DDoS in Indonesia

Has it improved?

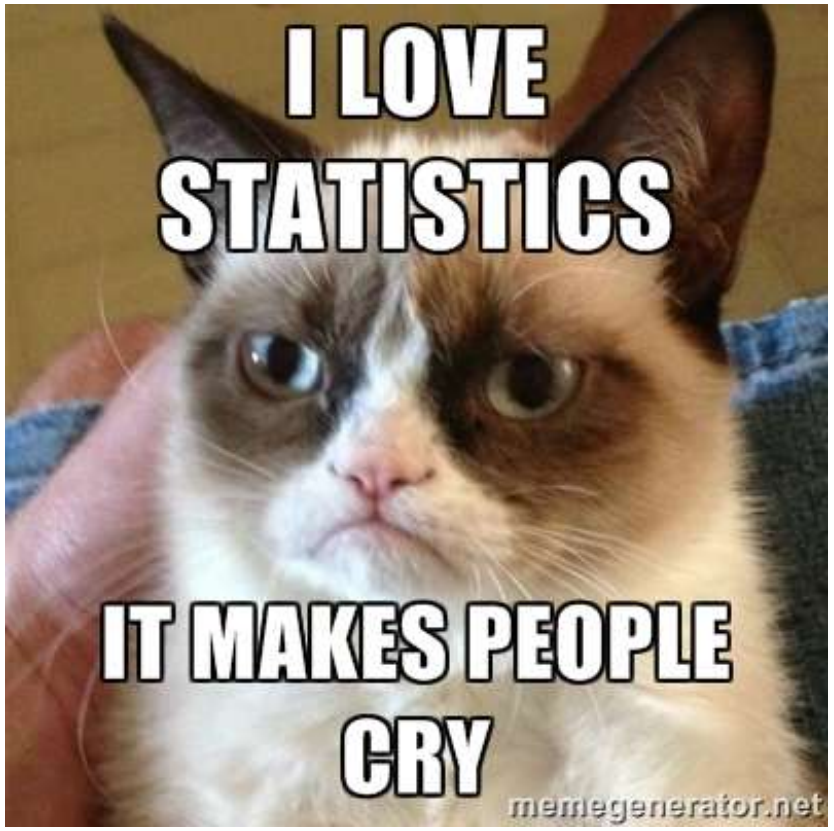
Dave Phelan - APNIC

Who Am I?

- Dave Phelan
  - Network and Infrastructure engineer for a LONG time
  - Policy Manager and Trainer at APNIC
  - Likes Cat memes

What are we going to talk about?

- Security Stats
  - How many doors are open?
  - How does this affect me (and the rest of the internet)
  - What can I do to help?



Why do we care about the numbers?

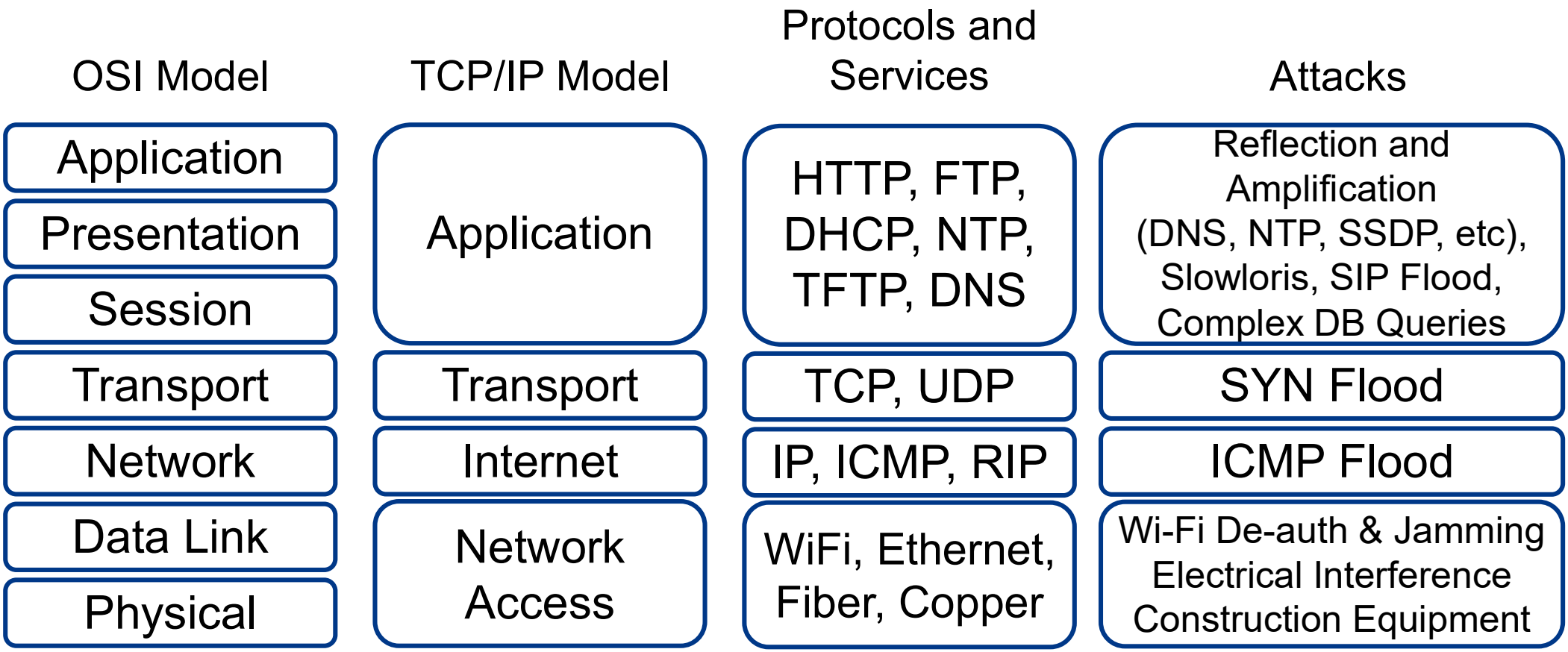
- We can use this as a benchmark
  - How are we performing
    - Network to Network
    - Economy to Economy
    - Region to Region
- What do we need to “fix”
  - Are we doing all we can within our region (see Benchmarks Above)
- Can we do better
  - For our networks and our users

