NOKIA

Jornadas FCCN

15-17 de abril de 2024 | Funchal

A rede como solução anti-DDoS

Ricardo Santos

IP Consulting Systems Engineering EMEA

ricardoj.santos@nokia.com

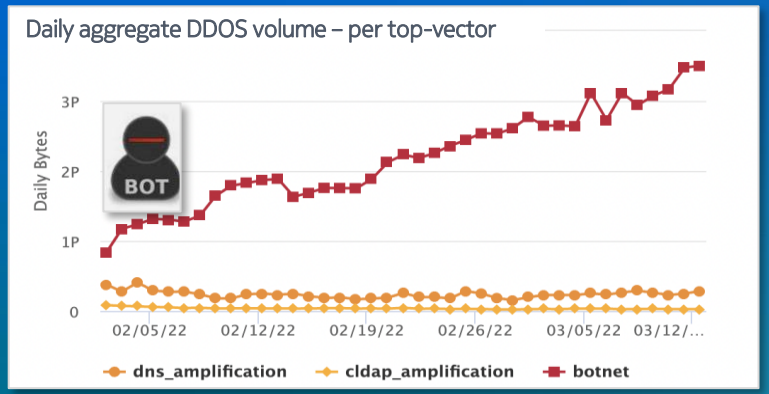
DDoS attacks on public services are impacting and mediatic

Worst cyberattack in Greece disrupts high school exams, causes political spat | AP News

It said the distributed denial of service, or DDoS, attacks aimed at overwhelming the platform occurred for a second consecutive day Tuesday. The attack involved computers from 114 countries, causing outages and delays in high school exams but failing to incapacitate the system, the ministry said.

Botnets became a dominant threat

Botnet DDoS
became dominant form of attack in first quarter 2022

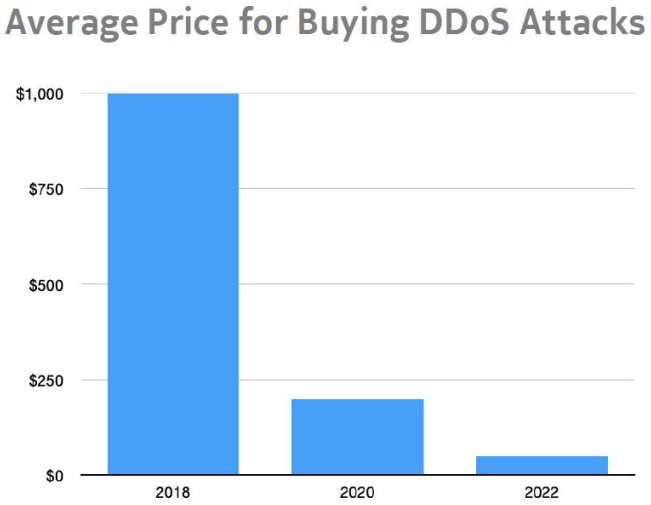


DVR x.7.5.9 is a DDOS botnet member

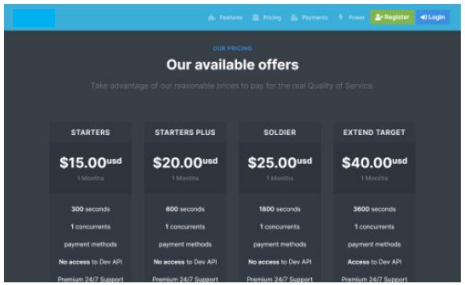
Parking meter
x.3.17.23 is a DDoS botnet member

Rise of Botnets

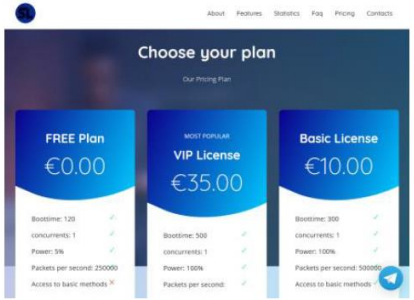
Increasingly competitive booter market and cheap IoT botnets



