Zvýšenie odolnosti webových aplikácií proti DDoS útokom

(Horizontálne škálovanie)

Miroslav Hájek

1. Progress report
Princípy informačnej bezpečnosti
2020 / 2021

Dostupnosť ako bezpečnostný pilier

Spoľahlivý, okamžitý a autorizovaný prístup k informáciam a zdrojom podľa potreby

Hrozby

Zvnútra

- Chyby softvéru
- Hardvérove zlyhania
- Preťaženie systému

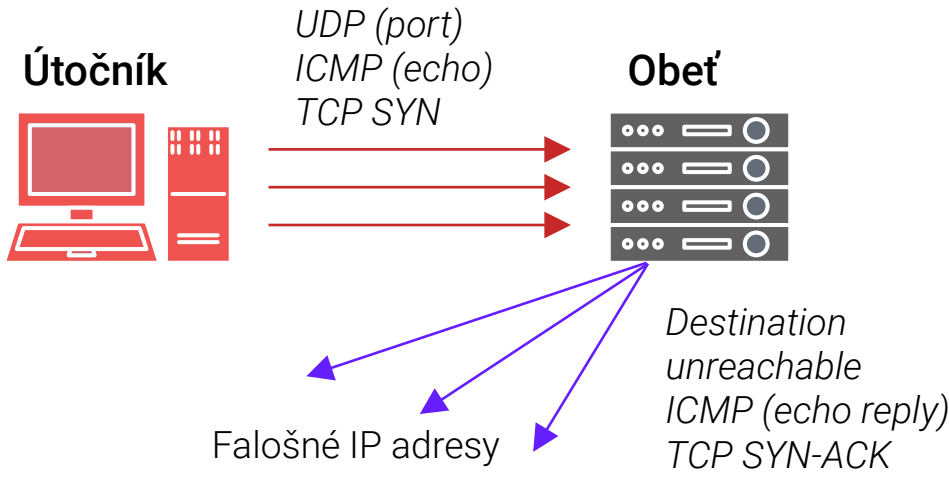
Zvonka

- Ekonomický zisk
- Pomsta
- Ideológia
- Intelektuálna výzva
- Kybernetická vojna

Varianty útokov odmietnutia služby

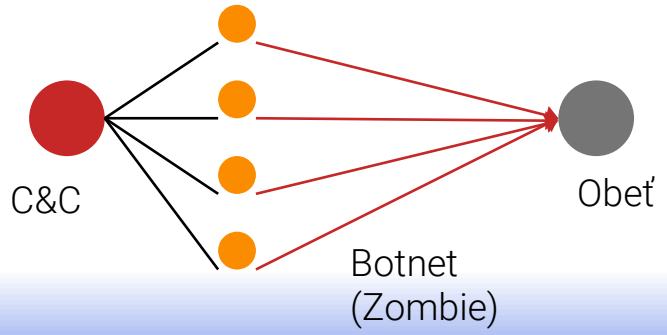
Klasifikácia:

- Veľkoobjemové – UDP a ICMP záplava, DNS a NTP amplifikácia
- Protokolové – SYN záplava
- Aplikačné – Slow Lorris, R-U Dead Yet, GET záplava



Techniky:

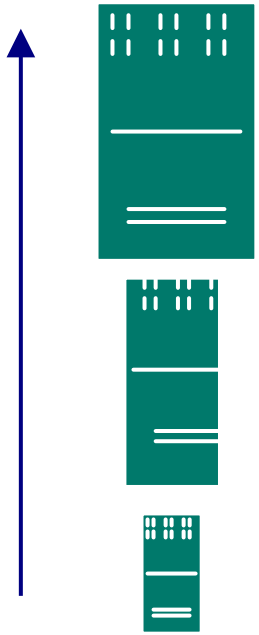
- IP Spoofing
- Command & Control pre Botnet



Škálovanie aplikácie

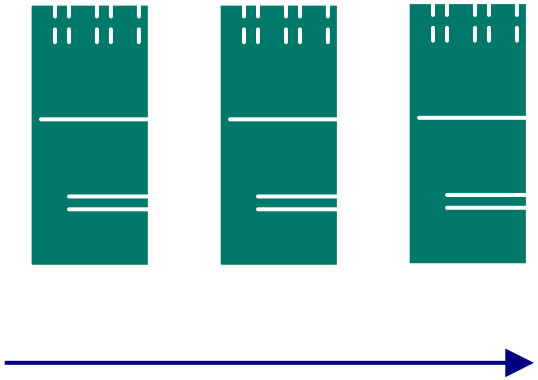
Vertikálne škálovanie

pridanie zdrojov (CPU, RAM)