Sources

- Data for this presentation have come from numerous sources
  - https://radar.cloudflare.com
  - https://shodan.io
  - https://cybergreen.net

Through the Layers

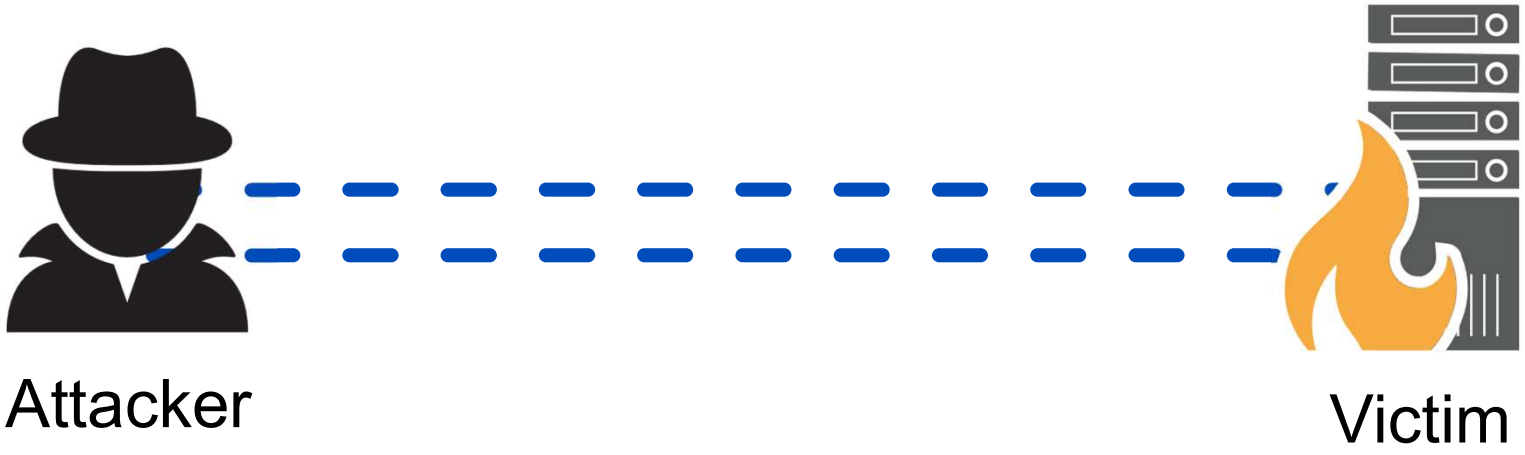
DoS by Layers



* Colour animated slide

Simple DoS

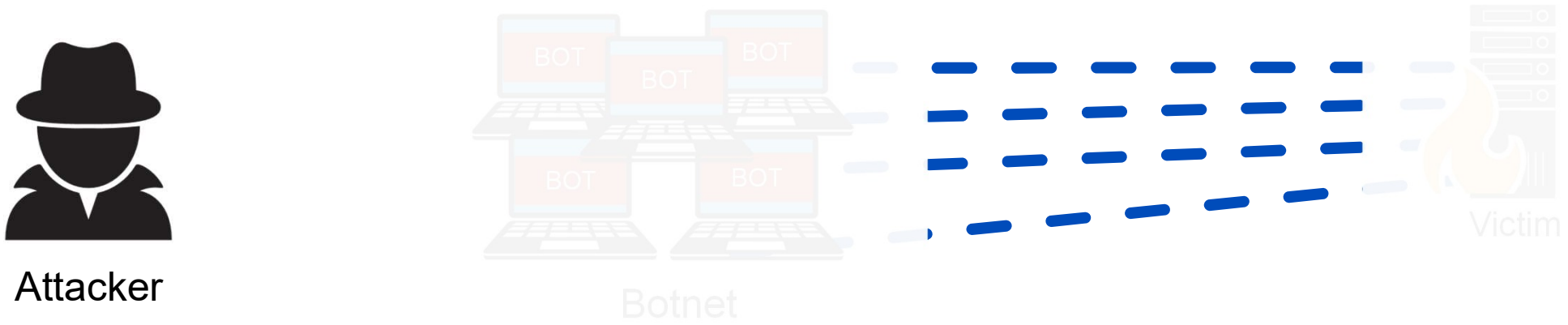
1 Attacker sends any valid or invalid traffic to the victim



Simple DDoS

1 Attacker directs bots to begin attack

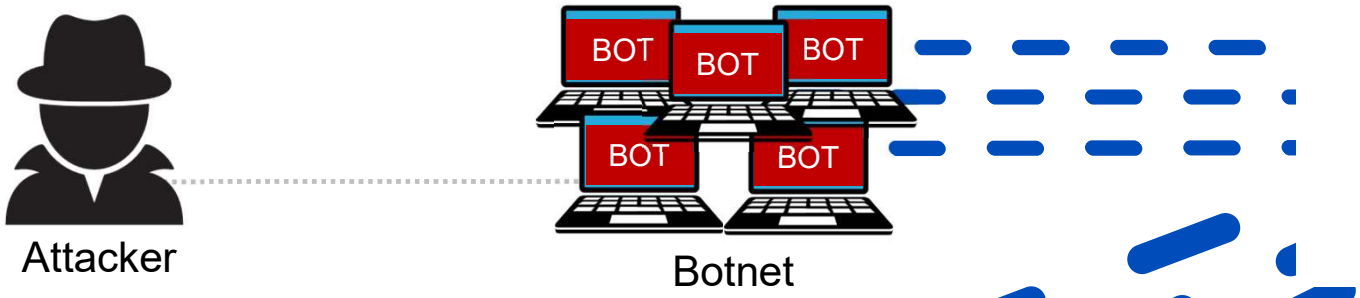
2 All bots send any valid or invalid traffic to the victim



