How to act as a good NSP peer?

Sam Sham

RETN®

2023

PEERING ASIA 5.0

Why peering?

- Cost saving
- Latency
- Better routing control

How to evaluate your potential peers?

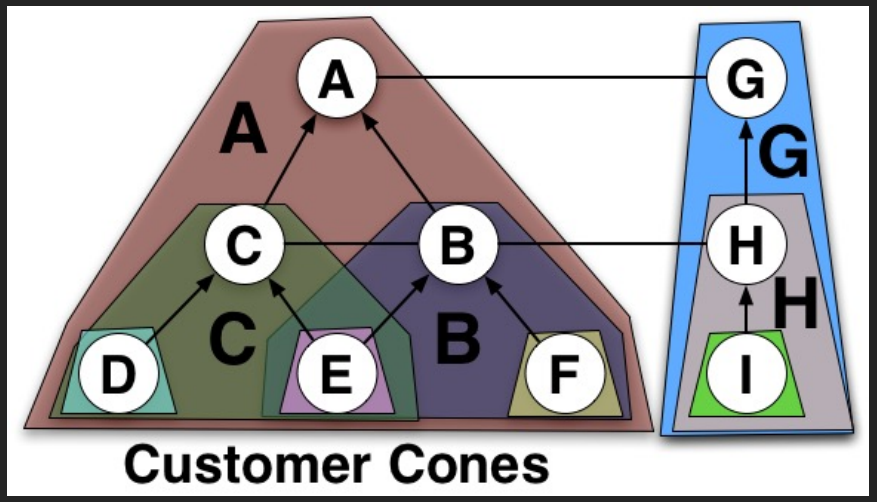
- Company peering policy.
- Own flow data
- Peeringdb
- AS data, ASRank by ASCaida.

ASRank

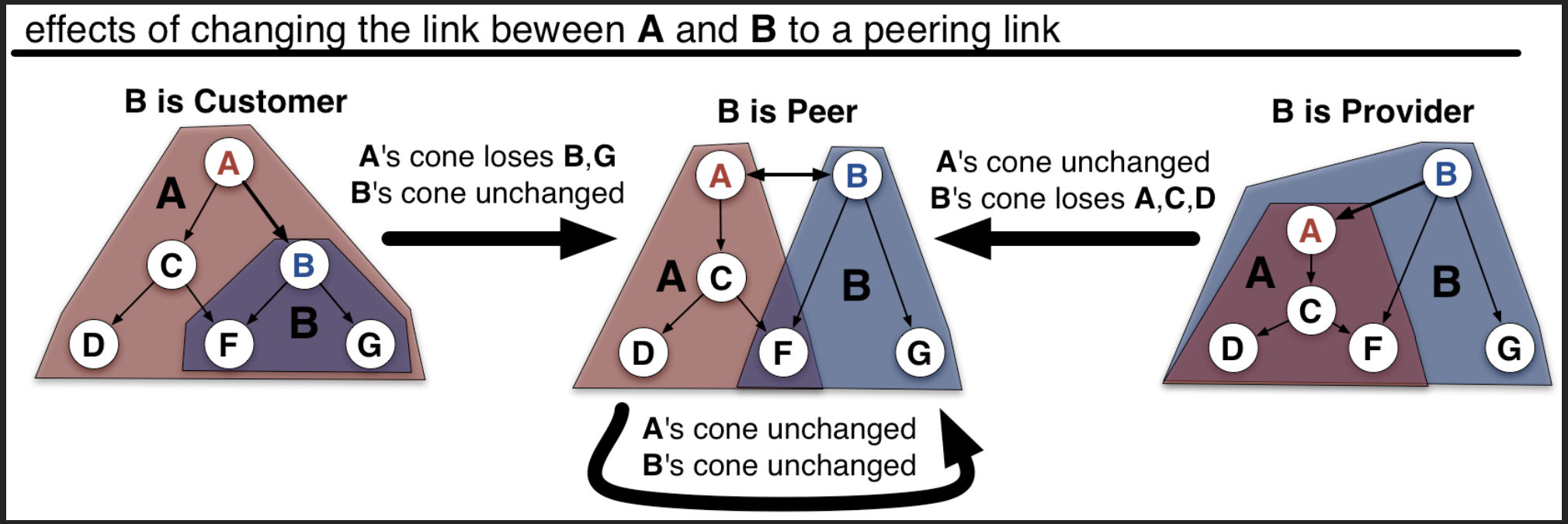
Looking Glass URL	http://lg.retn.net/
Network Type	NSP
IPv4 Prefixes	80000
IPv6 Prefixes	8000
Traffic Levels	10-20Tbps
Traffic Ratios	Balanced
Geographic Scope	Global
Protocols Supported	Unicast IPv4 Multicast IPv6 Never via route servers

