Segurança integrada nas redes de nova geração

Um novo paradigma

30 de Novembro de 2023

Ricardo Santos

ricardoj.santos@nokia.com

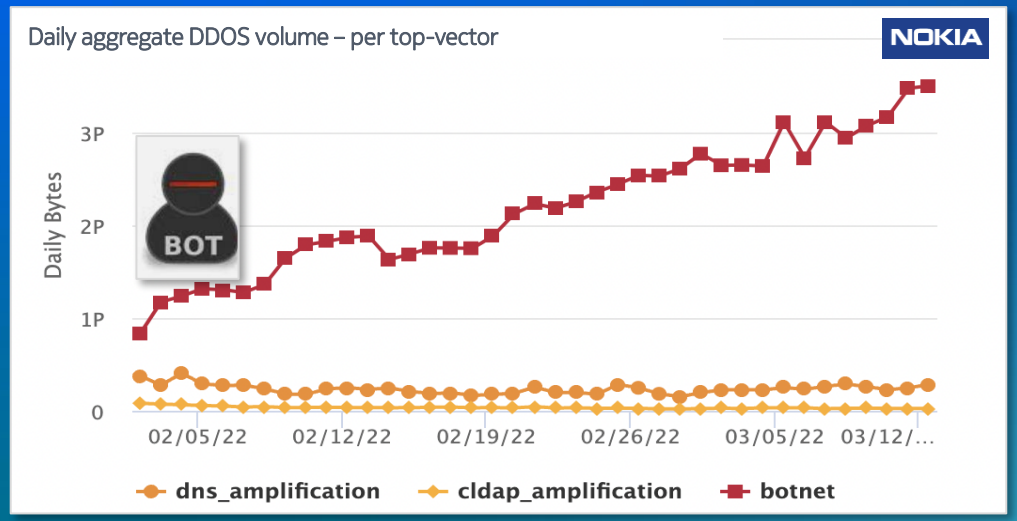
Tiago Amado

tiago.amado@nokia.com

Parking meter
x.3.17.23 is a DDoS botnet member

DVR x.7.5.9 is a DDOS botnet member

Botnets became the dominant threat

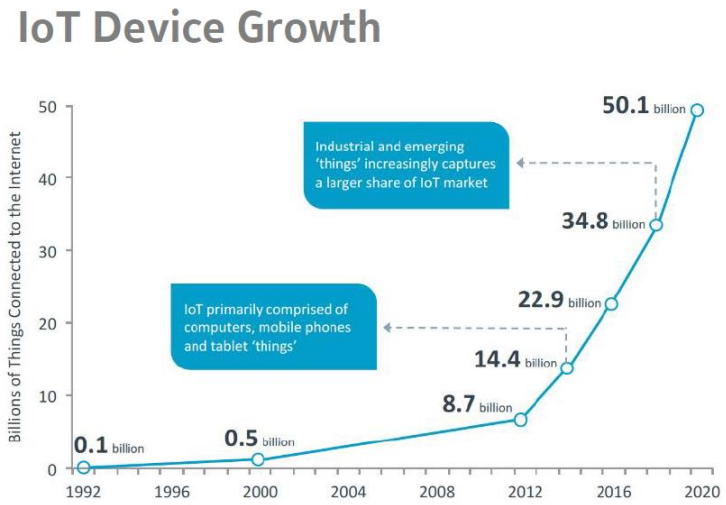


Botnet DDoS

became dominant form of attack in first quarter 2022

Rise of Botnets

Compromised IoT devices are driving DDoS atack size growth



'Popular' botnet members include:

- Home routers, IP cameras, thermostats
- Other connected consumer devices
- Cloud servers and aplliances

Compromised IP per device type

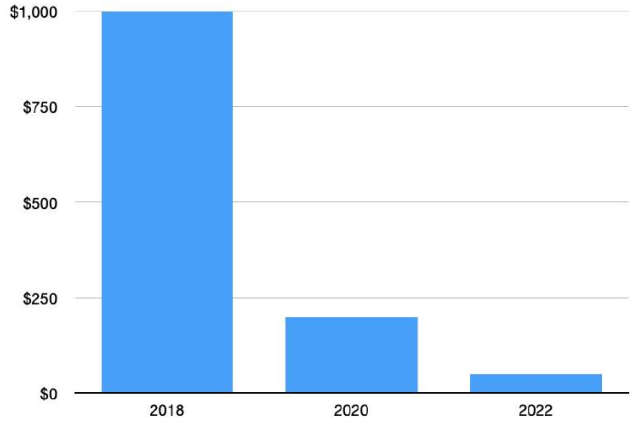
DDoS Botnet unique IP counts (2023'Q3)

Device	Count
other	48746
mikrotik	23856
webcam	9644
openssh	9135
hikvision	6878
sip_device	6797
rfjs	5080
commax	2689
speco	2075
cobra	1509
cisco	903
boa	878
asus_device	706
embedthis	484
draytekvigor	481

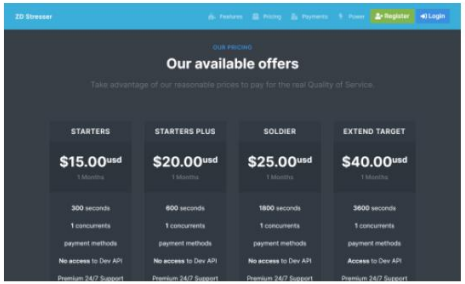
Rise of Botnets

Increasingly competitive booter market and cheap IoT botnets

Average Price for Buying DDoS Attacks



Collapse in daily average US price for launching a 100 Gbps DDoS using illegal booter web sites 2018 - 2022



zdstresser.net

stresslab.sx

The technical challenge with botnet DDOS

Traditional payload pattern detection techniques are no longer useful

Traditional DDoS (1990 – 2021)

- Spoofed IP addresses to trigger reflected amplified responses
- Or floods of crafted packets
- Often from well-known domains

From threshold-based detection…

Botnet-based DDoS

- Real devices, real IP-addresses and full TCP stack
- Appears as "regular" HTTP(s) bypass typical scrubbing payload ML
- Growing armies of devices connected anywhere