Reflected and Amplified DDoS

1 Attacker directs bots to begin attack

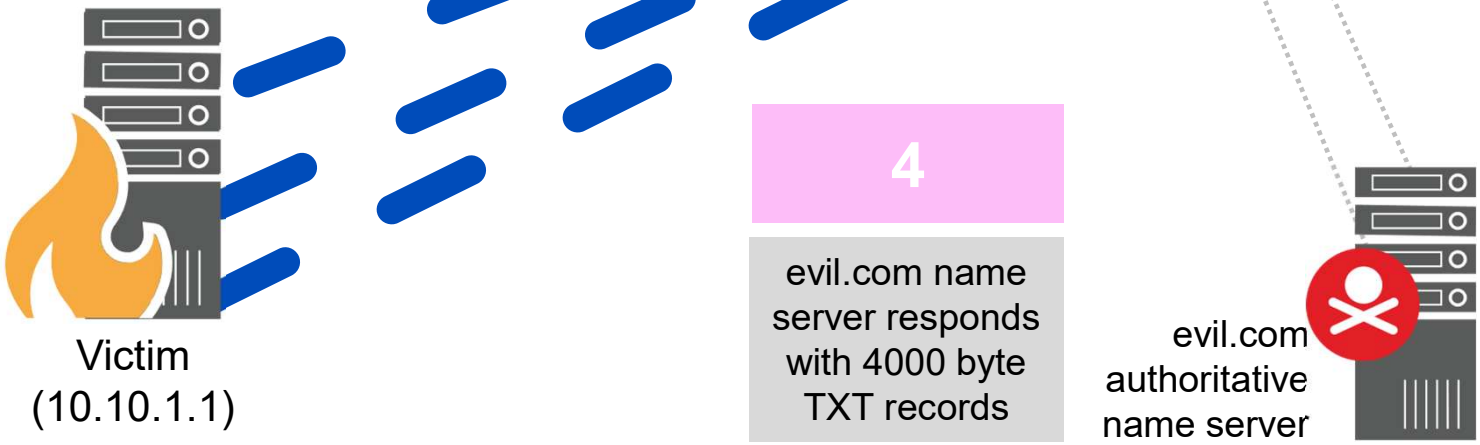
2 All bots send DNS queries for the TXT record in domain “evil.com” to open recursive DNS servers and fake "my IP is 10.10.1.1"



3 Open resolvers ask the authoritative name server for the TXT record “evil.com”

4 evil.com name server responds with 4000 byte TXT records

5 Open resolvers cache the response and send a stream of 4000 byte DNS responses to the victim



Reflection and Amplification

- What makes for good reflection?
  - UDP
    - Spoofable / forged source IP addresses
    - Connectionless (no 3-way handshake)
- What makes for good amplification?
  - Small command results in a larger reply
    - This creates a Bandwidth Amplification Factor (BAF)
    - Reply Length / Request Length = BAF
      - Example: 3223 bytes / 64 bytes = BAF of 50.4
    - Chart on next slide created with data from https://www.us-cert.gov/ncas/alerts/TA14-017A

Amplification Factors

Protocol	Bandwidth Amplification Factor
Multicast DNS (mDNS)	2-10
BitTorrent	3.8
NetBIOS	3.8
Steam Protocol	5.5
SNMPv2	6.3
Portmap (RPCbind)	7 to 28
DNS	**28 to 54**
SSDP	**30.8**

Protocol	Bandwidth Amplification Factor
LDAP	46 to 55
TFTP	60
Quake Network Protocol	63.9
RIPv1	131.24
QOTD	140.3
CHARGEN	358.8
NTP	**556.9**
Memcached	**up to 51,000**

So why are you telling me this?

- Operators Complain about DoS/DDoS
- Do the minimum to ensure they are not contributing

- But how bad is it really?

Global Numbers

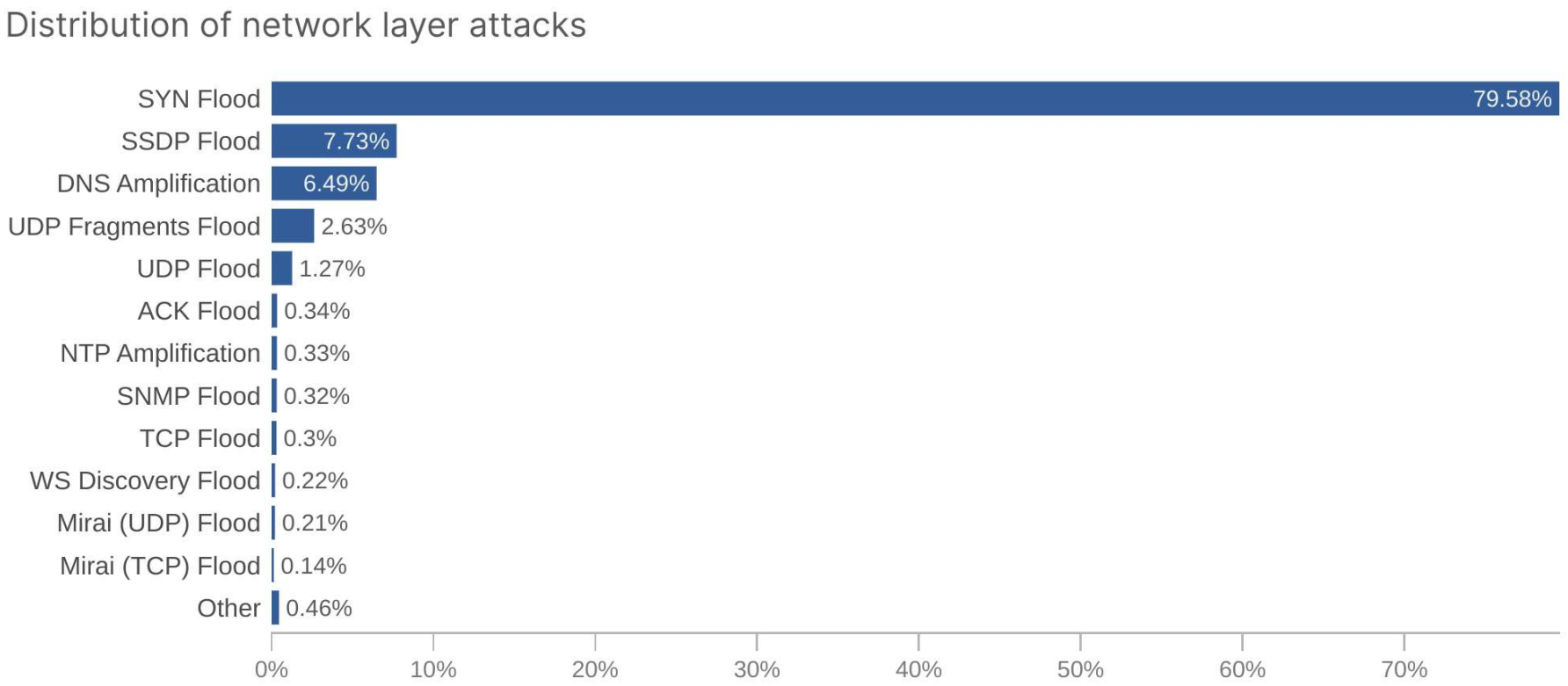
- Most data sourced from
  - Cloudflare Radar
  - Shodan.io

