How the Evolving DDoS Attack Landscape Has Re-invented Our Defence Architecture

Global Secure Layer

Who We Are

- Global Secure Layer (GSL) is a leading IP transit, colocation, DDoS protection, and ethernet service provider headquartered in Australia with a global presence
- Expansive subsea and terrestrial fibre network with metro dark fibre between sites
- Over 3,500 IPv4 peers in 50 sites
- 30+Tbps of border capacity, 6+Tbps of active scrubbing capacity
- Patent-pending DDoS mitigation solution, Goliath, was built on the principle of detecting complex, multi-vector DDoS attacks with high accuracy
- Leveraging our global anycast network to intelligently share state across all sites

What We Will Be Discussing

DDoS attack landscape

- Attack trends in throughput as well as the Internet ecosystem as a whole
- Historical attack volumes and how they influence capacity planning
- Challenges for effectively mitigating attack traffic

Journey of building our own appliances

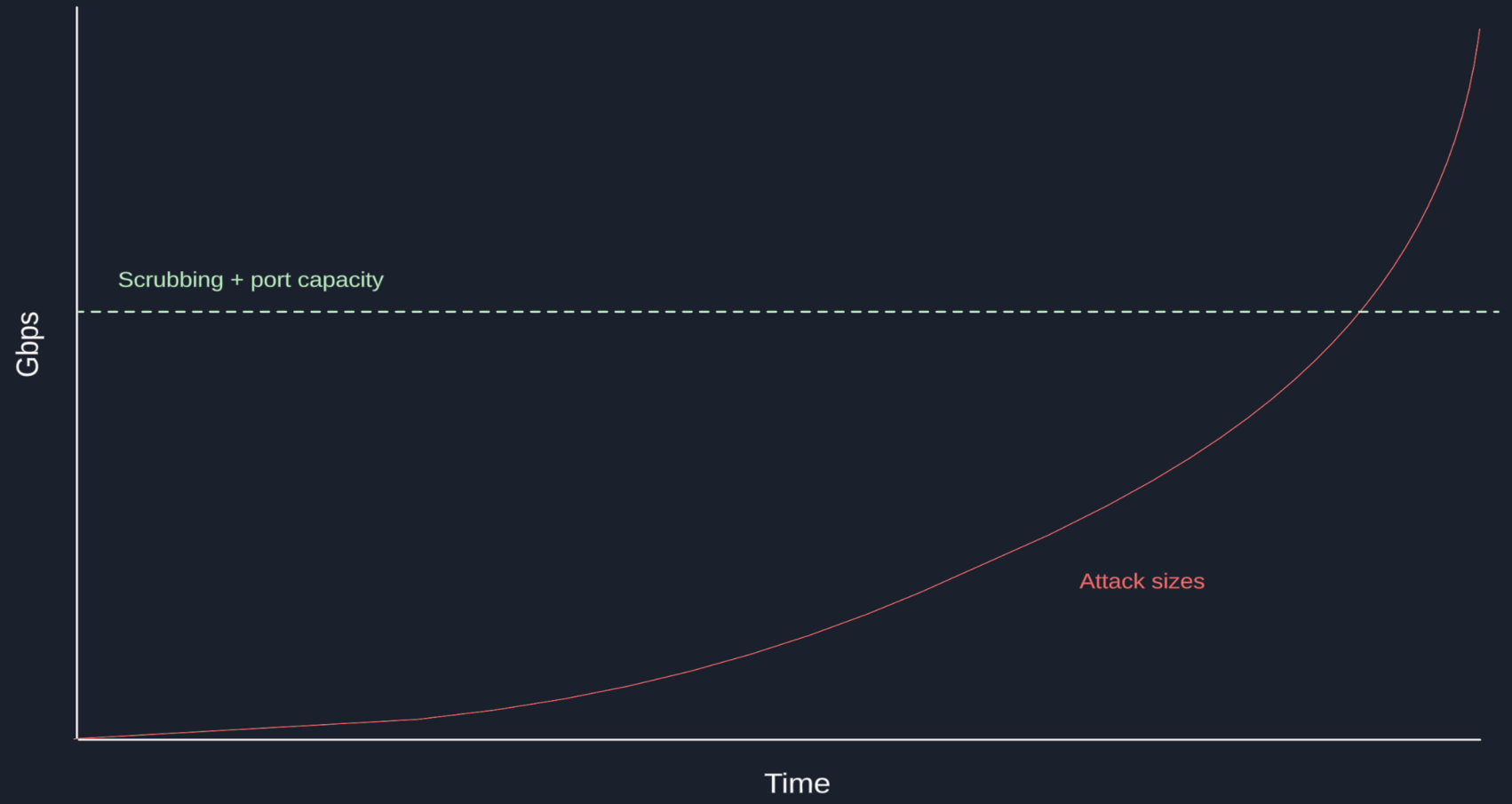
- Why we did it, and what challenges it solved
- Design problems we faced early on, and tradeoffs we needed to consider
- Technical challenges of processing high packet rate at scale

DDoS Mitigation Challenge #1
Capacity and Attack Sizes

- Attack sizes remain exponential while port sizes do not
  - Often on the defenders side, the port capacities are fixed
  - This may result from a mix of contracts, capacity planning issues, or misjudging capacity for at-risk ingress sites
  - This is especially critical when operating anycast
- Attack sizes follow Moore's Law
  - As transistor counts double every ~2 years, attack sizes tend to follow suit
  - We also see this pattern in port sizes
  - As residential broadband upload speeds increase, attack sizes will also
  - 10Gbps is the new 1Gbps, ~95% of attacks fall below 10gbps

