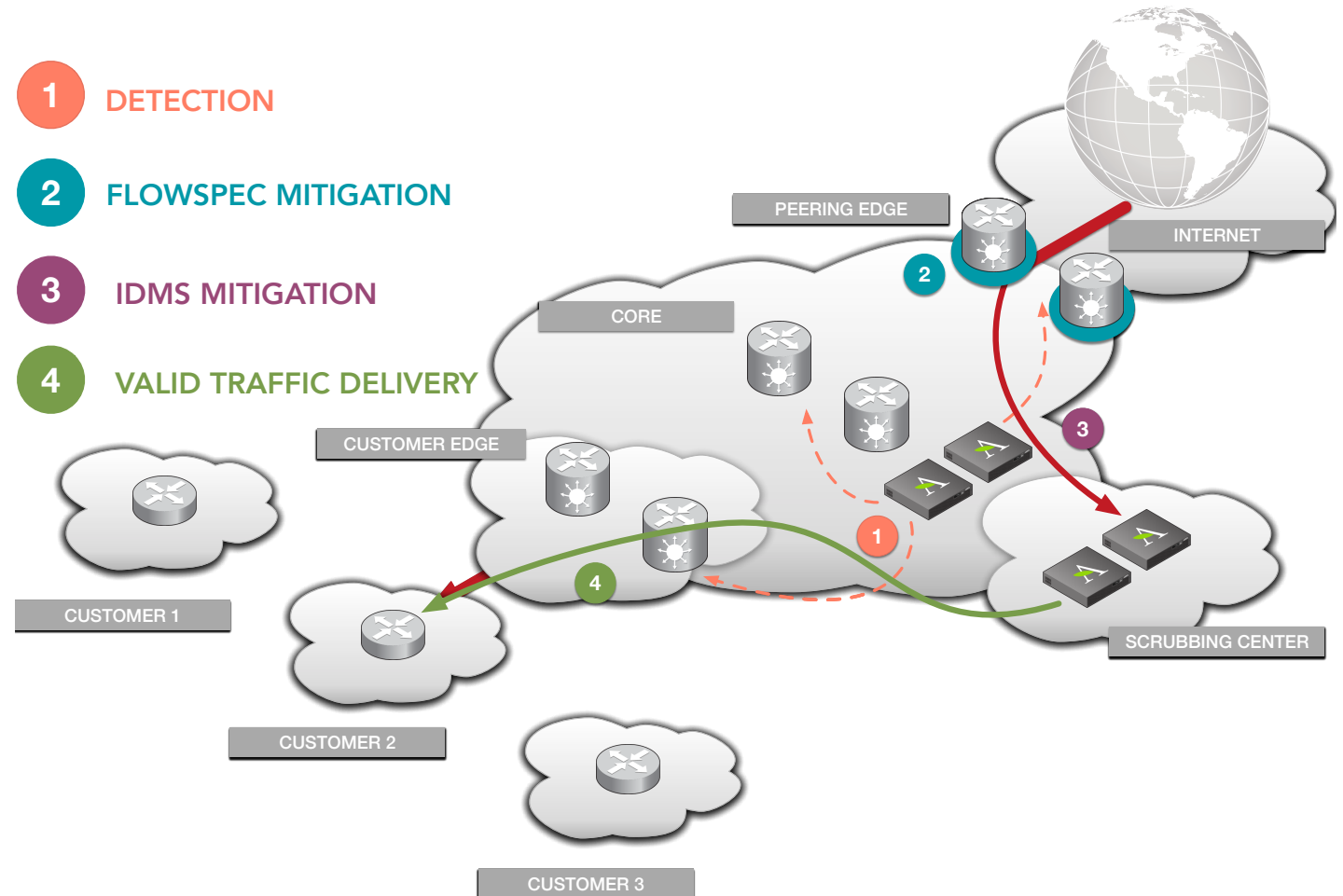
History of flowspec



Why you should use flowspec?

Volumetric mitigation

- DDoS attack directed to a customer
- Attack traffic is detected and alerted
- Flowspec starts mitigation of attack's volumetric component
- IDMS mitigation takes care of remaining attack traffic
- IDMS delivers legitimate traffic to its destination



Where you should enable flowspec?

