AKO SME ODRAZILI ÚTOK

Peter Vilhan

Obsah prezentácie

- motivácia
- technologický rozmer
- vplyv tretích strán
- optimalizácia
- možnosti ochrany
- ako to funguje v praxi

Motivácia

Zabezpečenie kontinuity obchodných aktivít

- technologický rozmer
  - spoľahlivé dátové centrá
- vplyv tretích strán
  - dostupnosť služieb bez ohľadu na okolnosti

Technologický rozmer

Spoľahlivé dátové centrum

- redundancia napájania
- redundancia sieťových prvkov
- stabilné prostredie
- geograficky oddelené optické trasy
- zabezpečenie/kontrola prístupu do DC

Vplyv tretích strán

Blokovanie IP adresy/rozsahu

- cielené útoky
  - vyhľadávanie/zneužívanie zraniteľností
- DDoS
  - volumetrické utoky – zahltenie linky
  - sofistikované útoky L4...L7
  -

Možnosti detekcie anomálií

Priama detekcia

- monitoring pomocou Zabbix, Nagios
- analýza netflow dát

Nepriama detekcia

- analýza spotreby servera na PDU/IPMI
- meranie času/rýchlosti načítania stránky

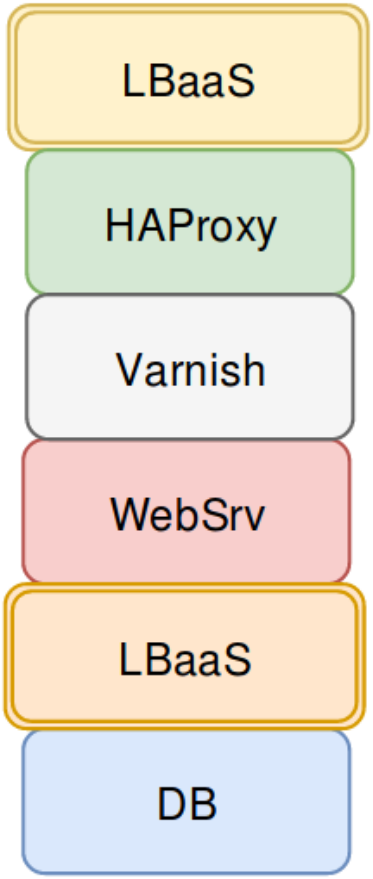
Optimalizácia

Úprava architektúry

- horizontálna škálovateľnosť
- vysoká dostupnosť

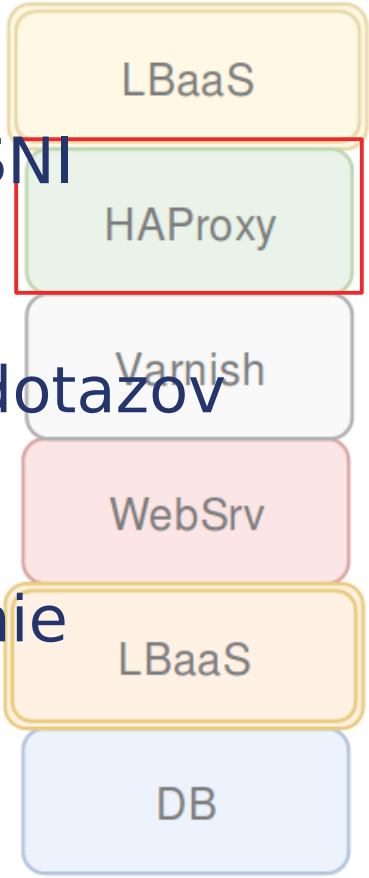
Optimalizácia nastavení

- Webserver
- DB server
- Varnish, Haproxy



HAproxy

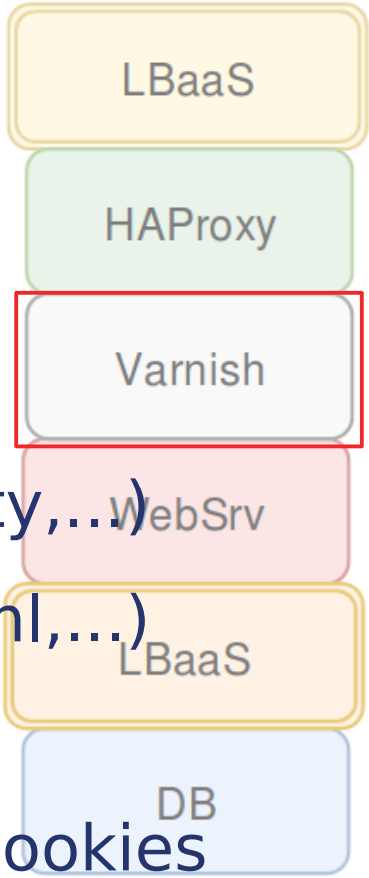
- Layer 4 /Layer 7 load balancer
- ukončuje TLS tunel, podporuje SNI
- podporuje health checks
- definovanie logiky smerovania dotazov
- HTTP rewrite, redirects
- umožňuje horizontálne škálovanie
- prioritizácia backend serverov
- poskytuje prehľadné štatistiky