…to big-data **knowledge-based** detection

A new DDoS protection paradigm is needed

1 Surgical Detection based on big-data principles

From threshold-based…

…to knowledge-based detection

2 Leverage advances in IP Silicon to filter DDoS attacks

From expensive/limited scale DPI scrubbing…

…to scalable line-rate scrubbing on IP silicon

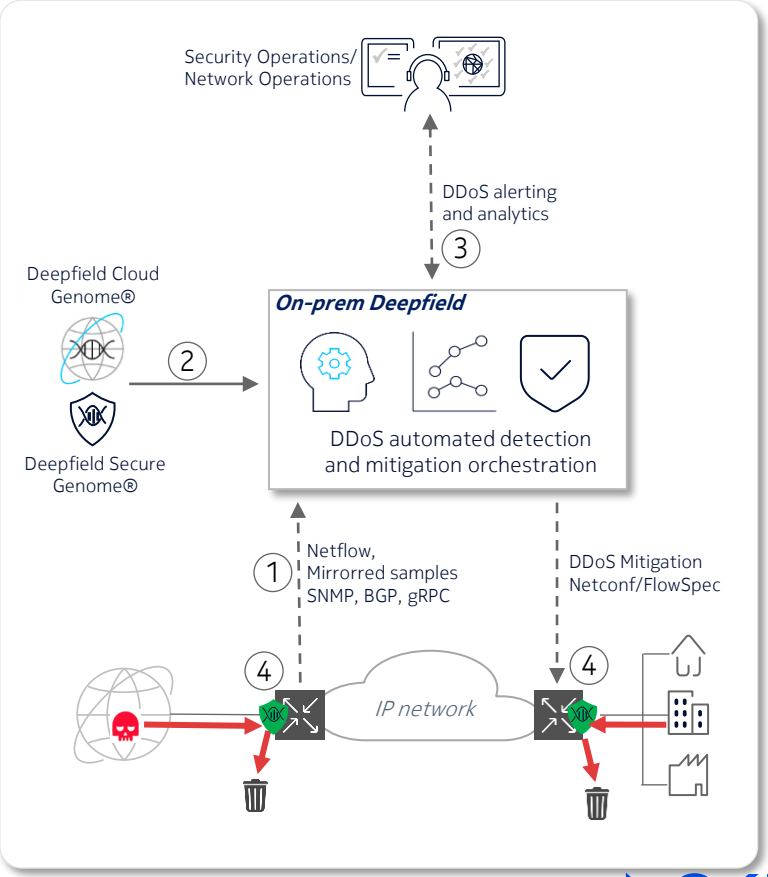
… with a different approach…

A high-scalable **software platform** that combines

1. A **big data** based Supply and Security map of the Internet
2. **Telemetry** from your routers
3. with the power of **high-performance Router silicon**

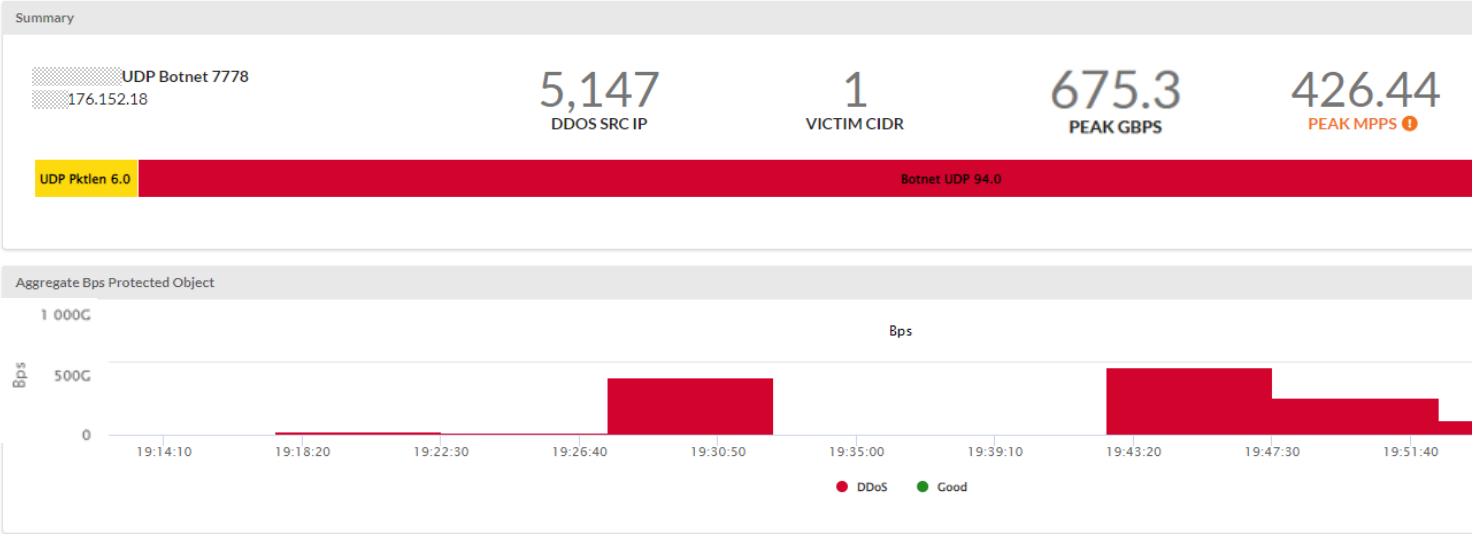
to provide **DDOS protection**

- **at every edge** – the most efficient point
- and **for every customer**
- **at a fraction of the cost** of appliance-based solutions



… so that when a Botnet attacks (or any other DDOS attack)…

Botnet attack against EU customer



… the network is able to natively* classify DDoS traffic

Time	TTL	Proto	TCP Flag	Peer	Src IP	SPort	Dst IP	DPort	Drop	Src Genome	Bytes	Len
13:45:00	60	17		[redacted]	[redacted]131.99.238	22897	[redacted].152.18	7778	44	lighttpd webcam [redacted]k.jp ddosbot	536094310	1,428
13:45:00	58	17		[redacted]	[redacted]56.86.130	61792	[redacted].152.18	7778	44	[redacted] commax webcam ulwsd ddosbot	536094310	1,428
13:30:00	60	17		[redacted]	[redacted]66.250.12	828157	[redacted].152.18	7778	16	[redacted] ddosbot	534757427	1,427
13:45:00	61	17		[redacted]	[redacted]84.1.105	5306	[redacted].152.18	7778	16	unknown_web fujitsu.com ddosamp rfjs ddosbot	534757427	1,427
13:45:00	61	17		[redacted]	[redacted]59.11.196	48338	[redacted].152.18	7778	16	ntt.com ddosbot	534757427	1,427
13:45:00	60	17		[redacted]	[redacted]11.137.76	41311	[redacted].152.18	7778	44	commax webcam ulwsd speco [redacted]zon.net [redacted].com ddosbot	534024294	1,428
13:50:00	55	17		[redacted]	[redacted].157.33	27181	[redacted].152.18	7778	16	app-webs httpd webcam [redacted]e.com unknown_dns hikvision myfritz ddosbot	533827788	1,427
13:55:00	62	17		[redacted]	[redacted]2.99.28	2823	[redacted].152.18	7778	44	[redacted] ddosbot	533722419	1,428

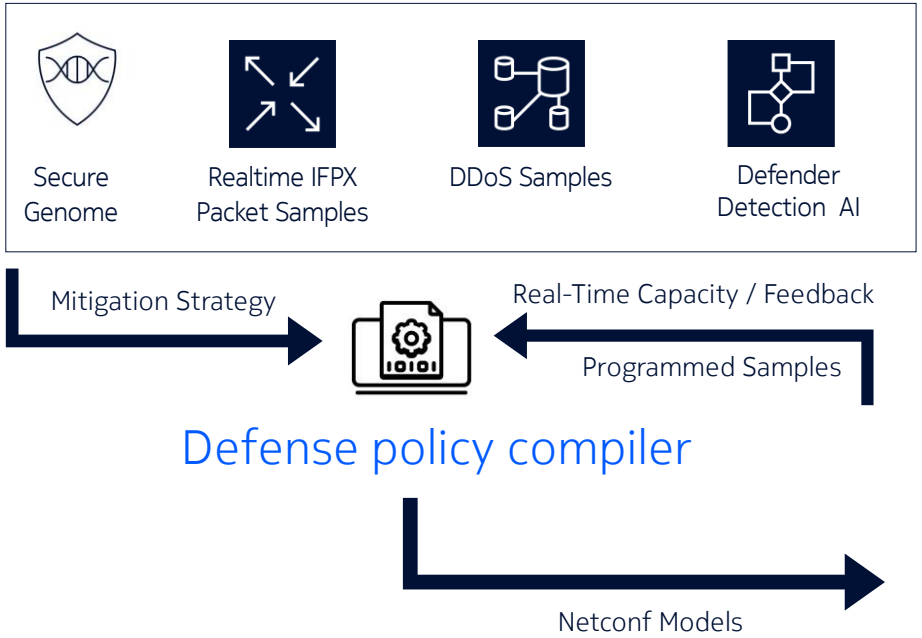
Advanced detection logic Combining:

