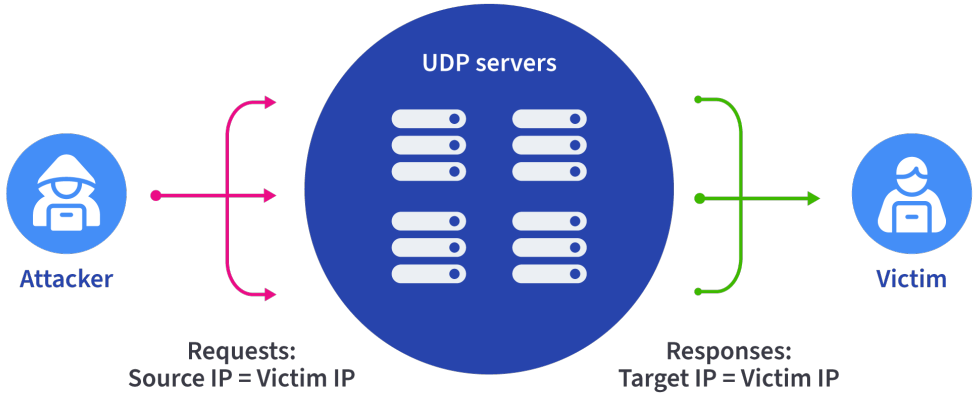
Using NetFlow to Fight DDoS at the Source

Doug Madory

NANOG 90
Charlotte, NC

Fighting DDoS at the Source

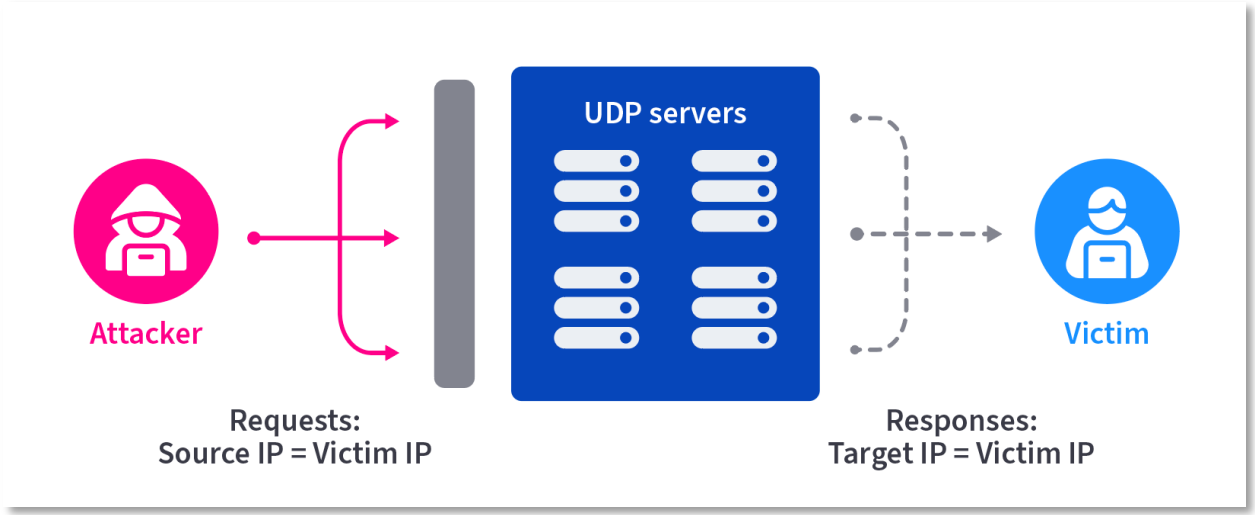
- Distributed denial of service (DDoS) attacks continue to plague the Internet.
- One of the most common forms of DDoS attack is the **reflection attack**.
- The attacker sends thousands of requests with “spoofed” source IP addresses.



Reflection attack

Addressing the problem

1. Secure internet devices from responding to UDP queries from the Internet



2. Eliminate spoofed traffic via technical means (BCP38)
3. Identify and engage networks originating spoofed traffic

Let's talk about #3

Using NetFlow to traceback DDoS sources

A backbone provider uses a customized workflow to identify customer networks which are sending traffic in violation of BCP38.

Methodology boils down to two steps:

1

Find spikes of packets from customer networks to a large set of unique destination IP addresses using commonly abused UDP ports.