unet
telecommunication solutions

Varnish cache

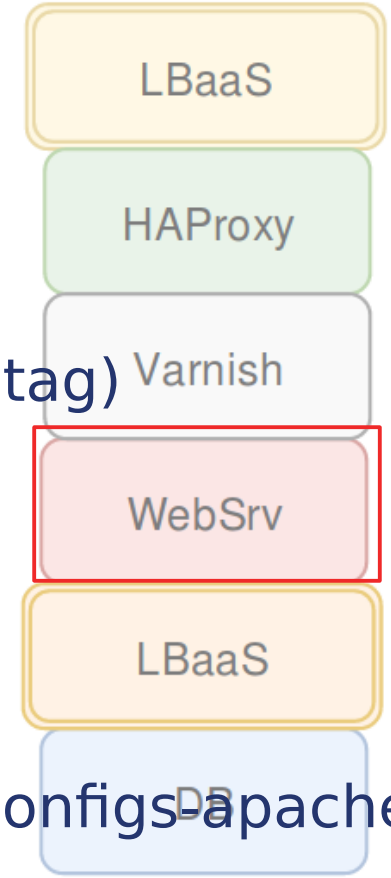
- cached content priamo z RAM!
- 300-1000x zrýchlenie
- saturuje sieťové rozhranie
- použiteľné pre:
  - statický obsah (jpeg,js,css,fonty,...)
  - pseudostatický obsah (html,xml,...)
  - TLS podporuje len Pro verzia
- rôzne TTL, BAN, manipulácia s cookies



Optimalizácia Apache

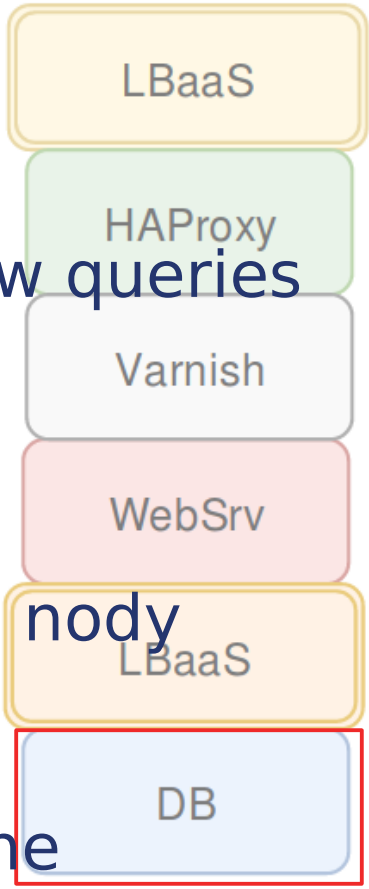
- Google PageSpeedTools
  - minimalizácia zdrojov
  - inline kompresia, inline css,
  - browser caching(Cache-control,Etag)
  - mod_pagespeed, mod_remoteip

- H5BP apache configs
  - https://github.com/h5bp/server-configs-apache



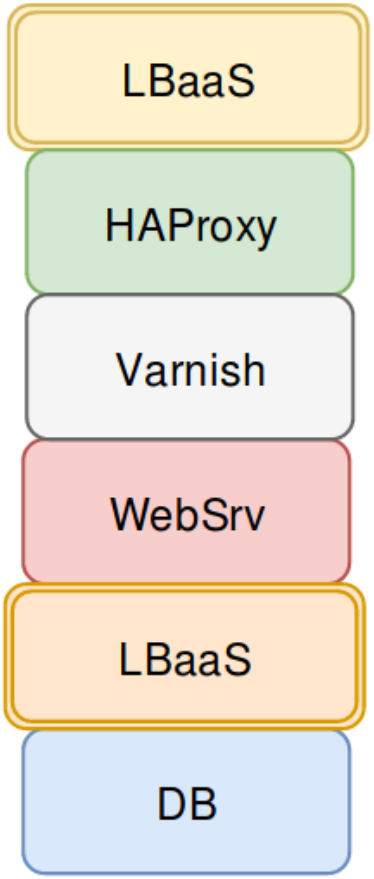
Optimalizácia SQL servera

- RAMdisk pre tmp tabuľky
- cache + buffers
- indexy, logovanie + analýza slow queries
- cluster aware DB design (PK)
- MySQLtuner
- Galera cluster for Mysql - min. 3 nody
- PostgreSQLtuner
- sysbench pre stanovenie baseline