What’s ASRank?

- Long term research project from Center for Applied Internet Data Analysis(CAIDA) based at the San Diego Supercomputer Center in US.
- Interpret the data from Route Views Project and RIPE NCC to infer the relationship between ASes.
- Ranking is concluded based on the customer cone.



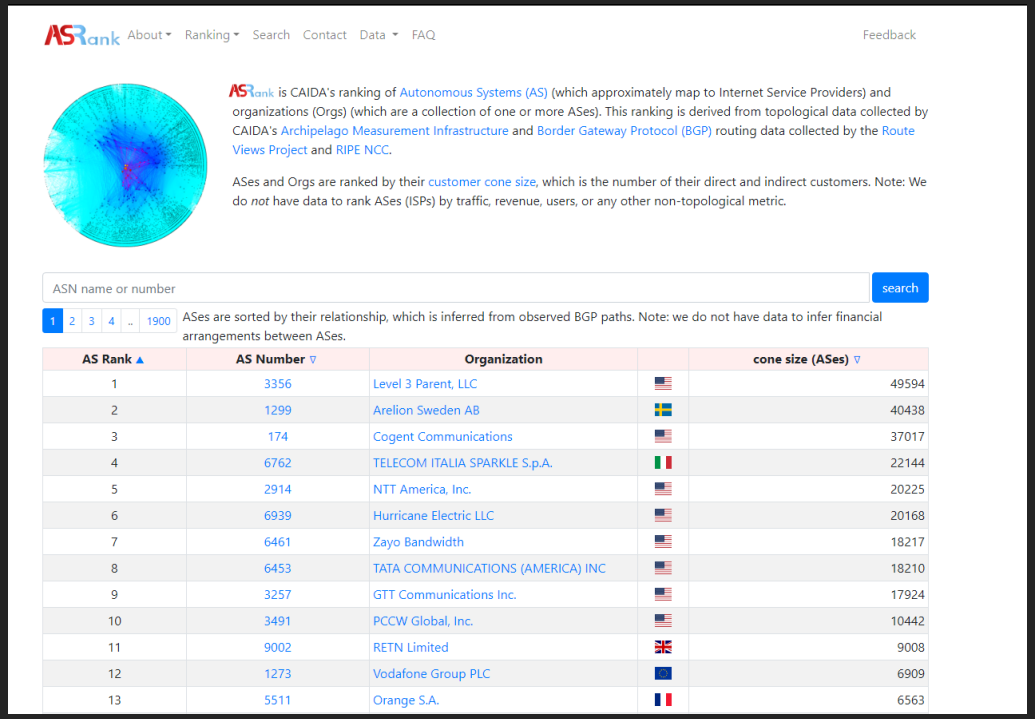
Customer cone



When there is a change of relationship between ASN, customer size would be changed accordingly!!

How can ASRank help?

- Provide an objective way on evaluating the peering
- Open-source data so that you can integrate with your own system
- Monthly update on the source data/Quarterly update on WebUI usually.
- Ranking for content-related ASN is not appropriate because they seldom do transit for another ASNs.