On external facing interfaces (beware of hw/sw limitations, like sub-interfaces)

Why?

- It provides ingress policy application on a router interface.
- It essentially allows PBR (Policy Based Routing)
- It specifies where flowspec rules get applied.

Benefits

- It allows flowspec rules to be applied only to untrusted places on the network (where the attack comes from).
- Removes return-traffic complexities with scrubbing centers: **No need of GRE/VRF Clean!**
- Simplifies East > West mitigation (customer to customer attacks).

Use Case: DNS Amplification attacks mitigation

Mitigating DNS amplification – Toolset

Task: use ACLs / FlowSpec, but do not block UDP/53 completely.



What you shouldn't do? And why ?

Block traffic from UDP/53 completely

- It drops legitimate DNS replies
- It doesn't drop non-initial fragments since they don't contain UDP header
 - Amplified responses are 3-4k bytes long
 - Initial fragment is 1,500 bytes long, followed by 2-3 additional fragments
 - By blocking UDP/53 you miss **50-60%** of attack traffic



Use toolset instead!

- Run flowspec to drop initial fragments.
- Run BGP redirect to divert non-initial fragments to IDMS
- Let IDMS Invalid packets take care of non-initial fragments
- Things to keep in mind:
 - Requires IDMS capacity around **50-70%** of attack size (bps)
 - Test fragmentation bitmask before use them.

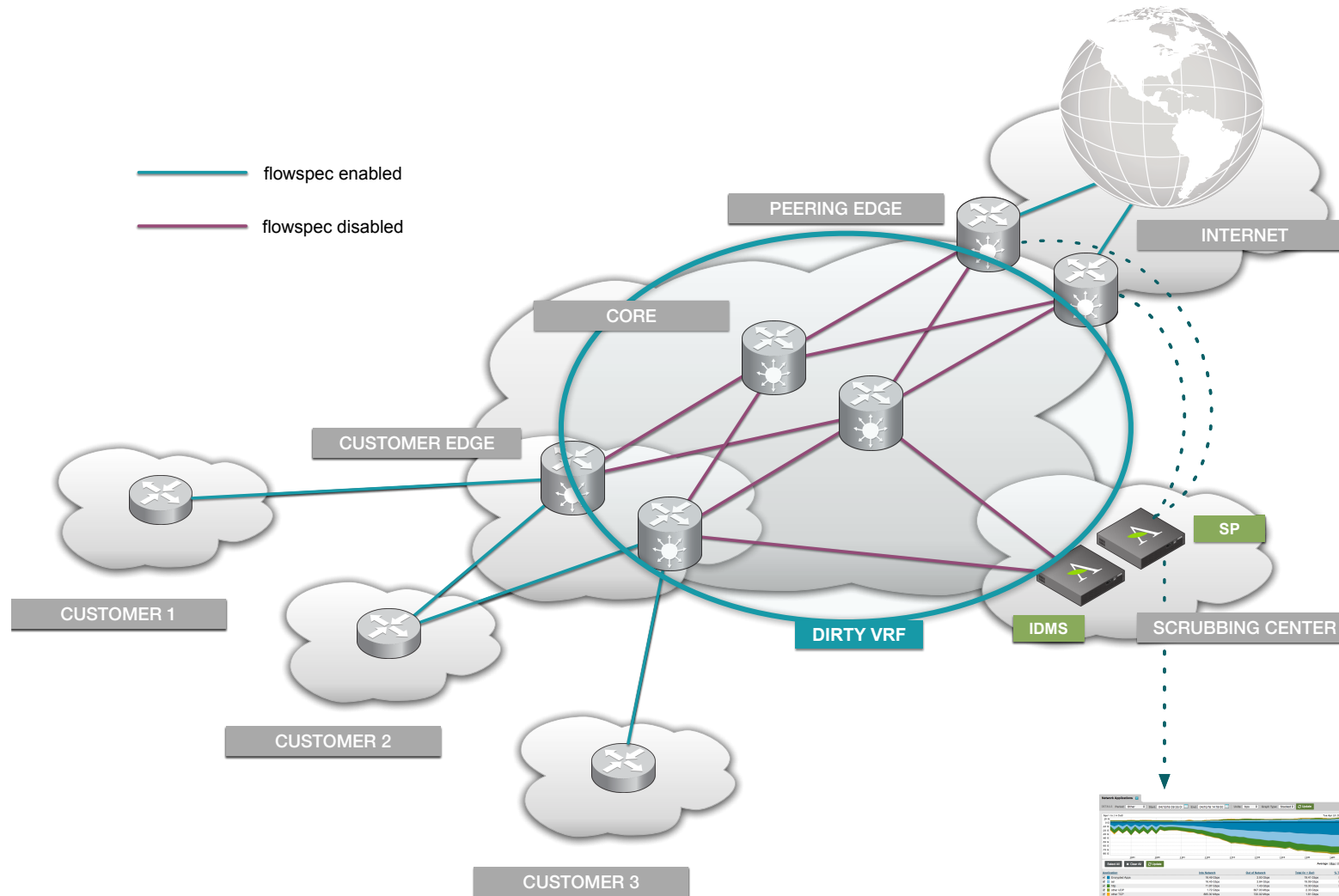
Bitmask Value	Purpose
0	Do not fragment
1	Is a fragment
2	First fragment
3	Last fragment