OCT 2023	APR 2024	JUL 2024	FEB 2026
USA - 31%	USA – 22.6%	USA – 18.8%	USA - 20.2%
India – 9.2%	Germany – 6.5%	Germany – 8.45%	**Singapore - 5.0%**
Germany – 5.4%	**China - 5.5%**	**China - 7.49**	**China – 4.9%**
Brazil – 5.2%	**Indonesia – 4.7%**	**Pakistan – 5.9%**	Germany – 4.8%
China – 3.3%	Brazil – 4.3%	UK – 4.5%	**Indonesia – 4.7%**

https://radar.cloudflare.com/security-and-attacks

Global Numbers – July 2024

Network layer attack distribution (Worldwide)

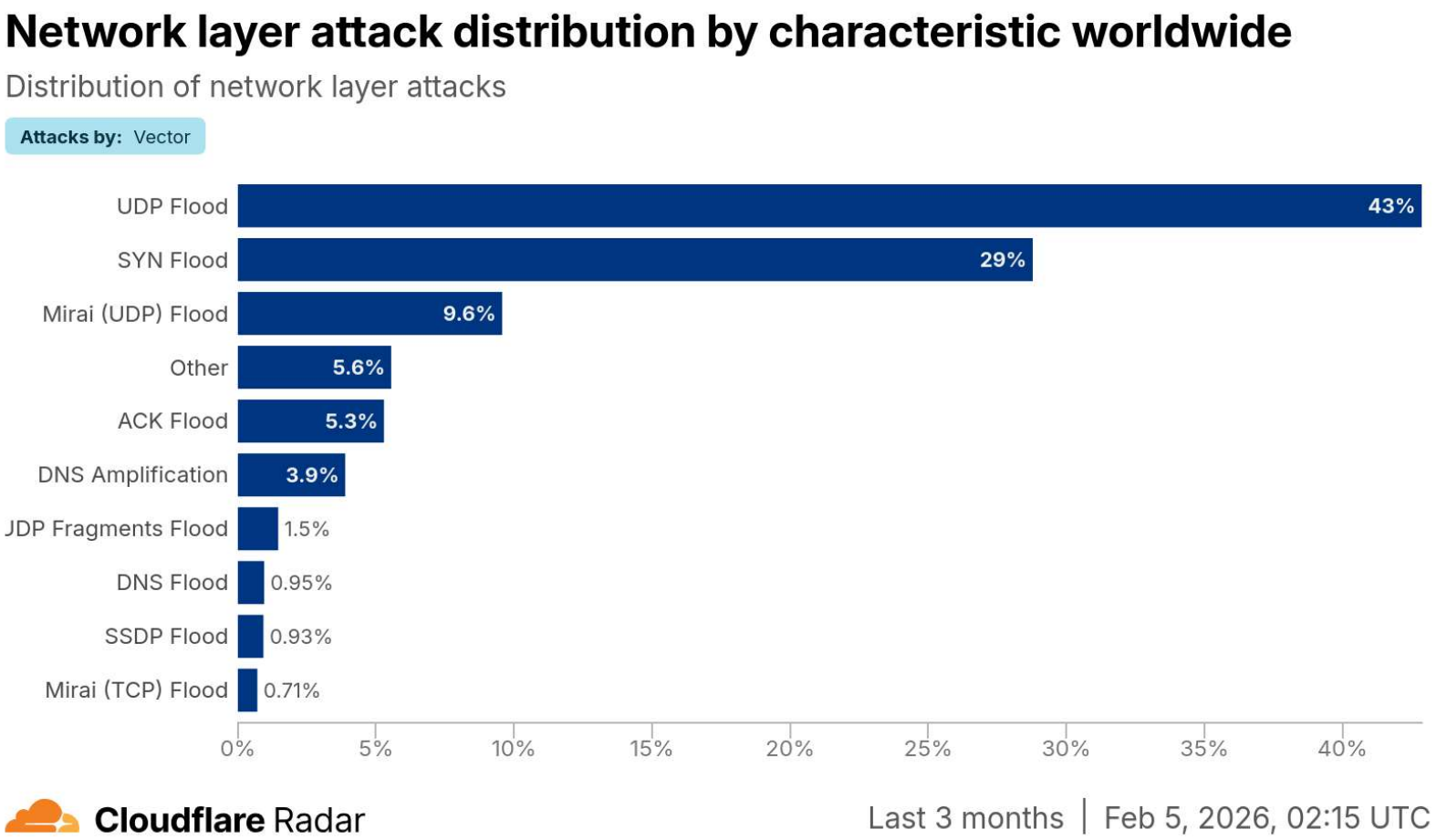


Cloudflare Radar

Last 7 days | Jul 21 2024 03:50 UTC

https://radar.cloudflare.com/security-and-attacks

Global Numbers – February 2026



https://radar.cloudflare.com/security/network-layer?dateRange=12w

Indonesia

Top Source Networks August 2024:

#	ASN	%
1	7713 - TELKOMNET-AS-AP PT Telekomunikasi Indonesia	**12.0%**
2	17451 - BIZNET-AS-AP BIZNET NETWORKS	**3.4%**
3	23693 - TELKOMSEL-ASN-ID PT. Telekomunikasi Selular	**2.5%**
4	4761 - INDOSAT-INP-AP INDOSAT Internet Network Provider	**2.2%**
5	38511 - TACHYON-AS-ID PT Remala Abadi	**2.1%**