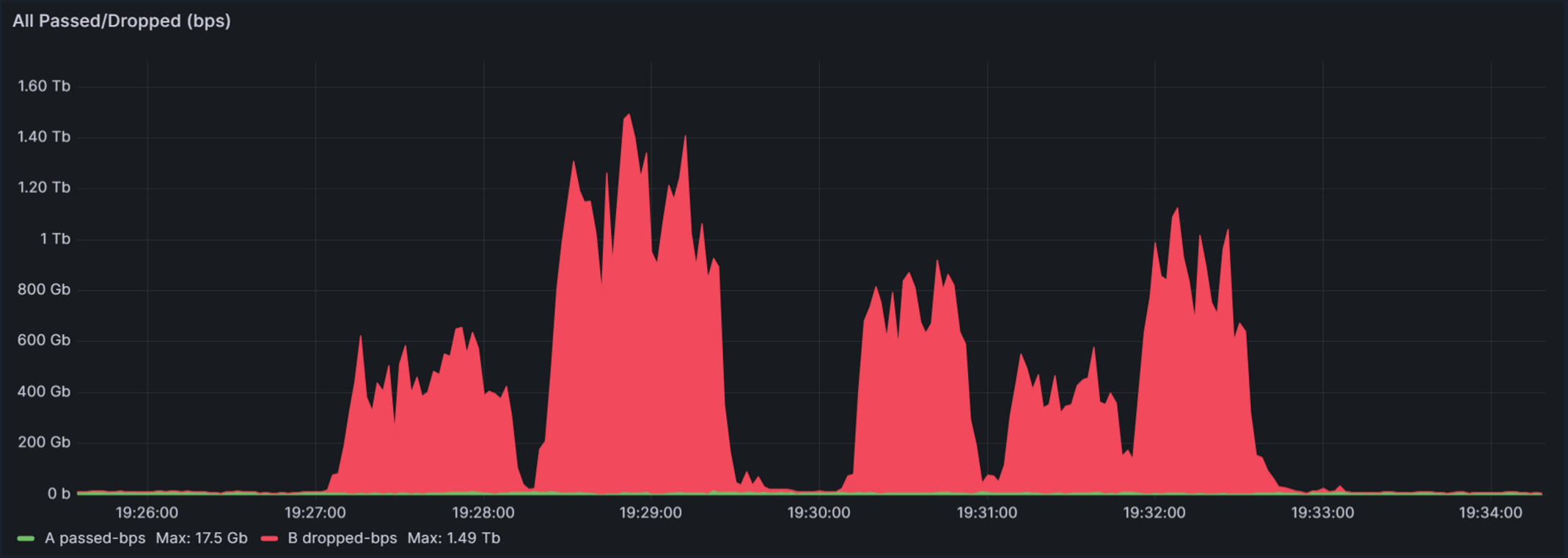
DDoS Mitigation Challenge #1

Capacity and Attack Sizes



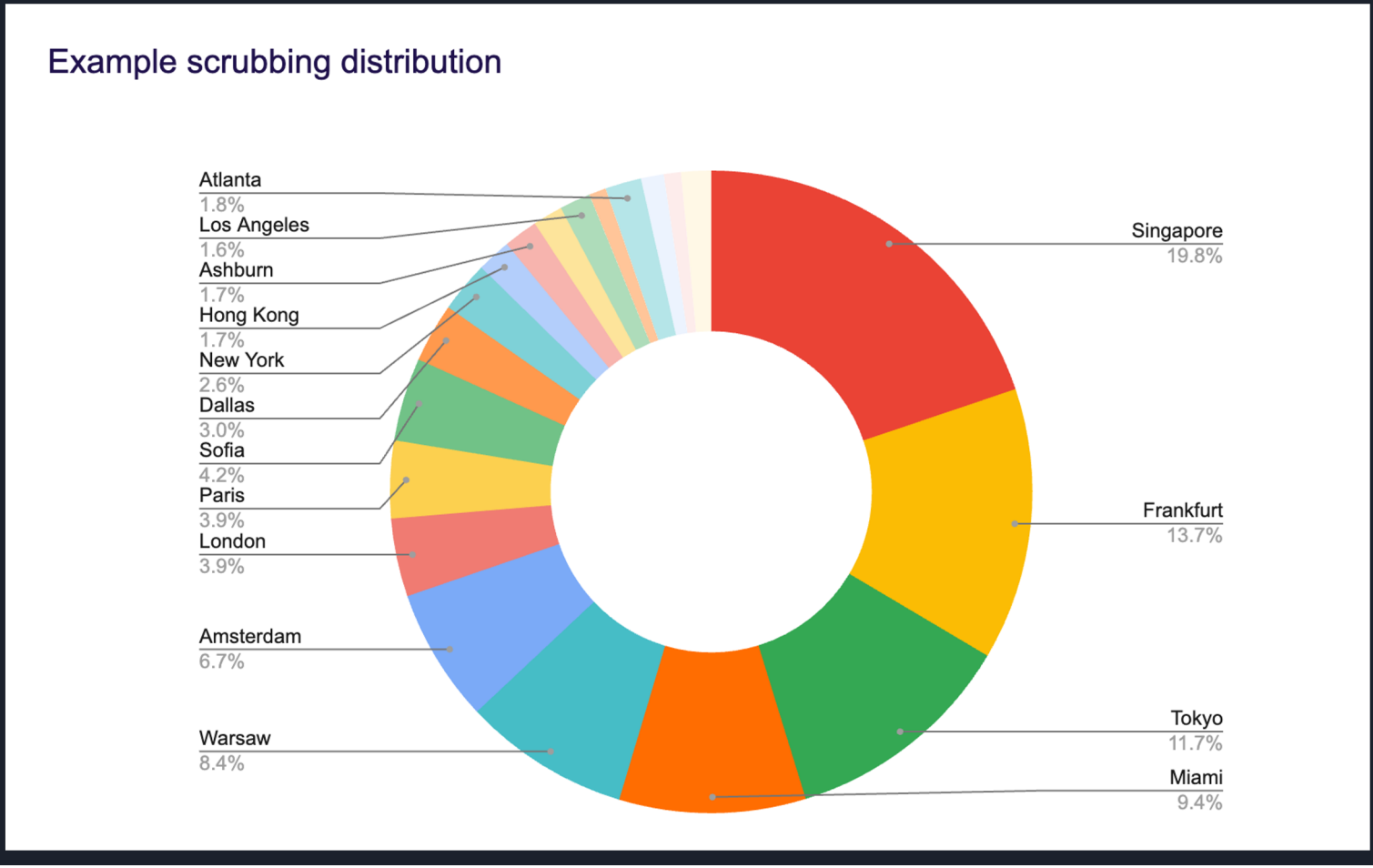
DDoS Mitigation Challenge #1

Capacity and Attack Sizes



DDoS Mitigation Challenge #1

Capacity and Attack Sizes



DDoS Attacks at the Network Border (Anycast)

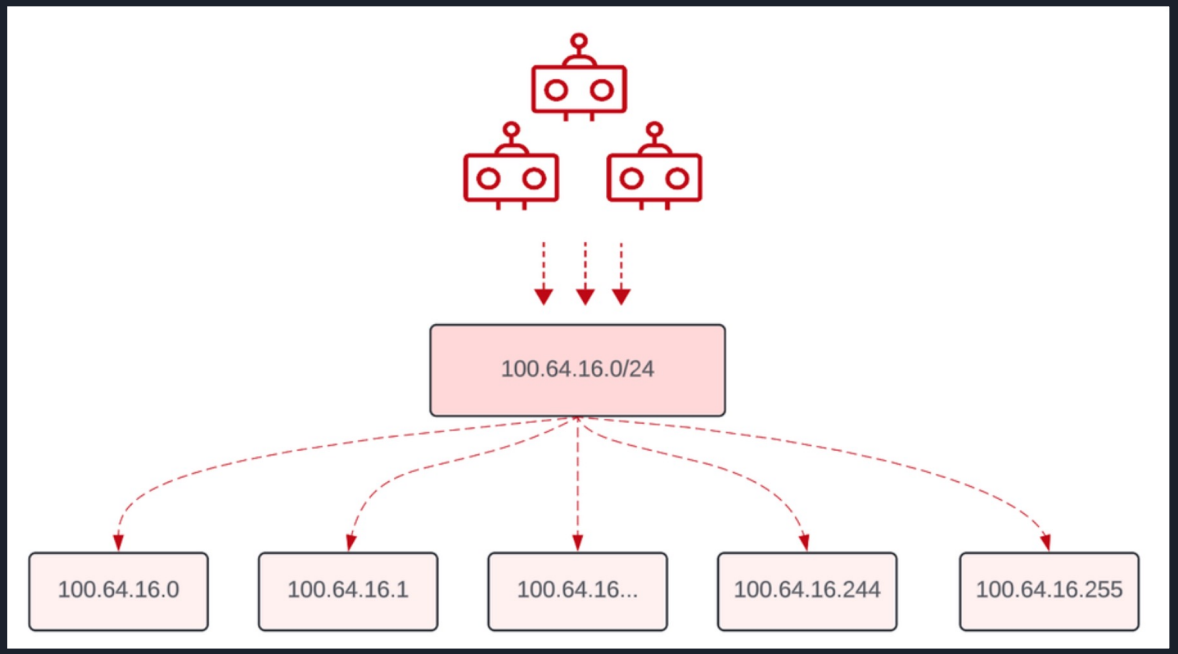
DDoS Mitigation Challenge #2
Changing Attack Methodology

- Moving from volumetric to application layer
- Stateful / in-session TCP attacks, aiming to mimic legitimate traffic
- Combining L7 methods with highly volumetric execution. Example: 398 million requests per second “rapid reset” HTTP/2 botnet
- Inter-customer attacks

Attacks Methods
What We Need To Account For

Reflective	Volumetric	Protocol
• DNS • NTP • SSDP • Memcached	• Generic UDP • DNS (nameserver attacks) • TCP SYN • TCP ACK • TCP STOMP (stateful) • GRE IP • GRE Ethernet	• RakNet • HTTP • VSE (Valve Source Engine) • FiveM • TeamSpeak • OpenVPN
Reflective attacks have become larger over the last year, peaking at 1.2Tbps for DNS and 600Gbps for NTP Common reflection sources include unsecured DNS resolvers, and NTP servers supporting Monlist query type Memcached was primarily cloud providers, which involves sending spoofed requests to a vulnerable server producing a response up to 5000x in size	Modern operating systems do not handle SYN floods efficiently, oftentimes dying at 50kpps Unlike reflective, involves thousands of compromised hosts sending large volumes of traffic to the victim in hopes of saturating port speeds, packet processing capacity, or both. TCP ACK difficult to mitigate without the mitigation device knowing the full state of the connection (state table helps)	Targets the underlying hosted application, or targets a particular weakness in the underlying transport protocol Typically needs a stateful component or layer 7 inspecting application to perform validity checks on new incoming clients HTTPS effectively impossible to mitigate without decrypting in-flight traffic

Carpet Bomb Attacks



Carpet Bomb attacks aim to flood traffic to all IPs within a subnet on a victim network, with the goal to bypass per destination attack detection.

DDoS Mitigation Challenge #3
False Positives

- How do we avoid impacting legitimate traffic flows when we don’t always know the target application?
- How can we share intelligence of attacks across all sites with low latency?
- As attack complexity grows, the need to have comprehensive protocol-level validation becomes key

Why An In-House Appliance

- Existing DDoS appliance vendors on the market are built to be on-premise, single location, with no anycast deployment
- Often built as one size fits all, does not consider:
  - Asymmetric traffic scenarios
  - Multiple ingress points or sites
  - Multiple ingress transit providers and peering ports
- This pigeon-holes the solution into a limited operation mode that implies all traffic terminates at one central site, rather than a distributed deployment model
- Greater control and reaction time to new threats → iteration speeds often within hours.

Heuristics Engine

Inline traffic sampling

- To build a comprehensive mitigation system, we need one that automatically samples end-user traffic and detects anomalies quickly.

