DDOS Attack Mitigation with RTBH

Author: Thein Myint Khine

Version: 0.0

Last Update: October 15, 2025

MYANMAR NETWORK OPERATORS GROUP

Volume Metric Attack

ICMP/TCP/UDP Flood, NTP/DNS Amplification

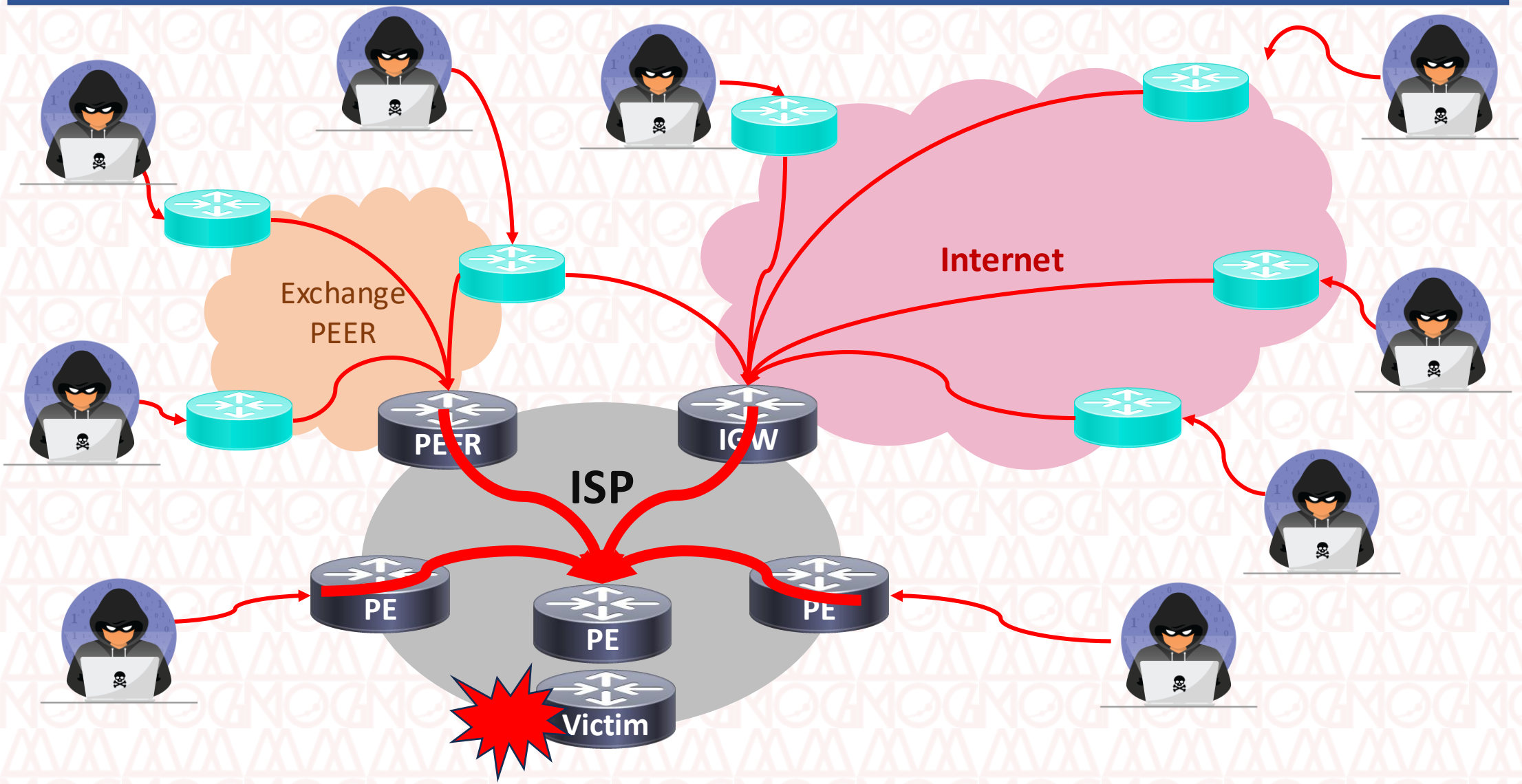
How to prevent DDOS?