IOT and customer x customer attacks

Flowspec to leverage existing IDMS

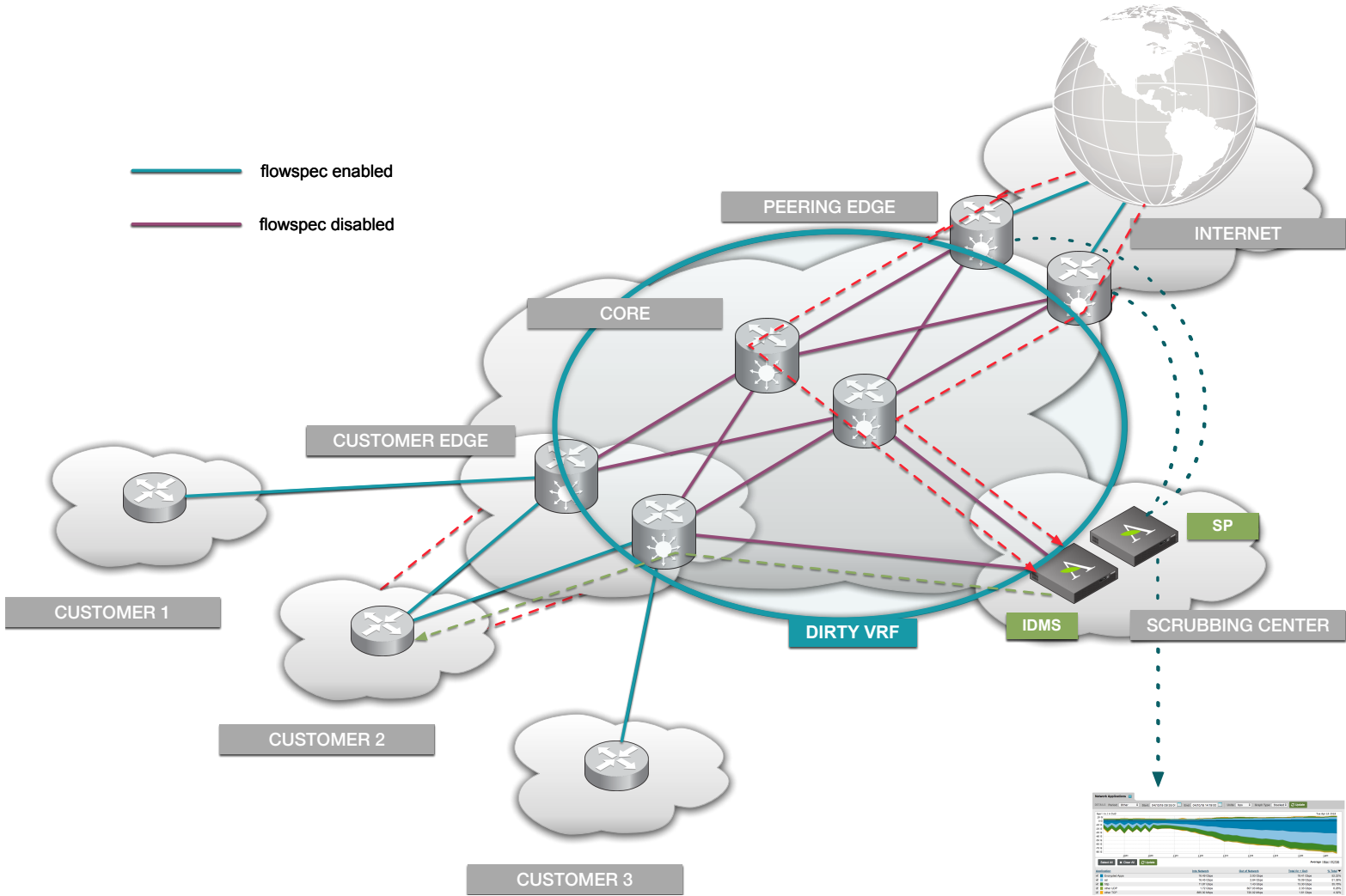
Solution diagram

Enable per interface and setup “dirty” VRF



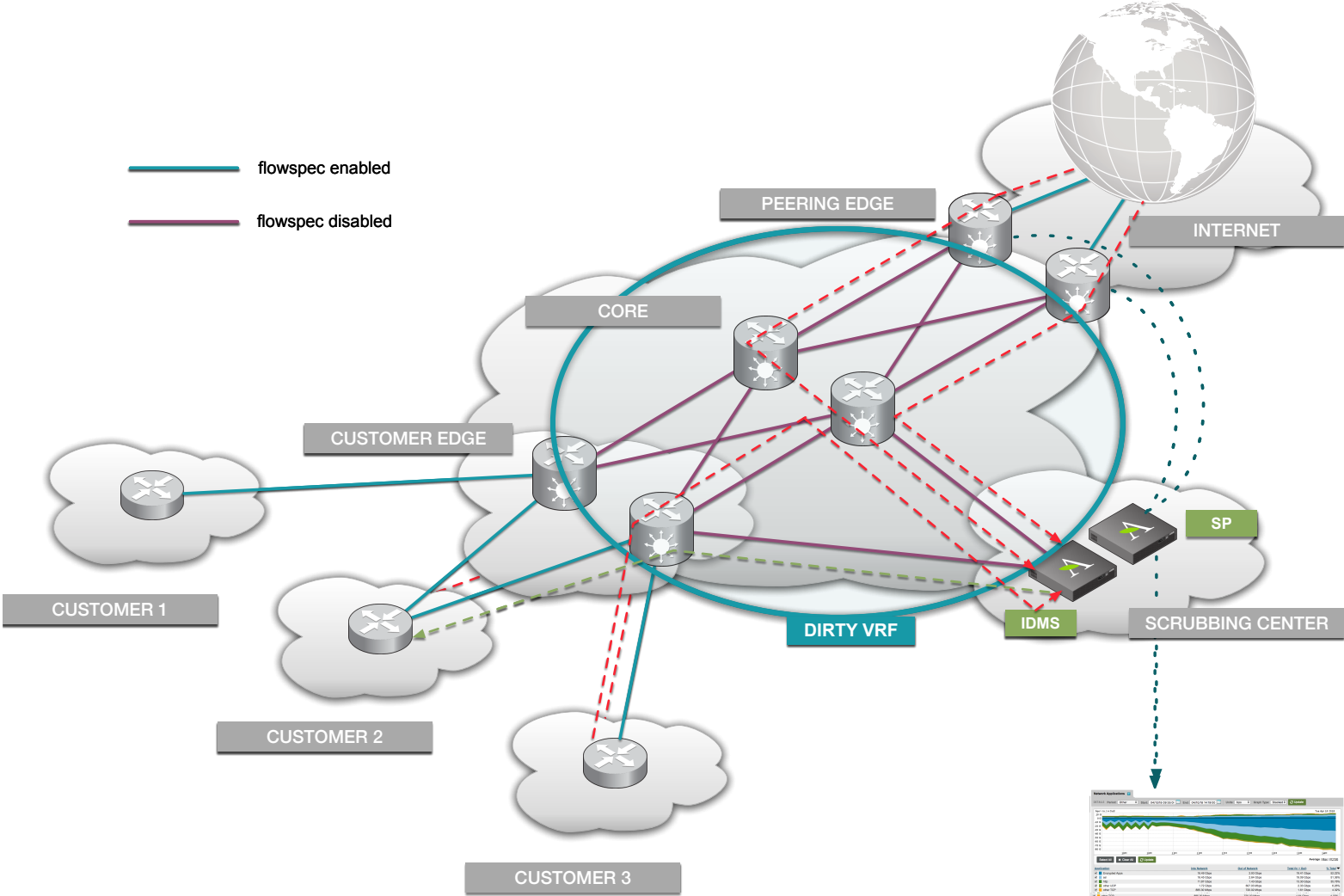
Attack scenario

North > South



Attack scenario

East > West



Why use "dirty" VRF for diversion?

- VRF (Virtual Router and Forwarding) + MPLS
- Lets you further leverage network resources for attack mitigation
- Contains attack ("dirty") traffic within a known logical entity
- Minimal routing requirements and overhead for moving traffic to scrubbers
- Easier to manage resources and protect backhaul
- With selective application of flowspec, traffic can be put back into the global routing tables without encapsulation

What if you don't have an IDMS?

- Volumetric attack diversion is not desirable if your IDMS resources are limited or non-existent.
- You can create flowspec filters to drop both amplified responses components:
 - Initial fragments (UDP header)
 - Non-initial fragments (no UDP header)

Drop initial DNS fragments

Dst: 1.1.0.1/32 **Protocols:** 17 **Src Ports:** 53 **Fragment:** 4