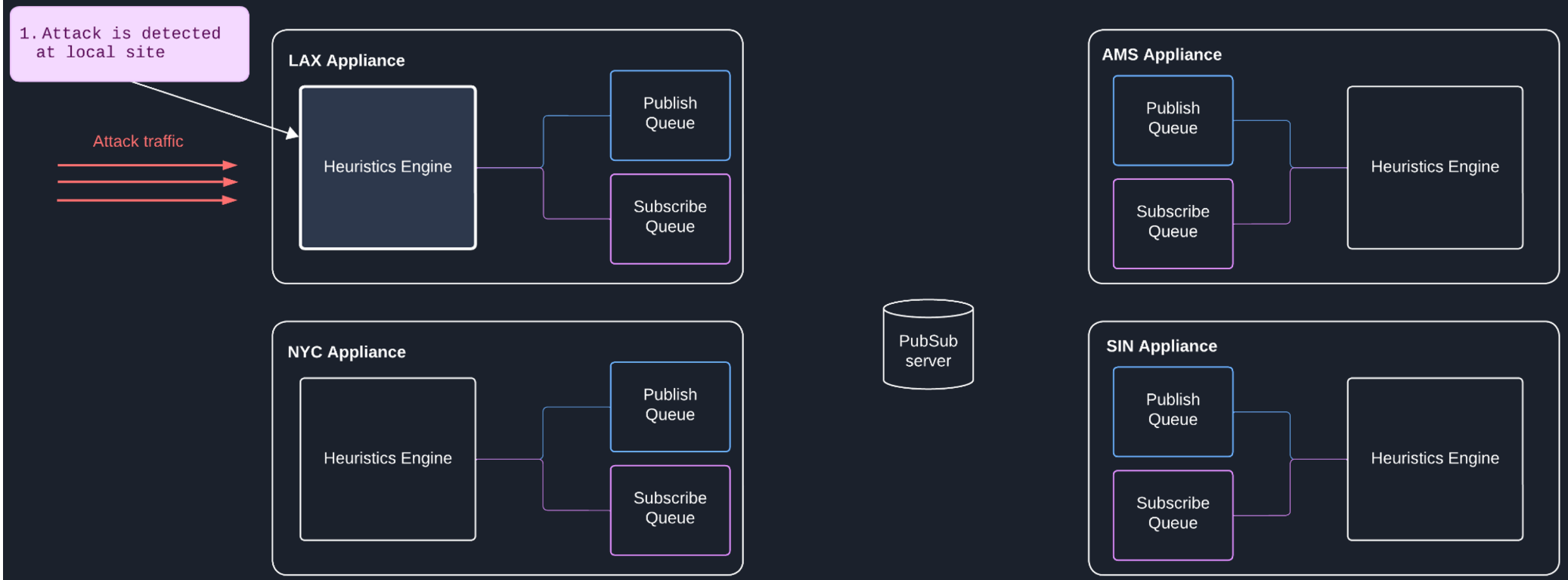
Time-series anomaly detection

- On anomaly detection for a sampled subnet, a mitigation rule is created
- This rule is inserted locally onto the device for the attacked prefix

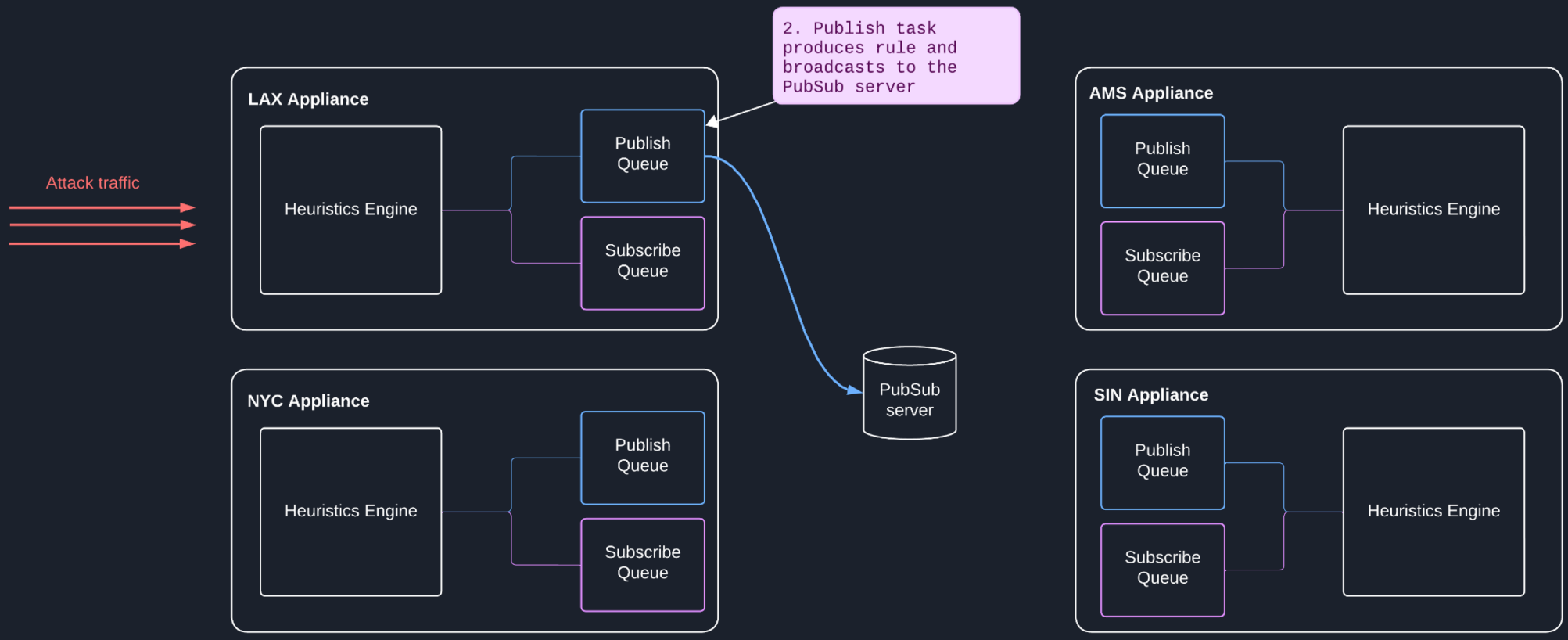
Uniform scrubbing experience (LOBE)

- Rules produced are broadcasted to all mitigation devices on the network which ensures a uniform scrubbing experience across the whole network