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



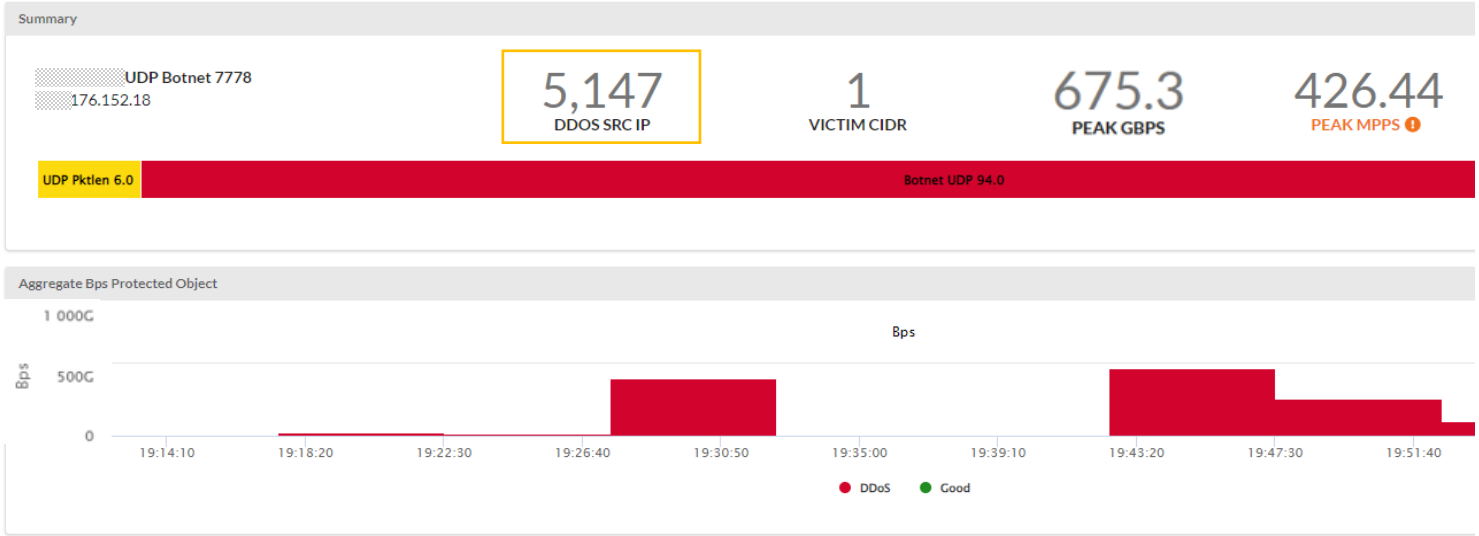
[redacted]er.net



[redacted]ab.sx

Allowing the proliferation of DDoS attacks

Botnet attack against EU customer



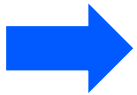
The technical challenge with botnet DDOS

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

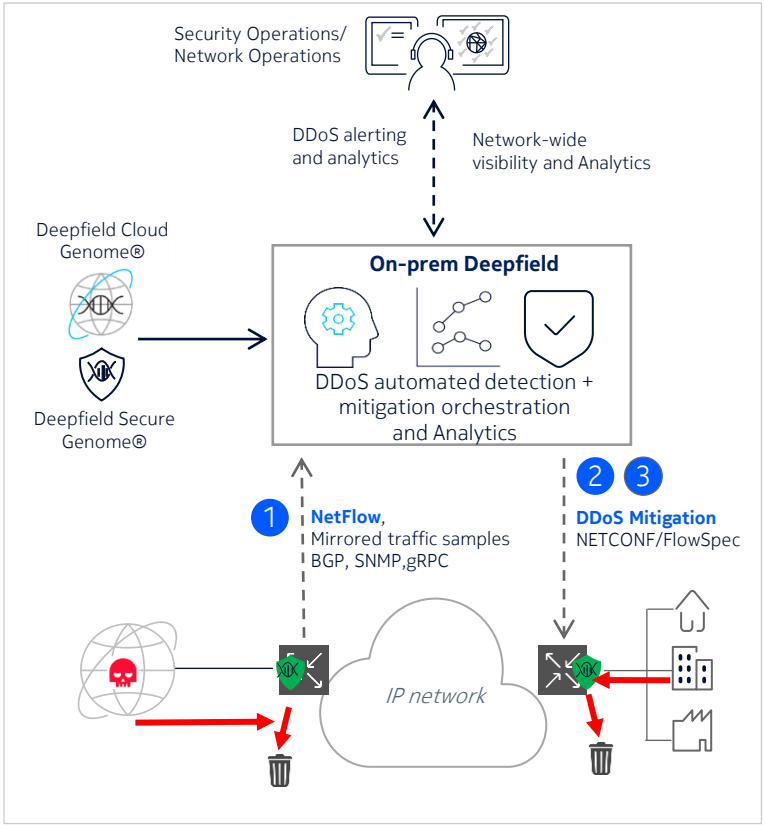
From expensive/limited scale DPI scrubbing…

…to scalable line-rate scrubbing on IP silicon

...with anti-DDoS at the Peering routers

Requires from the IP silicon:

1. **Telemetry performance**
   - sampling rate OR mirroring
2. Packet **filtering scale**
3. Packet **filtering performance**
   - line rate (!)