- Cloud-based DDoS protection services
- CDNs to absorb and distribute traffic
- rate limiting to control request volume
- web application firewalls (WAFs) to protect against application-layer attack

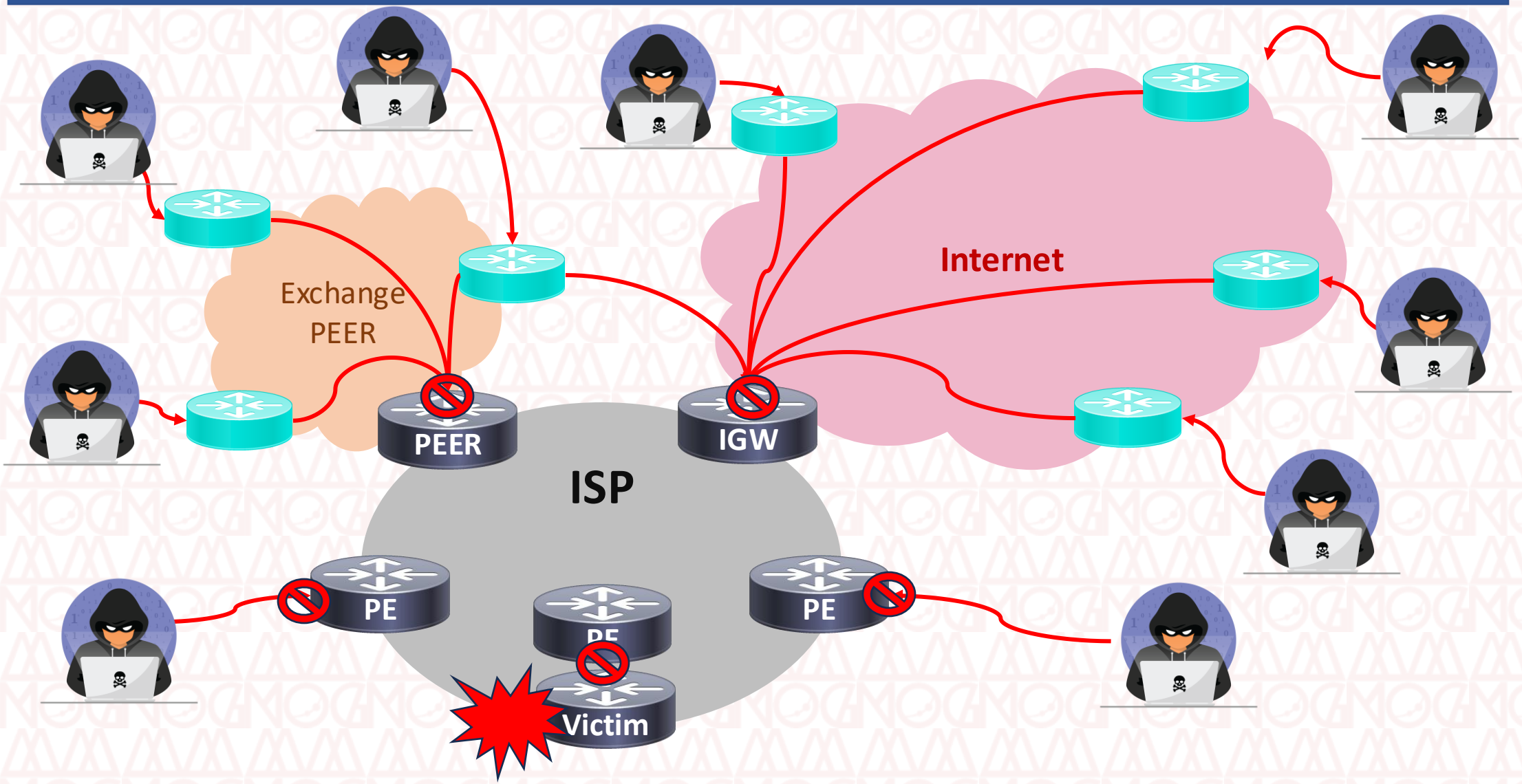
How to prevent DDOS?

