

# DDOS Attack Mitigation with RTBH



**mmnog**

Author: Thein Myint Khine

Version: 0.0

Last Update: October 15, 2025

**MYANMAR NETWORK OPERATORS GROUP**

# DDOS Attack Types

1. **Volumetric attack**  
(Bandwidth overload)
2. **Protocol level attack**  
(server resource exhaustion)
3. **Application Layer attack**  
(service-specific, low rate)



# Volume Metric Attack

ICMP/TCP/UDP Flood, NTP/DNS  
Amplification



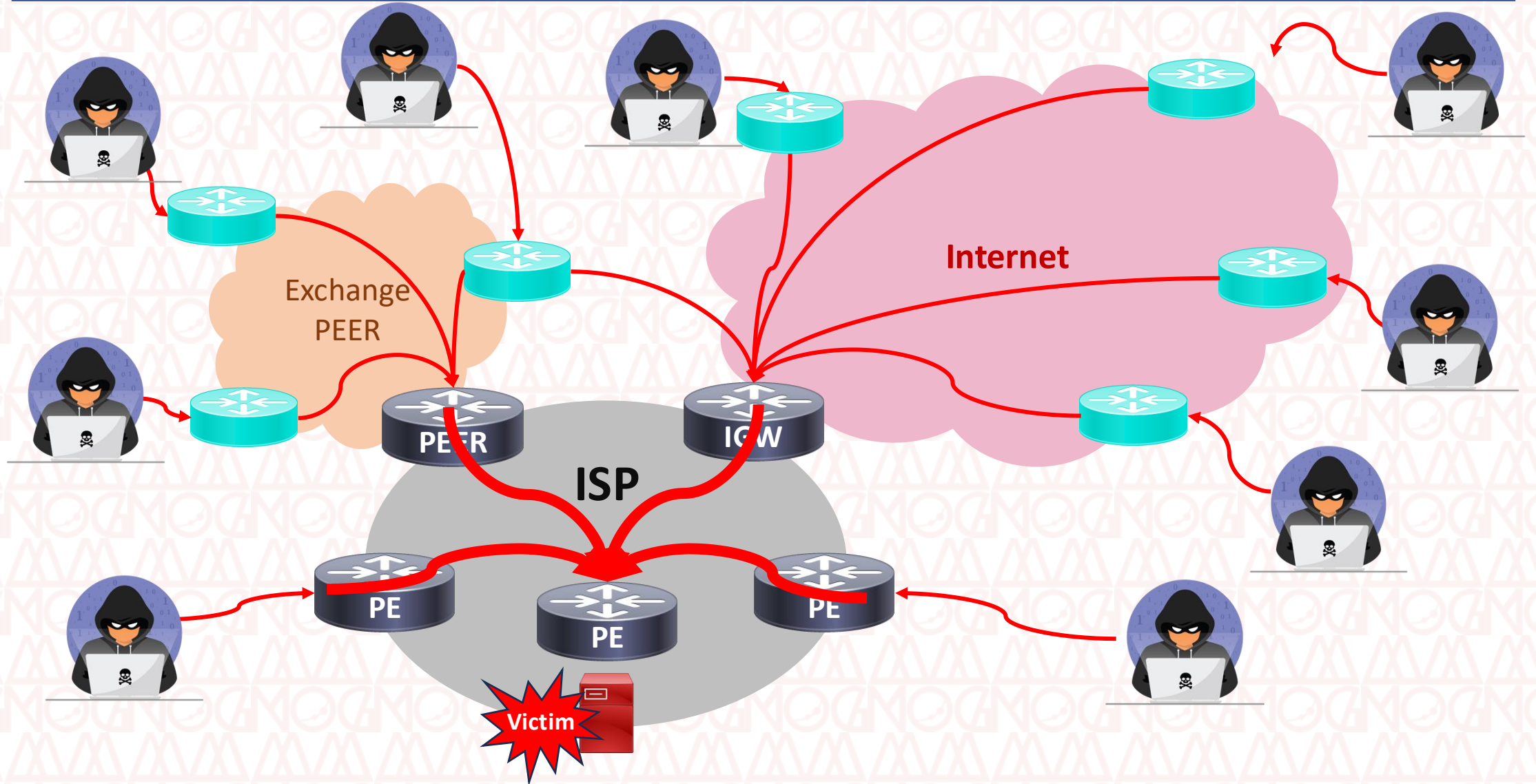
# How to prevent DDoS?