Horizontálne škálovanie

zväčšovanie počtu inštancie



Vyvažovanie záťaže podľa vrstiev RM OSI

L7 – Vyvažovanie na HTTP reláciu
DNS A záznamy

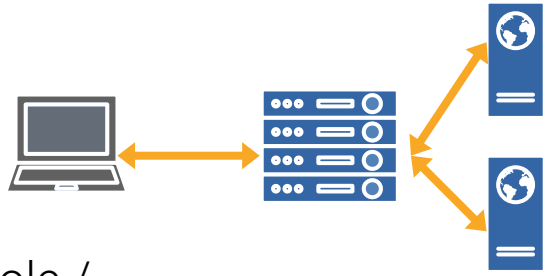
L4 – Vyvažovanie na TCP spojenie

L3 – Smerovanie a filtrovanie

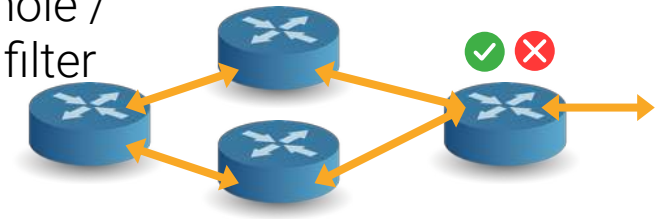
L2 – Agregácia liniek (Trunking)

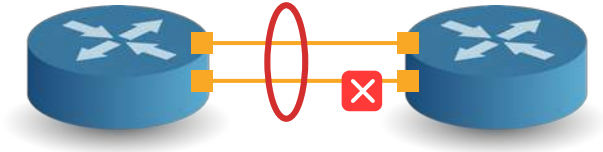
L1 - Obmedzenie šírkou pásma

Reverzná proxy



ECMP, Black hole /
Ingress / ACL filter

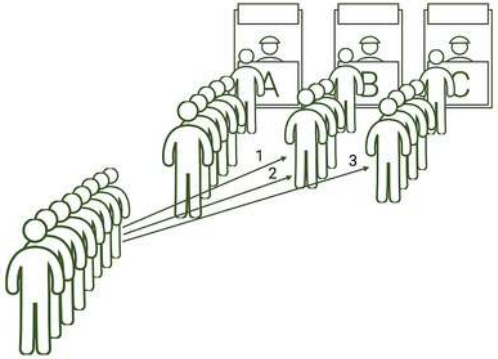


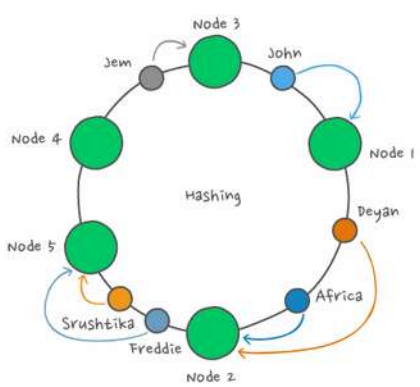


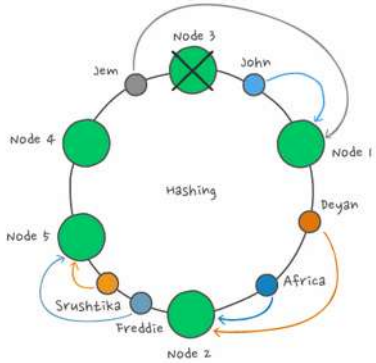
⇧ Rýchlosť komunikácie
⇧ Odolnosť proti zlyhaniam

Algoritmy pre load balancing

- Náhodný uzol
- Round robin
- Najmenej aktívnych spojení
- Najmenej času na vybavenie
- ** Váhované verzie predošlých*
- Konzistentné hašovanie
  podľa IP zdroja / URL cieľa







Softvérové riešenia vyvažovania záťaže

NGINX

```
upstream website {
    server web-one;
    server web-two;
}

server {
    listen 80;
    server_name localhost;

    location / {
        proxy_pass "http://website/";
    }
}
```

