eBGP Flowspec Peering for DDoS Mitigation

Rich Compton
Thomas Bowlby

Taylor Harris
Pratik Lotia

DDoS Situation At A Glance

- Attacks ⬆ in terms of frequency & size
- Scrubbers perfect for small attacks (10G/40G/400G)
- Recent attacks > 1 Tbps
- Scrubbing capacity not enough for big attacks
  - RTBH (Remote Triggered Black Hole) only option – not preferable
  - Complaints from customer (residential/business)

What Do You Notice?

- 75% of attacks are volumetric*
- Simple but consume bandwidth
- 60% attacks are under 6 hours*
- DNS/NTP/LDAP/SSDP amplifications most common attacks
- Scrubbers get busy in mitigating small attacks
- No capacity to mitigate simultaneous large attacks

*https://pages.arbornetworks.com/rs/082-KNA-087/images/13th_Worldwide_Infrastructure_Security_Report.pdf

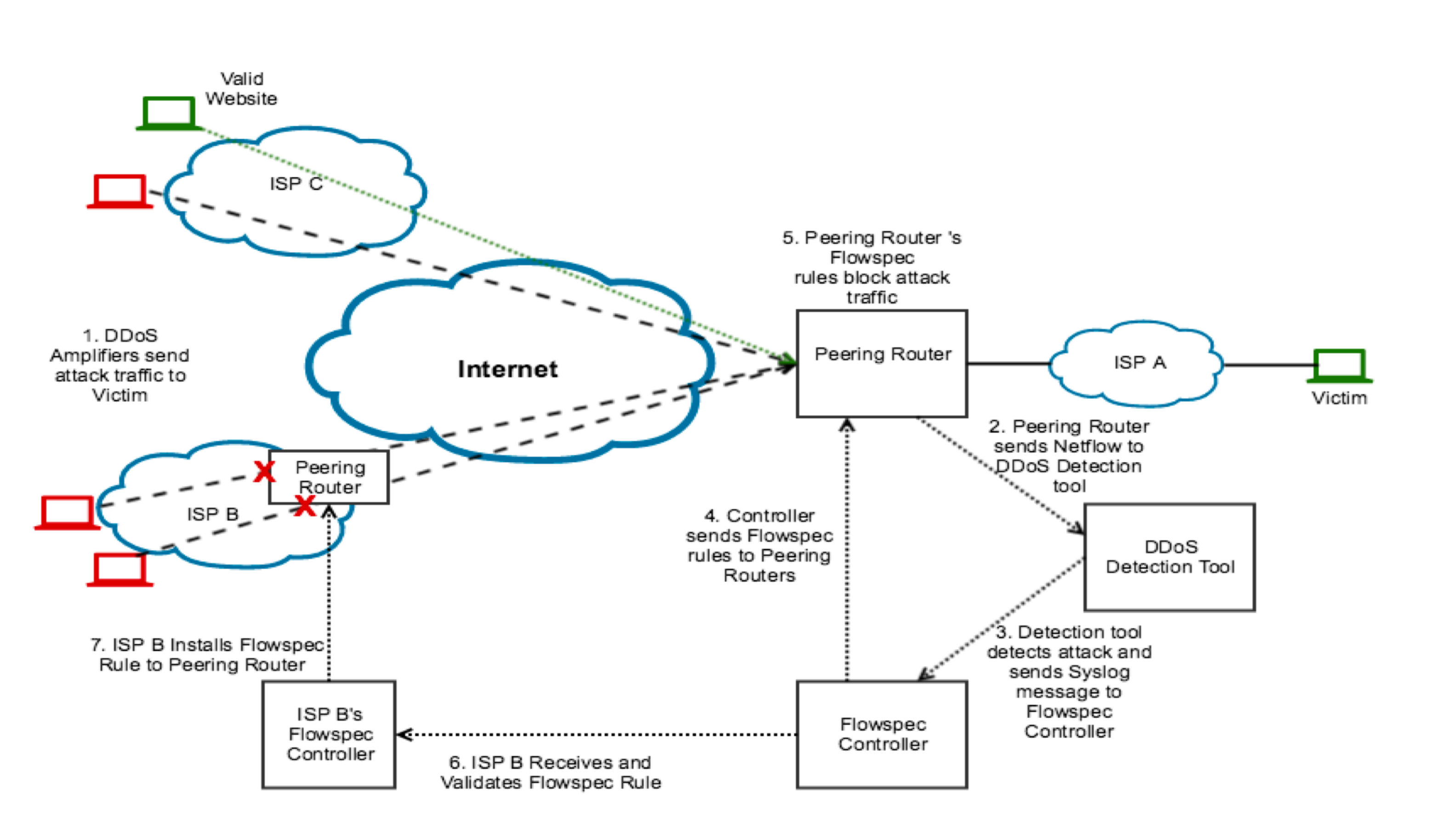
Existing Solution

- Traffic-cleanup using Scrubbers (Distributed/Centralized)
  - Complex/simultaneous attacks can exhaust scrubbing capacity
- Minimized spoofed traffic by restriction incoming traffic to known sources
  - BCP 38, 84
- Rule of thumb – block as close to source as possible
- Flowspec – some boxes support, old ones do not