- 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

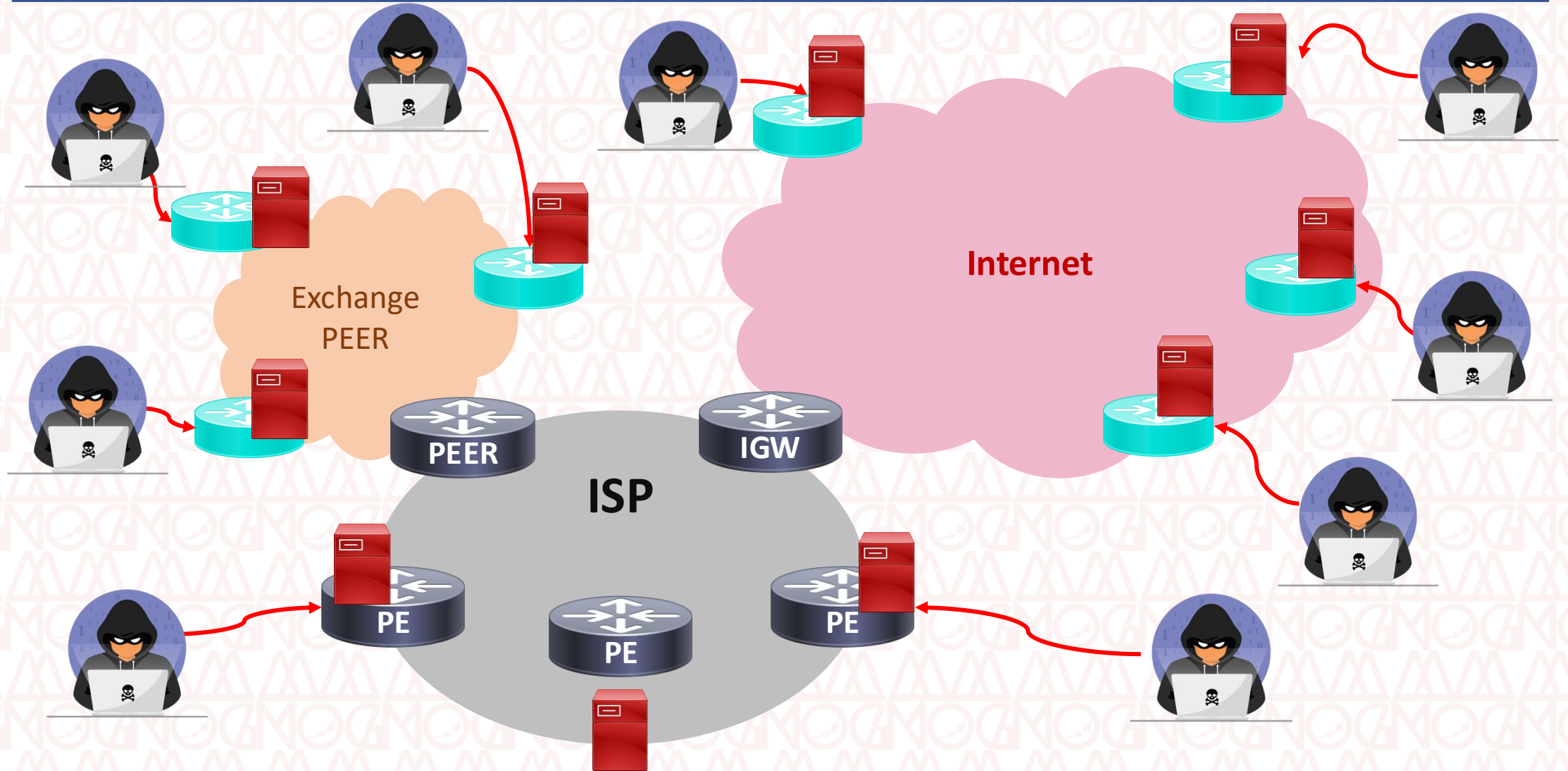
# How to prevent DDOS?