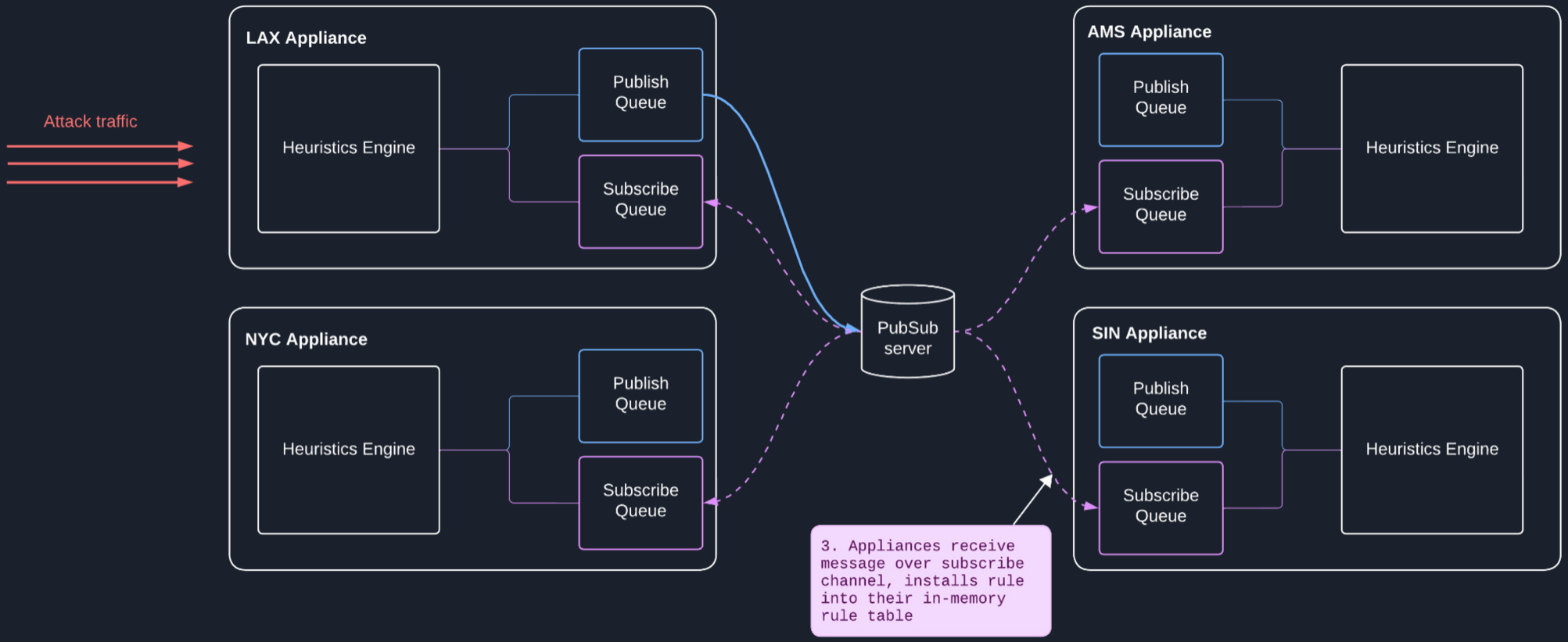
Learn Once Block Everywhere
LOBE



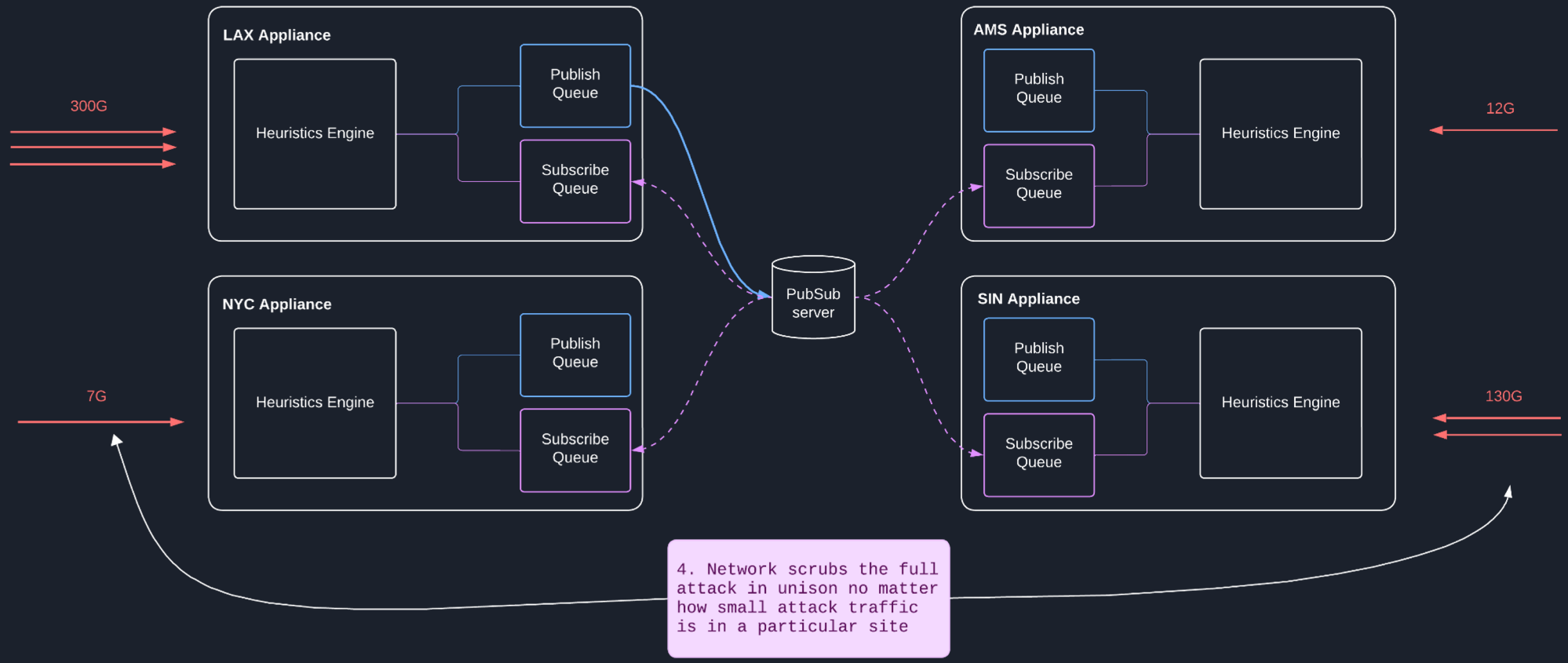
Learn Once Block Everywhere
LOBE



Learn Once Block Everywhere
LOBE



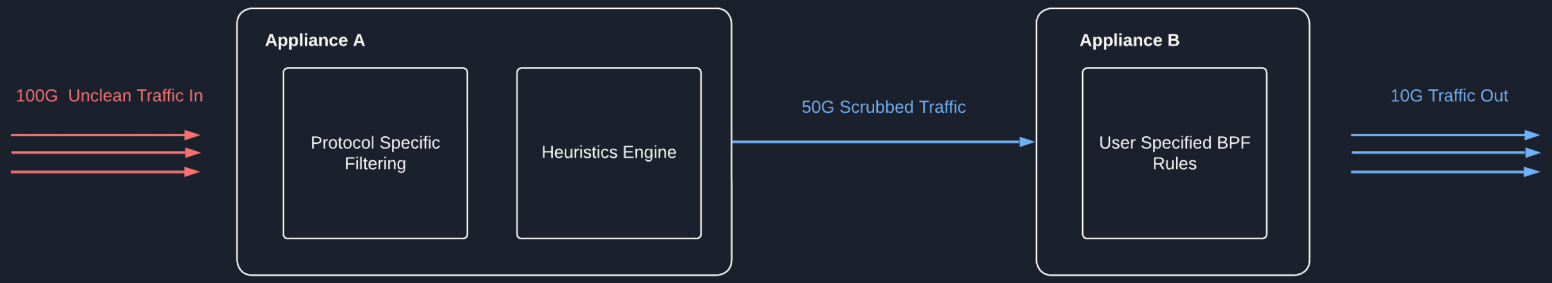
Learn Once Block Everywhere
LOBE

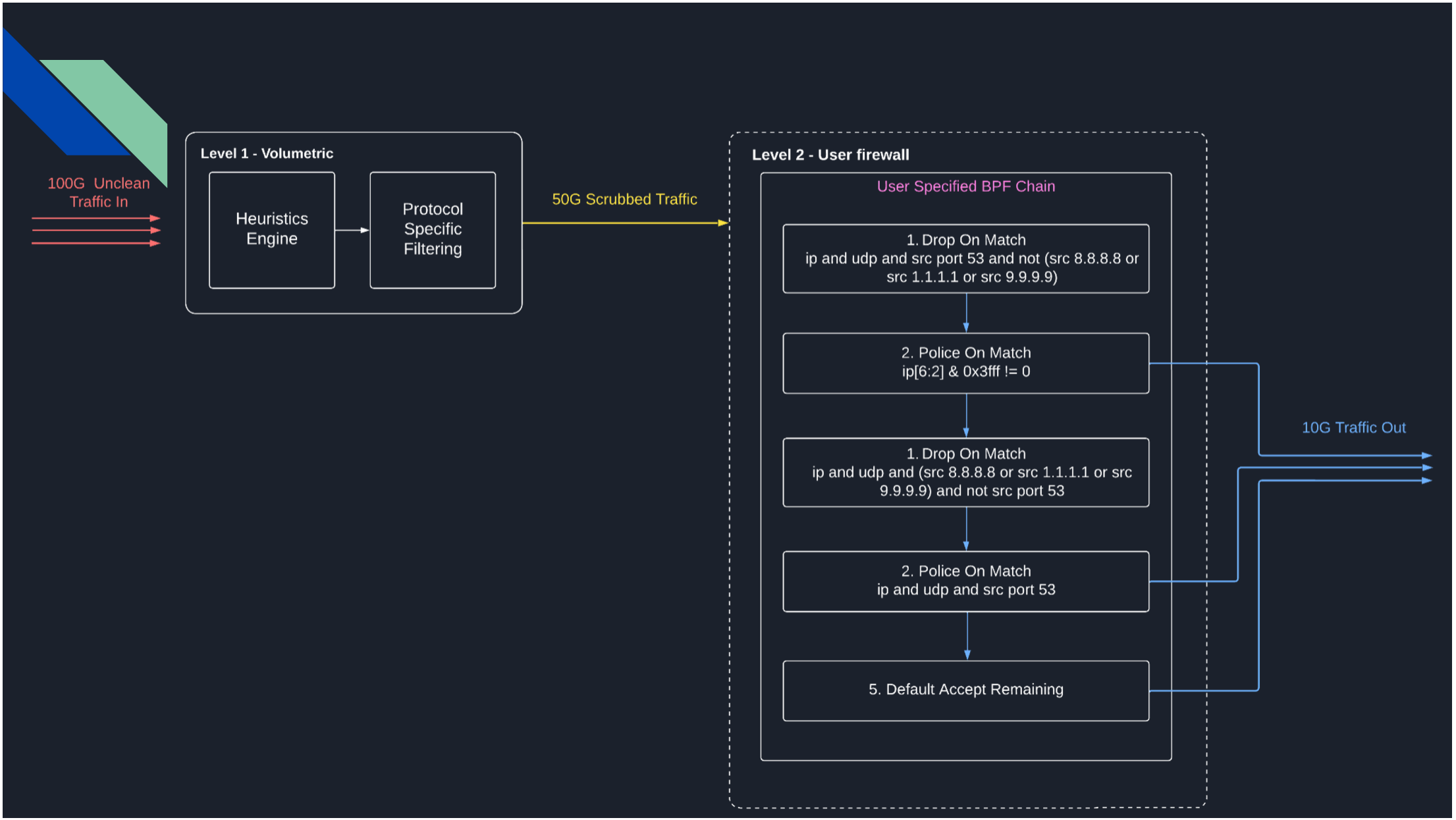


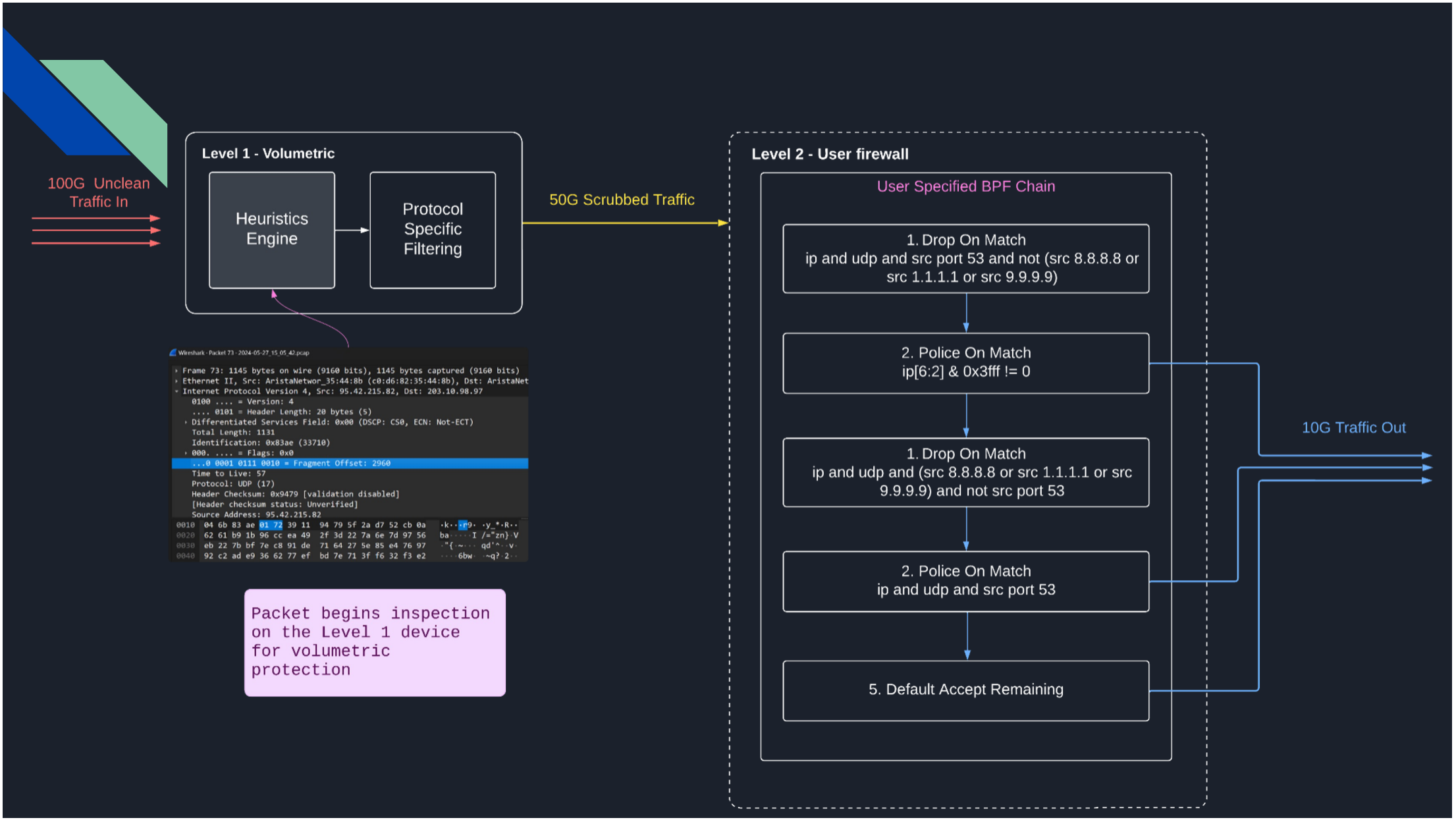
Putting The Power In Users Hands

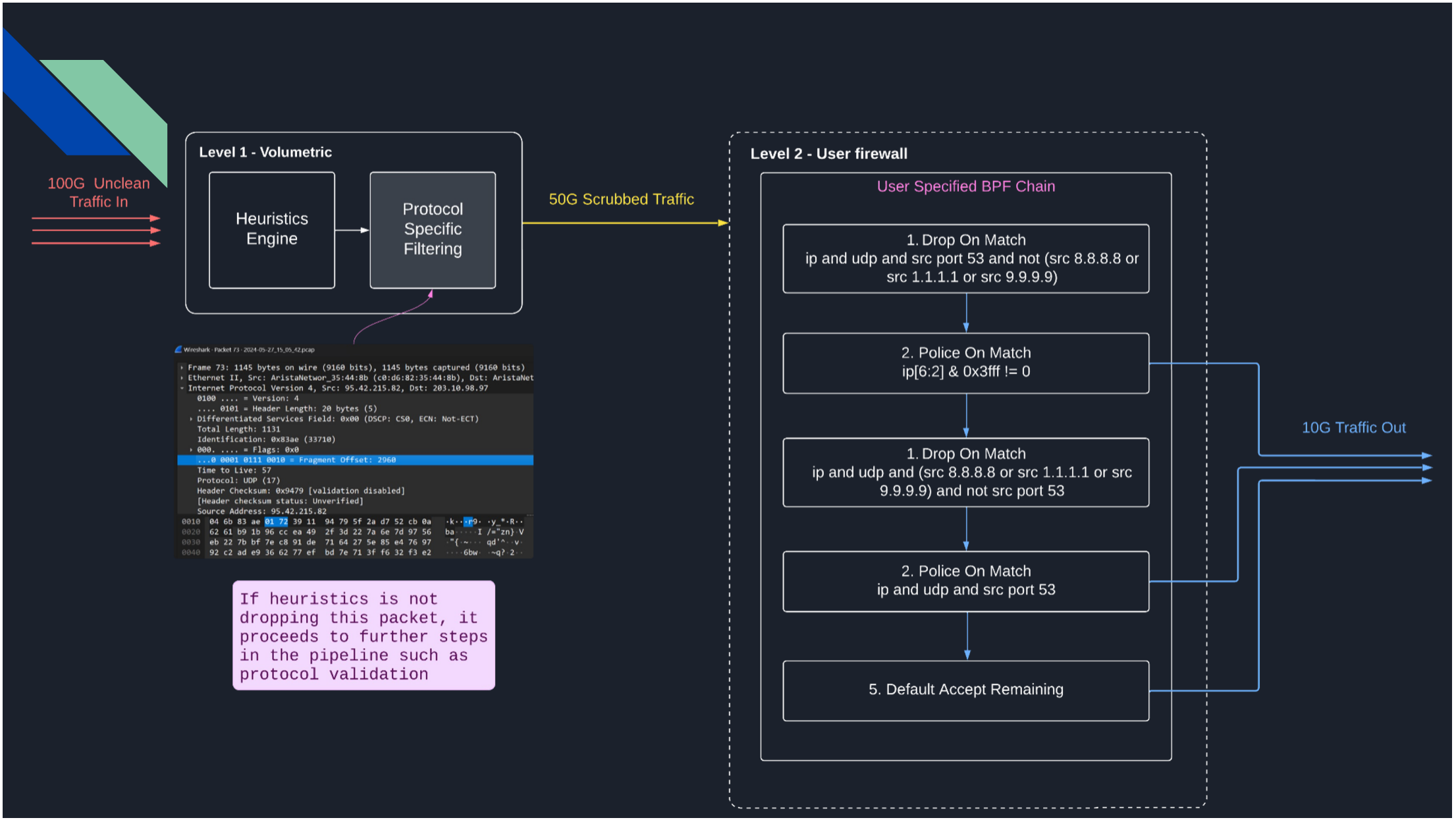
Reasoning and Challenges

- We realised it was not enough to build a solution that protects our network. To provide a complete solution, it needed to protect the end user as well.
- How might end users expect to be able to use a solution?
  - Last mile user defined firewall rules
  - Edge device to remove volumetric traffic
  - Protocol specific filtering




100G Unclean Traffic In
Level 1 - Volumetric
Heuristics Engine
Protocol Specific Filtering
50G Scrubbed Traffic
Level 2 - User firewall
User Specified BPF Chain
1. Drop On Match
ip and udp and src port 53 and not (src 8.8.8.8 or src 1.1.1.1 or src 9.9.9.9)
2. Police On Match
ip[6:2] & 0x3fff != 0
1. Drop On Match
ip and udp and (src 8.8.8.8 or src 1.1.1.1 or src 9.9.9.9) and not src port 53
2. Police On Match
ip and udp and src port 53
5. Default Accept Remaining
10G Traffic Out


100G Unclean Traffic In