- DOTS (DDoS Open Threat Signaling) – work in progress / will take time

DDoS Peering - The Way Forward

- eBGP Flowspec Peering – Collaborative approach with other ISPs
- Not new! (Smith/Schiel/Levy – NANOG71)
- Mitigate simpler attacks to ensure scrubbing capacity is not exhausted
  - Complex attacks will still be handled by scrubbers
- Inter-ISP Flowspec
  - Flowspec advertisements sent by a DDoS peer to rate-limit/block attack traffic towards victim IP
  - Victim IP must be an IP managed by the initiating peer
  - DDoS peer filters traffic for another peer to restrict malicious traffic

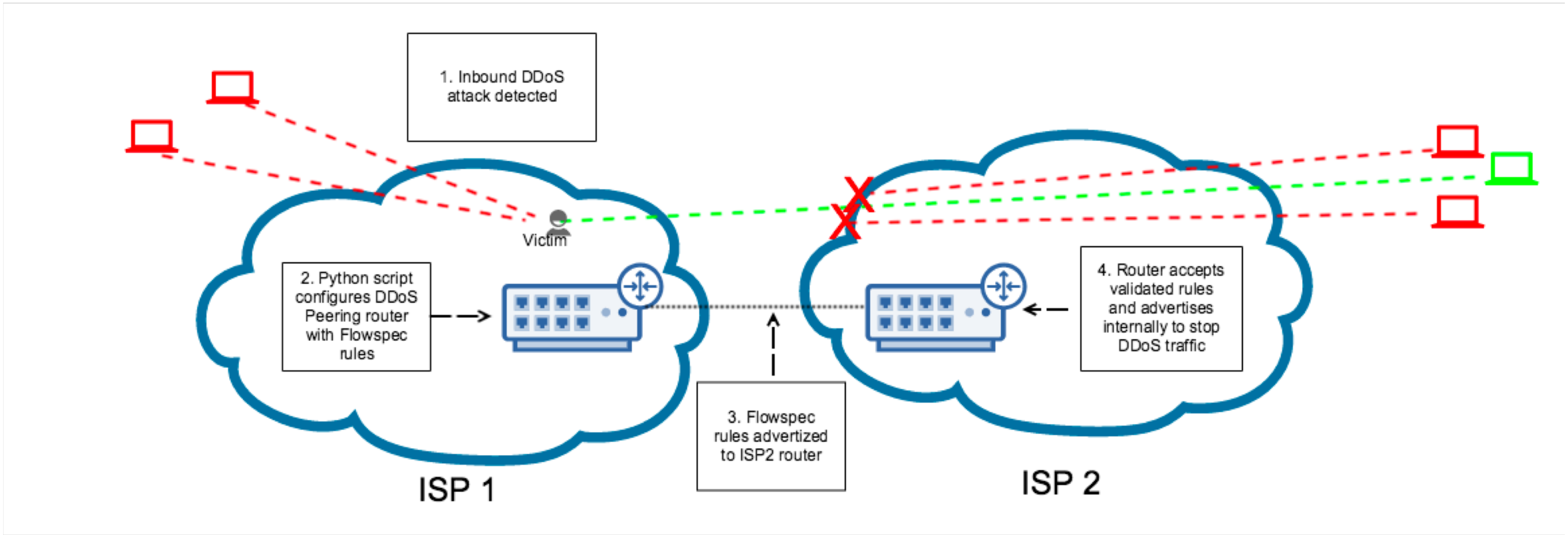
DDoS Peering Overview


Valid Website
ISP C
1. DDoS Amplifiers send attack traffic to Victim
Internet
5. Peering Router 's Flowspec rules block attack traffic
Peering Router
ISP A
Victim
Peering Router
ISP B
2. Peering Router sends Netflow to DDoS Detection tool
4. Controller sends Flowspec rules to Peering Routers
DDoS Detection Tool
7. ISP B Installs Flowspec Rule to Peering Router
3. Detection tool detects attack and sends Syslog message to Flowspec Controller
ISP B's Flowspec Controller
Flowspec Controller
6. ISP B Receives and Validates Flowspec Rule