- Anycast
- Scaling network capacity
- Traffic filtering
- Blackholing (or null routing)
- Sinkholing

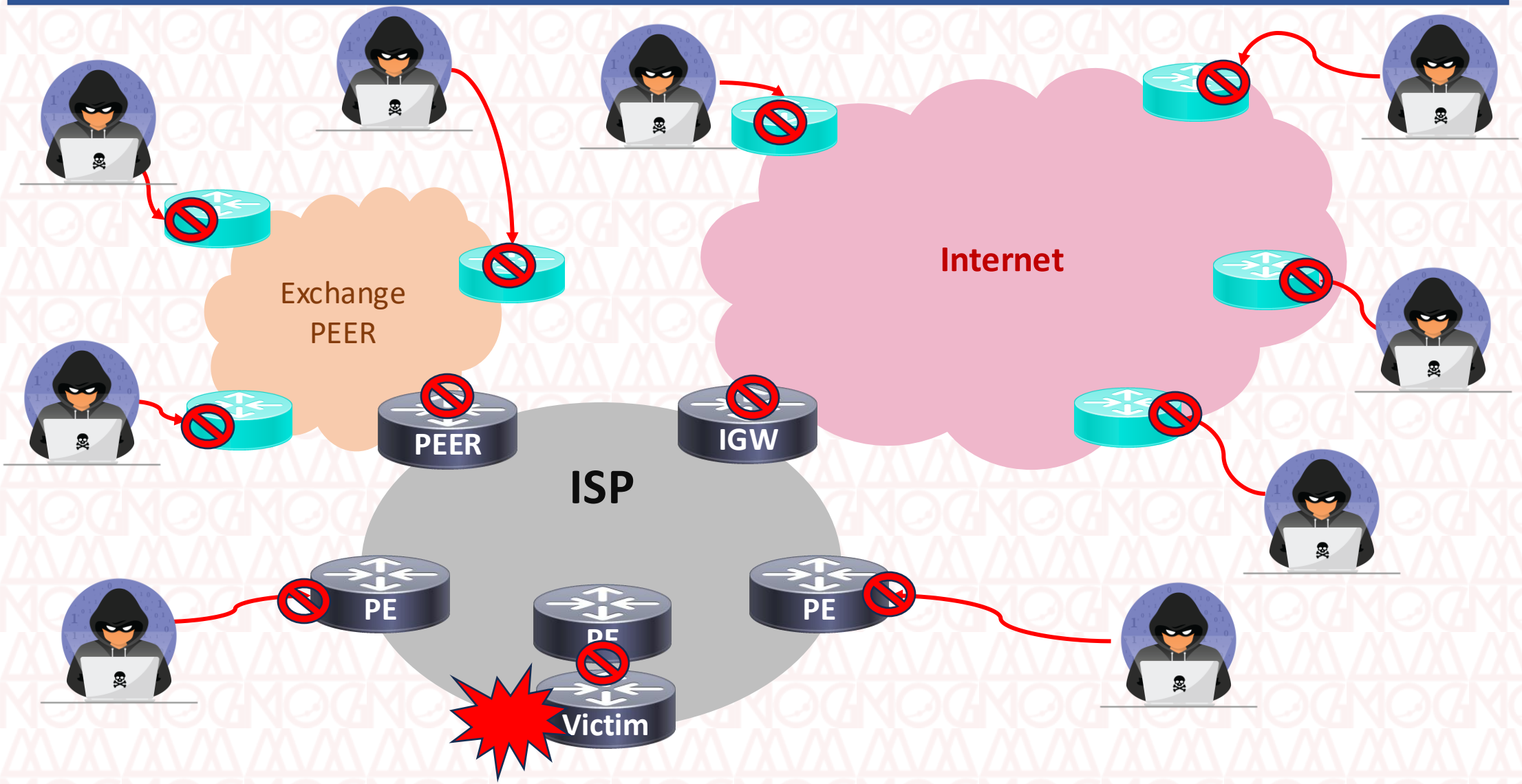