Level 1 - Volumetric
Heuristics Engine
Protocol Specific Filtering
50G Scrubbed Traffic
Level 2 - User firewall
User Specified BPF Chain
1. Drop On Match
ip and udp and src port 53 and not (src 8.8.8.8 or src 1.1.1.1 or src 9.9.9.9)
2. Police On Match
ip[6:2] & 0x3fff != 0
1. Drop On Match
ip and udp and (src 8.8.8.8 or src 1.1.1.1 or src 9.9.9.9) and not src port 53
2. Police On Match
ip and udp and src port 53
5. Default Accept Remaining
10G Traffic Out
Wireshark · Packet 73 · 2024-05-27_15_05_42.pcap
Frame 73: 1145 bytes on wire (9160 bits), 1145 bytes captured (9160 bits)
Ethernet II, Src: AristaNetwor_35:44:8b (c0:d6:82:35:44:8b), Dst: AristaNet
Internet Protocol Version 4, Src: 95.42.215.82, Dst: 203.10.98.97
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 1131
Identification: 0x83ae (33710)
000. .... = Flags: 0x0
...0 0001 0111 0010 = Fragment Offset: 2960
Time to Live: 57
Protocol: UDP (17)
Header Checksum: 0x9479 [validation disabled]
[Header checksum status: Unverified]
Source Address: 95.42.215.82
0010 04 6b 83 ae 01 72 39 11 94 79 5f 2a d7 52 cb 0a
0020 62 61 b9 1b 96 cc ea 49 2f 3d 22 7a 6e 7d 97 56
0030 eb 22 7b bf 7e c8 91 de 71 64 27 5e 85 e4 76 97
0040 92 c2 ad e9 36 62 77 ef bd 7e 71 3f f6 32 f3 e2
Packet begins inspection on the Level 1 device for volumetric protection