Drop non-initial UDP fragments

Dst: 1.1.0.0/32 **Protocols:** 17 **Fragment:** 2

NETSCOUT.

Flowspec Automation



Previous considerations

- Safe to apply with certain protocols
- Care must be taken with others
- Think about SLA's requisites
 - Residential users
 - Enterprise customers
 - Critical infrastructure
- Identify critical services you need to be concerned about
- **Flowspec + IDMS integration adds to the solution**

Remember this is a business rather than technical problem!

Previous considerations

Continuation

- Keep in mind that flowspec typically operates at L3/L4
- Be aware that L3/L4 classification is not static (i.e. UDP/443 – QUIC)
- Ensure you clearly identify critical traffic patterns and whitelist them:
 - Name servers
 - Content Delivery Networks (CDN's)
 - Carrier-grade Network Address Translation (CGNAT)
 - Proxies

About flowspec announcements

Ensure protection when using flowspec

- Control rule update rates
- Implement prefix match validation (BGP ACL's)
- Restrict amount of announced routes
- Use BGP Communities
 - Control announcements regionally or globally
 - Tag, mark and track **who** is announcing, **what** is being announced and **where**.

If all else fails you can still use it

- Flowspec Blacklist Offloading in 8.1

The screenshot shows a configuration page for 'Blacklist Offloading'. On the left is a sidebar with a list of menu items: Appliance, SNMP, Deployment, ArborFlow, Patch Panel, IPv4 Forwarding, IPv6 Forwarding, Subinterfaces, Ports, IPv4 GRE, IPv6 GRE, Blacklist Offloading (highlighted), and Advanced. The main content area is titled 'Blacklist Offloading' and contains the following sections:

- Blacklist Offloading:** Two buttons, 'None' and 'Flow Specification', with 'Flow Specification' selected.
- Block on:** Two buttons, 'Source' and 'Source+Mitigation', with 'Source+Mitigation' selected.
- Flow Specification Router:**
 - Target Router:** A dropdown menu with an information icon, currently showing 'WHS Test Router: Test (2.2.2.3)'.
 - Rules Limit (optional):** A text input field with an information icon, currently empty.

At the bottom of the configuration area are two buttons: 'Cancel' and 'Save'.

Conclusions

Just do it?

Yes, but with a clear understanding about it...

