Santa Monica Networks

Three Reasons Why DDoS Protection Fails

Tomas Savėnas

2023-10-25

About me

Tomas Savėnas,

an IT security engineer with a strong passion for ensuring digital security.

With years of experience in the field, I have dedicated my expertise to safeguarding digital landscapes, primarily through my focus on Web Application Firewall (WAF) solutions.

Santa Monica Networks

What is a DDoS Attack and Why it's Important?

Threat actors

- Coordinated DDoS Attacks

Threat Actors targeting „unfriendly countries“ everyday

in Lithuania multiple online services went down during NATO Summit

Lessons lerned, but recently they came back again

Do we know everything about those threat actors?

Understanding DDoS attacks

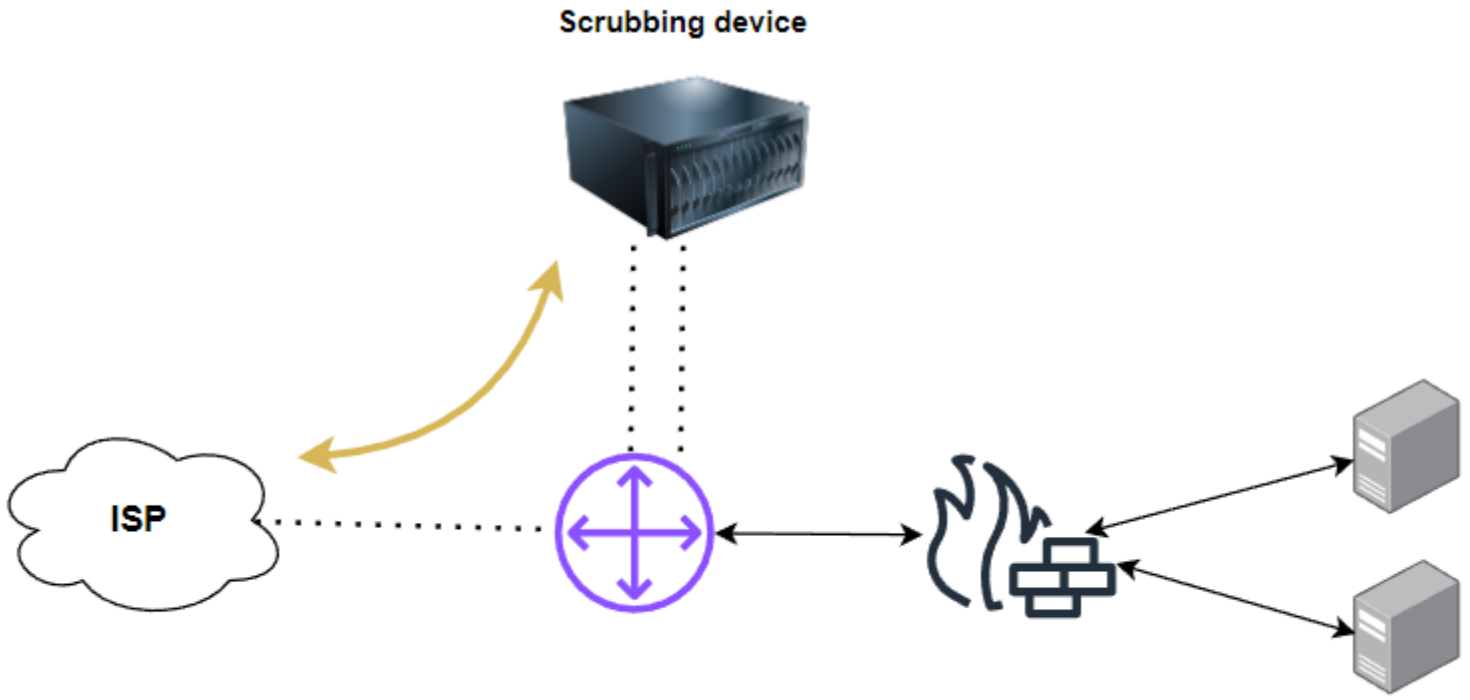
- By OSI model

Layer 3 attacks involve high packet volume in network traffic;

In Layer 7 attacks weak application endpoints.