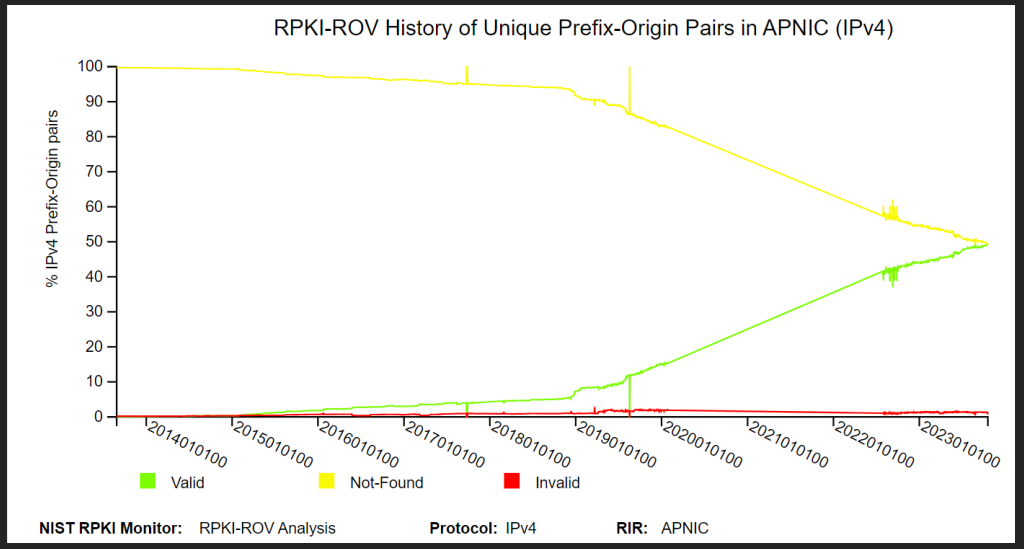


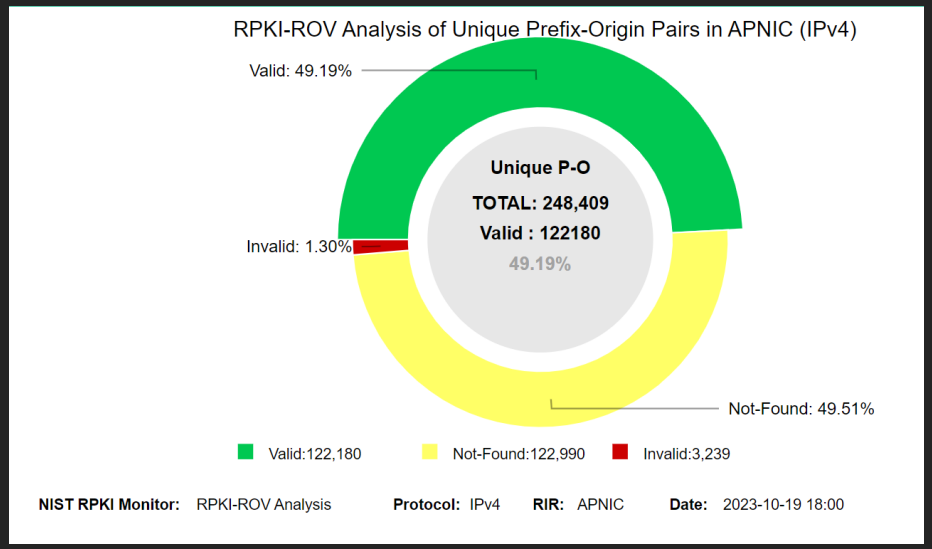
AS Rank	AS Number	Organization	cone size (ASes)
1	3356	Level 3 Parent, LLC	49594
2	1299	Arelion Sweden AB	40438
3	174	Cogent Communications	37017
4	6762	TELECOM ITALIA SPARKLE S.p.A.	22144
5	2914	NTT America, Inc.	20225
6	6939	Hurricane Electric LLC	20168
7	6461	Zayo Bandwidth	18217
8	6453	TATA COMMUNICATIONS (AMERICA) INC	18210
9	3257	GTT Communications Inc.	17924
10	3491	PCCW Global, Inc.	10442
11	9002	RETN Limited	9008
12	1273	Vodafone Group PLC	6909
13	5511	Orange S.A.	6563

https://asrank.caida.org/
https://www.caida.org/catalog/datasets/as-relationships/

How to secure your network?