Proof of Concept

- Developed a mechanism for DDoS peers to receive, process & accept flowspec rules
- All received rules (announce/withdraw) subject to validation
  - Rule of thumb: Don’t blindly trust eBGP routes
  - Flowspec rules must meet a set of criteria
  - Peer can request filtering only for /32 (or/128) which it originates
  - Only filtering for /32 destinations (for now)
  - Log everything: Invalid requests will be dropped & logged
- Mechanism for sending rules is being automated
  - Script identifies when DDoS tool detects attack and signals the peering router to advertise rules
  - Will be dependent on detection tool

How It Works!



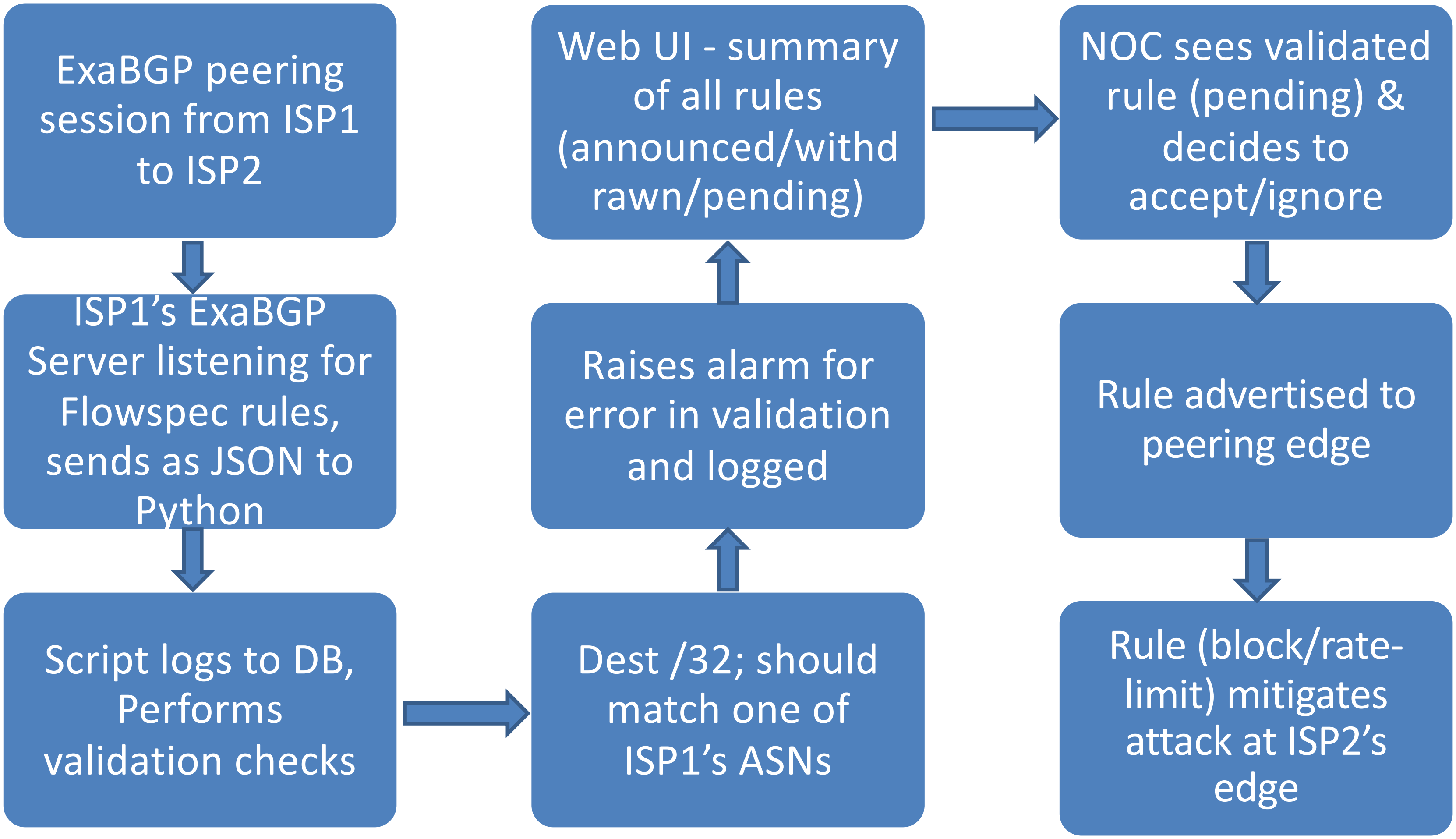
1. Inbound DDoS attack detected

2. Python script configures DDoS Peering router with Flowspec rules

3. Flowspec rules advertized to ISP2 router

4. Router accepts validated rules and advertises internally to stop DDoS traffic

Route Advertisements From ISP1 To ISP2



ExaBGP peering session from ISP1 to ISP2

ISP1’s ExaBGP Server listening for Flowspec rules, sends as JSON to Python

Script logs to DB, Performs validation checks

Dest /32; should match one of ISP1’s ASNs

Raises alarm for error in validation and logged

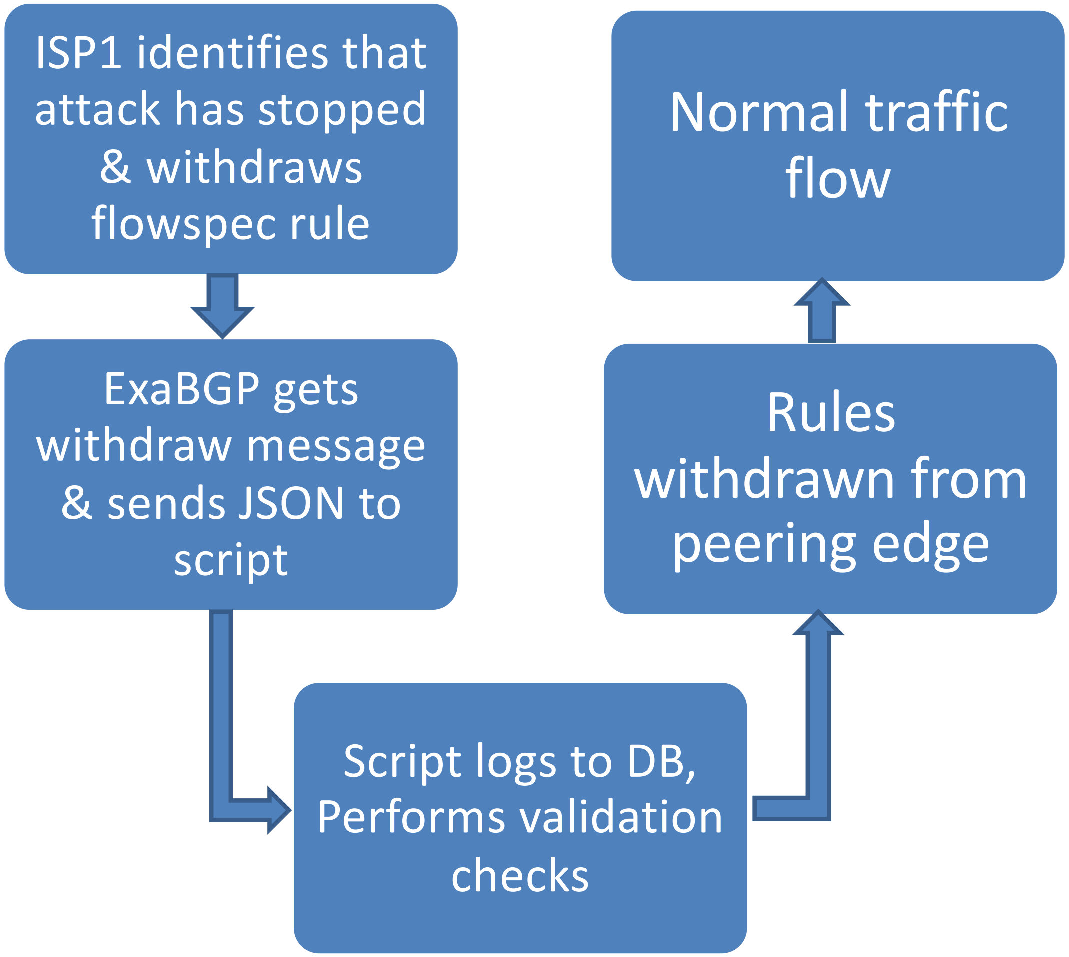
Web UI - summary of all rules (announced/withdrawn/pending)