DDOS Attach from all direction



DDOS Self-Prevention



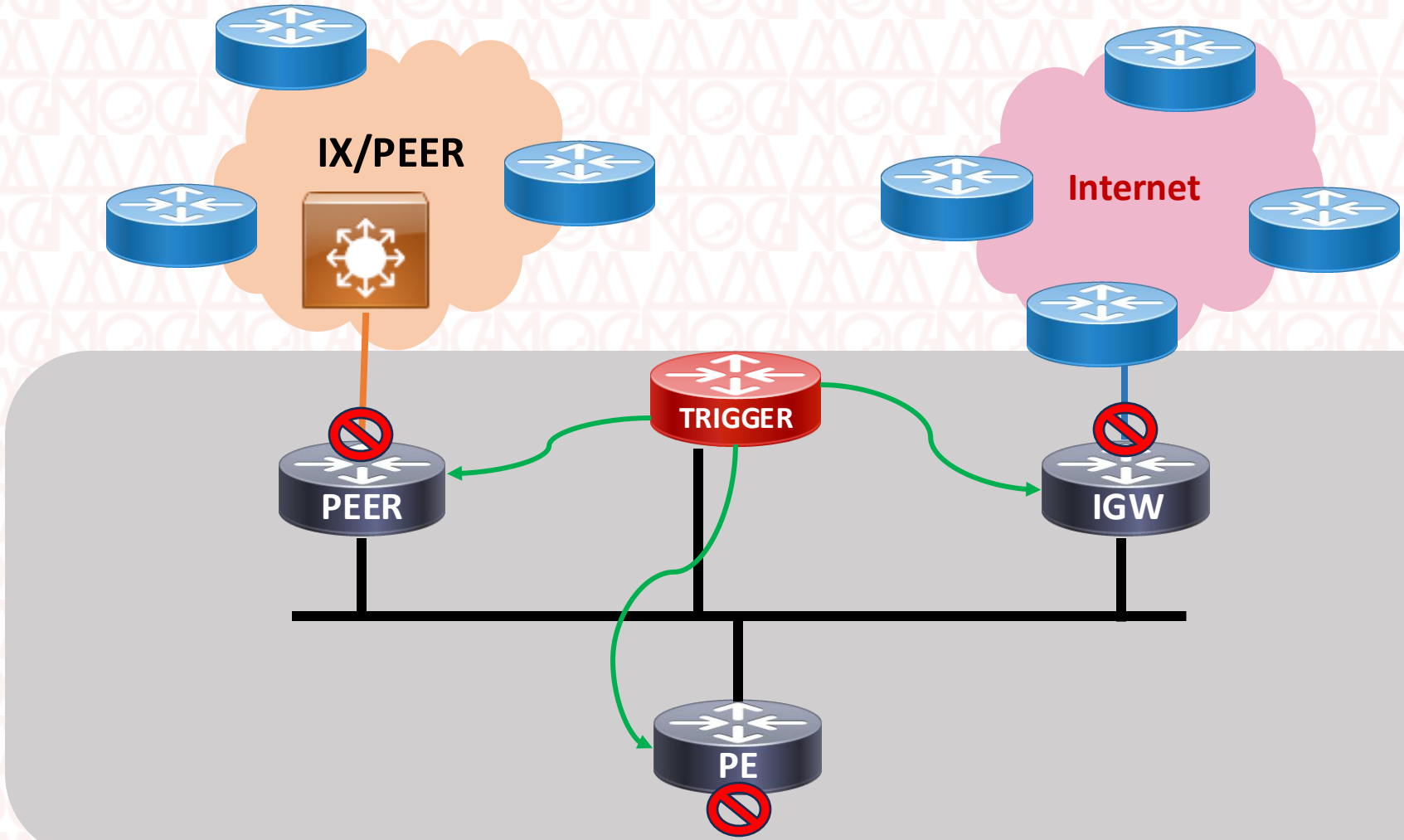
DDOS Prevention – drop nearest to sources