- RPKI – Reduce the risk of route leak and BGP hijacking.

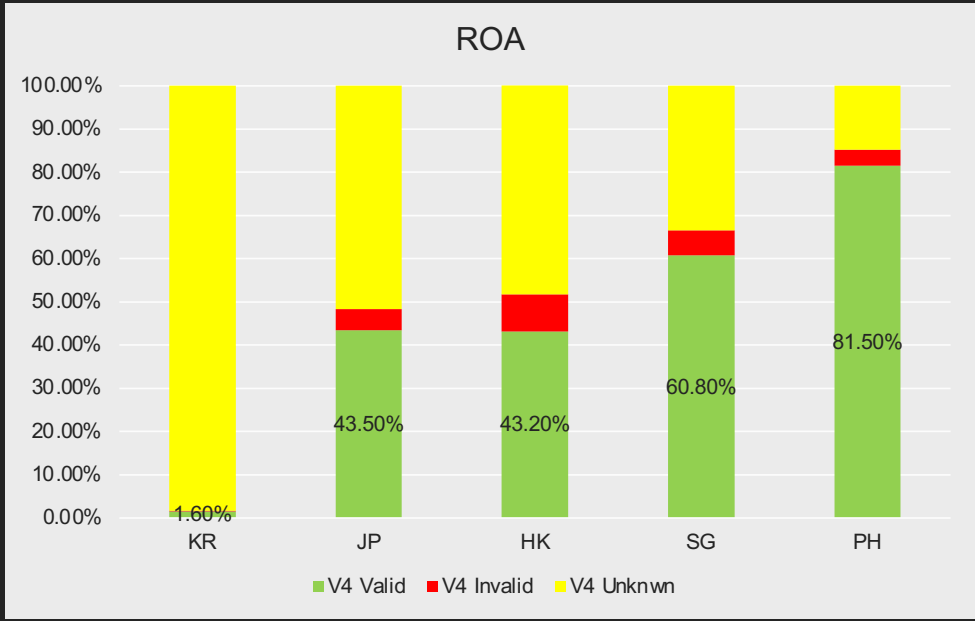


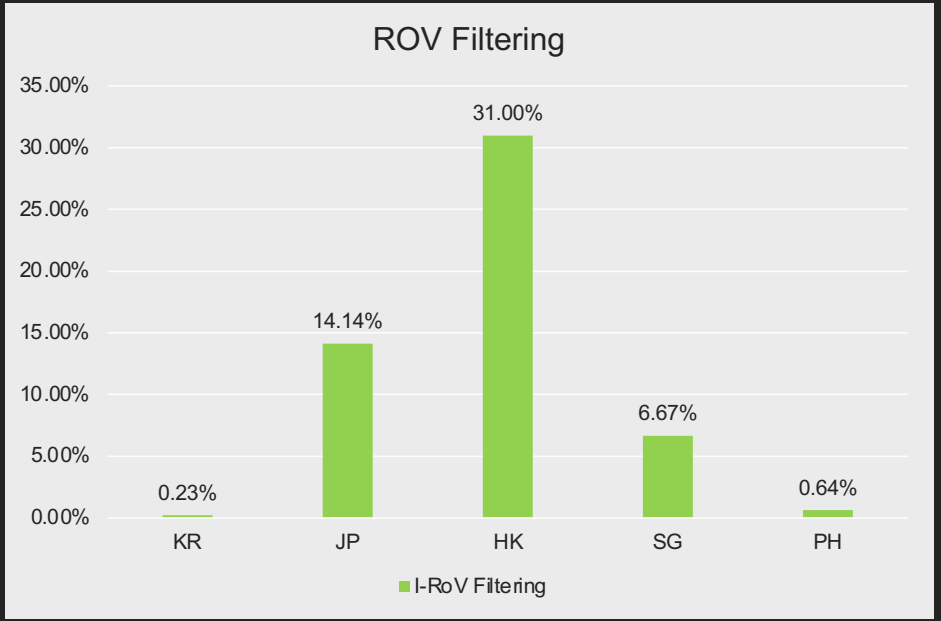


Source: NIST RPKI monitor 19 Oct 2023

How to secure your network?