- Be aware of different functionalities between technology vendors.
- Leverage flowspec capabilities by using a single management mechanism.
- Use flowspec as part of a layered protection in conjunction with an IDMS to provide a robust security strategy.
- As ANY protocol that interfere with packet flow, establish sanity policies

Thank You.

Julio Arruda

jarruda@arbor.net

Kleber Carriello

kco@arbor.net

www.netscout.com

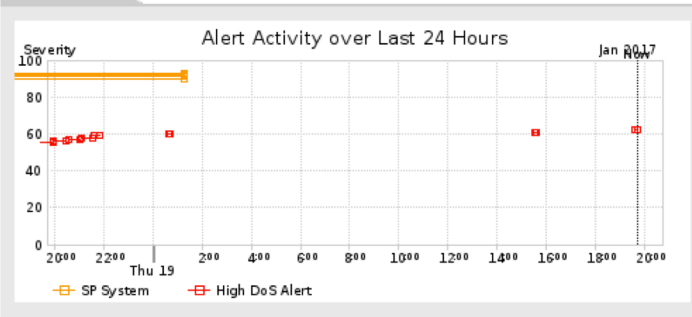
Example of SYN/UDP flood

Arbor Networks® SP

System Alerts Explore Reports Mitigation Administration

Thu 19 Jan 2017 19:44:10 UTC
 Logged in as: tsundstrom@arbor.net (Log Out)

Alert Activity



All Alerts Alert Classes

Severity Level	Ongoing	Recent	Last 24 Hours
High	1	676	8
Medium	0	2408	4
Low	0	88	6
Total	1	3172	18

Top Traffic Patterns (last 5 min of selected timeframe)

No patterns found in the last 5 minutes of the selected timeframe.

Download All Patterns

Interface	Router	Router Severity	Direction	Boundary	ASNs	Max Observed	Average Observed
GigabitEthernet0/18 PEER-ESX3.VM3...COM	edge-frankfurt	High	IN	Network	6504	22.2 Mbps 27.5 Kpps	141.7 Mbps 18.2 Kpps
ib7 CUSTVMVIC1-VM7...IRM	edge-rio	High	OUT			239.5 Mbps 27.8 Kpps	141.5 Mbps 18.0 Kpps
xe-0/1/0 BB-CNYK-AS4.1006...530	edge-rio	High	IN			127.9 Mbps 14.8 Kpps	77.3 Mbps 9.4 Kpps
Bundle-Ether2 BB-CNYK-AS4.1004...530	edge-frankfurt	High	OUT			122.5 Mbps 15.3 Kpps	76.8 Mbps 8.5 Kpps
Bundle-Ether1 BB-CSJC-AS4.1004...530	edge-frankfurt	High	OUT			115.2 Mbps 14.3 Kpps	64.9 Mbps 8.7 Kpps

Recent Annotations

- "Total Traffic" host alert signature has been triggered at router "edge-rio", (expected rate: 100.00 Mbps/100.00 Kpps, observed rate: 198.16 Mbps/20.40 Kpps) auto-annotation on Thu Jan 19 19:38:45
- "TCP SYN" host alert signature has been triggered at router "edge-frankfurt", (expected rate: 20 pps, observed rate: 2.83 Kpps) auto-annotation on Thu Jan 19 19:38:45
- "IP Private" host alert signature has been triggered at router "edge-rio", (expected rate: 20 pps, observed rate: 33 pps) auto-annotation on Thu Jan 19 19:38:45

Ongoing Alerts Ongoing Mitigations Appliances

13447 **High** **Fast Flood** **DoS Host Alert** **Incoming Host Alert to 7.7.7.7 using Victim 7** **Start Time** Jan 19 19:38 – Ongoing (0:06) **Classification & Annotations** Possible Attack The "Total Traffic" host alert signature has been triggered at router "edge-rio", (expected rate: 100.00 Mbps/100.00 Kpps, observed rate: 198.16 Mbps/20.40 Kpps) (by auto-annotation)

Misuse Types: IP Private, TCP SYN, Total Traffic, UDP

Arbor Networks SP

System Alerts Explore Reports

DoS Host Alert 13447

Duration: Jan 19 19:38 – Ongoing (0:06)