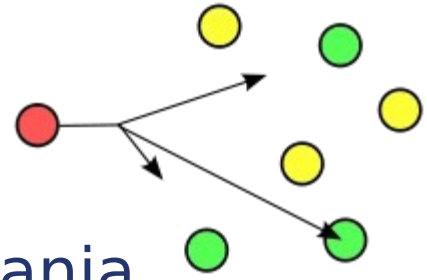
Benchmarking

- Apache benchmark
  - rps
  - requests time
- WebPageTest
  - waterfall view
  - prehľad optimalizácie
  - content breakdown



Možnosti ochrany

- ONE size fits ONE
- aplikačné útoky
  - slowloris
  - mod_security
  - request limiting
- IPv4+IPv6 Anycast
  - DC failover
  - definovanie logiky smerovania



Možnosti ochrany

- HW firewall cluster
  - komplexná fw ochrana L3-L7
  - IPS
  - VPN SSL/IPSEC
  - AntiSPAM/Antivirus
  - možnosť vlastnej správy
  - cenovo dostupné riešenie

Možnosti ochrany

- self-defending network infrastructure
  - analyzujeme komunikáciu na hraničných smerovačoch
  - non-stop profilovanie služieb v sieti
  - detekcia anomálií, per IP/rozsah
  - notifikácie v závislosti od incidentu
  - možnosť automatickej reakcie podľa preferencii (RTBH/scrubbing)

Reprezentácia netflow dát

Možnosti ochrany voči DDoS

- Ochrana voči DDoS
  - volumetrické útoky – scrubbing – hybridný
  - L7 útoky (presmerovanie, javascript, Captcha)
  - technológia Radware
  - reakčný čas cca 2 min.
  - možnosť definovať akcie podľa času (RTBH/scrubbing)