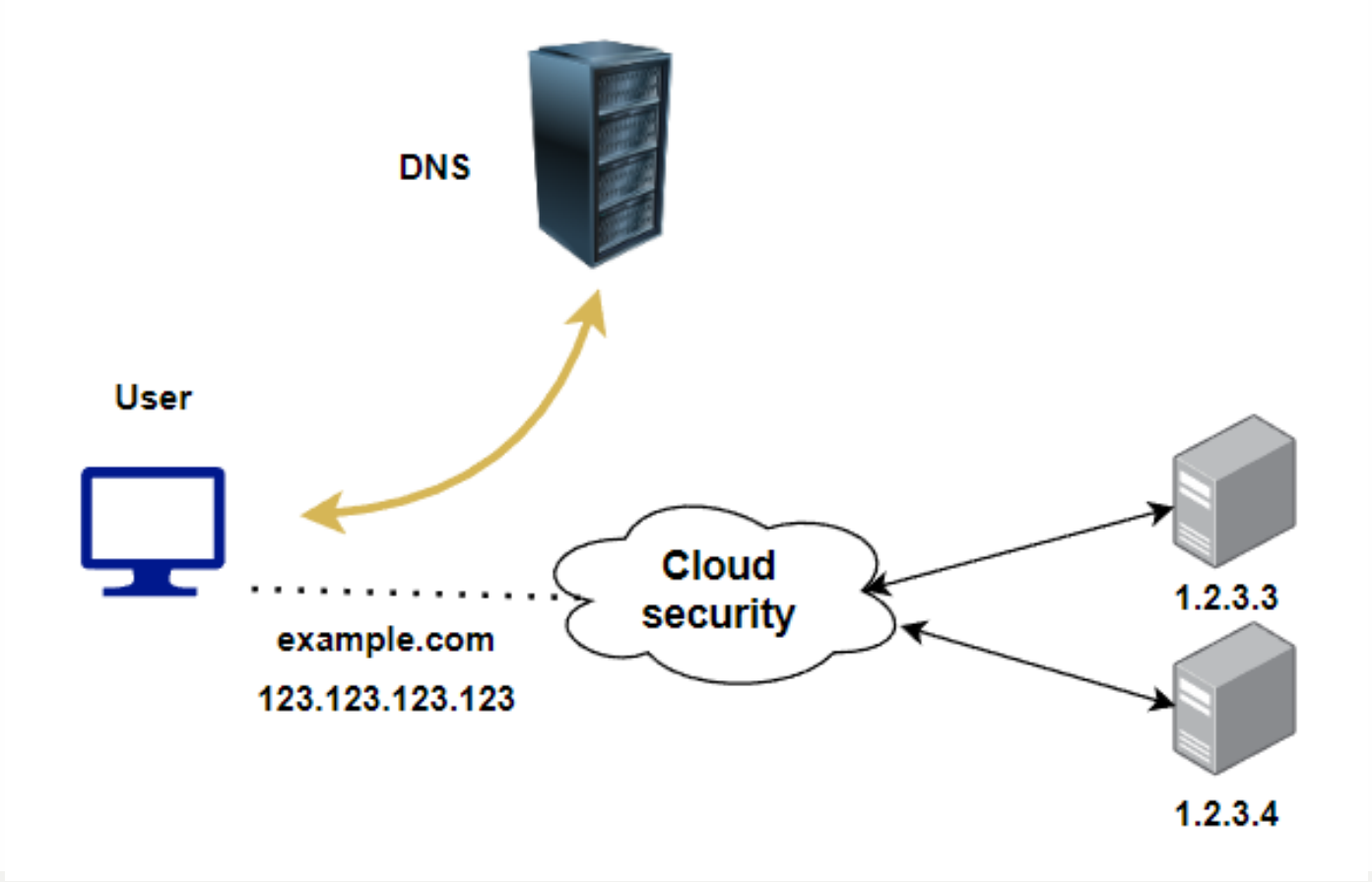
Solutions for Layer 3

- How Does L3/4 DDoS Protection Work?



Solutions for Layer 7

- How Does L7 DDoS Protection Work?



Three Ways DDoS Protection Fails

- 1) End of service license or support

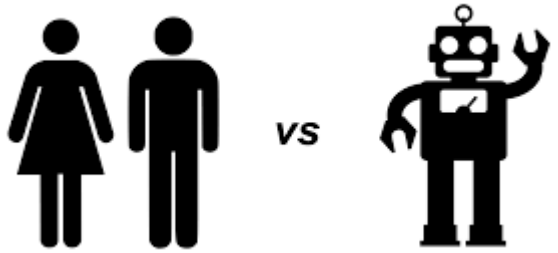
The Internet Has No National Borders:
This means that IP addresses can frequently change, making our protection rules, which are based on a country's basis inadequate.