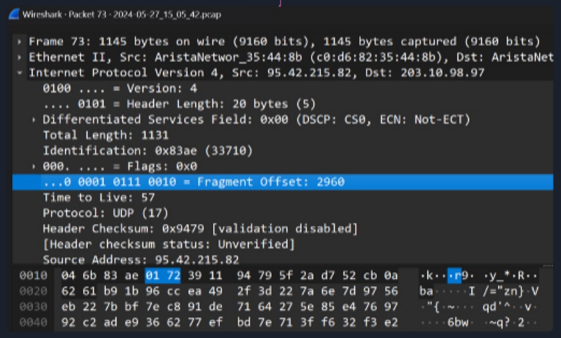

100G Unclean Traffic In
Level 1 - Volumetric
Heuristics Engine
Protocol Specific Filtering
50G Scrubbed Traffic
Level 2 - User firewall
User Specified BPF Chain
1. Drop On Match
ip and udp and src port 53 and not (src 8.8.8.8 or src 1.1.1.1 or src 9.9.9.9)
2. Police On Match
ip[6:2] & 0x3fff != 0
1. Drop On Match
ip and udp and (src 8.8.8.8 or src 1.1.1.1 or src 9.9.9.9) and not src port 53
2. Police On Match
ip and udp and src port 53
5. Default Accept Remaining
10G Traffic Out
Wireshark · Packet 73 · 2024-05-27_15_05_42.pcap
Frame 73: 1145 bytes on wire (9160 bits), 1145 bytes captured (9160 bits)
Ethernet II, Src: AristaNetwor_35:44:8b (c0:d6:82:35:44:8b), Dst: AristaNet
Internet Protocol Version 4, Src: 95.42.215.82, Dst: 203.10.98.97
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 1131
Identification: 0x83ae (33710)
000. .... = Flags: 0x0
...0 0001 0111 0010 = Fragment Offset: 2960
Time to Live: 57
Protocol: UDP (17)
Header Checksum: 0x9479 [validation disabled]
[Header checksum status: Unverified]
Source Address: 95.42.215.82
0010 04 6b 83 ae 01 72 39 11 94 79 5f 2a d7 52 cb 0a
0020 62 61 b9 1b 96 cc ea 49 2f 3d 22 7a 6e 7d 97 56
0030 eb 22 7b bf 7e c8 91 de 71 64 27 5e 85 e4 76 97
0040 92 c2 ad e9 36 62 77 ef bd 7e 71 3f f6 32 f3 e2
If heuristics is not dropping this packet, it proceeds to further steps in the pipeline such as protocol validation

100G Unclean Traffic In

Level 1 - Volumetric

Heuristics Engine → Protocol Specific Filtering

50G Scrubbed Traffic



Packet is egressed from Level 1 appliances to user defined firewall for chain processing

Level 2 - User firewall

User Specified BPF Chain

1. Drop On Match
ip and udp and src port 53 and not (src 8.8.8.8 or src 1.1.1.1 or src 9.9.9.9)

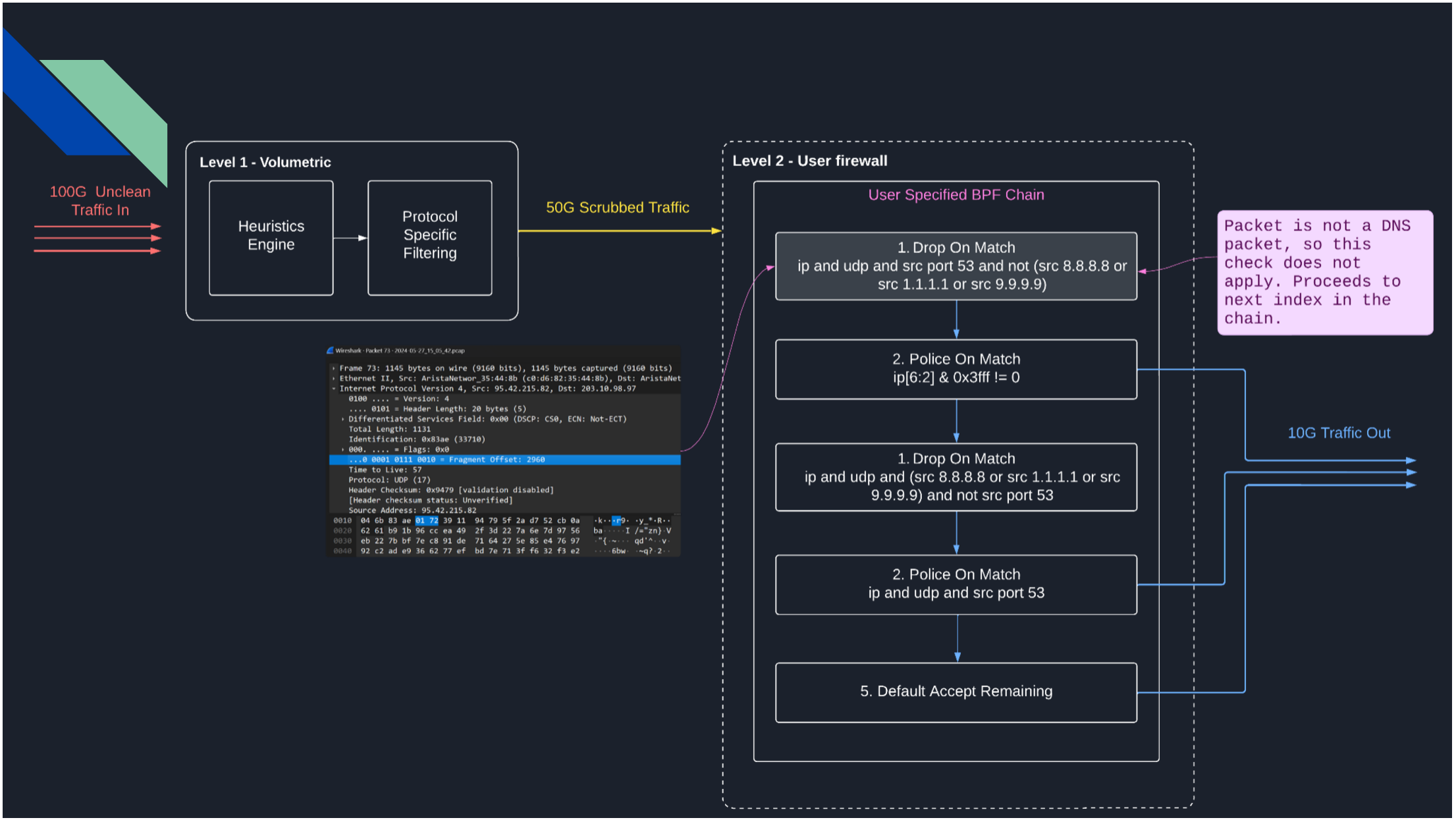
2. Police On Match
ip[6:2] & 0x3fff != 0