NOC sees validated rule (pending) & decides to accept/ignore

Rule advertised to peering edge

Rule (block/rate-limit) mitigates attack at ISP2’s edge

Rule Withdrawn From ISP1



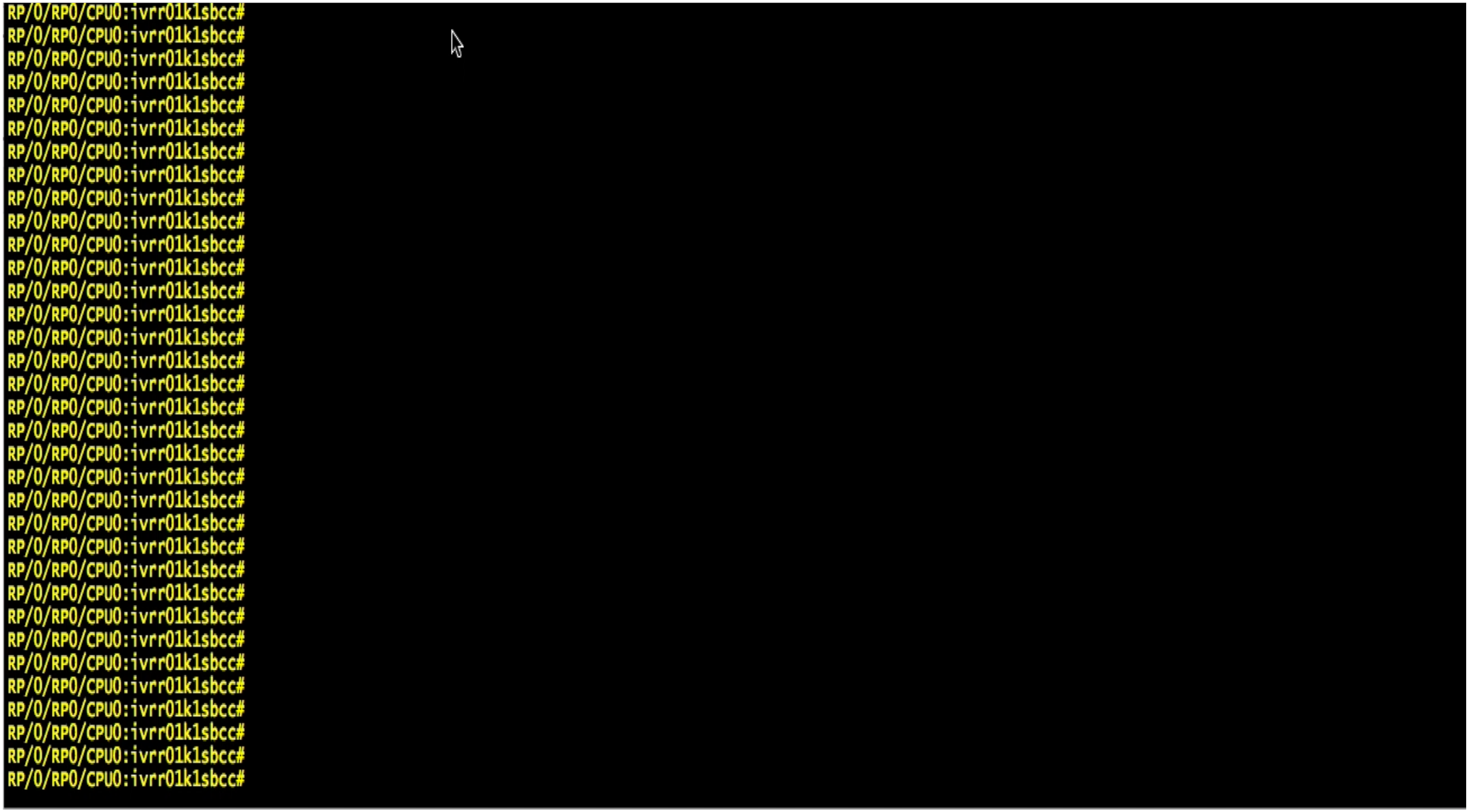
ISP1 identifies that attack has stopped & withdraws flowspec rule