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

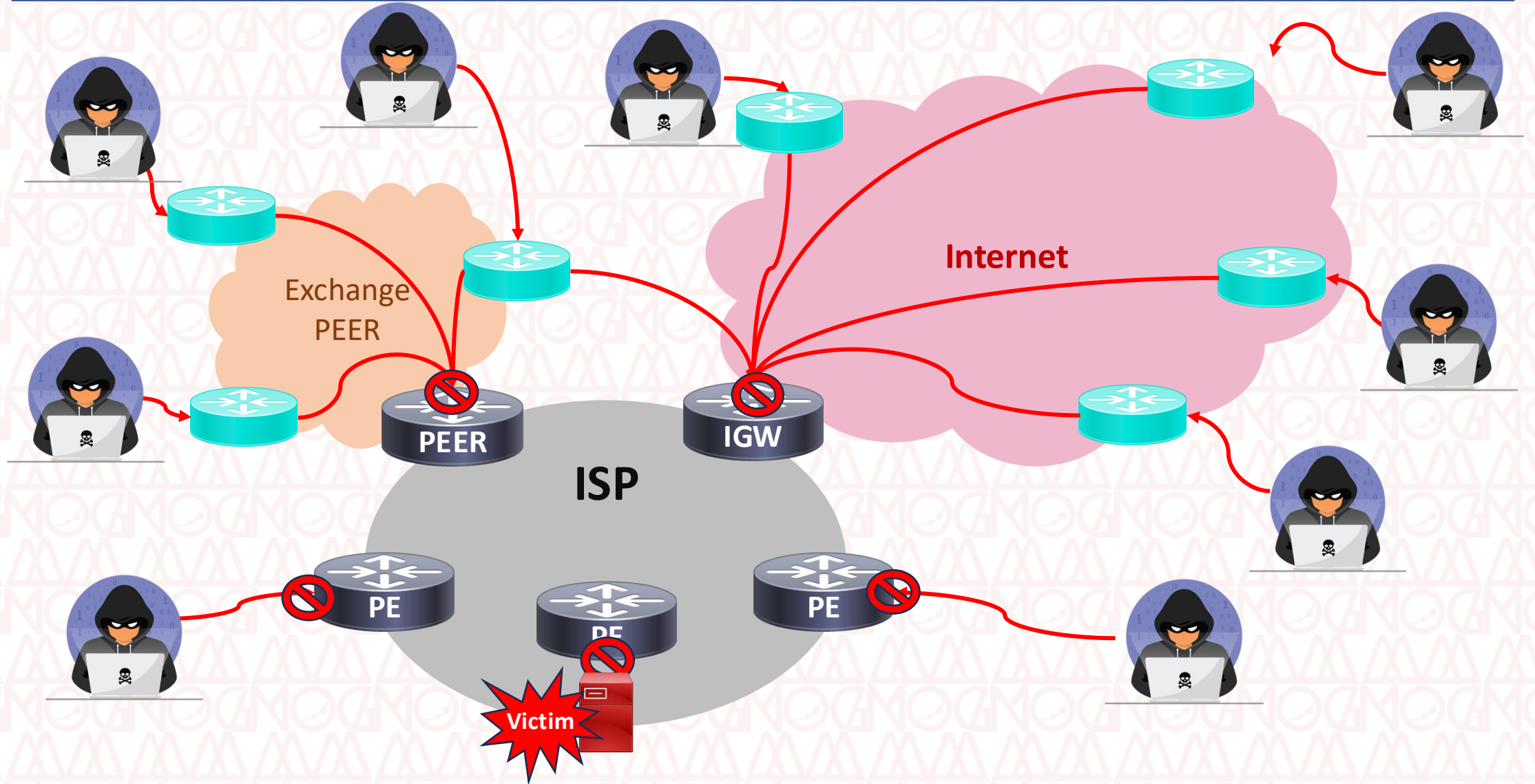