- Genome info on src&dst IPs
- traffic rates and traffic patterns
- traffic ‘invariants’
- Source-IP cardinality
- Info on Internet topology (TTL, peering/transit networks)

(*): Native detection = no need to configure traffic thresholds for each type of potentially malicious traffic

… and then compiles the most efficient filter list…

Genome, AI/ML, Compiler, FP4/5 as protection enablers



All data processing / filtering on-premise

```
entry 8 create
    description ";#DFA;acl_90"
    match protocol 17
        dst-ip ip-prefix-list "VLAB_7_1"
        packet-length lt 40
        fragment false
    exit
    action
        drop
    exit
exit
entry 9 create
    description ";#DFA;acl_571"
    match protocol 6
        dst-ip ip-prefix-list "VLAB_7_1"
        tcp-fin true
        tcp-syn true
    exit
    action
        drop
    exit
exit
entry 10 create
    description ";#DFA;acl_579"
    match protocol 6
        src-ip ip-prefix-list "VLAB_9_518"
    exit
    action
        drop
    exit
exit
entry 4 create
    description ";#DFA;acl_13498"
    match
        dst-ip ip-prefix-list "VLAB_9_495"
        ttl range 1 37
    exit
    action
        drop
    exit
```

… with minimal false positive rate

Summary

1,057
FILTERS

0%
FALSE POSITIVE BYTES

Plan

Search:

Order	Counter Measure	Num Filters	% Bytes	% Packets
10	drop_udp_avg_pktlen_inariant (gid 44)	1	91	83
20	drop_bot (gid 16)	1,057	9	8

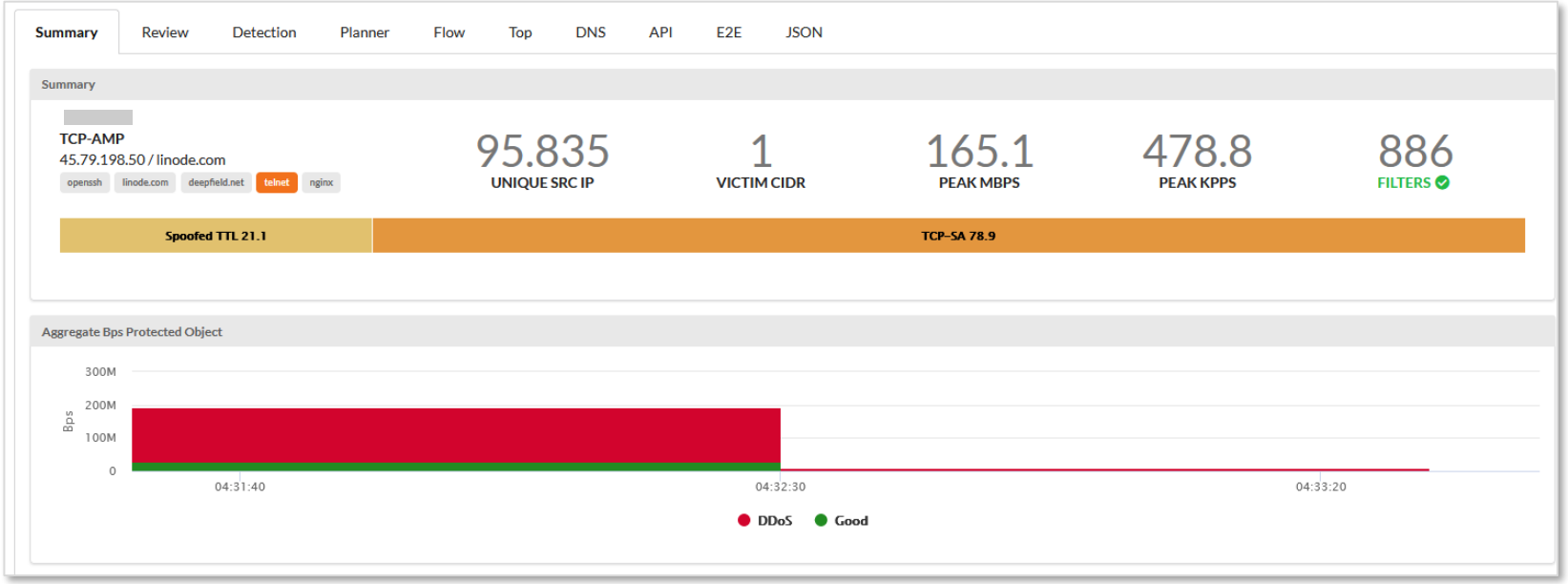
Showing 1 to 2 of 2 entries

Previous 1 Next

Blocking even the most challenging session attacks

Example: TCP SA Reflection attack

One of the most challenging DDoS to mitigate because: legitimate servers source IP and legitimate headers & payload



Blocking even the most challenging session attacks

Example: TCP SA Reflection attack

One of the most challenging DDoS to mitigate because: legitimate servers source IP and legitimate headers & payload

Summary | Review | Detection | Planner | Flow | Top | DNS | API | E2E | JSON

Summary

TCP-AMP

50 / linode.cc

openssh | linode.com | deept

Spoofed

Aggregate B

300

200

100

Bps

Time	TTL	Proto	TCP Flag	Peer	Src IP	SPort	Dst IP	DPort	Detect	Src Genome	Bytes	Len
22:32:07	50	6	SA		104.27.206.204	80	198.50	9090	41	cloudflare.com	44	44
22:32:09	50	6	SA		104.25.102.226	443	198.50	9090	41	invalid_tls cloudflare.com	44	44
[illegible]	[illegible]	[illegible]	SA		104.25.102.229	443	198.50	9090	41	invalid_tls cloudflare.com	44	44
[illegible]	[illegible]	[illegible]	SA		104.25.102.229	443	198.50	9090	41	invalid_tls cloudflare.com	44	44
[illegible]	[illegible]	[illegible]	SA		104.25.102.232	443	198.50	9090	41	cloudflare.com	44	44
[illegible]	[illegible]	[illegible]	SA		104.25.102.232	443	198.50	9090	41	cloudflare.com	44	44
22:32:08	50	6	SA		104.25.102.234	443	198.50	9090	41	cloudflare.com	44	44
22:32:09	50	6	SA		104.25.102.234	443	198.50	9090	41	cloudflare.com	44	44
22:32:07	51	6	SA		104.25.102.235	443	198.50	9090	41	invalid_tls cloudflare.com	44	44

Ugh!

All of the IPs are legitimate Cloudflare CIDRs.

How can we mitigate this?

The Cloudflare global network

Our vast global network, which is one of the fastest on the planet, is trusted by millions of web properties.

With direct connections to nearly every service provider and cloud provider, the Cloudflare network can reach 95% of the world's population within 50 ms.