- RPKI status – South Korea

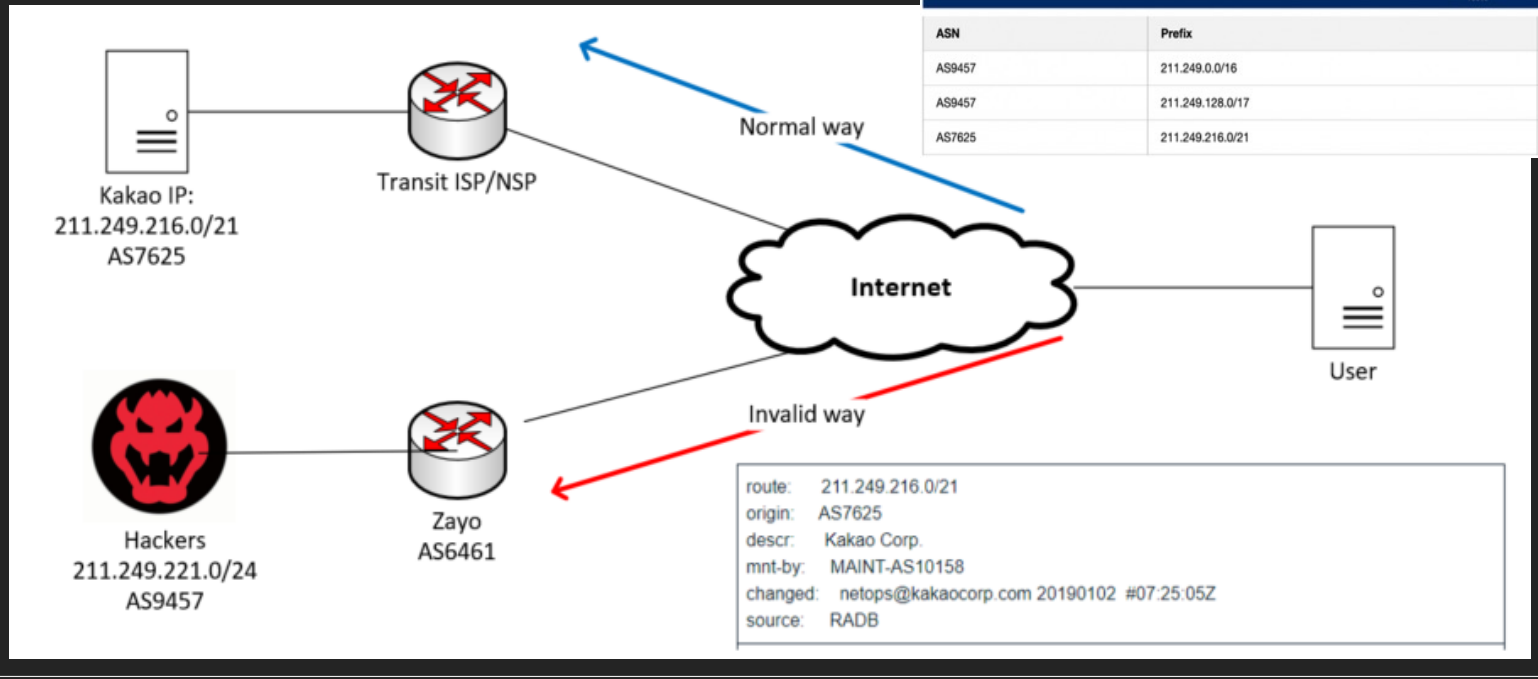




Source: Stats Lab APNIC 19 Oct 2023

How to secure your network?

- BGP hijack South Korea in 2022---- KlaySwap, cryptocurrency platform.
- Hackers stole USD$1.9million worth of digital assets by redirecting the user to a malicious version of KakaoTalk.



Unsigned
100%

ASN	Prefix	IP Family	ROA
AS9457	211.249.0.0/16	IPv4	None
AS9457	211.249.128.0/17	IPv4	None
AS7625	211.249.216.0/21	IPv4	None

Source: https://www.manrs.org/2022/02/klayswap-another-bgp-hijack-targeting-crypto-wallets/

How to secure your network?