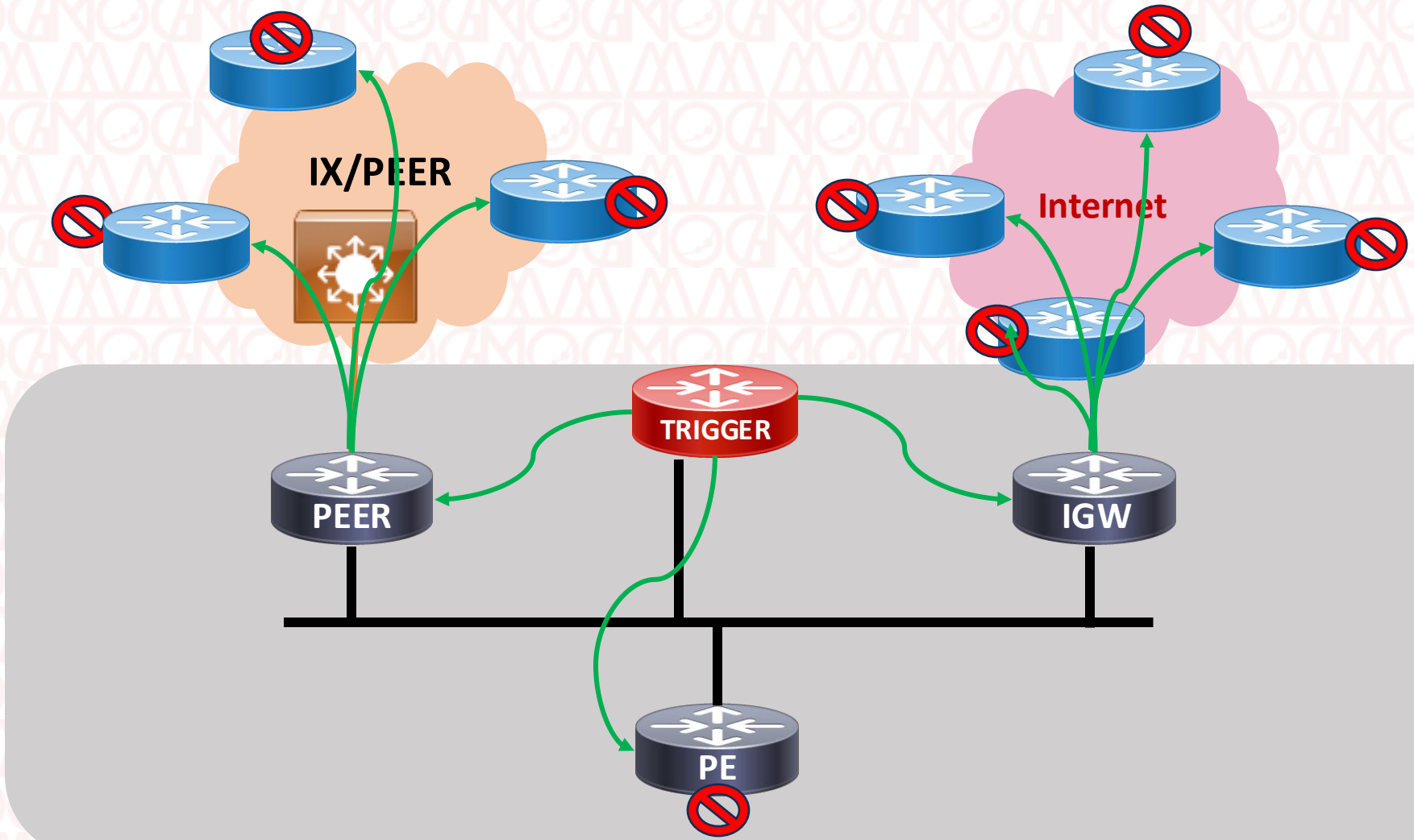
Zero Cost Protection

RTBH/UTRS

Prevention with RTBH



Dealing with Others



RTBH Prons & Cons

Pros	Cons
Efficient for large volumetric attacks	**Indiscriminate traffic dropping:** can impact legitimate traffic.
Simple and fast deployment	**Ineffective against certain attacks:** can't solve Application-level attack.
Protects shared infrastructure	**Can cause more problems:** If attacks are directed at multiple IP
Flexible	**Limited control:** If a customer relies on an ISP to trigger RTBH, they lose some control and reactiveness in an emergency.

Thank you

Q&A

Thein Myint Khine
theinmyintkhine@mm-ix.net

www.mmnog.net.mm

event@mm-ix.net