2

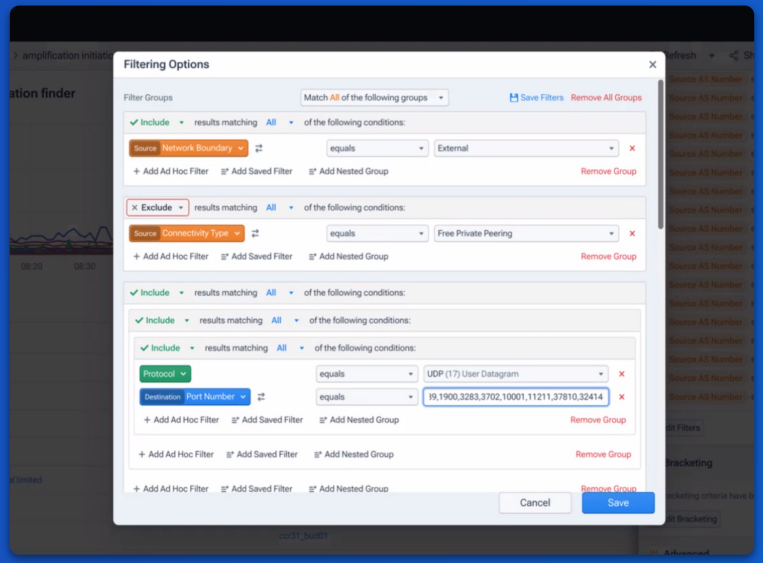
For any suspicious spikes in packets to those selected UDP ports, investigate the source IPs of these packets coming from that customer.

Using NetFlow to traceback DDoS sources

1

Run a query that captures the following:

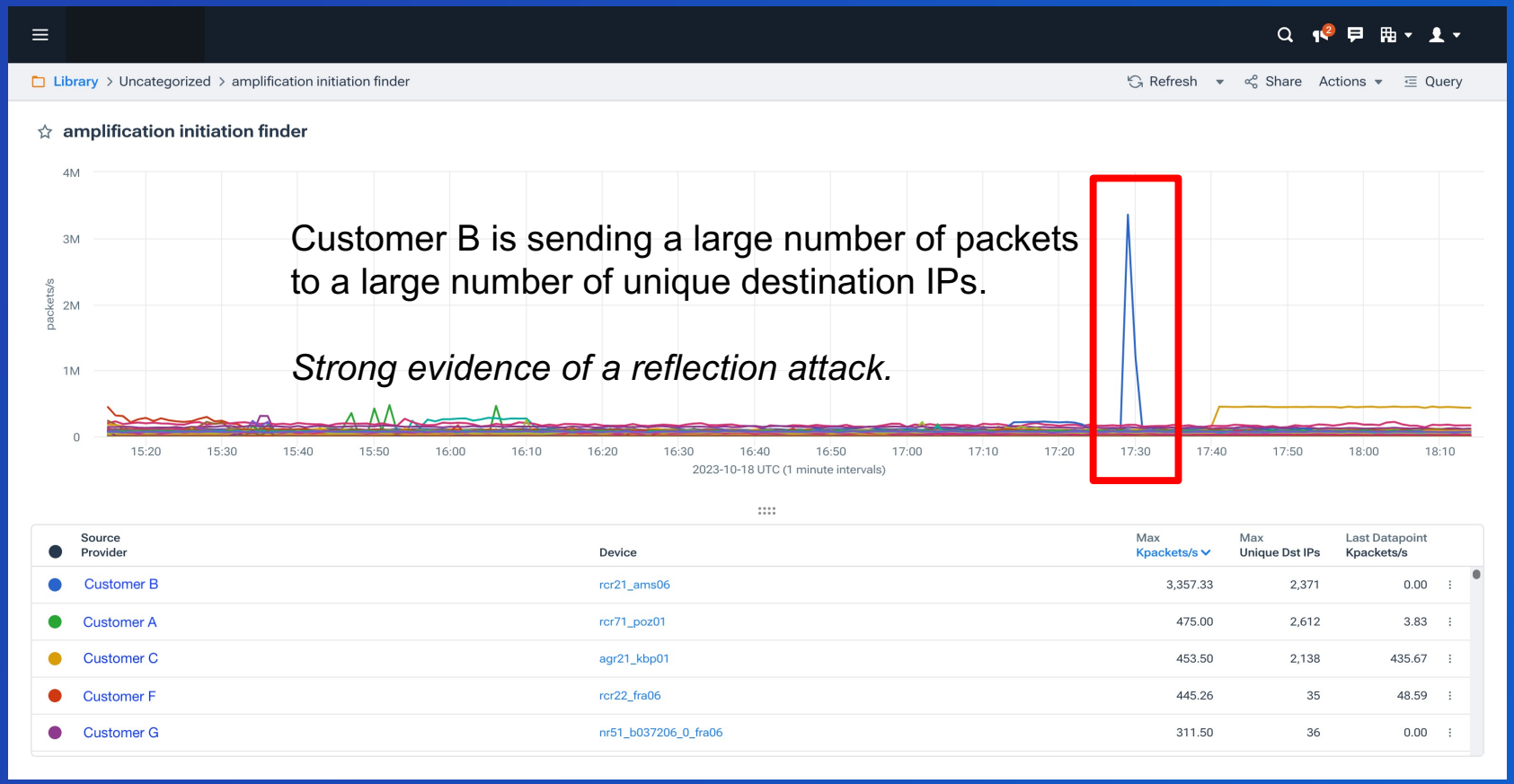
- Only traffic from an external source
- Only packets directed to commonly abused reflection ports.*
- Set metrics to
  - Packets/sec (not bps)
  - Unique number of destination IPs
- Group by device (to identify source interface)