270

cities in 100+ countries, including mainland China

10,500

networks directly connect to Cloudflare, including every major ISP, cloud provider, and enterprise

142 Tbps

global network edge capacity, consisting of transit connections, peering and private network interconnects

50 ms

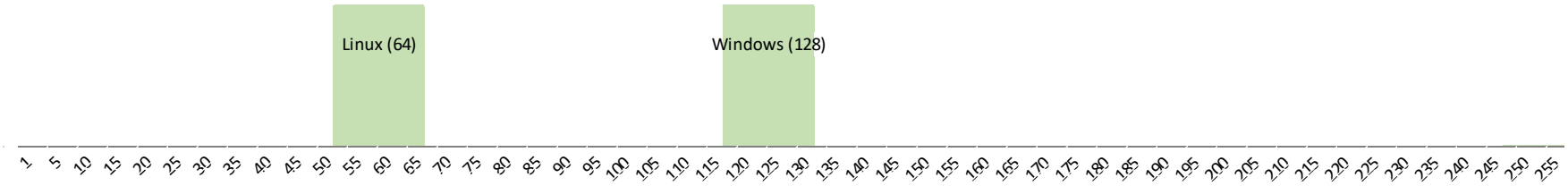
from 95% of the world's Internet-connected population

Use of TTL for DDOS detection and mitigation

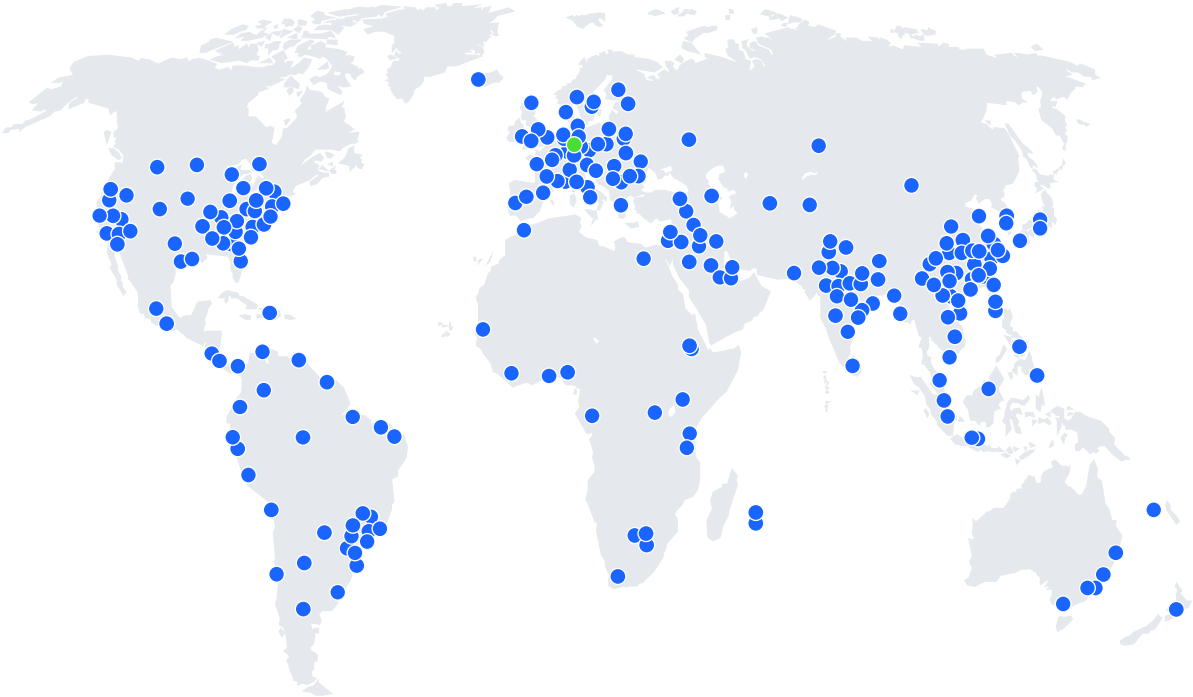
- Default “ttl values” depend on OS:
  - Linux: 64
  - Windows: 128

- Global OTT services serve content from closest regional CDNs
  - Vast majority of global OTT traffic delivered from within 10 hops of the peering routers

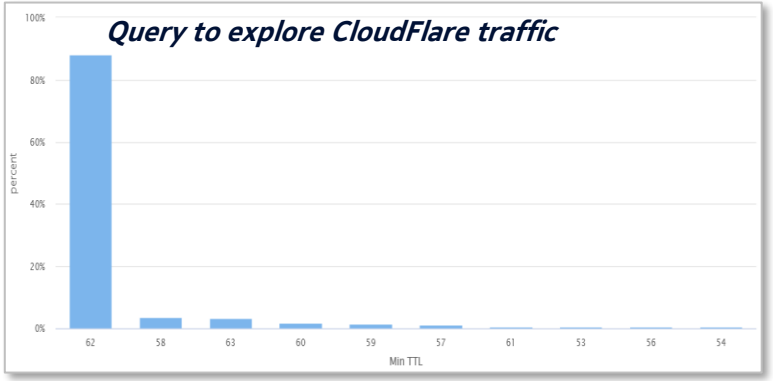
Common TTL ranges seen in legitime traffic (green ranges)