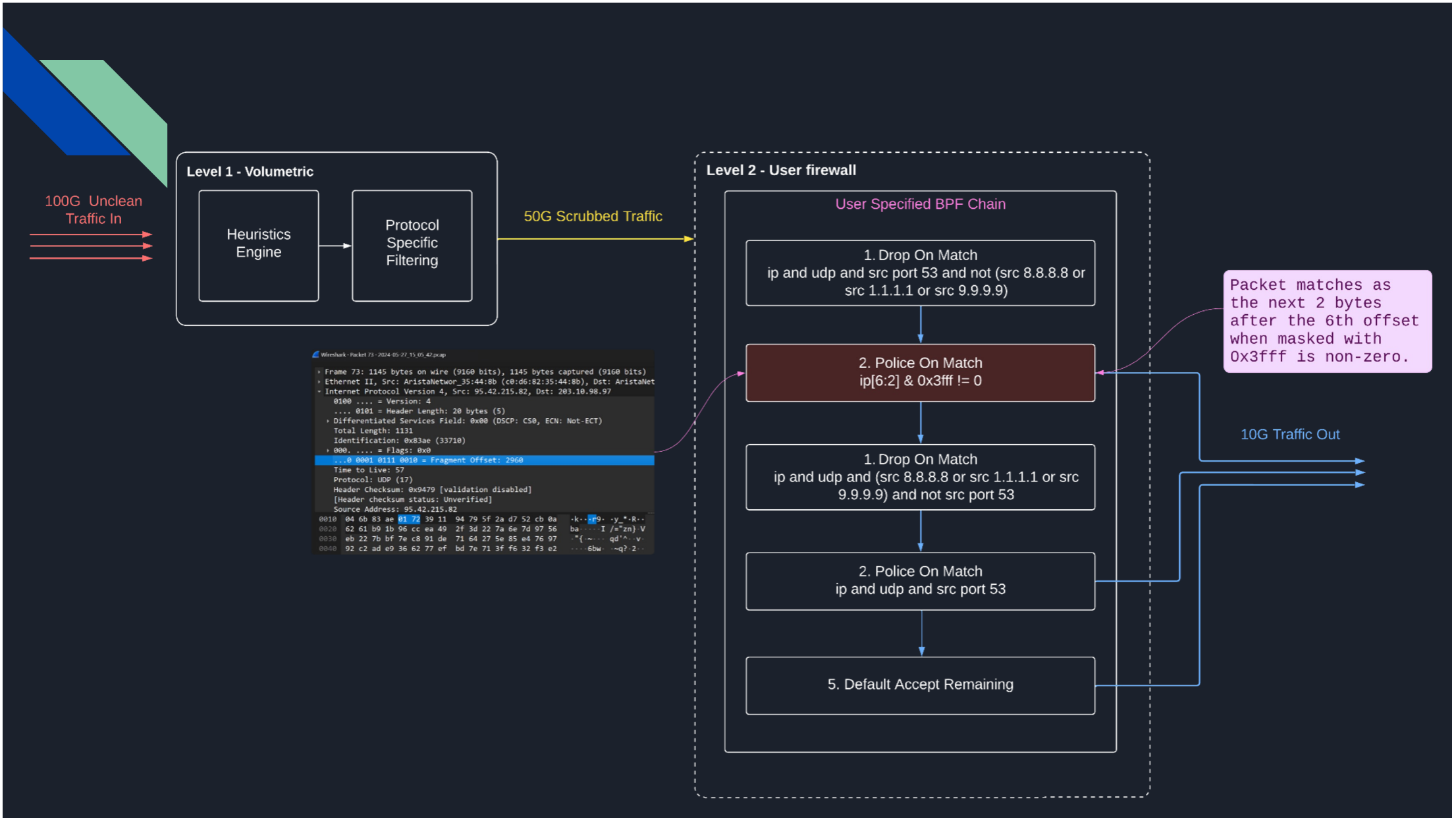
1. Drop On Match
ip and udp and (src 8.8.8.8 or src 1.1.1.1 or src 9.9.9.9) and not src port 53

2. Police On Match
ip and udp and src port 53

5. Default Accept Remaining

10G Traffic Out


100G Unclean Traffic In
Level 1 - Volumetric
Heuristics Engine
Protocol Specific Filtering
50G Scrubbed Traffic
Level 2 - User firewall
User Specified BPF Chain
1. Drop On Match
ip and udp and src port 53 and not (src 8.8.8.8 or src 1.1.1.1 or src 9.9.9.9)
Packet is not a DNS packet, so this check does not apply. Proceeds to next index in the chain.
2. Police On Match
ip[6:2] & 0x3fff != 0
1. Drop On Match
ip and udp and (src 8.8.8.8 or src 1.1.1.1 or src 9.9.9.9) and not src port 53
2. Police On Match
ip and udp and src port 53
5. Default Accept Remaining
10G Traffic Out
Wireshark · Packet 73 · 2024-05-27_15_05_42.pcap
Frame 73: 1145 bytes on wire (9160 bits), 1145 bytes captured (9160 bits)
Ethernet II, Src: AristaNetwor_35:44:8b (c0:d6:82:35:44:8b), Dst: AristaNet
Internet Protocol Version 4, Src: 95.42.215.82, Dst: 203.10.98.97
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 1131
Identification: 0x83ae (33710)
000. .... = Flags: 0x0
...0 0001 0111 0010 = Fragment Offset: 2960
Time to Live: 57
Protocol: UDP (17)
Header Checksum: 0x9479 [validation disabled]
[Header checksum status: Unverified]
Source Address: 95.42.215.82
0010 04 6b 83 ae 01 72 39 11 94 79 5f 2a d7 52 cb 0a
0020 62 61 b9 1b 96 cc ea 49 2f 3d 22 7a 6e 7d 97 56
0030 eb 22 7b bf 7e c8 91 de 71 64 27 5e 85 e4 76 97
0040 92 c2 ad e9 36 62 77 ef bd 7e 71 3f f6 32 f3 e2


100G Unclean Traffic In
Level 1 - Volumetric
Heuristics Engine
Protocol Specific Filtering
50G Scrubbed Traffic
Level 2 - User firewall
User Specified BPF Chain
1. Drop On Match
ip and udp and src port 53 and not (src 8.8.8.8 or src 1.1.1.1 or src 9.9.9.9)
2. Police On Match
ip[6:2] & 0x3fff != 0
1. Drop On Match
ip and udp and (src 8.8.8.8 or src 1.1.1.1 or src 9.9.9.9) and not src port 53
2. Police On Match
ip and udp and src port 53
5. Default Accept Remaining
Packet matches as the next 2 bytes after the 6th offset when masked with 0x3fff is non-zero.
10G Traffic Out
Wireshark · Packet 73 · 2024-05-27_15_05_42.pcap
Frame 73: 1145 bytes on wire (9160 bits), 1145 bytes captured (9160 bits)
Ethernet II, Src: AristaNetwor_35:44:8b (c0:d6:82:35:44:8b), Dst: AristaNet
Internet Protocol Version 4, Src: 95.42.215.82, Dst: 203.10.98.97
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 1131
Identification: 0x83ae (33710)
000. .... = Flags: 0x0
...0 0001 0111 0010 = Fragment Offset: 2960
Time to Live: 57
Protocol: UDP (17)
Header Checksum: 0x9479 [validation disabled]
[Header checksum status: Unverified]
Source Address: 95.42.215.82
0010 04 6b 83 ae 01 72 39 11 94 79 5f 2a d7 52 cb 0a
0020 62 61 b9 1b 96 cc ea 49 2f 3d 22 7a 6e 7d 97 56
0030 eb 22 7b bf 7e c8 91 de 71 64 27 5e 85 e4 76 97
0040 92 c2 ad e9 36 62 77 ef bd 7e 71 3f f6 32 f3 e2

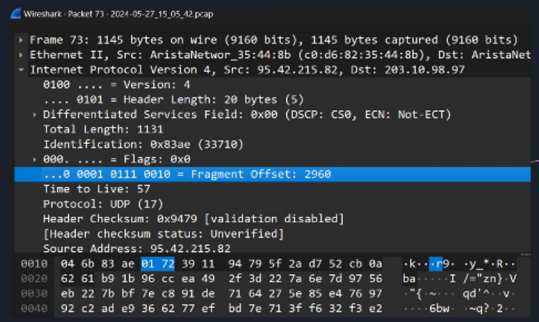
100G Unclean Traffic In

Level 1 - Volumetric

Heuristics Engine

Protocol Specific Filtering

50G Scrubbed Traffic



Level 2 - User firewall

User Specified BPF Chain

1. Drop On Match
ip and udp and src port 53 and not (src 8.8.8.8 or src 1.1.1.1 or src 9.9.9.9)

2. Police On Match
ip[6:2] & 0x3fff != 0

1. Drop On Match
ip and udp and (src 8.8.8.8 or src 1.1.1.1 or src 9.9.9.9) and not src port 53

2. Police On Match
ip and udp and src port 53

5. Default Accept Remaining

If packet has exceeded ratelimit for this rule, it is dropped, else egressed.

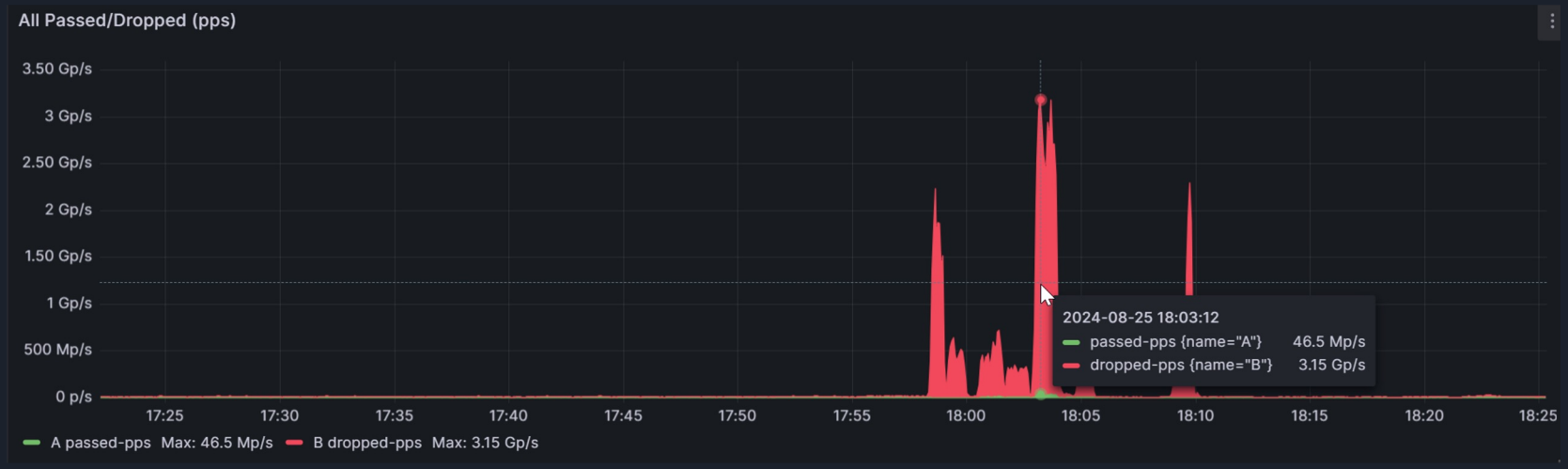
10G Traffic Out

Design Considerations (Creatia)