* 19, 53, 123, 161, 389, 427, 1900, 3283, 3702, 10001, 10074, 11211, 37810, 32414

Using NetFlow to traceback DDoS sources

1

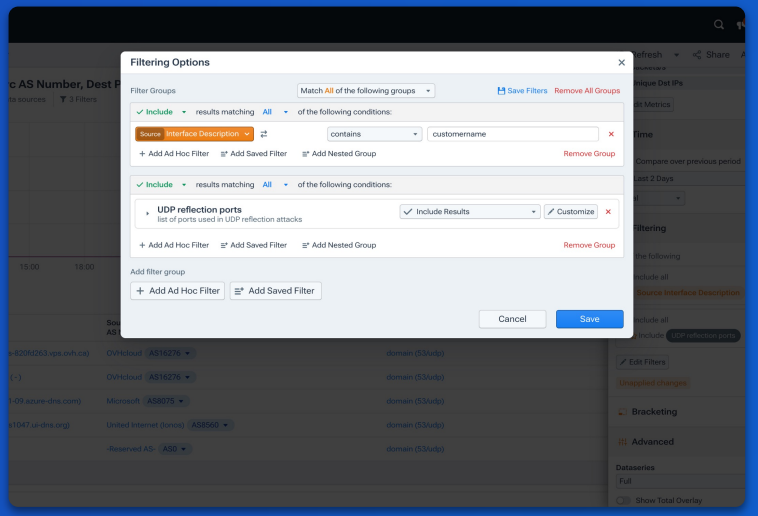


Source Provider	Device	Max Kpackets/s	Max Unique Dst IPs	Last Datapoint Kpackets/s
Customer B	rcr21_ams06	3,357.33	2,371	0.00
Customer A	rcr71_poz01	475.00	2,612	3.83
Customer C	agr21_kbp01	453.50	2,138	435.67
Customer F	rcr22_fra06	445.26	35	48.59
Customer G	nr51_b037206_0_fra06	311.50	36	0.00