# DDOS Attack from all direction



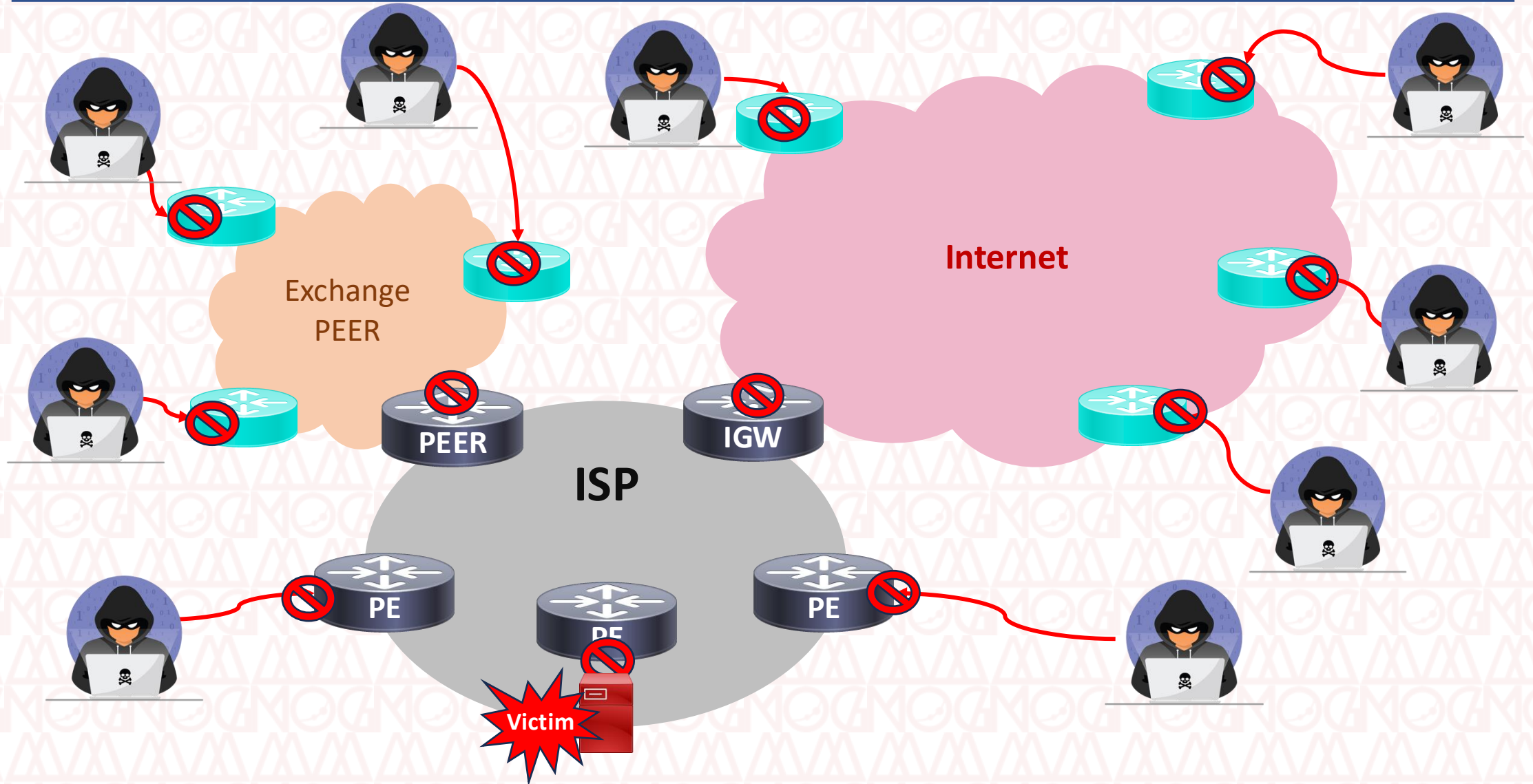
# Anycast / CDN



# DDOS