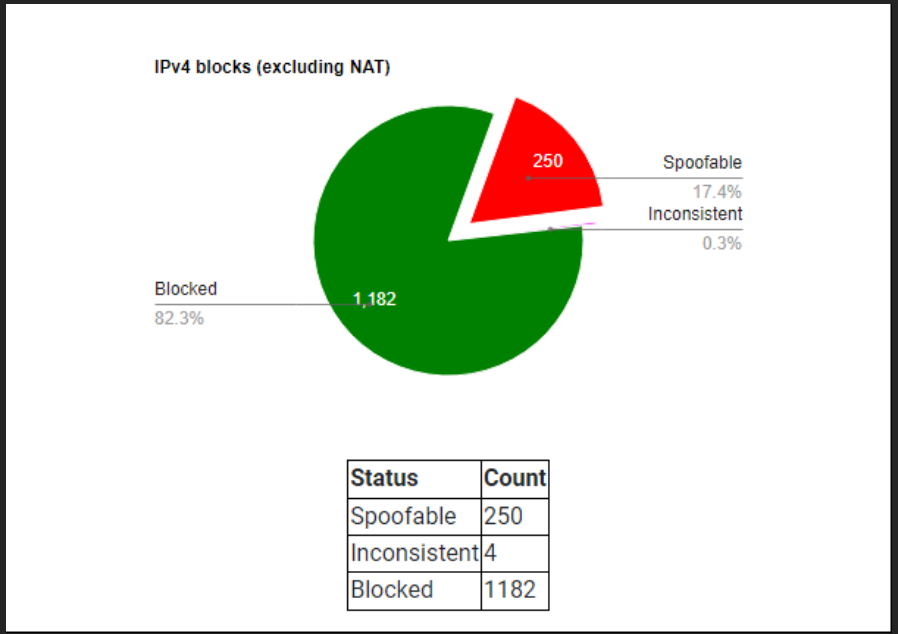
- Does RoV filtering really helps?
- Answer: **YES!**
- 75% of traffic goes to the correct destination
- Invalid route propagation has been reduced by 1/2 to 2/3

source: How much does RPKI ROV reduce the propagation of invalid routes? (Doug Madory & Job Snijders, 2023)
https://www.kentik.com/blog/how-much-does-rpki-rov-reduce-the-propagation-of-invalid-routes/

source: Where Did My Packet Go? Measuring the Impact of RPKI ROV(Koen van Hove, 2022)
https://labs.ripe.net/author/koen-van-hove/where-did-my-packet-go-measuring-the-impact-of-rpki-rov/

How to secure your network?

- Anti-spoofing - BCP38 aka RFC2827 Network Ingress Filtering
- Validate the packet at the inbound
- Easy to implement:
  Juniper/Cisco/Huawei are all supporting for uRPF(unicast Reverse Path Forwarding)
- Save bandwidth and minimize the amount of malicious traffic.
- No additional cost.
- Our practice:
  rpf-check strict mode for IP customer
  rpf-check loose mode for IPT customer.