https://radar.cloudflare.com/security-and-attacks/id?dateRange=12w

Indonesia

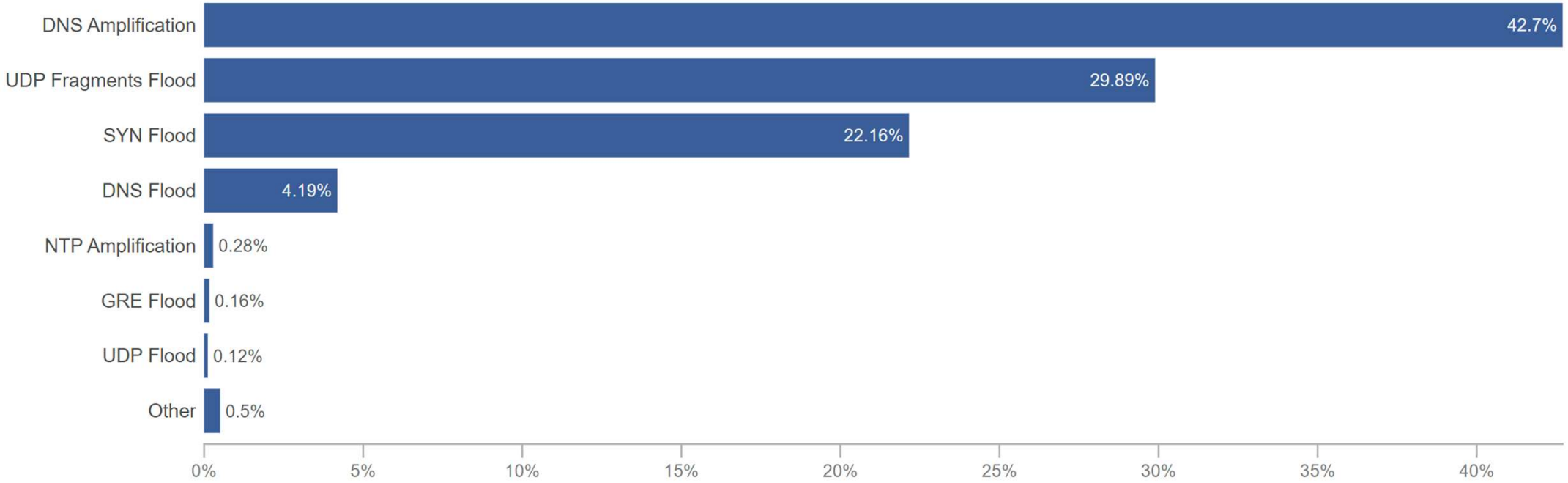
Top Source Networks February 2026:

#	ASN	%
1	7713 - TELKOMNET-AS-AP PT Telekomunikasi Indonesia	**8.0%**
2	23693 - TELKOMSEL-ASN-ID PT. Telekomunikasi Selular	**3.7%**
3	4761 - INDOSAT-INP-AP INDOSAT Internet Network Provider	**3.6%**
4	17451 - BIZNET-AS-AP BIZNET NETWORKS	**2.3%**
5	AS58821 - IDNIC-LJN-AS-ID PT Lintas Jaringan Nusantara	**2.2%**