Self-Prevention



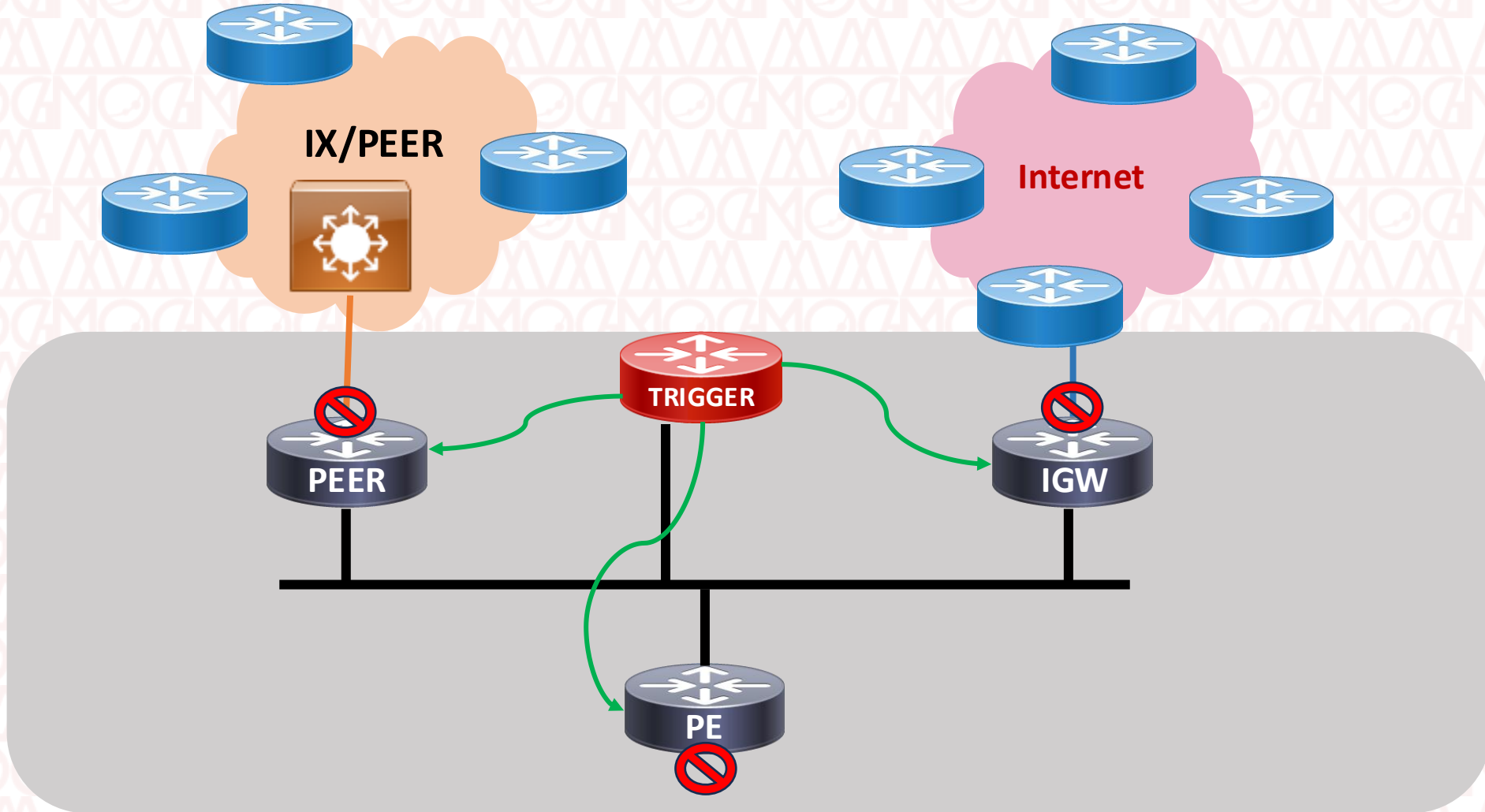
# DDOS Prevention – drop nearest to sources