Summary Traffic Details Routers Annotations Mitigations: None

Interface	Router	Router Severity	Direction	Boundary	Interface ASNs	Avg Packet Size	Max Observed	Average Observed
Normal (Interface)	edge-rio	High				864	239.5 Mbps	141.5 Mbps
edges-rio (2)	edge-rio	High				873	27.8 Kpps	18.0 Kpps
edge-frankfurt (1)	edge-frankfurt	High					27.5 Kpps	18.2 Kpps

DoS Host Alert 13447

Duration: Jan 19 19:38 – Ongoing (0:06)

Summary Traffic Details Routers Annotations Mitigations: None

Severity Level: High (Fast Flood)

Max Severity Percent: 15,833.0% of 100 pps

Max Impact of Alert Traffic: 216.3 Mbps/28.2 Kpps

Direction: Incoming

Misuse Types: IP Private, TCP SYN, Total Traffic, UDP

Managed Object: Victim 7

Target: 7.7.7.7

Misuse Types Exceeding Trigger Rate

- Total Traffic
- UDP
- NTP Amplification
- TCP SYN
- IP Private

Alert Characterization

- Misuse Types: Total Traffic (7) 100.00%
- UDP (9) 51.00%
- NTP Amplification (10) 51.00%
- Highly Distributed (10) 100.00%
- Destination IP Addresses: 7.7.7.7/32 100.00%
- Protocols: udp (17) 51.00%
- Source TCP Ports: 1024-65535 (Dynamic) 47.00%
- Destination TCP Ports: 80 (www-http) 48.00%
- Source UDP Ports: 123 (ntp) 51.00%

Packet Size Distribution

Page generation took 0.44 seconds (Details)

Misuse Types

- Total Traffic: 18.19 Kpps 100.00%
- UDP: 9.44 Kpps 51.91%
- NTP Amplification: 9.44 Kpps 51.91%
- TCP SYN: 8.75 Kpps 48.09%
- IP Private: 27.00 pps 0.15%

View Graph 5 reported

SYN, NTP amp using FS diversion and ACL

Diversion Method: BGP Flowspec

Redirect To: Route Target IP Address Example: 203.0.113.33:100, 64496:100, 65536L:100

BGP Peering Sessions: core-sanjose: primary (192.168.252.21)
core-newyork: primary (192.168.252.22)
edge-rio: primary (192.168.252.12)
edge-tokyo: primary (192.168.252.1)
edge-london: primary (192.168.252.3)

VSM Backplane Channel Group

logical10.100
IPv4 Address: IPv6 Address:
IPv4 Nexthop: IPv6 Nexthop:
Output Port:

logical10.200
IPv4 Address: IPv6 Address:
IPv4 Nexthop: IPv6 Nexthop:
Output Port:

logical10.300
IPv4 Address: IPv6 Address:
IPv4 Nexthop: IPv6 Nexthop:
Output Port:

```
RP/0/RSP0/CPU0:edge-frankfurt#
RP/0/RSP0/CPU0:edge-frankfurt#
RP/0/RSP0/CPU0:edge-frankfurt#show route vrf TMS9-Dirty-VRF afi-all
Sat Jan 14 15:42:13.916 UTC

IPv4 Unicast:
-----
Codes: C - connected, S - static, R - RIP, B - BGP, (>) - Diversion path
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - ISIS, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, su - IS-IS summary null, * - candidate default
U - per-user static route, o - ODR, L - local, G - DAGR, l - LISP
A - access/subscriber, a - Application route
M - mobile route, r - RPL, (!) - FRR Backup path

Gateway of last resort is 192.168.9.10 to network 0.0.0.0

S* 0.0.0.0/0 [1/0] via 192.168.9.10, 1w0d, Bundle-Ether9.300
C 192.168.9.8/30 is directly connected, 1w0d, Bundle-Ether9.300
L 192.168.9.9/32 is directly connected, 1w0d, Bundle-Ether9.300

IPv6 Unicast:
-----
Codes: C - connected, S - static, R - RIP, B - BGP, (>) - Diversion path
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - ISIS, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, su - IS-IS summary null, * - candidate default
U - per-user static route, o - ODR, L - local, G - DAGR, l - LISP
A - access/subscriber, a - Application route
M - mobile route, r - RPL, (!) - FRR Backup path

Gateway of last resort is fd0a:4b04:ebc:903::10 to network ::

S* ::/0
[1/0] via fd0a:4b04:ebc:903::10, 1w0d, Bundle-Ether9.300
C fd0a:4b04:ebc:903::/64 is directly connected, 1w0d, Bundle-Ether9.300
L fd0a:4b04:ebc:903::9/128 is directly connected, 1w0d, Bundle-Ether9.300

RP/0/RSP0/CPU0:edge-frankfurt#
RP/0/RSP0/CPU0:edge-frankfurt#show inter bundle-ether9.300
Sat Jan 14 15:42:49.195 UTC
Bundle-Ether9.300 is up, line protocol is up
Interface state transitions: 1
Hardware is VLAN sub-interface(s), address is d46d.507d.6161
Description: BS-TMS9FR0-100-400-AS65330 - (Flowspec - redirect to RT) diversion
Internet address is 192.168.9.9/30
MTU 1518 bytes, BW 800000000 Kbit (Max: 800000000 kbit)
reliability 255/255, txload 0/255, rxload 0/255
Encapsulation 802.1Q Virtual LAN, VLAN id 300, loopback not set,
Last link flapped 5w0d
ARP type ARPA, ARP timeout 04:00:00
Last input 00:00:00, output 00:00:00
Last clearing of "show interface" counters never
30 second input rate 0 bits/sec, 0 packets/sec
30 second output rate 0 bits/sec, 0 packets/sec
259660 packets input, 15308496 bytes, 0 total input drops
0 drops for unrecognized upper-level protocol
Received 90 broadcast packets, 0 multicast packets
1333129205 packets output, 1225420586332 bytes, 0 total output drops
Output 2 broadcast packets, 3789 multicast packets

RP/0/RSP0/CPU0:edge-frankfurt#
RP/0/RSP0/CPU0:edge-frankfurt#ping 192.168.9.10 vrf TMS9-Dirty-VRF
Sat Jan 14 15:42:55.583 UTC
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.9.10, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
RP/0/RSP0/CPU0:edge-frankfurt#
```

SYN, NTP amp using FS diversion and ACL

Edit Appliance "Demo-TSMVSM60-9"

TMS Mitigation Status "CiscoLive-FSdiv-demo" (IPv4)

Deployment

Deployment Type: Diversion
Capabilities: Optimize for Mitigation Performance
Forwarding Mode: Patch Panel
Port for Challenge Packets: Input Port, Output Port

Flow Specification

Protocol Numbers: 6
Destination Ports: 80

Countermeasures

Status	Countermeasure	Dropped	Passed
ON	Invalid Packets		
OFF	IPv4 Address Filter Lists		
OFF	IPv4 Black/White Lists		
OFF	Packet Header Filtering		
OFF	IP Location Filter Lists		
ON	Zombie Detection		
OFF	UDP Reflection/Amplification Protection		
OFF	Per Connection Flood Protection		
ON	TCP SYN Authentication		
OFF	DNS Scoping		
ON	DNS Authentication		
ON	TCP Connection Limiting		
ON	TCP Connection Reset		
OFF	Payload Regular Expression		
OFF	Protocol Baselines		
ON	DNS Malformed		
OFF	DNS Rate Limiting		
OFF	DNS NXDomain Rate Limiting		
OFF	DNS Regular Expression		
ON	HTTP Malformed		
OFF	HTTP Scoping		

```
RP/0/RSP0/CPU0:edge-frankfurt#  
RP/0/RSP0/CPU0:edge-frankfurt#show flowspec afi-all  
Sat Jan 14 15:46:49.014 UTC  
RP/0/RSP0/CPU0:edge-frankfurt#  
RP/0/RSP0/CPU0:edge-frankfurt#show flowspec afi-all  
Sat Jan 14 15:51:14.330 UTC  
  
AFI: IPv4  
Flow :Dest:7.7.7.7/32,Proto:=6,DPort:=80  
Actions :Redirect: VRF TMS9-Dirty-VRF Route-target: ASN2-65530:9 (bgp.1)  
RP/0/RSP0/CPU0:edge-frankfurt#
```