https://radar.cloudflare.com/security-and-attacks/id?dateRange=12w

Indonesia

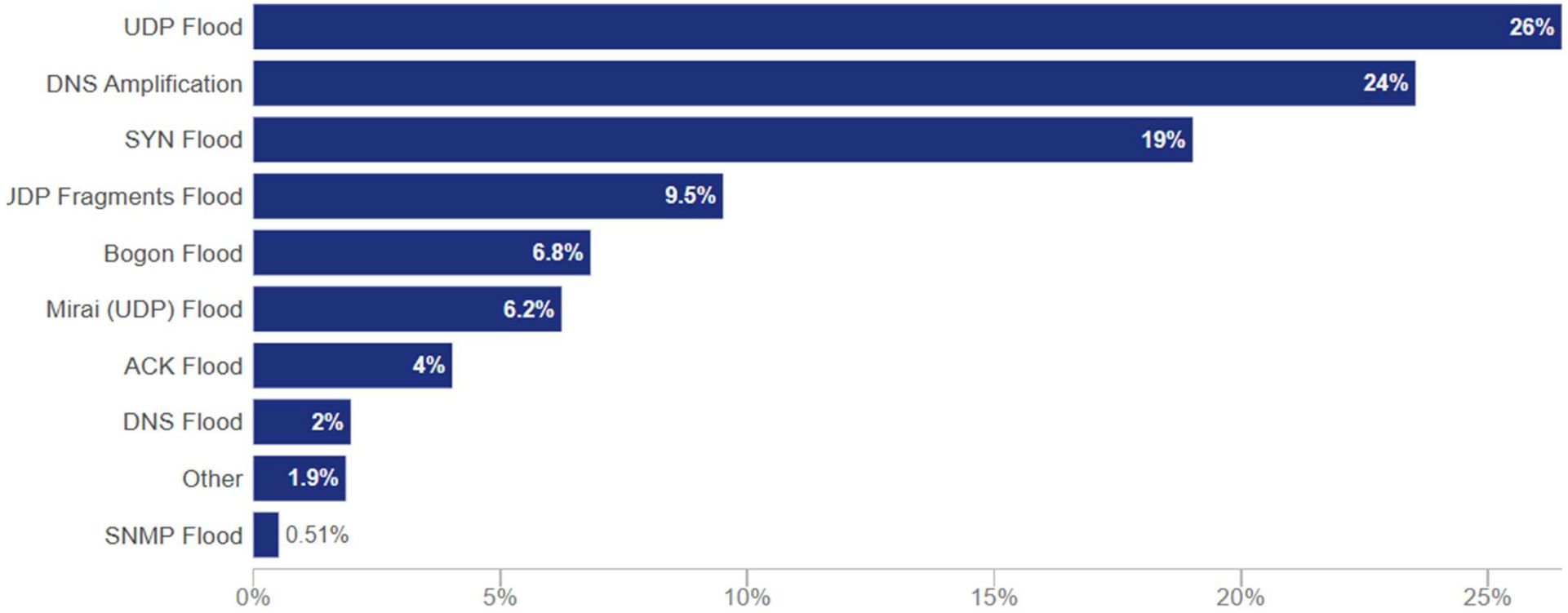
Attack Types – July 2024



https://radar.cloudflare.com/security-and-attacks/id?dateRange=12w

Indonesia

Attack Types – February 2026



https://radar.cloudflare.com/security/network-layer/id?dateRange=12w

Indonesia

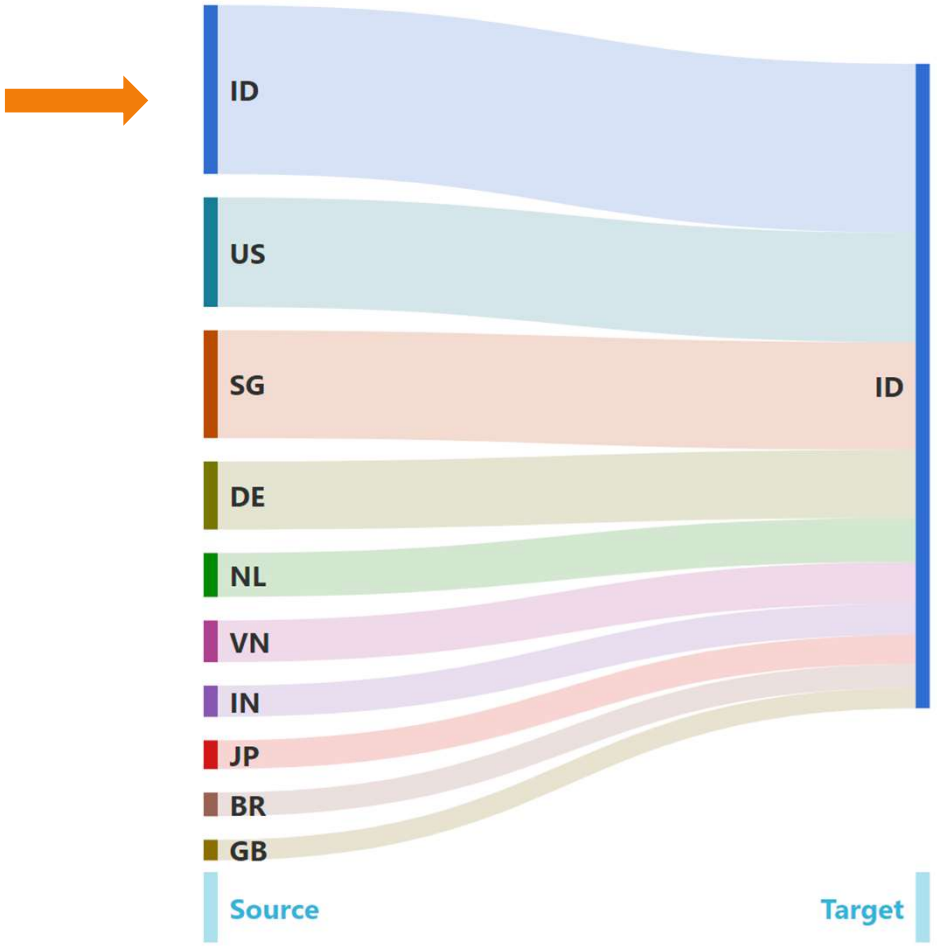
- Open Ports

Service	AUG-2024	FEB-2026
DNS	103,367	99,357
NTP	66,532	**73,814**
SSDP	556	**634**
MemcacheD	705	559
Telnet	15,838	10,186
SNMP	93,126	81,205
Winbox	73,809	56,182