Hackers are getting better every day:
Additionally, services that collect information about threat actors and generate rules based on their characteristics are impacted. When these services expire, we may lose the latest threat actor characteristics, which are left by internet bots.

Three Ways DDoS Protection Fails

2) Lack of Security Controls Against Bots

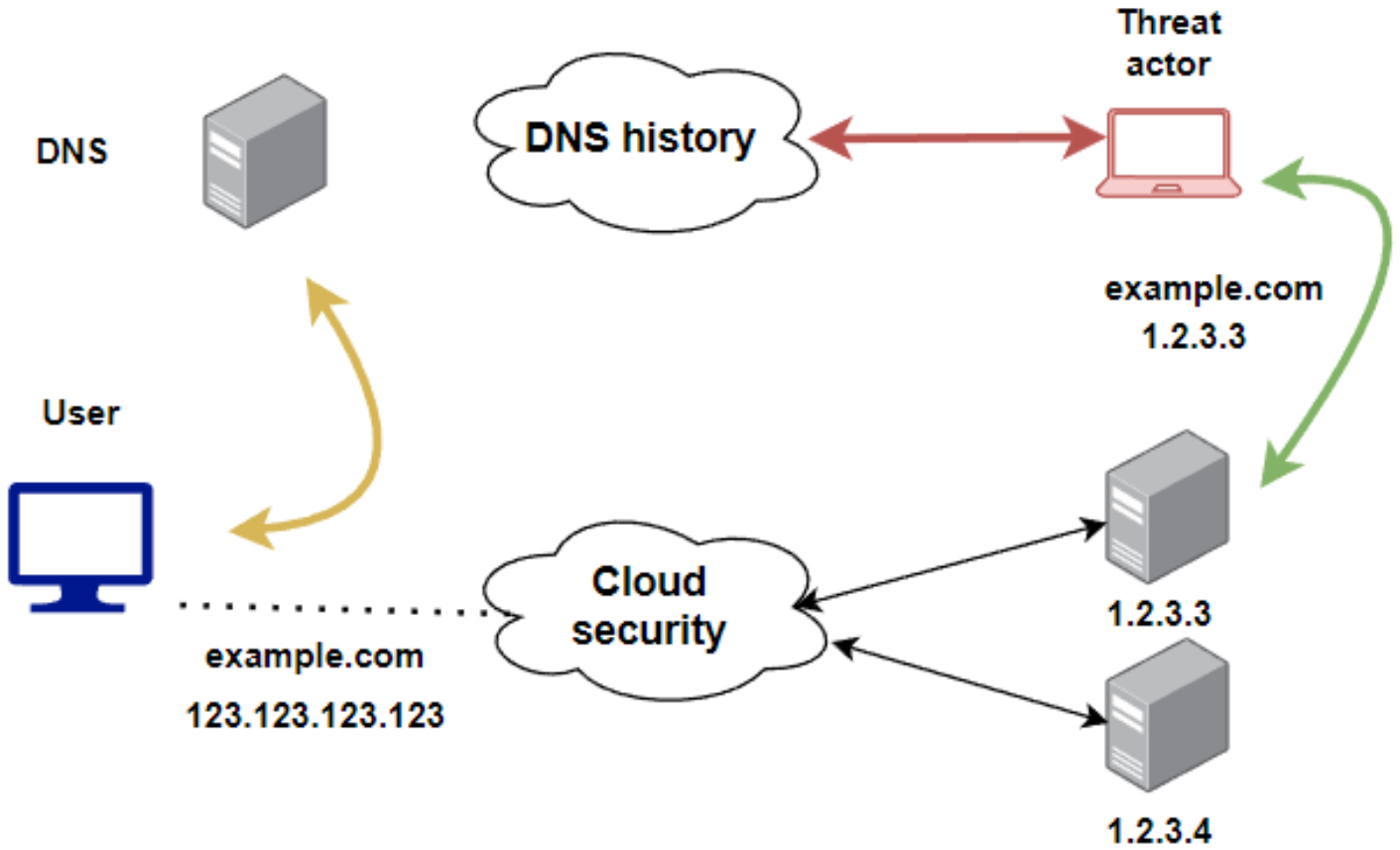
Internet Bots Prevalence:
More than 50% of all internet traffic consists of automated instruction sets, known as internet bots, which can perform various tasks without requiring significant computing resources.