… 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			131.99.238	22897	.152.18	7778	44	lighttpd webcam k.jp ddosbot	536094310	1,428
13:45:00	58	17			56.86.130	61792	.152.18	7778	44	commax webcam ulwsd ddosbot	536094310	1,428
13:30:00	60	17			66.250.12	828157	.152.18	7778	16	ddosbot	534757427	1,427
13:45:00	61	17			84.1.105	5306	.152.18	7778	16	unknown_web fujitsu.com ddosamp rfjs ddosbot	534757427	1,427
13:45:00	61	17			59.11.196	48338	.152.18	7778	16	ntt.com ddosbot	534757427	1,427
13:45:00	60	17			11.137.76	41311	.152.18	7778	44	commax webcam ulwsd speco zon.net com ddosbot	534024294	1,428
13:50:00	55	17			.157.33	27181	.152.18	7778	16	app-webs httpd webcam e.com unknown_dns hikvision myfritz ddosbot	533827788	1,427
13:55:00	62	17			2.99.28	2823	.152.18	7778	44	ddosbot	533722419	1,428

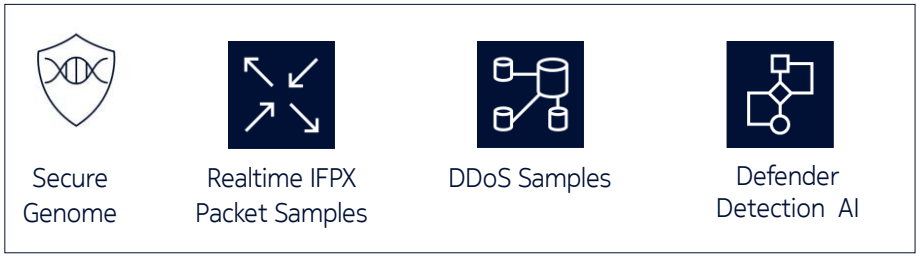
Advanced detection logic Combining:

- 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 compile the most efficient filter list…