https://www.shodan.io/search?query=country%3Aid

Indonesia

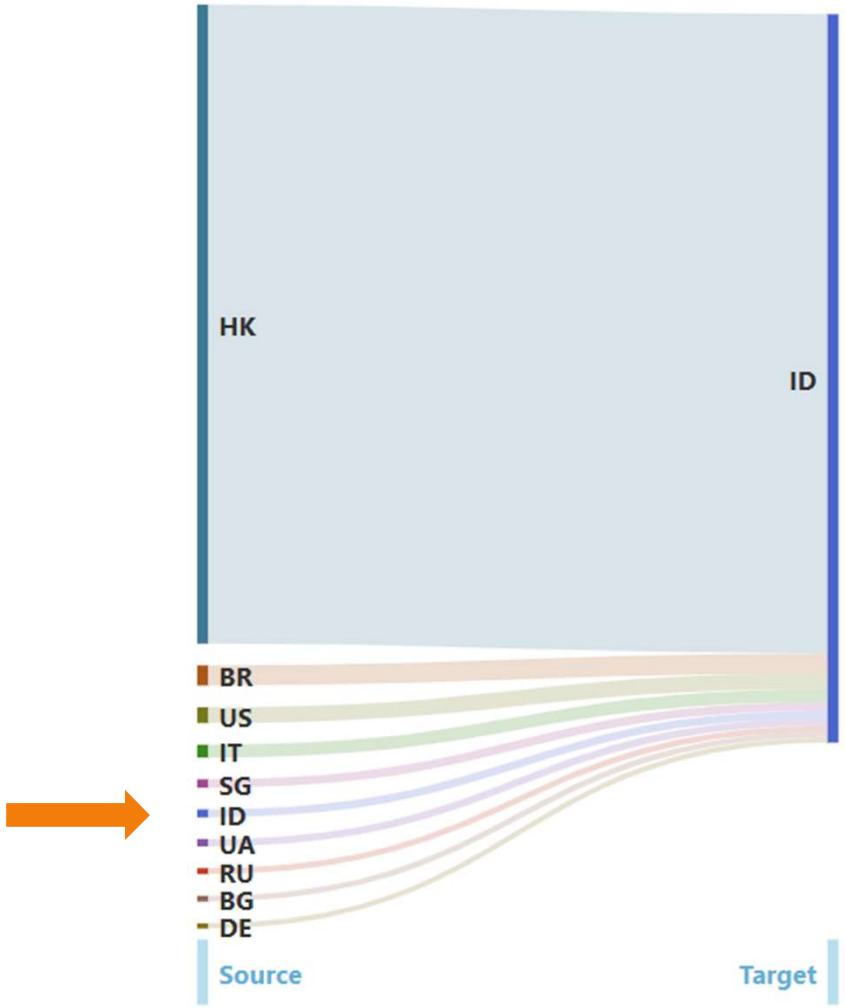
- Targets
  - Jul 2024



https://radar.cloudflare.com/security-and-attacks/id?dateRange=12w

Indonesia

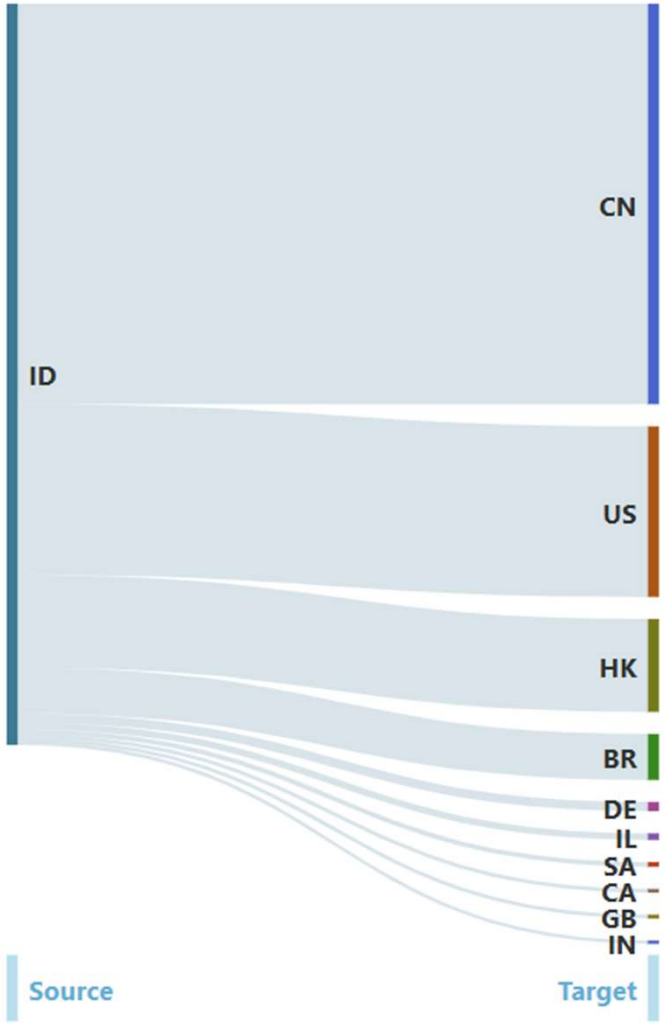
- Targets
  - Feb 2026



https://radar.cloudflare.com/security/network-layer/id?dateRange=12w

Indonesia

- Source
  - Feb 2026



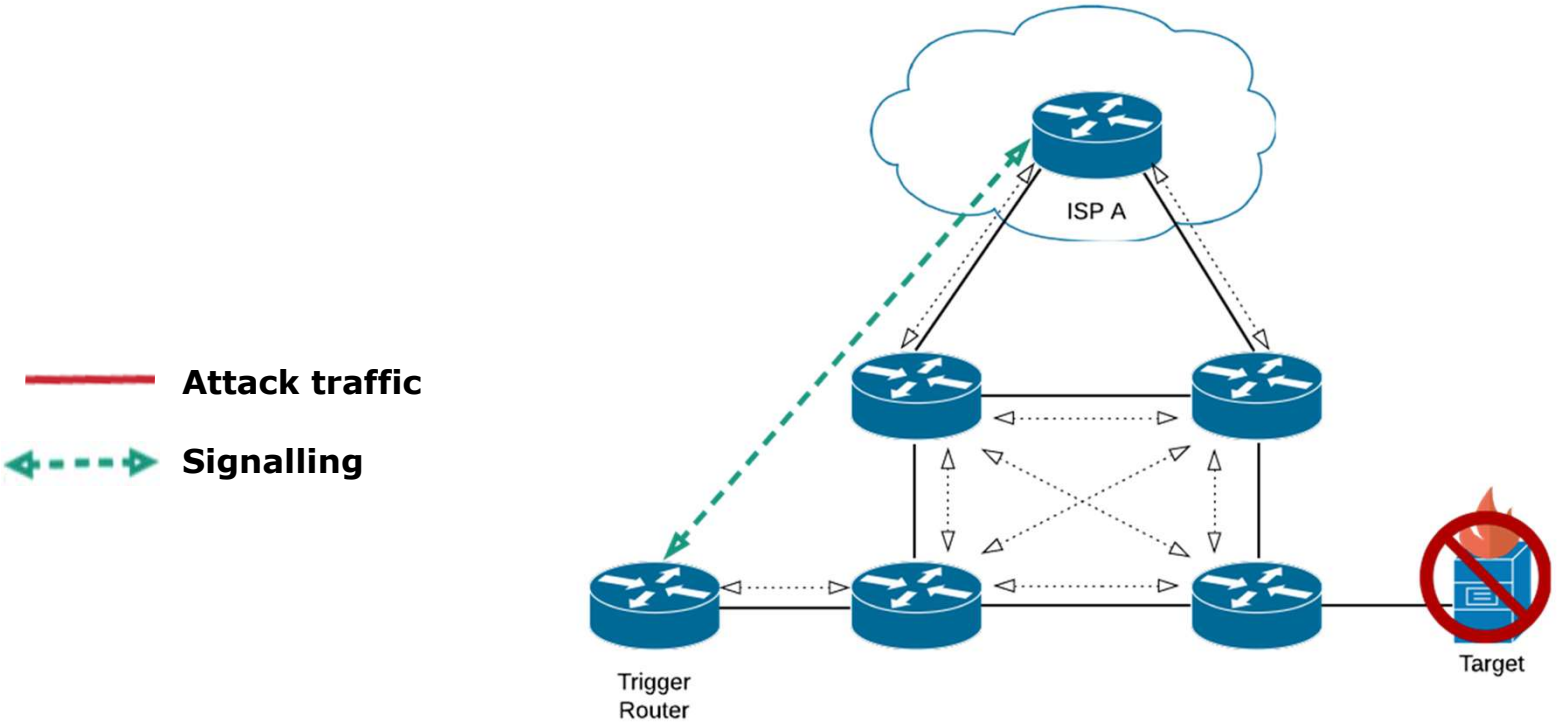
https://radar.cloudflare.com/security/network-layer/id?dateRange=12w

Mitigation Strategies

- Protect your services from attack
  - Anycast
  - IPS / DDoS protection
  - BGP Flowspec
  - Overall network architecture
- Protect your services from attacking others
  - Rate-limiting
  - BCP38 (outbound filtering) source address validation
  - Securely configured DNS, NTP and SNMP servers
  - No open resolvers!
    Only allow owned or authorised IP addresses to connect