HAPROXY

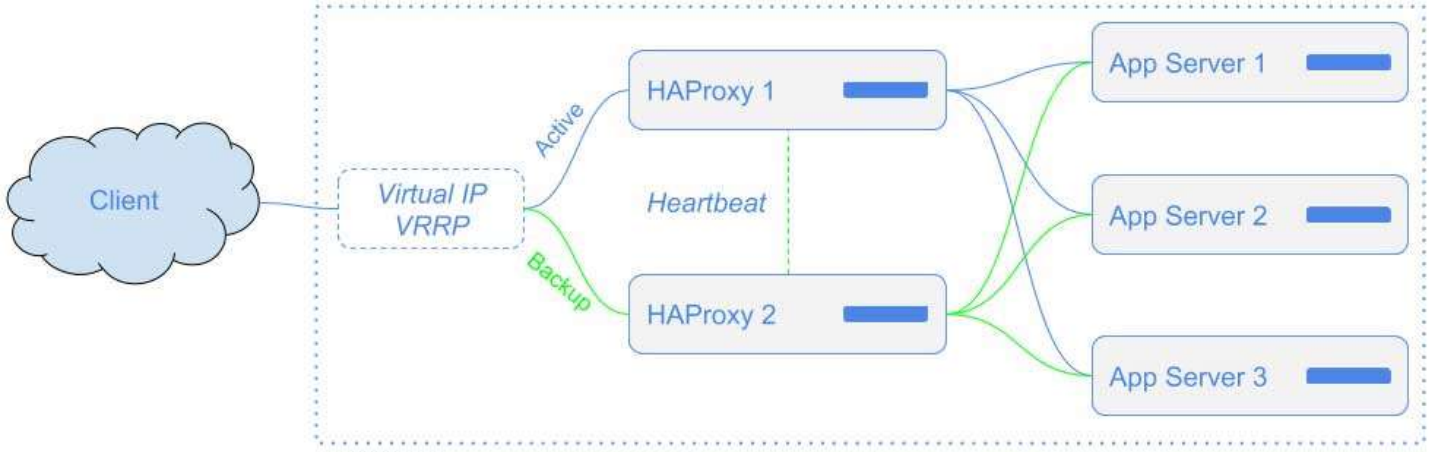
```
frontend http
    bind *:80
    timeout client 60s
    default_backend servers

backend servers
    balance source
    timeout connect 10s
    timeout server 100s
    server web-one web-one:80
    server web-two web-two:80
```

Zabezpečenie vysokej dostupnosti

Load balancer sa stáva **Single point of Failure** horizontálne škálovanej aplikácie

Virtuálna IP adresa pre klaster s Keepalived (Master/Backup)
Voľba primárneho uzla cez VRRP – odoslanie Gratuitous ARP



HTTP hlavičky webového servera

```
HTTP/1.1 200 OK
Server: Apache/2.4.43 (Debian)
X-Powered-By: PHP/7.3.27
Forwarded: for=192.0.2.60, by=203.0.113.43

Set-Cookie: PIBSESSION=7e730941e07bf4b02ca1ff4fabc2871f; path=/
Keep-Alive: timeout=5, max=100

Strict-Transport-Security: max-age=31536000
X-XSS-Protection: 1

Date: Thu, 04 Mar 2021 17:53:56 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 648
```

