Adaptive mitigation of DDoS attacks using BGP Flowspec

How to utilize BGP extension to fight with volumetric DOS attacks and other anomalies

Jiri Knapek, jiri.knapek@flowmon.com

Pavel Minarik, pavel.minarik@flowmon.com

Flowmon

Driving Network Visibility

Agenda

- What is Flowspec
- Prerequisites
  - Support in devices and softwares
  - Flow export
- How does it work
- Future possibilities
- Live demonstration

What is Flowspec

- Extension of BGP defined in RFC 5575[1], updated at RFC 7674[2]
- Handles distribution of traffic filtering rules
- Supported fields
  - Source and destination address
  - IP protocol
  - Source and destination port
  - ICMP type and code
  - TCP flags
  - Packet length, DSCP, Fragments, interface
- Actions are redirect to IP or VRF, marking and traffic rating
- Support also for IPv6

Advantages of using Flowspec

- “Surgical diversion” with option to redirect to VRF and mark
  - Allows to redirect only a subset of the traffic to the victim
  - Less overhead for the mitigation process
- No changes in global routing table
  - Diversion performed by Flowspec NLRI
  - Flowspec filter action configured to “Redirect to VRF”
- No need for tunneling design for reinjection/on-ramping

Support in devices and software

- Cisco (ASR - 3.15, IOS 15.5(1)S, NCS XR 5.2.4)
- Juniper (MX 15.1F5, PTX 17.1R1, T 10.0R1, SRX 10.3R2 basic since 7.3)
- Alcatel-Lucent (Nokia) 7750 SROS 9.0R1
- Huawei
- GoBGP
- ExaBGP
- Bird 2.0

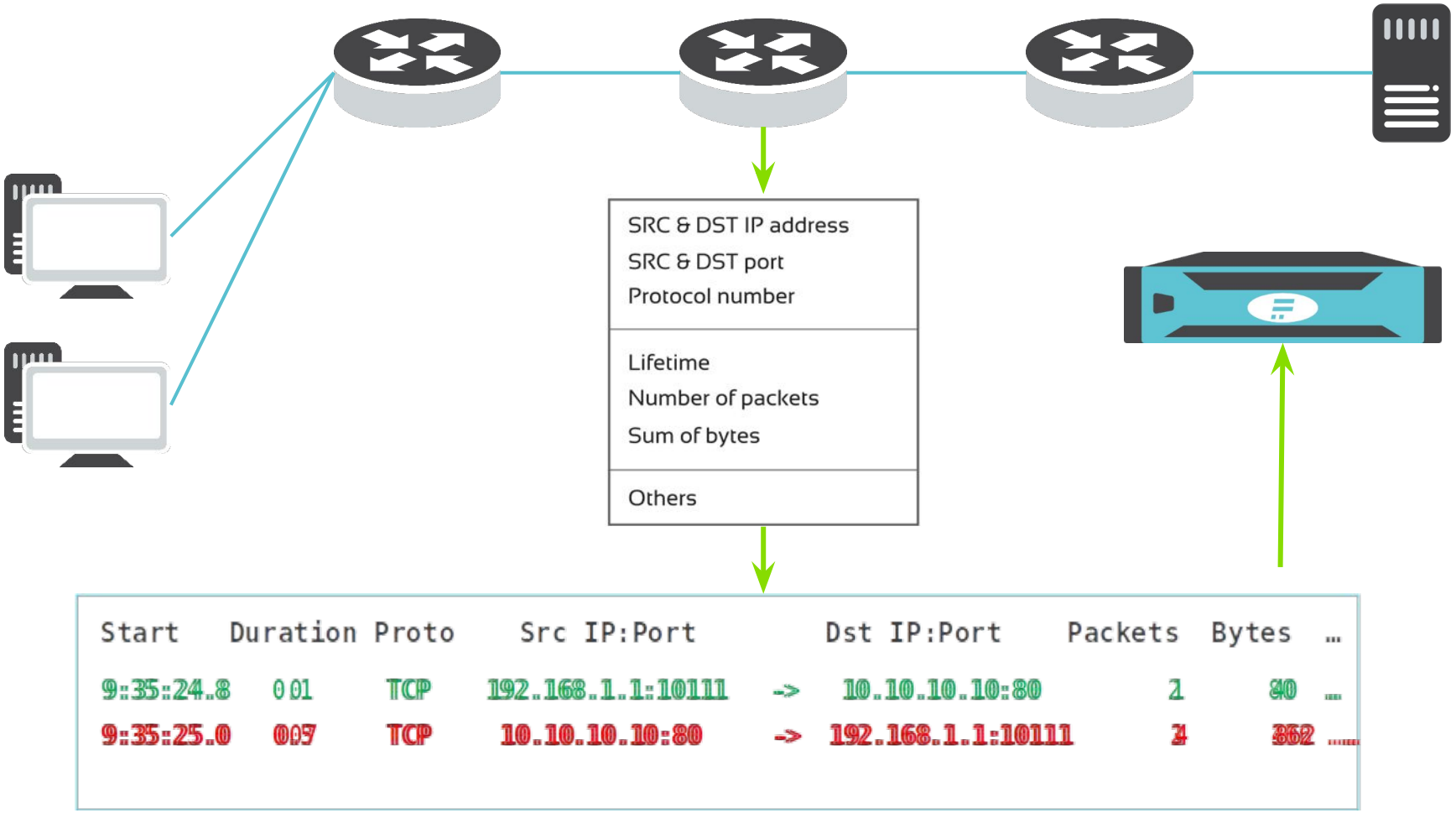
Flow export and collection

- Modern method for network monitoring – flow measurement
- NetFlow v5/v9, IPFIX, jFlow, sFlow,cflowd, NetStream, etc.
- Focused on L3/L4 information and volumetric parameters
- Flow statistics reduction ratio 500:1 and even more if sampling is configured