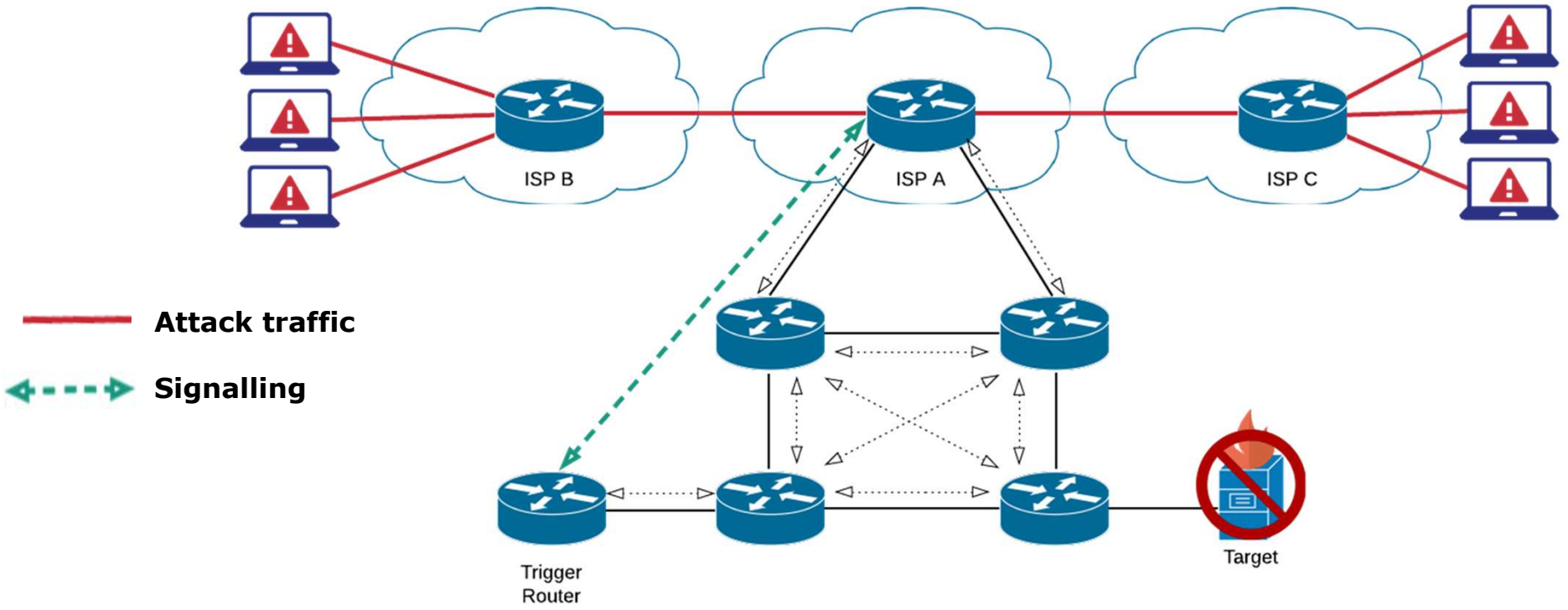
Mitigation Strategies

- Remote Triggered Black Hole (RTBH) filtering
  - With your ISP



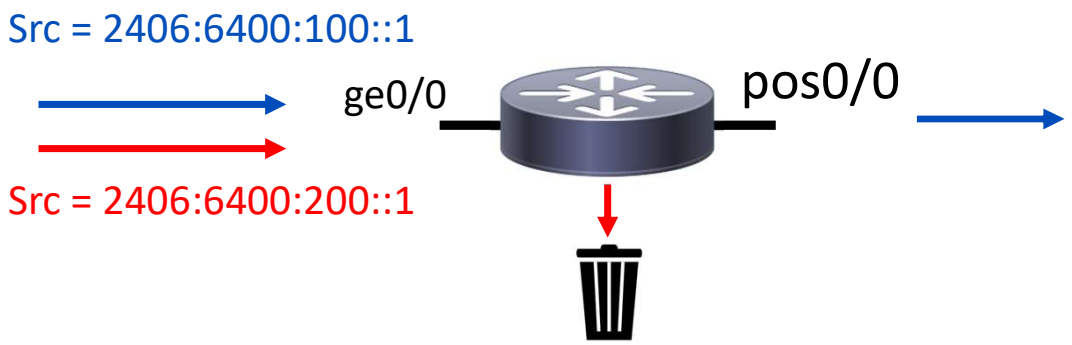
Mitigation Strategies

- Remote Triggered Black Hole (RTBH) filtering
  - With your ISP



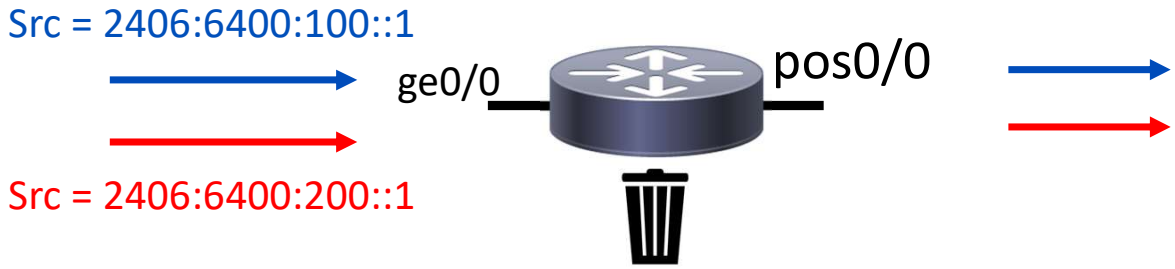
Mitigation Strategies

- uRPF
  - Strict: verifies both source address and incoming interface with entries in the forwarding table



Forwarding Table:
2406:6400:100::/48 ge0/0
2406:6400:200::/48 fa0/0

  - Loose: verifies existence of route to source address



Mitigation Strategies

- Source Remote Triggered Black Hole (sRTBH) filtering
  - RTBH with uRPF (Unicast Reverse Path Forwarding)
    - RFC5635
  - Basic Operation
    - Setup a RTBH Sinkhole (routing to a Null Interface)
    - Enable uRPF in loose mode
    - Create an appropriate community to NH traffic to your Sinkhole
    - When a source is identified
      - Tag with appropriate community to send to the Sink
      - uRPF check will fail (as it is routed to a Null)
      - Traffic Dropped

http://www.cisco.com/web/about/security/intelligence/blackhole.pdf

Questions?