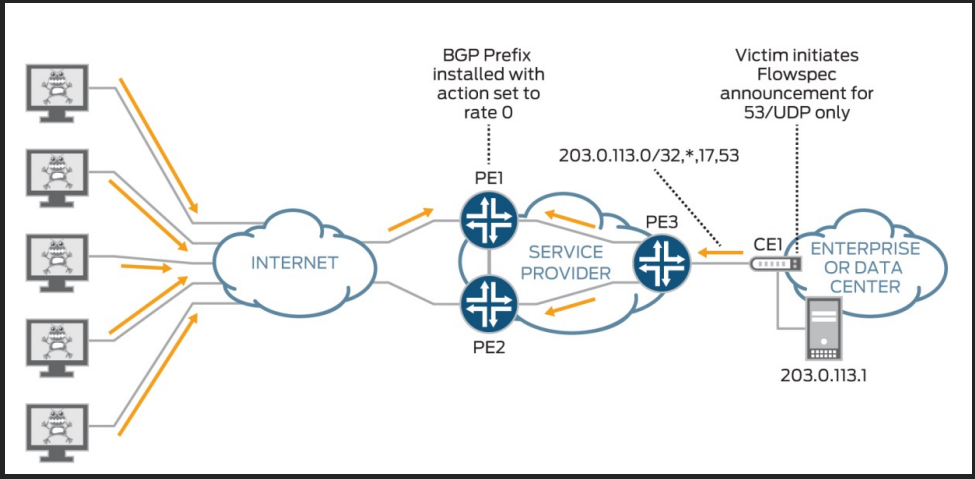


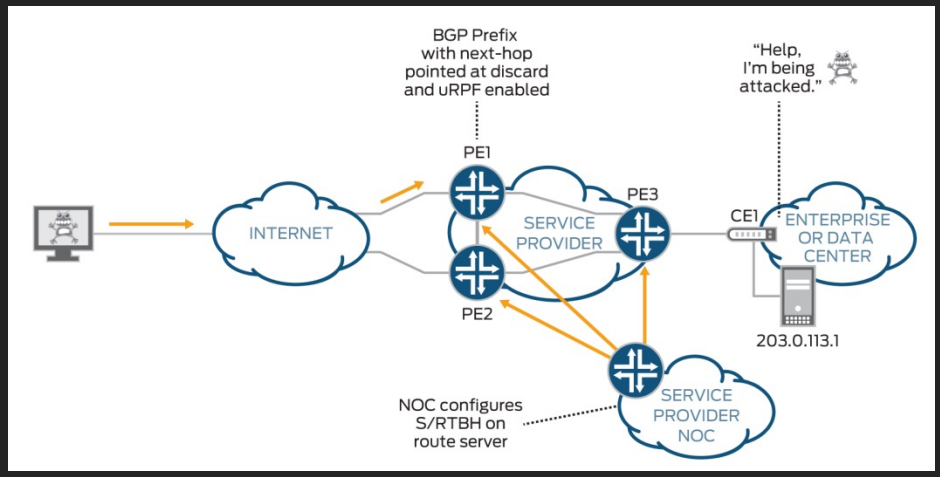
Status	Count
Spoofable	250
Inconsistent	4
Blocked	1182

Source: https://spoofer.caida.org/summary.php

How to secure your network?

- Flowspec – introduced in 2009 RFC5575
- Implemented on eBGP and control via NLRI(Network Layer Reachability Information)
- Enable features to exchange the information about specific flows in network.



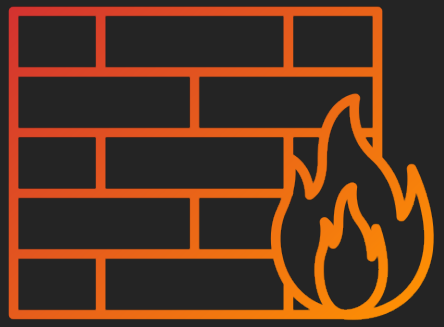


Source: https://www.juniper.net/documentation/en_US/day-one-books/DO_BGP_FLowspec.pdf

How to secure your network?

- Simple word: Dynamic firewall implemented on eBGP connections/Upgraded RTBH.

Traffic match	Traffic action
drc/dst IP	Drop
Length	Rate-limit (shaper)
IP protocol	Mark (DSCP)
src/dst ports	Redirect to VRF(e.g., to DPI scrubber)
TCP flags	
DSCP	
Fragment	



How to secure your network?

Pros	Cons
Easy to implement	Hardware limitation(up to several thousands of rules)
Multiple vendor supported(Cisco/Juniper/Huawei/etc)	Need to identify the attack flow properly
Provide granularity to control the flow of the DDoS attack	

Minor but also important

- Maintain a network without packet loss
- Responsive 24x7 support
- Maintain an up-to-date peeringdb profile for your ASN. This is one of the requirement to peer with major CDNs and operators (Eg. Cloudflare, AWS, MS, etc)

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

PeeringDB


Collaborate