Real user vs bots:
they make normal HTTP request and L3/4 tools can't protect.

Three Ways DDoS Protection Fails

- 3) Publicly available origin server



DNS has short term memory, but the internet will remember everything

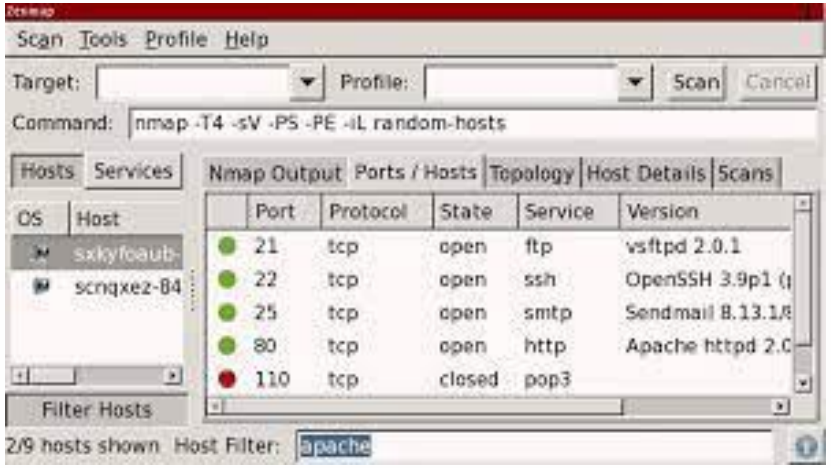
Three Ways DDoS Protection Fails

- **Publicly available ports on backend servers**

Informacija apie WWW ir IP adresus.

lrs.lt Tikrinti

Svetainės pavadinimas:	**Just a moment...**
Svetainės serveris (A):	**104.18.22.128**
Svetainės serveris (AAAA):	**2606:4700:0:0:0:0:6812:1680**
El. pašto serveris (MX):	**mx4.lrs.lt -> 193.219.60.148 (mx4.lrs.lt)**
Šalis:	**United States (US)**



lrs.lt

0 / 89

Community Score

At least 2 detected files communicating with this domain

lrs.lt

government misc top-100K

DETECTION DETAILS RELATIONS COMMUNITY

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to

Passive DNS Replication (8)

Date resolved	Detections	Resolver	IP
2023-02-03	0 / 89	VirusTotal	104.18.22.128
2023-02-03	0 / 88	VirusTotal	104.18.23.128
2019-11-17	0 / 88	VirusTotal	107.154.236.31
2019-11-17	0 / 88	VirusTotal	107.154.141.31
2018-11-23	0 / 88	VirusTotal	107.154.138.31
2016-04-17	0 / 88	VirusTotal	192.230.77.16
2016-04-15	0 / 88	VirusTotal	192.230.78.16
2013-11-15	0 / 88	VirusTotal	193.219.60.42

Problem

- Research (2023)

Top 10 providers by ASN

```
$ head LietuvosImones.txt
  25575  INTERNETO-VIZIJA, LT
   3839  CLOUDFLARENET, US
   3508  TELIA-LIETUVA, LT
   2584  AS-HOSTINGER, CY
   1634  RACKRAY UAB Rakrejus, LT
   1196  HETZNER-AS, DE
   1057  BALTNETA Customers AS, LT
    917  AMAZON-02, US
    872  WIX_COM, IL
    871  GOOGLE-CLOUD-PLATFORM, US
$
```

~ 200.000 Registered Legal Entities in Lithuania

~ 60.000 websites I was able to find on Internet

~ 50.000 website domains are operational

Using cookies to determinate bot protection:
Cloudflare ~ 300 website
F5 – 150 websites

- Conclusions

The vanilla configuration is insufficient for addressing the challenges posed by the current threat landscape, highlighting the imperative need for continuous security enhancements.

Recommendation

Santa Monica Networks

- Recommendations

1. Renew licenses
2. Take care of bots
   - Block User-Agent: go-http-client/1.1
3. Limit access for backend servers
   - Allow trusted IP addresses, rest of all deny acess
   - Secret header, or mTLS between edge with backend
   - Hide backend using brand-new IP address

End

Thank you!