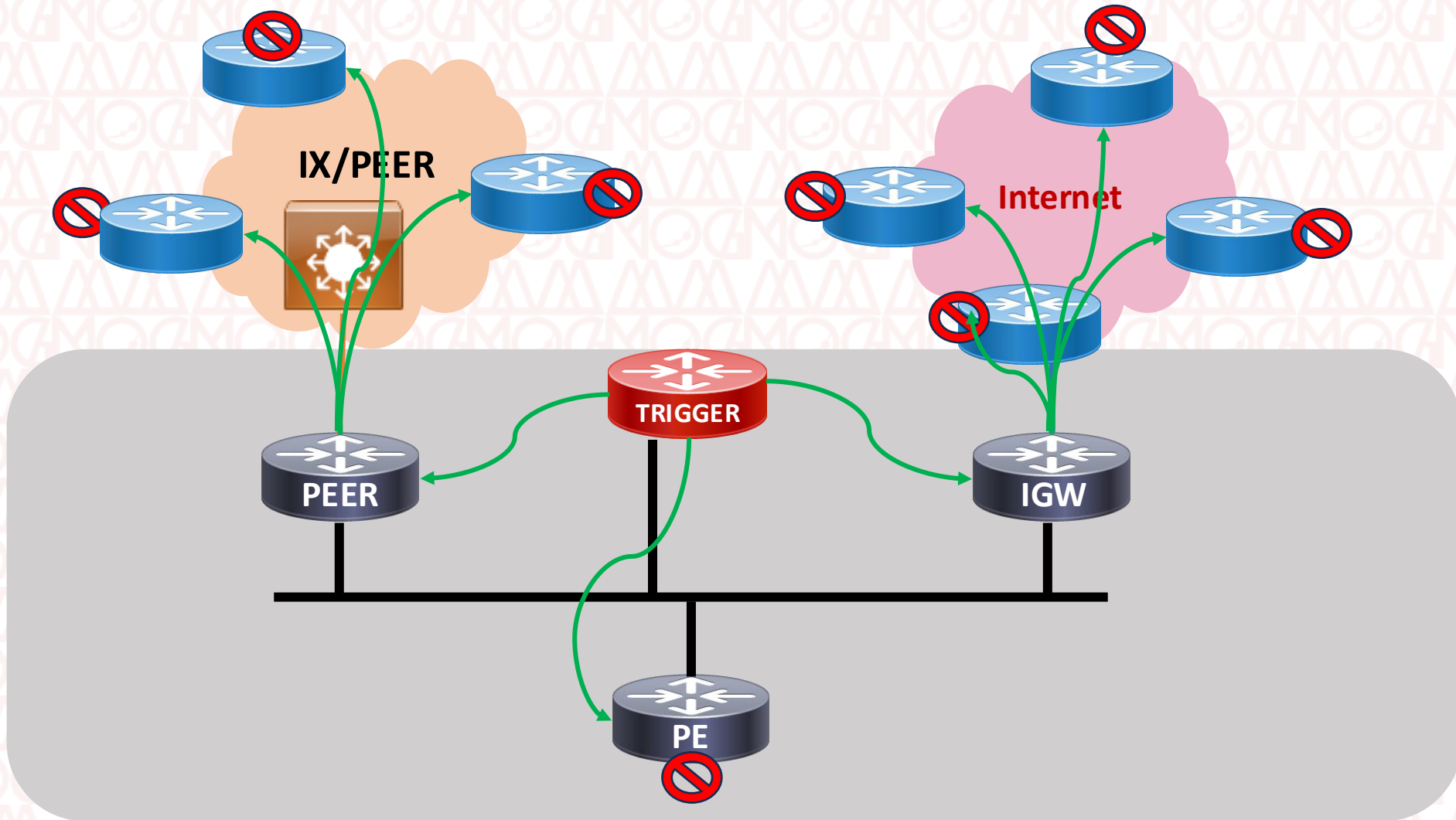
# Zero Cost Protection

## RTBH/UTRS

# Prevention with RTBH



# Dealing with Others





Pros	Cons
<b>Efficient for large volumetric attacks</b>	<b>Indiscriminate traffic dropping</b> can impact legitimate traffic.
<b>Simple and fast deployment</b>	<b>Ineffective against certain attacks:</b> can't solve Application-level attack.
<b>Protects shared infrastructure</b>	<b>Can cause more problems:</b> If attacks are directed at multiple IP
<b>Flexible</b>	<b>Limited control:</b> 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](http://www.mmnog.net.mm)

[event@mm-ix.net](mailto:event@mm-ix.net)