- We need to consider what end users need to be able to configure
  - Granular control without an overwhelming amount of features
- Convenient self-service onboarding processes can be a key differentiator for any given platform, particular in industries where self-service onboarding is largely unserved
- Giving end users access to granularity can empower them during attacks that may otherwise cause stress and impact bottom-line

August 25th 2024
Largest Packet Rate DDoS Attack Reported to the Public

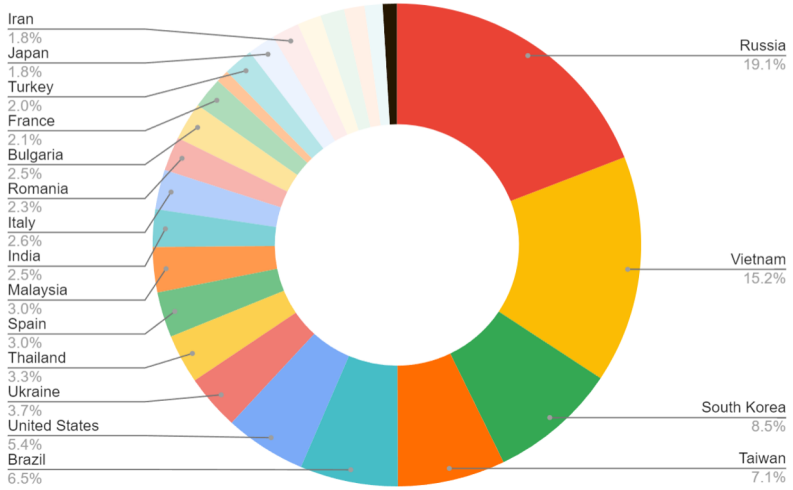
- Targeted towards a Minecraft gaming end-user with peak packet rate reaching 3.15 Gpps (billion packets per second)
- When contrasted with historically reported records, this size outpaces these headlines at a factor of 3.2 - 3.5x.
- Top sources include Russia, Vietnam, and Korea



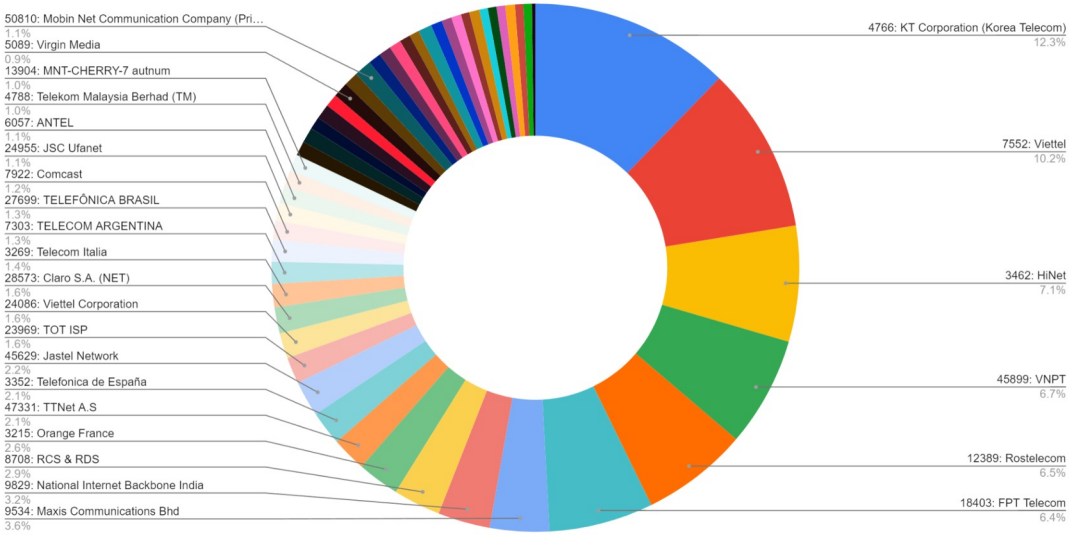
August 25th 2024

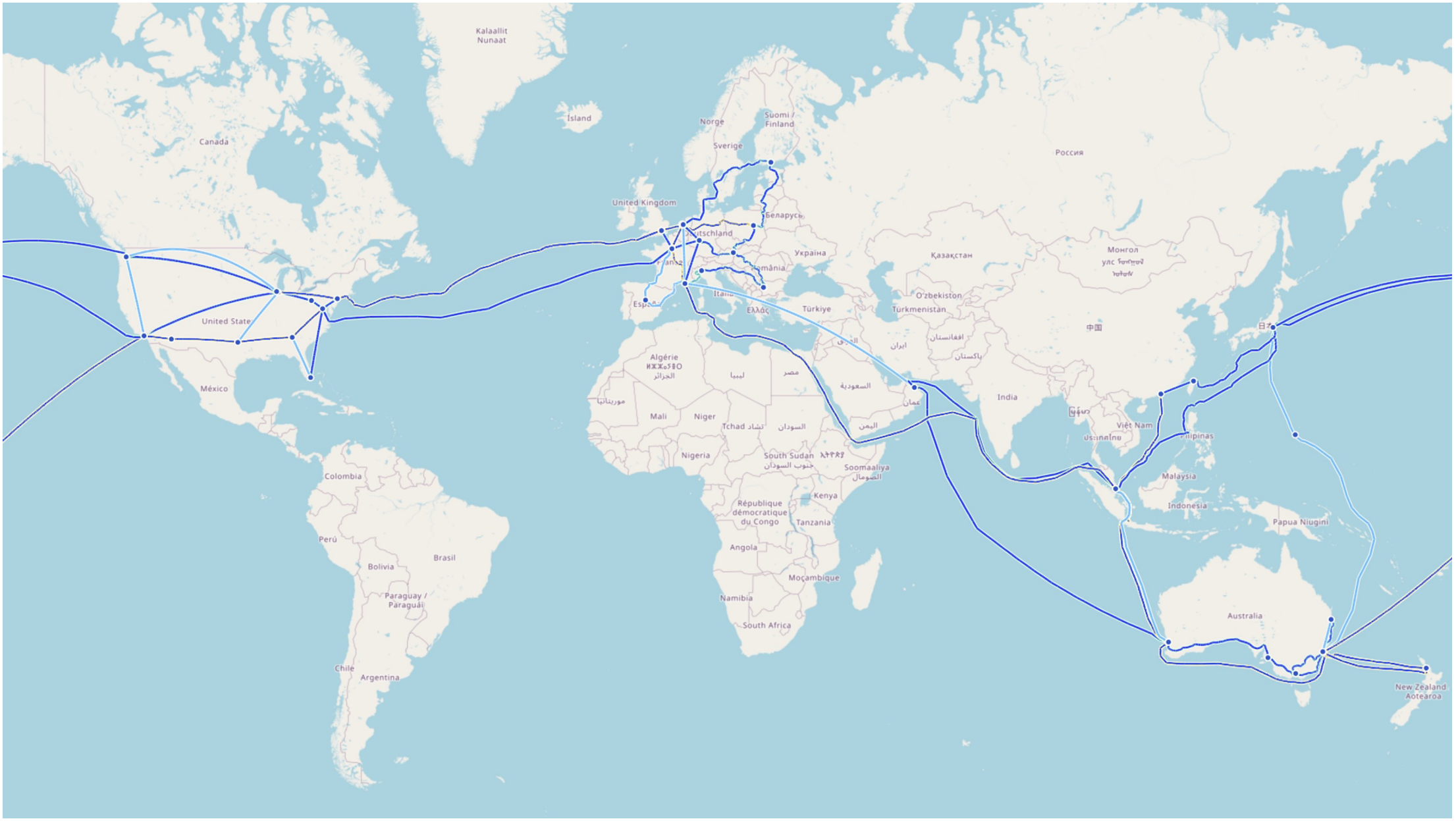
Largest Packet Rate DDoS Attack Reported to the Public

Top attack countries



Top source ASNs




Kalaallit Nunaat
Canada
Ísland
Norge
Suomi / Finland
Sverige
Россия
United Kingdom
Беларусь
Україна
Қазақстан
Монгол улс
United State
México
Algérie
الجزائر
ليبيا
مصر
السعودية
عمان
ایران
افغانستان
پاکستان
India
Mali
Niger
Tchad تشاد
السودان
اليمن
Nigeria
South Sudan جنوب السودان
Soomaaliya الصومال
Kenya
République démocratique du Congo
Tanzania
Angola
Moçambique
Namibia
South Africa
Türkiye
Ελλάς
Türkmenistan
O'zbekistan
中国
日本
Việt Nam
Filipinas
Malaysia
Indonesia
Papua Niugini
Australia
New Zealand Aotearoa
Colombia
Perú
Bolivia
Brasil
Paraguay / Paraguái
Chile
Argentina

Thank you