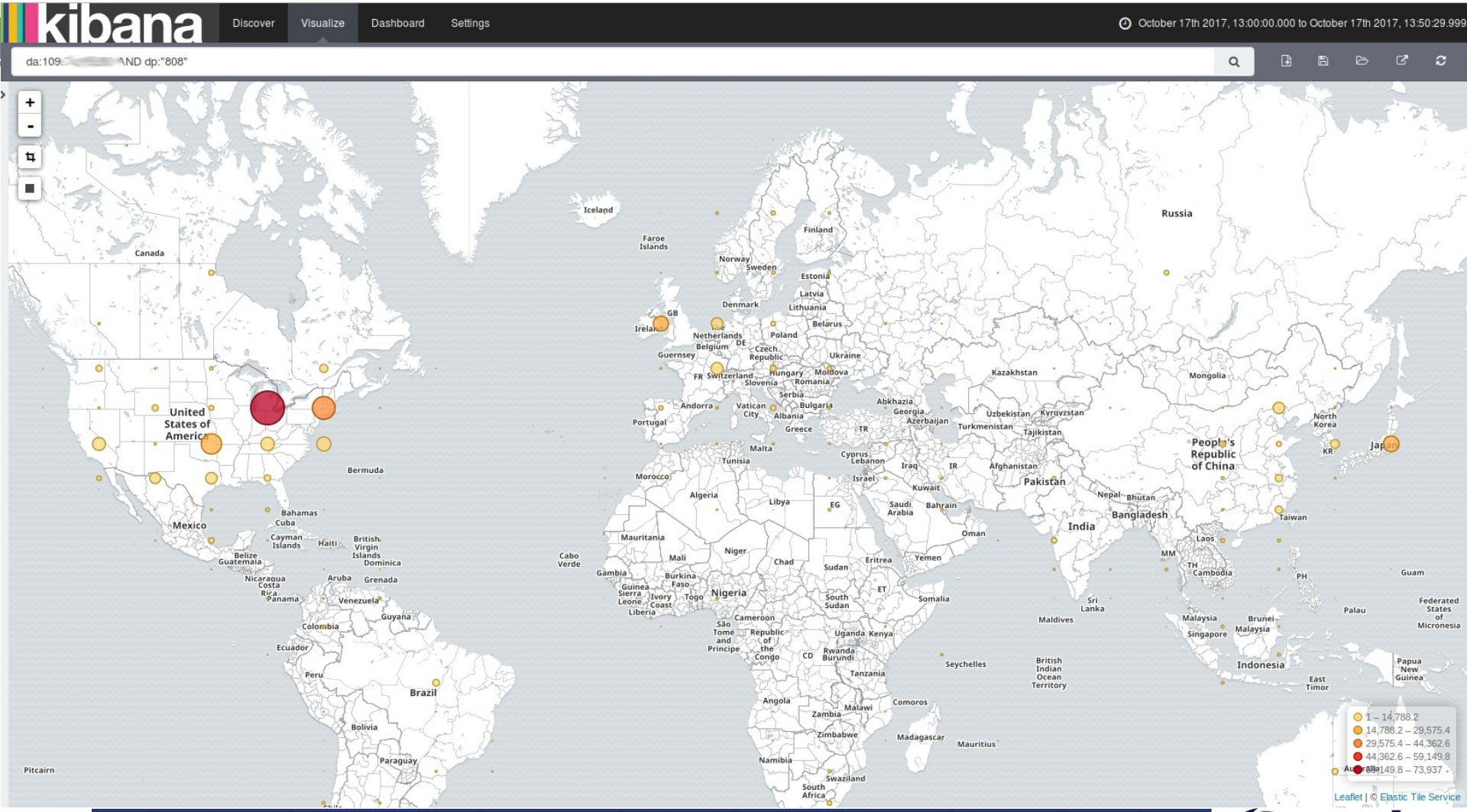
Možnosti ochrany voči DDoS

- útok v sile do 10 Gbps
  - v cene paušálneho poplatku
- útok v sile do 70 Gbps
  - nad rámec paušálneho poplatku
  - v závislosti od preferencií klienta (čas, región, sila vs. dĺžka trvania)
- útok v sile nad 300 Gbps
  - individuálna ponuka

Incident č.1

- cieľ
  - control plane smerovača
- BOTNET lokalizovaný najmä v USA
- sila DDoS útoku
  - 1 - 4 Gbps
- protokol TCP, dst. port 808

GEO distribúcia uzlov BOTNETu



unet
telecommunication solutions

Protiopatrenia

1) obnovenie dostupnosti in-band mng.
   - aktivácia Remote Triggered Black Hole (RTBH)
2) rekonfigurácia zariadenia a presmerovanie dát do scrubbing centra
3) nedostupnosť menej ako 5 minút

Incident č.2

- E-shop, nad CMS Drupal
- 400 online klientov
- Apache 2.4 + PHP 5.6 + Mysql 5.5
- 32GB RAM, 2xE5-2640 v3, 240GB SSD, 2x1gbps
- QPS 2k, QcacheHit 69%, BpsOut 60MB/s
- CPU Load > 60, CPU user 97%,sys 3%, Outgoing traffic < 8Mbps.
- Apache avg.82 workers sending reply

Protiopatrenia - Varnish

- analýza IS nad CMS
  - ext.systémy, IPN z platobných brán
- nasadenie varnish
  - ttl 10min pre html, xml – BAN,sklad
  - ttl 30m js,css,..
  - ttl 4h pre obrázky
  - backend: apache2 bez TLS

unet
telecommunication solutions

Protiopatrenia - HAProxy

- definovanie pravidiel
  - ktoré URL obsluhovať priamo z Apache
  - detekcia prihlásenia používateľa
  - health checks, redirects
- backendy: varnish, apache2 (80,443)
- X-Forwarded-For
- X-Forwarded-Proto

unet
telecommunication solutions

Protiopatrenia – Apache2

- optimalizácia
  - expiry, compresia
- reconfig virtual hostov – int. iface
- varnish<->apache len cez http!
  - mixed contend?!
    - SetEnvIf X-Forwarded-Proto https HTTPS=on
- awstats - mod_remote_ip

Záver

- odolnosť systému je definovaná hodnotou najslabšieho článku reťazca
- potreba dizajnovania škálovateľných aplikácií – idú vianoce
- VNET Cloud - vysoká flexibilita
- DDoS ochrana
- cacheovanie obsahu

vnet
telecommunication solutions

Ďakujem za pozornosť