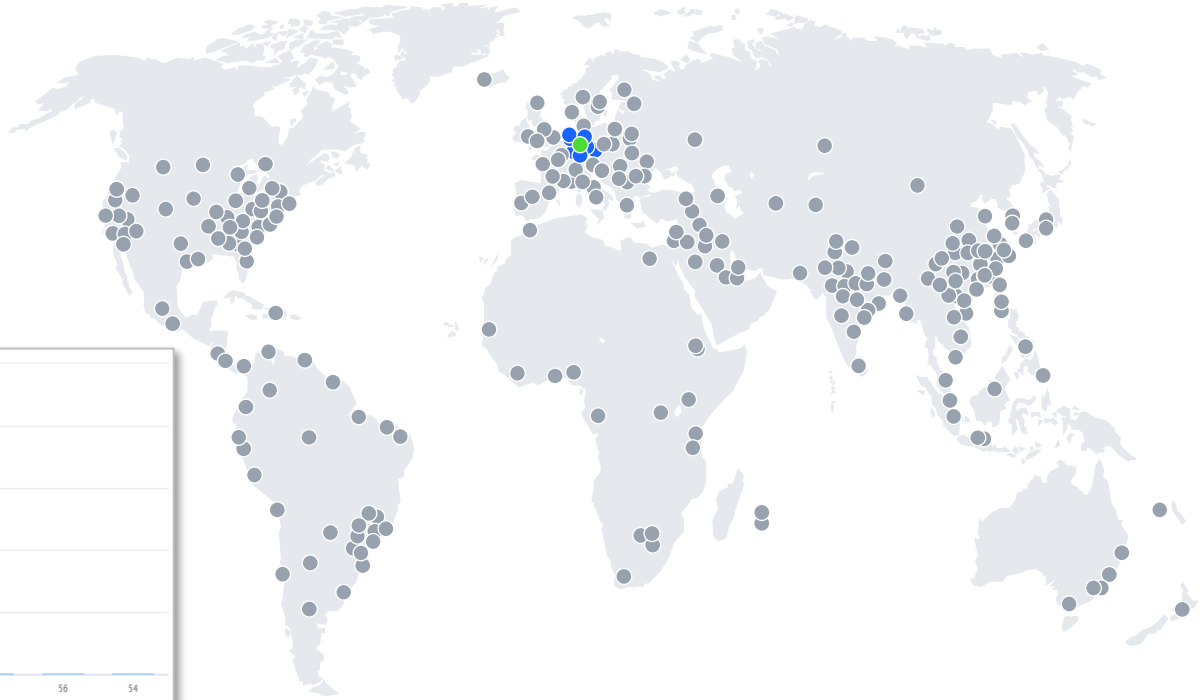


A next-gen DDoS protection system builds knowledge on peace time traffic…

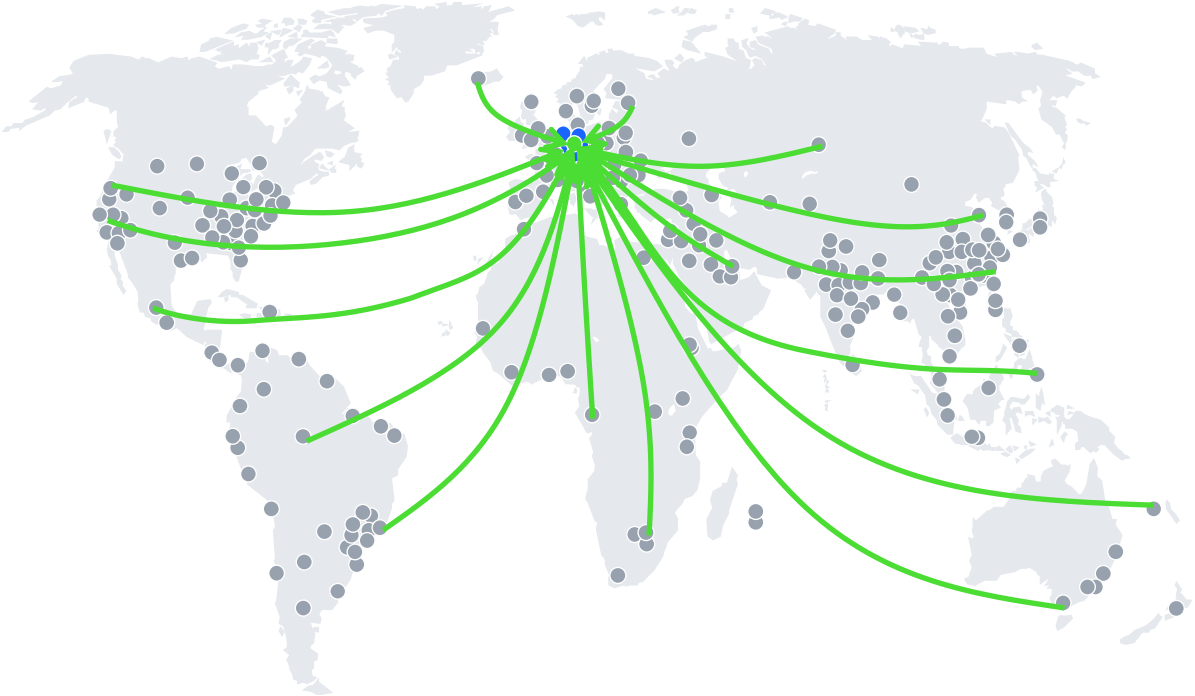


... and it knows that 98% of Cloudflare traffic to this location is sourced from within 10 hops...

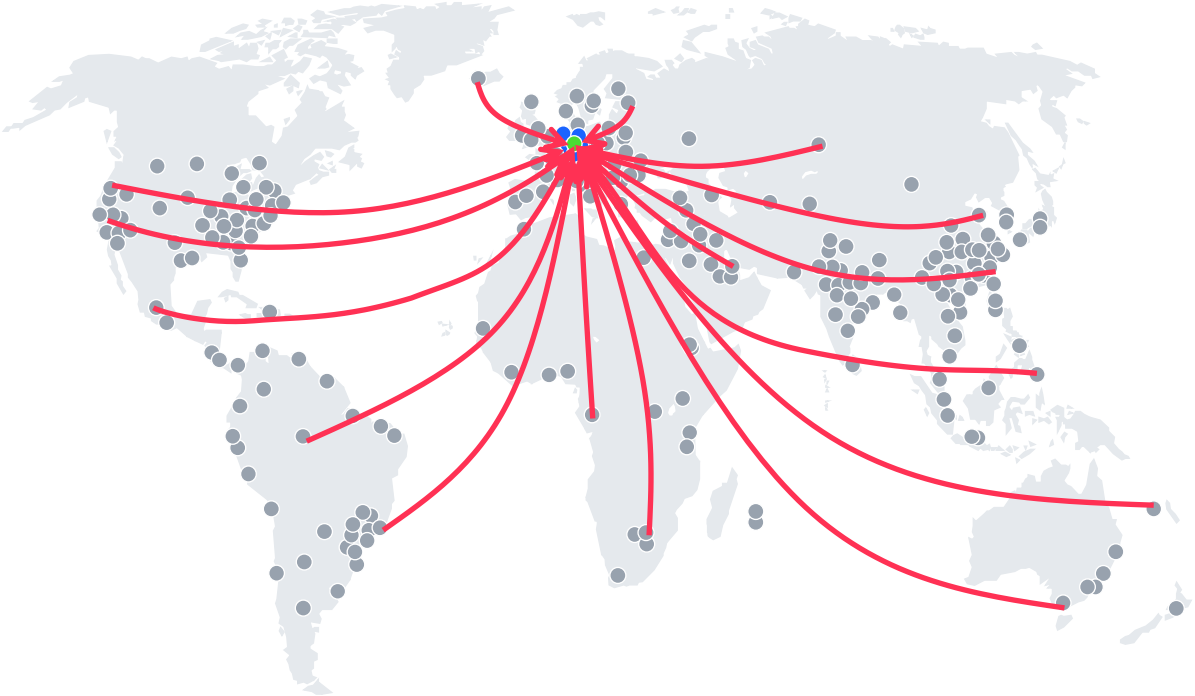




...so that when it suddenly sees an unusual amount of ‘Cloudflare’ traffic sourced from many of the remote Cloudflare PoPs...



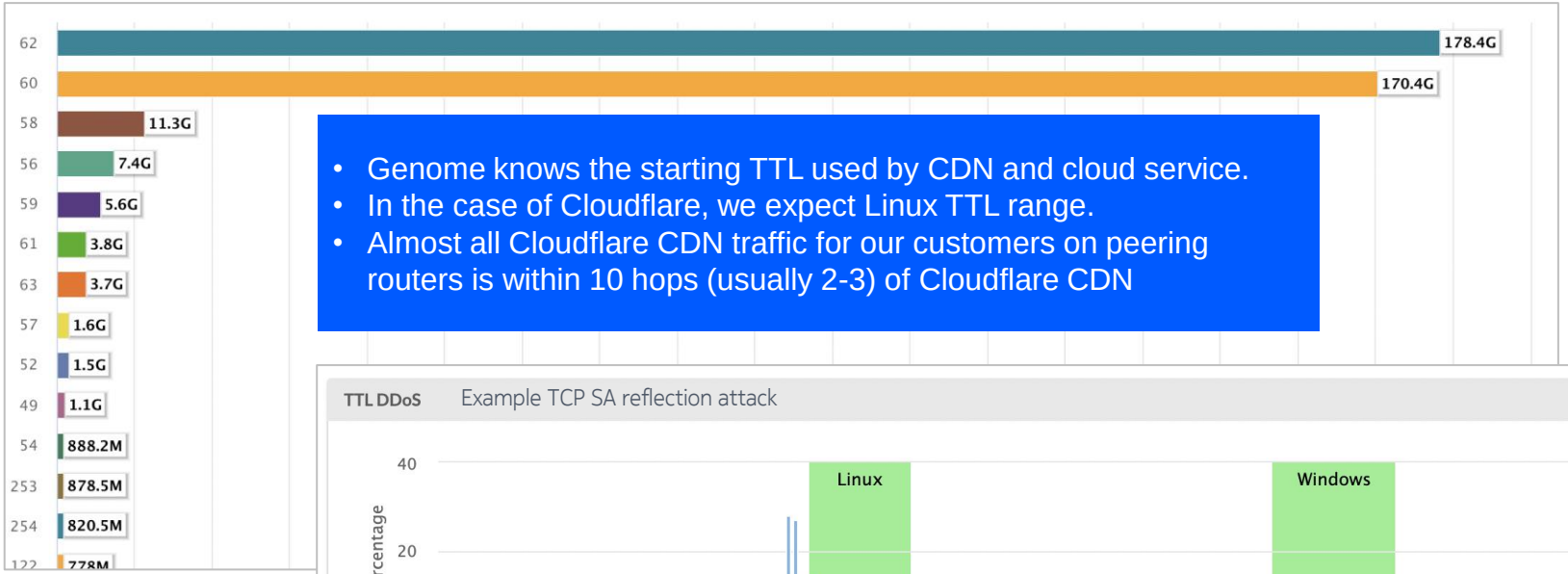
...it automatically knows this is DDoS traffic...