Using NetFlow to traceback DDoS sources

2

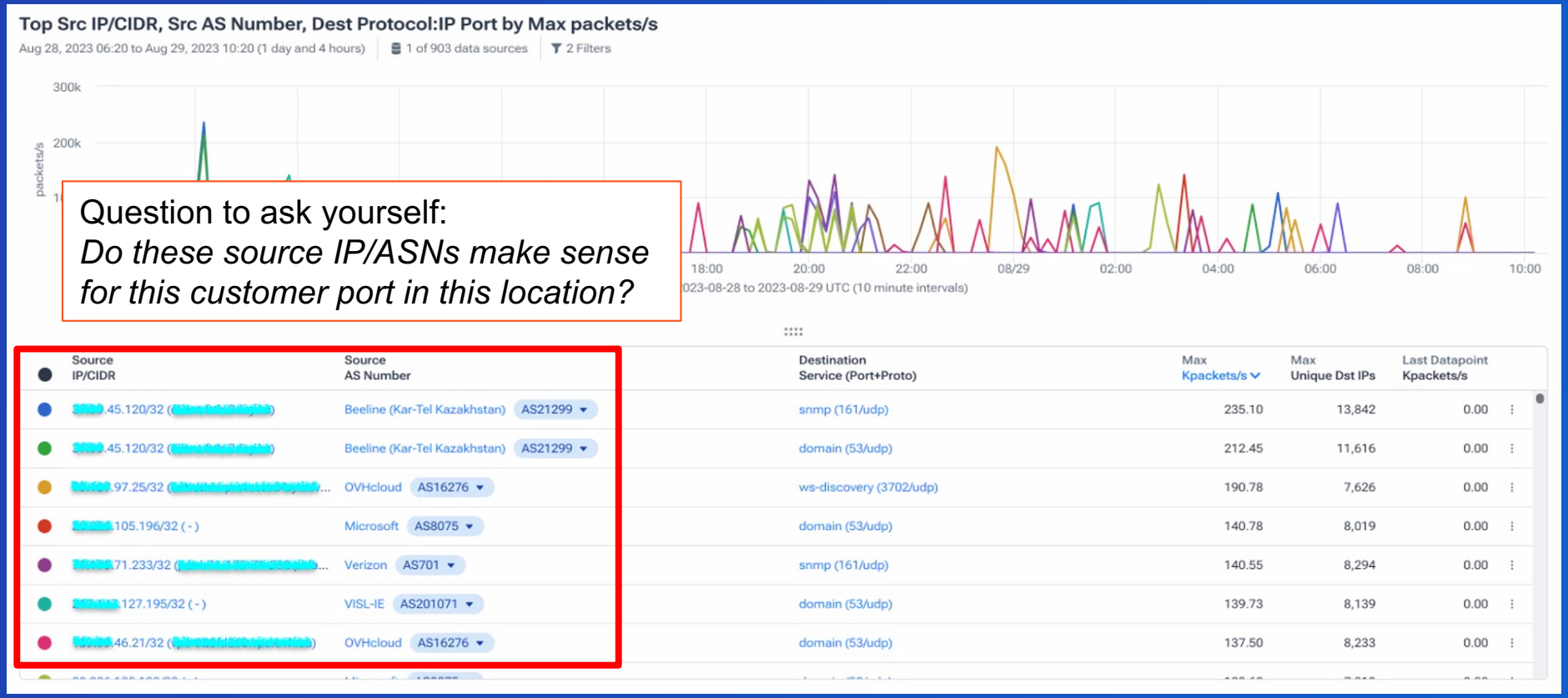
Now we want to investigate the source IPs of these packets coming from that customer by running a query that captures the following:



- Only packets to abused UDP ports from the customer interface.
  - Group by source IP/ASN
  - Group by source port
- Still set metrics to
  - Packets/sec (not bps)
  - Unique number of destination IPs

Using NetFlow to traceback DDoS sources

2



Question to ask yourself:
Do these source IP/ASNs make sense for this customer port in this location?

Now the fun begins — contacting customers!

- Service providers could simply refer the traffic to the abuse team to take action (e.g. disconnect).
- Customer would just continue activity with another provider.
- A service provider's objective should be to get the customer's netops team to understand the issue and address it.

A very time-consuming process:

1. Language barriers
2. Network engineers who are either overworked or poorly trained
3. Unfortunately, networking teams who are simply uninterested in fixing the problem
4. Other reasons…

Anti-Spoofing Reflection / Amplification Peer Response

BINGO

That's not our IP	Okay, we blocked those UDP ports on the customer	Misinterprets the data and claims you sent it	Our routers can't do ACLs or uRPF	Asks what destination IPs are being attacked
NetFlow tool screenshot looking for desination IPs	We only have NetFlow on our internet edge	I can't find the traffic	We're a transit provider; we can't do this	Shares link to an internal tool I can't access
Due to privacy, we don't collect NetFlow data	Insults	FREE	Those IPs you reported are yours	We notified the customer
"show route" output of the IP in question	Using the wrong timezone	cc's 15 other people on the email thread who can't help	Customer is multi-homed; can't BCP38	Includes novice security team on thread
We put a policer to limit the pps	We don't know what server generated this	No response from peer	We don't have NetFlow	Promotes buying DDoS protection service

Source: a certain cat at a cloud provider

Call to action

If your network is allowing spoofed traffic, someone is probably using your infrastructure to launch DDoS attacks against victims around the world.

If you run a network that operates as a service provider, you have a responsibility to the rest of the Internet to actively look for and eliminate spoofed traffic.

If contacted, you need tools in place to investigate and address the claims

Don’t want to be the one to complete someone’s ***anti-spoofing response bingo card***.

Thank you!

Doug Madory
dmadory@kentik.com

@dougmadory
in/dougmadory