Odpoveď na HTTP požiadavku

- reaguje iba na GET, POST

Hlavičky prezrádzajúce použité technológie a internú infraštraktúru

Relácia

Hlavičky na zabezpečenie + TLS/SSL

Ostatné metadáta správy

Monitorovanie a metriky

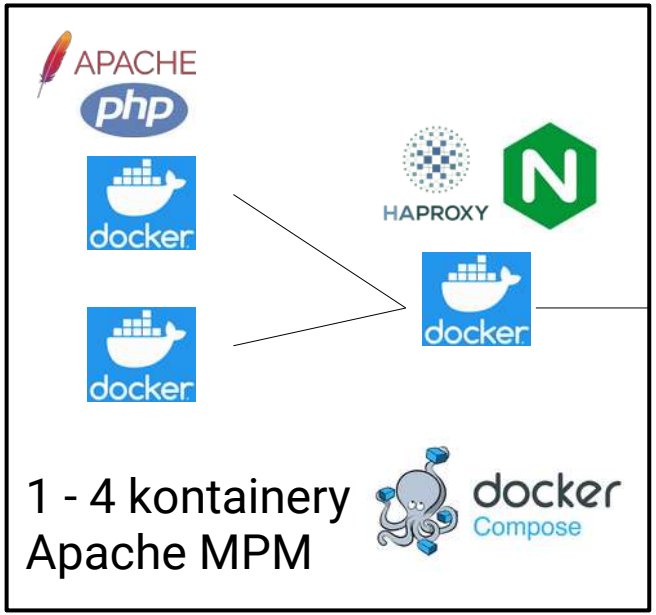
- Inbound / Outbound / Aggregate traffic (bytes)
- Počet a frekvencia spojení (počet, počet/s, s/spojenie)
- Session per IP (počet)
- Response latency (oneskorenie) a vhodné timeouts
- HTTP error rate (Kódy: 400, 500)
- Utilizácia CPU, RAM na load balancer / na server
- Koľko spojení spôsobí odmietnutie služby

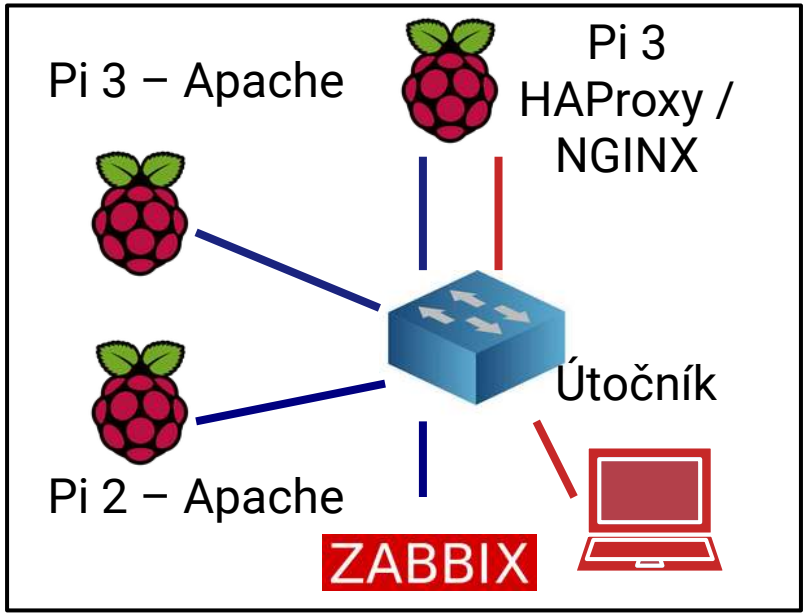
ZABBIX

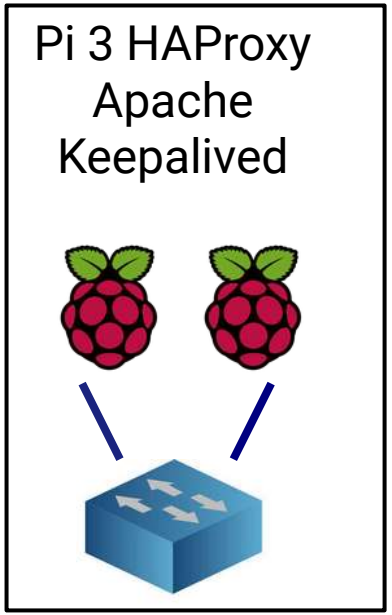
Common Log Format

```
84.245.120.177 - - [04/Mar/2021:18:55:50 +0000]
"GET /v1/health HTTP/1.1" 200 40 "-" "Mozilla/5.0  Firefox/86.0"
```

Experimentovanie so silou útokov







Nástroje: ab, t50, thc-ssl-dos, SlowHTTPTest, Ion Orbit Cannon
Vlastné viacvláknové skripty: UDP, SYN Flood, Slow Lorris

Zhrnutie

Otázky k témam?

- Útoky odmietnutia služby (DoS)
- Vysoká dostupnosť
  - Smerovanie a vyššia priepustnosť
  - Horizontálne škálovanie
- Vyvažovanie záťaže
  - Failover v klastroch
- Monitorovanie záťaže
- HTTP Server s webovou aplikáciou