...which Deepfield blocks with Topology Based Filtering rule on IP Routers...

```
If
    tcp_flags = SA,
    source_ip = Cloudflare,
    destination_ip = Protected_object
    topology_distance > 10
Then
    drop
```

Comparing expected TTL for Cloudflare CDN vs TTL in attack traffic



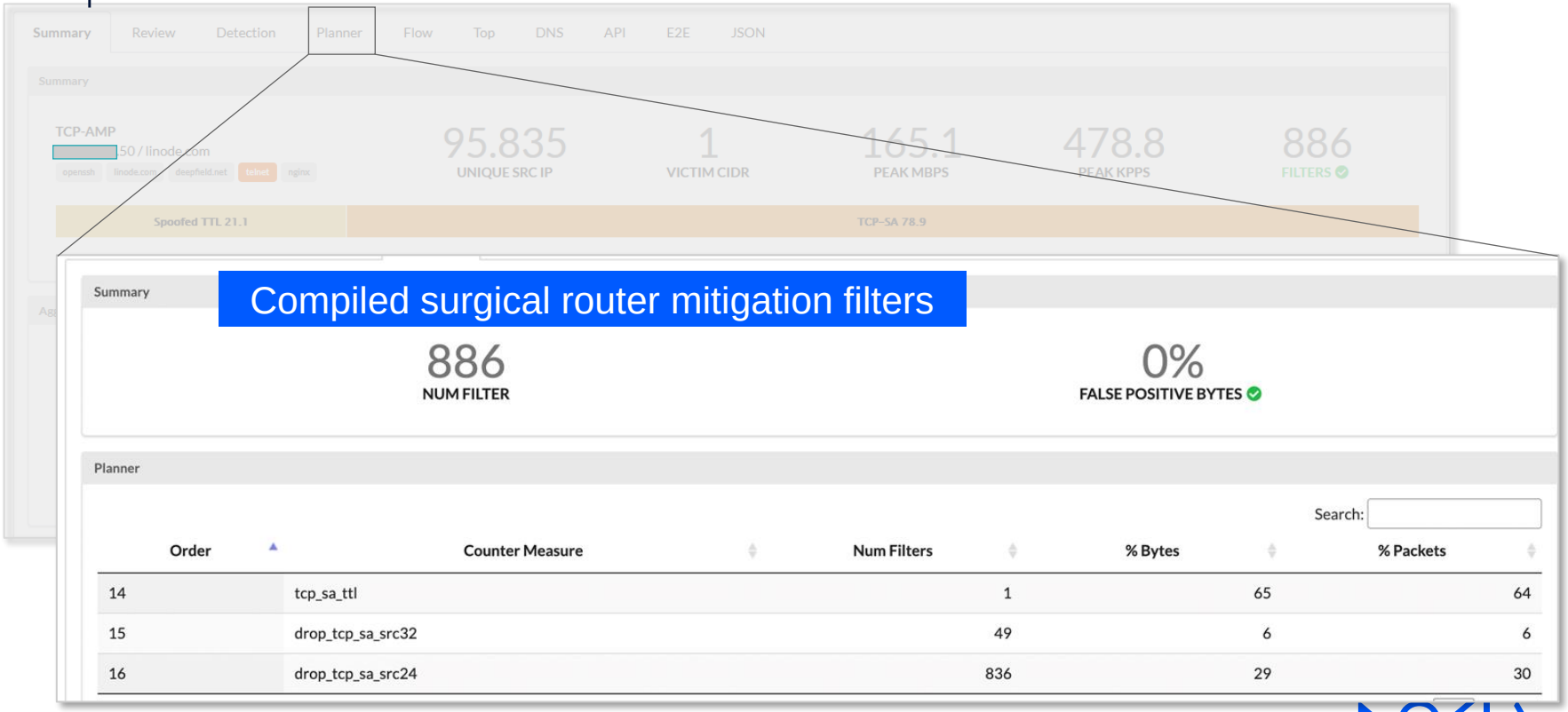
- Genome knows the starting TTL used by CDN and cloud service.
- In the case of Cloudflare, we expect Linux TTL range.
- Almost all Cloudflare CDN traffic for our customers on peering routers is within 10 hops (usually 2-3) of Cloudflare CDN

Genome significantly raises the bar for TCP SA DDoS!

(But sometimes we also need to fall-back to baseline based filtering… with the help of ML/AI)

Deepfield solution blocking even the most challenging session attacks

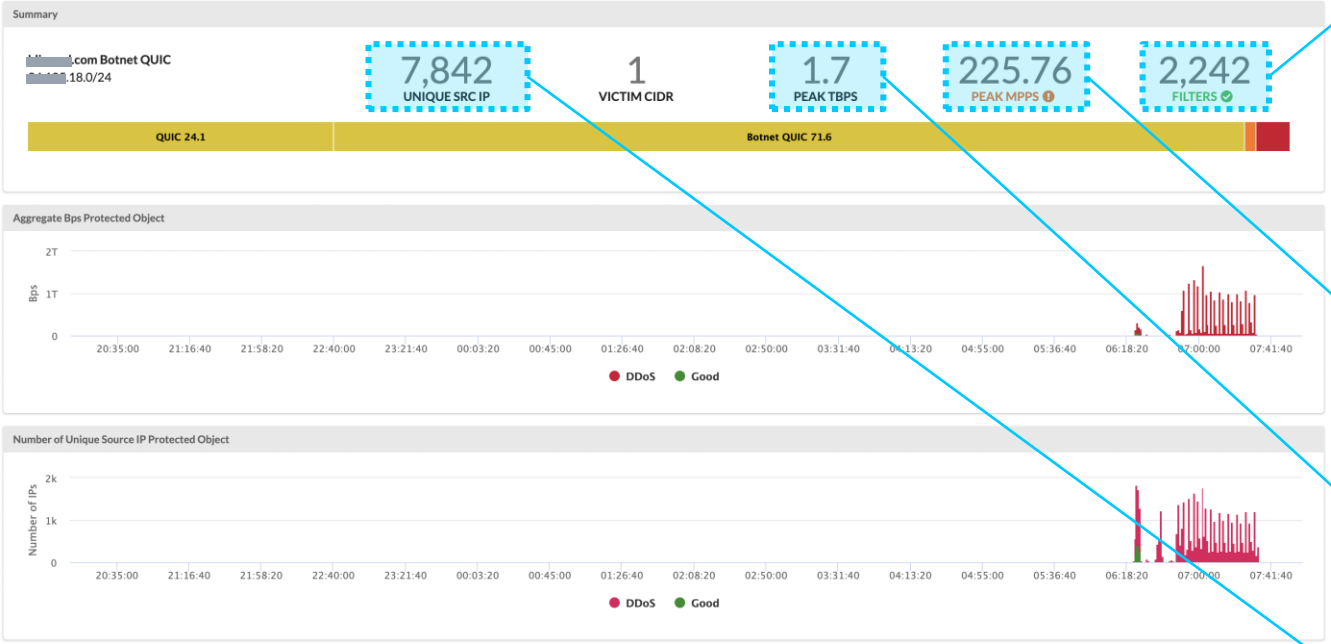
Example: TCP SA Reflection attack



Order	Counter Measure	Num Filters	% Bytes	% Packets
14	tcp_sa_ttl	1	65	64
15	drop_tcp_sa_src32	49	6	6
16	drop_tcp_sa_src24	836	29	30

Another example of a Botnet Quic flooding attack …

Example Botnet Quic Flooding atack



More complex to mitigate as generally no common patterns:

- can require as many filters as there are bot source IPs (fewer if we can identify invariants).
- **Secure Genome™ helps to classify botnet.**

Can also be packet-per-second intensive (similar to spoofed direct flood).