ExaBGP gets withdraw message & sends JSON to script

Script logs to DB, Performs validation checks

Rules withdrawn from peering edge

Normal traffic flow



```
RP/0/RP0/CPU0:ivrr01k1sbcc#
RP/0/RP0/CPU0:ivrr01k1sbcc#
RP/0/RP0/CPU0:ivrr01k1sbcc#
RP/0/RP0/CPU0:ivrr01k1sbcc#
RP/0/RP0/CPU0:ivrr01k1sbcc#
RP/0/RP0/CPU0:ivrr01k1sbcc#
RP/0/RP0/CPU0:ivrr01k1sbcc#
RP/0/RP0/CPU0:ivrr01k1sbcc#
RP/0/RP0/CPU0:ivrr01k1sbcc#
RP/0/RP0/CPU0:ivrr01k1sbcc#
RP/0/RP0/CPU0:ivrr01k1sbcc#
RP/0/RP0/CPU0:ivrr01k1sbcc#
RP/0/RP0/CPU0:ivrr01k1sbcc#
RP/0/RP0/CPU0:ivrr01k1sbcc#
RP/0/RP0/CPU0:ivrr01k1sbcc#
RP/0/RP0/CPU0:ivrr01k1sbcc#
RP/0/RP0/CPU0:ivrr01k1sbcc#
RP/0/RP0/CPU0:ivrr01k1sbcc#
RP/0/RP0/CPU0:ivrr01k1sbcc#
RP/0/RP0/CPU0:ivrr01k1sbcc#
RP/0/RP0/CPU0:ivrr01k1sbcc#
RP/0/RP0/CPU0:ivrr01k1sbcc#
RP/0/RP0/CPU0:ivrr01k1sbcc#
RP/0/RP0/CPU0:ivrr01k1sbcc#
RP/0/RP0/CPU0:ivrr01k1sbcc#
RP/0/RP0/CPU0:ivrr01k1sbcc#
RP/0/RP0/CPU0:ivrr01k1sbcc#
RP/0/RP0/CPU0:ivrr01k1sbcc#
RP/0/RP0/CPU0:ivrr01k1sbcc#
RP/0/RP0/CPU0:ivrr01k1sbcc#
RP/0/RP0/CPU0:ivrr01k1sbcc#
RP/0/RP0/CPU0:ivrr01k1sbcc#
RP/0/RP0/CPU0:ivrr01k1sbcc#
RP/0/RP0/CPU0:ivrr01k1sbcc#
```

Next Steps

- Ongoing POC to test workflow – start with rate-limiting
- Automating sending of flowspec rules
  - Needs integration with DDoS detection tool
- Resolve issues (if necessary)
- Accept Flowspec rules advertised from peering ISP’s customer & validate by inspecting path

Summary

- Pre-established trust
  - Trust with DDoS = get rid of manual review of each rule NOC to evaluate advertisements in near future
- Less strain on resources
  - Handle more attacks before RTBH becomes the only option
- ISP helps maintain network health of internet
- One step at a time
- Feedback/Suggestions appreciated

References

- BCP 38 http://www.bcp38.info/index.php/Main_Page
- BCP 84 https://tools.ietf.org/html/bcp84
- UTRS http://www.team-cymru.org/UTRS/index.html
- Flowspec https://tools.ietf.org/html/rfc5575
- DOTS draft https://datatracker.ietf.org/doc/draft-ietf-dots-architecture/
- DDoS Peering draft – Don Smith

Charter
COMMUNICATIONS
Spectrum

Rich.Compton@charter.com

Thomas.Bowlby@charter.com

Taylor.Harris@charter.com

Pratik.Lotia@charter.com

Thank You

- Questions?

Backup slides

Talking Points / Pain Points / Concerns

- Validation won't work if ISP using it's own RADb (IP<-->ASN)
- # of flowspec rules to accept (depending on router capabilities)
- ISP should first cover its own base before helping
- ISP wants victim privacy
- Type of peering – settlement free?
  - One ISP accepting more rules then advertising

Future Development

- Validation using RPKI?
- IPv6 support
- Validating whether peer actually filtered requested traffic
  - Counters from peering router(s)
- Response/Acknowledgement, NOC Workflow, ticketing/emails
  - Request + Action = Feedback