Genome, AI/ML, Compiler and high-performance IP silicon as protection enablers



Mitigation Strategy

Real-Time Capacity / Feedback

Programmed Samples

Defense policy compiler

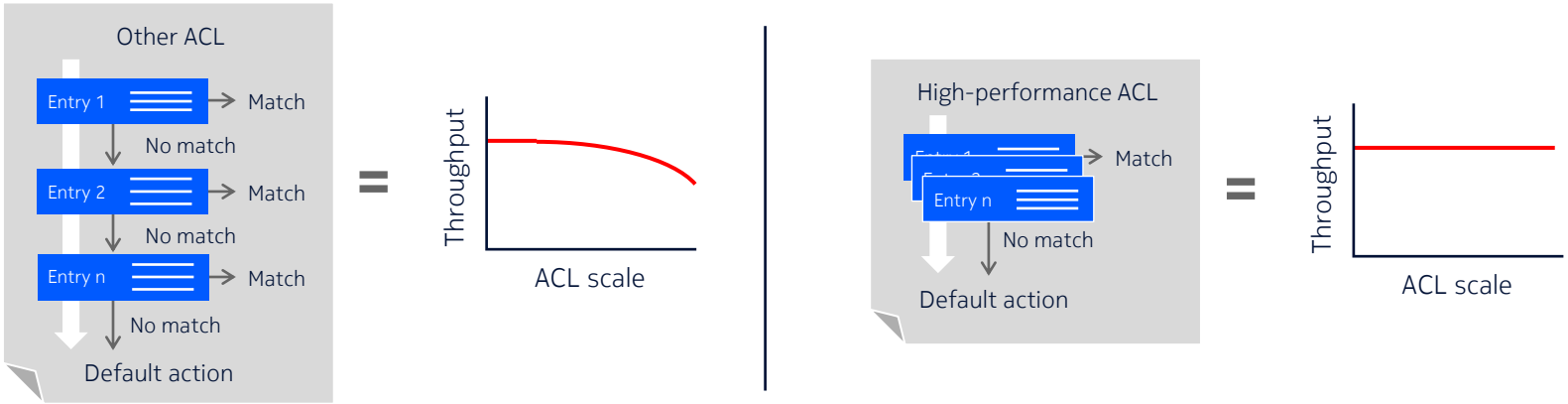
Netconf Models

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
```

Linerate filtering capacity at the peering router

Performance with scale

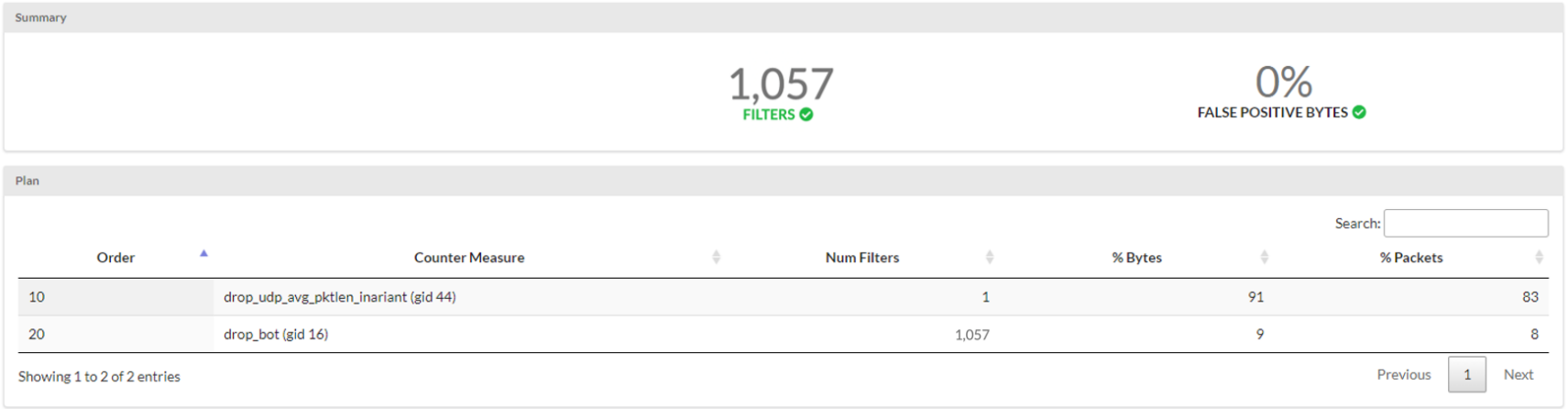


Large filter scale (256k filter entries) for increased filter granularity → **Minimize false positives**

Perform ACL packet match in a single pass regardless of the number of ACL entries or ordering → **Fast** attack mitigation

Router capacity is maintained, which cannot be guaranteed for implementations that parse through each entry sequentially → Deterministic **linerate protection**

… with minimal false positive rate



  | Public

Take aways

Knowledge

The network as source of traffic big-data

AI/ML

Compile efficient filters to minimize false positives

Network Performance

Deterministic and high-performance filters capacity at the Peering routers

More information here

[DDoS security | Nokia]

NOKIA

DDoS security

Everything you need to know about Distributed Denial of Service (DDoS)

What is DDoS?

Distributed Denial of Service or DDoS is malicious traffic that aims to deny access or degrade or stop connectivity for individual users, internet hosts and service provider network infrastructure.

Malicious players have been exploiting IP protocol and systems vulnerabilities for more than a couple of decades now to launch DDoS attacks on their targets: network hosts and systems. Some protocols, such as BGP and Domain Name System (DNS), have gained additional security features to make them more robust. Also, industry-wide initiatives using best practices have been implemented to curb DDoS traffic (BPM-23). However, many hosts still use protocols that rely on open principles set by the internet community a long time ago. Some of them never envisaged malicious exploits that could jeopardize the intended operation of router-based networks.

On this page

- What is DDoS?
- What are the different types of DDoS?
- How large is DDoS (danger)?
- What is the impact on service provider networks?
- Botnet DDoS
- Why is a new approach to DDoS security needed?
- Related products and solutions
- Learn more

What are the different types of DDoS?

Broadly, all DDoS traffic can be categorized into:

- Amplification and reflection DDoS
- Flooding DDoS traffic (using IP address spoofing or IP header modification, IPHM)
- Application DDoS.

Please check out our application note, DDoS Protection for the cloud, 5G and IoT era.

Community

Global DDoS Threat Alliance →


NOKIA
jornadas
FCCN