From **tens of Gbps** to **multiple Tbps**. (Some individual IoT bots can send about a Gbps of traffic!)

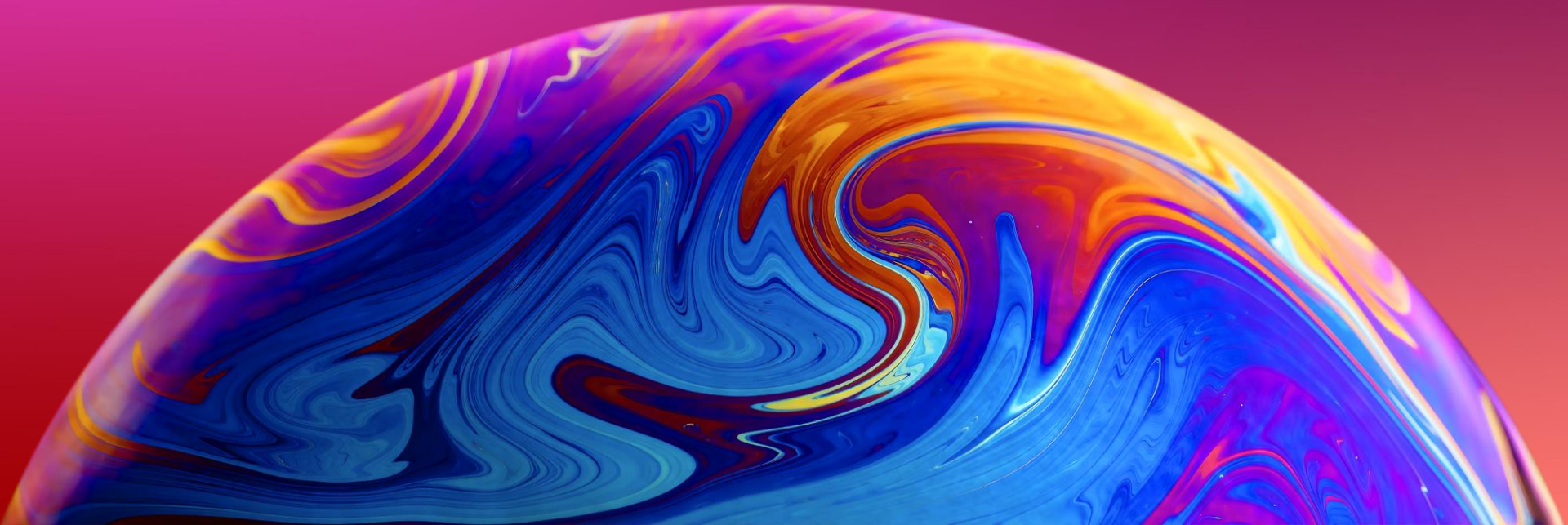
Typically, **several thousands IPs** (more rarely several tens of thousands).

Example Botnet Quic Flooding atack

Flow details

Time	TTL	Proto	TCPFlag	Peer	Src IP	SPort	Dst IP	DPort	Detect	Src Genome	Bytes	Len
00:57:20	60	17		209	174.18.9.218	59608	24.105.18.126	443	57 botnet_quic	ddosbot lumen.com	536735692	927
01:02:30	57	17		13285	92.6.230.143	24726	24.105.18.67	443	57 botnet_quic	tr069 ddosbot talktalkgroup.com	536500070	928
01:02:30	61	17		13285	79.77.189.45	48010	24.105.18.73	443	57 botnet_quic	webcam talktalk.co.uk ddosbot	534390681	928
00:54:50	61	17		3491	65.181.73.131	41139	24.105.18.125	443	57 botnet_quic	pccw.com ddosbot	533049344	928
01:27:20	60	17		8708	82.77.129.138	26216	24.105.18.66	443	57 botnet_quic	ddosbot blacklists rcs-rds.ro apache httpd	533018880	928
01:02:10	61	17		13285	92.20.68.29	33532	24.105.18.68	443	57 botnet_quic	rfjs lighttpd ddosbot talktalkgroup.com	532225433	928
01:02:30	60	17		5607	149.241.32.137	16558	24.105.18.127	443	57 botnet_quic	sky.com ddosbot	531578060	928
01:02:30	58	17		5607	176.27.214.149	25593	24.105.18.75	443	57 botnet_quic	sky.com ddosbot	530874931	928

The Big Picture…



The need for multi-layer security

DDoS Protection from Cloud or Upstream Provider

when DDoS Attack size > free peering BW

DDoS Service from cloud scrubbing service or from upstream provider or from IXP

Edge/onnet DDoS protection

Edge-mitigation

Protect the entire network and all your services /customers against all Volume and large session attacks on scalable Nokia/Juniper Edge routers

or Defender Mitigation System

or other scrubbing appliance

When edge routers not fit for surgical DDoS filtering or for Premium business customers (or when security teams want their own thing)

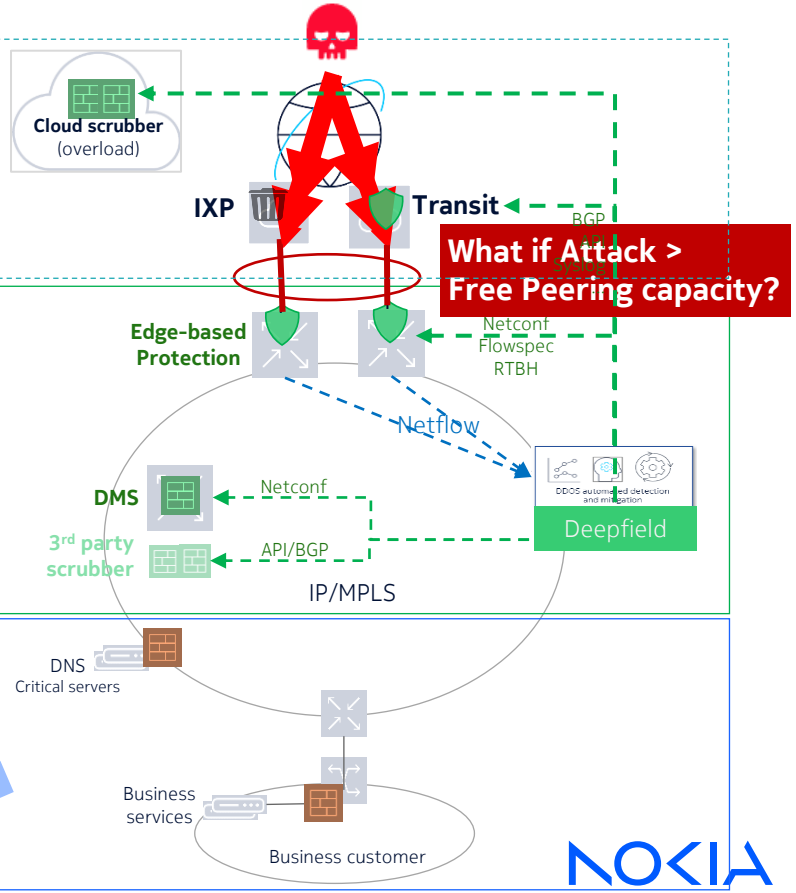
Inline FW/IDS/IPS require also protection against DDoS!!

Inline Next-Gen FW or WAF

Protection DNS & critical servers against application attacks

Controlling access to DMZ/networks & servers

Inline server/ app/network protection



How can we improve detection time even further?