Flow export and collection

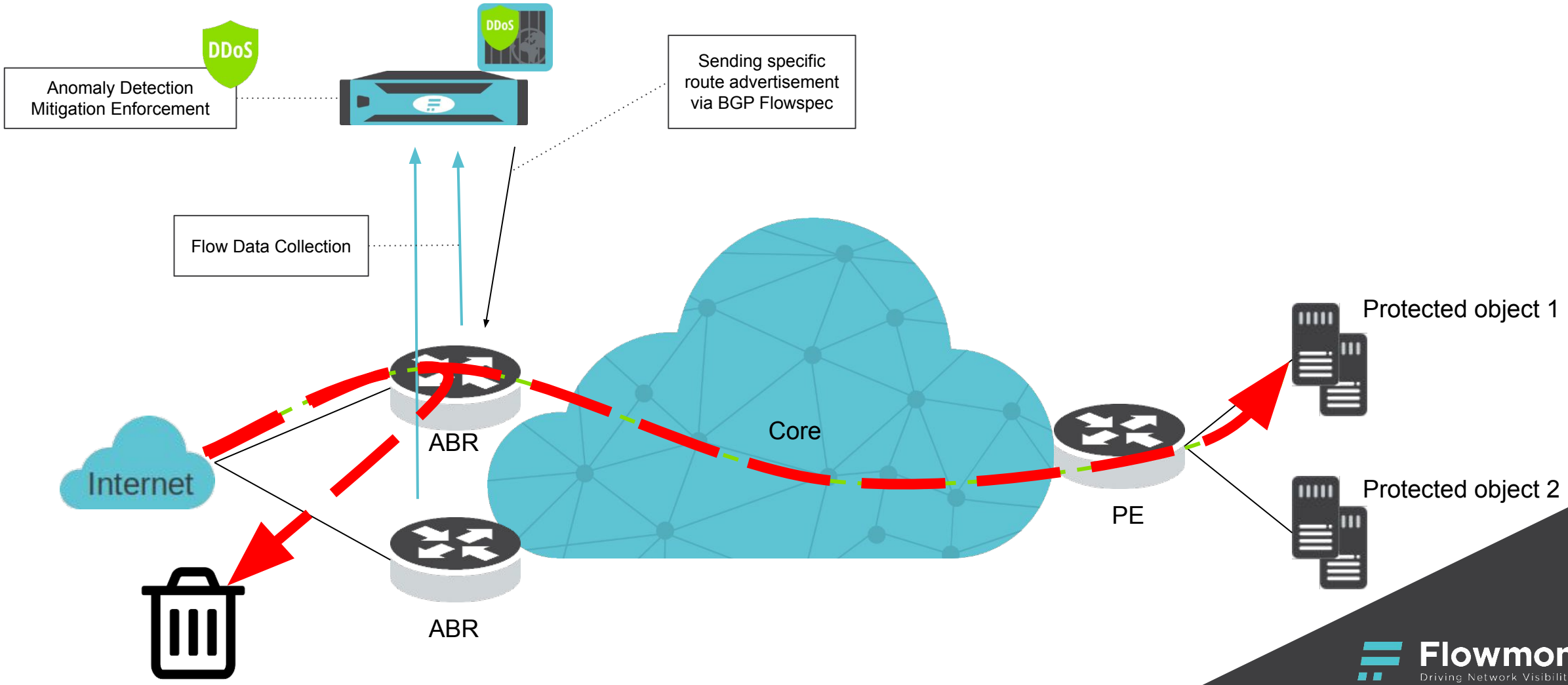
- Sampling is often needed but it does limit DDoS detection
- It’s important to have properly configured export timers
  - Shorter is better but also increasing a load on Flow exporter
- Number of devices with some flow export is growing
  - In carrier grade devices de facto standard
- Various use cases what can be done with exported data

Flow monitoring principle



Flowmon
Driving Network Visibility

How does it work



Flowmon
Driving Network Visibility

Live demonstration

Flowmon Networks

is an international vendor devoted to innovative network traffic & performance & security monitoring

800+ customers
35+ countries

First 100G probes in the world

Strong R&D background

European origin

Customer references

SEGA, AVG, KBC, Konica Minolta, vodafone, TDK, Oriflame Sweden, Siemens, Slovenská sporiteľňa, Volkswagen, orange, Telefónica, Allianz, hp, T-Mobile, GÉANT Networks • Services • People, KIA, upc, Raiffeisen BANK, e·on

Flowmon
Driving Network Visibility

Thank you

Performance monitoring, visibility and security with a single solution

Jiri Knapek, senior presales engineer

jiri.knapek@flowmon.com

Pavel Minarik, Chief Technology Officer

pavel.minarik@flowmon.com

Flowmon Networks a.s.
Sochorova 3232/34
616 00 Brno, Czech Republic
www.flowmon.com

Flowmon
Driving Network Visibility

References

[1] https://www.rfc-editor.org/info/rfc5575

[2] https://www.rfc-editor.org/info/rfc7674