Sampled Port Mirroring instead of Netflow

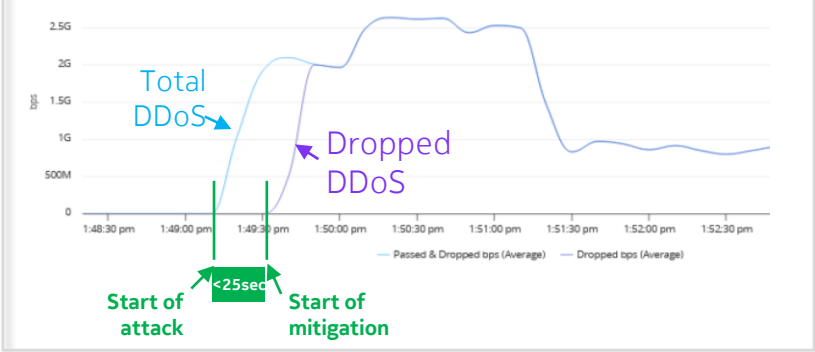
Fastest mitigation within 30 seconds

Comparing SPM vs Netflow based detection for same live attack.

Netflow	77.127/32	1.89 Gbps	225.68 kpps	udpflood	84,850	FINISHED Start: Sep 23, 2023 11:12:11 pm Duration: 7 min	Not Mitigated
Sampled Port Mirror	77.127/32	1.88 Gbps	224.18 kpps	udpflood	87,709	FINISHED Start: Sep 23, 2023 11:11:10 pm Duration: 9 min	Completed: 41

SPM detection is 61 sec faster!!

Mitigation started within <25 sec after start of attack

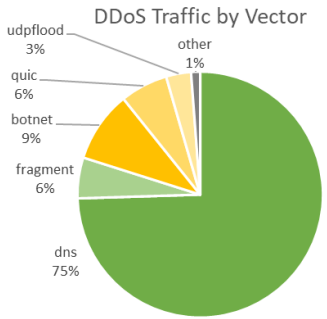


.. and it unlocks mitigation via payload patterns!

Are you curious on how frequent are attacks?...

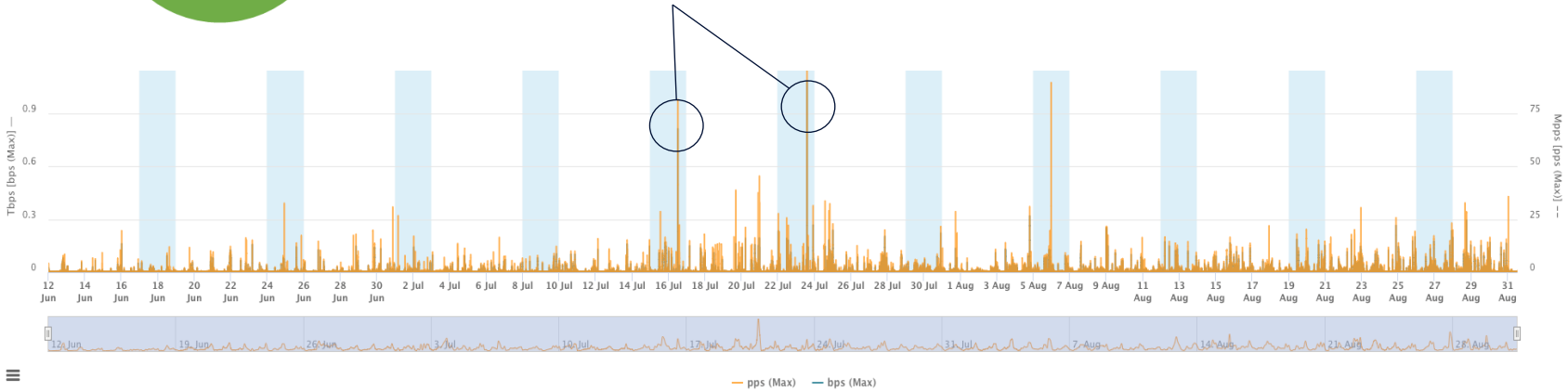
DDoS traffic analysis

Tier 1 provider June-Aug 2023



- 80% of DDoS traffic corresponds to DNS amplification attacks (*dns, fragment*)
- 18% is coming from Botnets (*botnet, quick, udpflood*)
- Significant activity during mid July, with 2 attacks in the 1Tbps range

- ~100 ISP IP addresses regularly attacking other ISP destinations and/or Internet destinations



Nokia IP network security

A multilayer embedded approach to IP network security

Big-data security analytics
- Deepfield Defender
- Deepfield Secure Genome ™

Router Net OS apps and tools
- Nokia security gateway • CG-NAT
- SR OS firewalls • ESM security

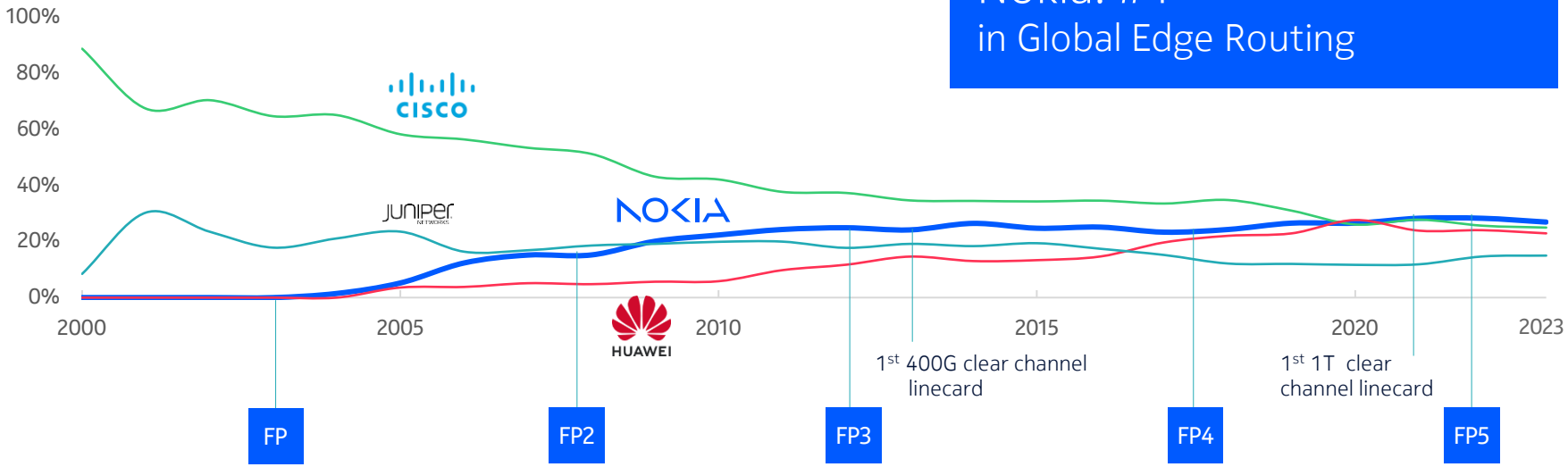
Router Net OS
- SR OS self-defending network OS

IP silicon
- High-performance DDoS filtering (FP4, FP5)
- ANYsec line-rate encryption (FP5)

Where is Nokia?

Decades of industry firsts

Nokia: #1
in Global Edge Routing



FP
1st 10G clear channel NPU

FP2
1st 100G clear channel NPU

FP3
1st 400G clear channel NPU

FP4
1st 1T clear channel NPU
1st 16 nm NPU
1st 56G SERDES
1st integrated HBM
1st intelligent memory
1st to ship QSFP56-DD 400G

FP5
1st 1.6T clear channel NPU
1st 112G SERDES
1st integrated HBM2e
1st to ship QSFPDD-800G
ANYsec encryption

Copyright and confidentiality