DDoS a IDS/IPS ochrana u WEDOS

Josef Grill
WEDOS Internet, a.s.
http://www.wedos.cz
http://datacentrum.wedos.com
21. 6. 2017

Datacentrum WEDOS Hluboká nad Vltavou a již brzo Datacentrum WEDOS 2
Držitel certifikátů **ISO 9001** a **ISO 14001** a **ISO 27001** od TÜV SÜD

WEDOS

WEDOS není WeDDoS

Podle některých komentářů to nevypadá, ale

WEDOS je skutečně zkratka

WEbhosting, **DO**mény, **S**ervery

a nemá to nic společného s DDoS

- Dnes žádný marketing, ale reálné zkušenosti :-)

Jak to začalo s DDoS u WEDOS

- Průběžně malé útoky, v létě 2014 začaly být silnější (desítky Gbps)
- Většinou řešeno ručně nebo poloautomaticky pomocí iptables na serverech nebo routerech (routovali jsme přes Linux)
- Úspěchy přinášejí DDoS útoky?
- Problémy s dodavateli
- Nutnost okamžitě řešit, ale jak ...

Slepé uličky

- Půjčili jsme si „krabičky“ a výsledek?
- Možnost rychlého nasazení, ale …
- Cena a neuvěřitelné licenční poplatky (navíc celé x 2)
- Nulová svoboda
- **Nevěřte PR materiálům dodavatelů**
- Co si nezměříme, tomu nevěříme ...

WEDOS – vždy vlastní cestou…

WEDOS

Operace kulový blesk

- Souběžně s testováním jsme vyvíjeli svoje řešení na Linuxu
- Důvěra a nedůvěra, změna myšlení je složitá...
- Jednoho krásného podvečera přišla operace „kulový blesk“ a vytrhl jsem kabel (bez ohledu na vůli techniků)
- **A ono to fungovalo...**

WEDOS

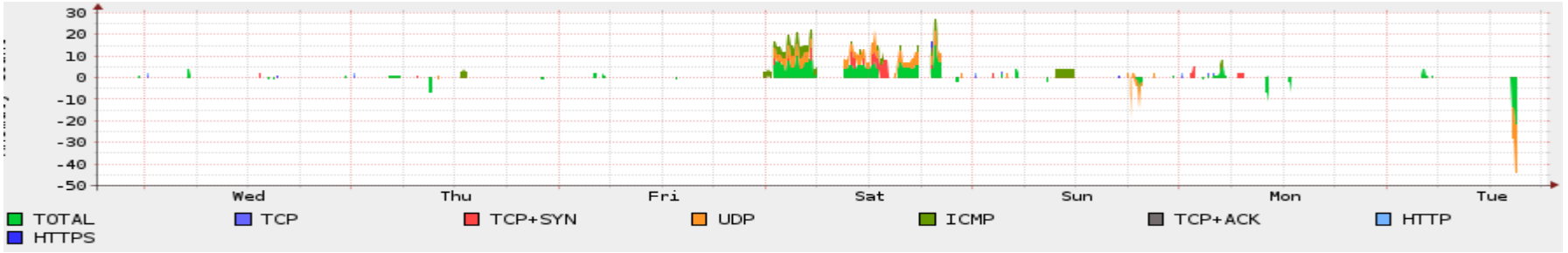
Jak to celé máme?

- Základ je Linux a 11 silných strojů a různé úpravy v routování a nastavení switchů (filtry + mirroring provozu + sflow)
- 1 server řídí (+ 1 backup), 3 servery jako **sondy** (celkem měříme 13 míst – část online a část přes sflow), 6 serverů (1 online a 5 jako „výhybky“) sloužících jako **filtry** (každý má jiné funkce), plus filtrace na routerech a switchích
- **Vše vyhodnocujeme v reálném čase**
- Pravidla a změny v routingu do 1,3 s
- Spočítáme 30 Gbps a 7,5 Mpps (důležité pro filtraci)
- Odfiltrujeme více (záměrně neříkám kolik) + BH v BGP

Jak to funguje?

- Online měření (vysoce náročné na výkon => hodně úprav Linuxu) a porovnávání s pevně nastavenými hodnotami (pro jednotlivé IP) nebo s běžným provozem (pro danou IP) – bps a pps
- Pokud je něco mimořádného, tak se aktivují změny v routingu a filtry (každý má jinou funkci)
- Co do provozu nepatří se filtruje a zbytek se vrátí zpět (nezdržujeme ostatní provoz)
- TCP/IP, TCP, UDP, TCP+SYN, SYN+ACK, ICMP, HTTP, HTTPS + lze TCP-NULL, TCP-RST, TCP-NULL
- Nové útoky musíme systém vždy naučit
- Filtrujeme i odchozí provoz a „neprovokujeme“ tak jinde

Výsledky po 31 měsících



Kam se útočí?

- Dříve na WEDOS.cz
- Postupně na VPS (různé TOR servery)
- Nyní převládá webhosting (velké množství webů – přes 130.000 aktivních webů)

Zajímavosti

- Chytré automaty na útoky
- Cca 21% byly útoky od nás

Rekordy:

- Přes 375.000 útoků
- Průměrně 387 za den
- Přes 71,3 Gbps
- Přes 7 Mpps
- 37 hodin

WEDOS

IPv6 a DDoS

Od propagátora IPv6 k velmi chladnému přístupu

- DDoS útok loni v srpnu na VPS, zvenku (sever-jih), zevnitř (východ-západ)
- U WEDOS máme přidělený rozsah sítě pro IPv6 /32, což je neuvěřitelných 4 294 967 296 podsítí /64, příčemž každá z podsítí /64 má 18 446 744 073 709 551 616 IPv6. Výsledkem je tedy to, že WEDOS má přiděleno $7{,}922816251 \times 10^{28}$ IPv6 adres a všechny k WEDOS směřovaly a teoreticky na jakoukoliv z nich mohl vést útok. Pro takový počet IP adres není v silách žádné technologie počítat pakety proti těmto IP adresám a chránit je před DDoS útoky.
- Srovnejme to s IPv4, kde máme k dispozici 10 240 IPv4 adres.
- Jistě chápete, že je rozdíl na jedné straně chránit $7{,}922816251 \times 10^{28}$ nebo 10 240 IP adres a zároveň to chráníte U IPv6 máte $3{,}4 \times 10^{38}$ potencionálních útočníků a u IPv4 jich máte pouhé cca 4 miliardy (2^{32} adres (cca $4 \times 10^{9} = 4$ rozdíly. Velké rozdíly.
- Root VPS jsou zdrojem problémů, útoky uvnitř sítě

  a tak omezení root věcí ohledně sítového provozu
- IPv4 za peníze versus následně zdarma
- Omezení IPv6 na pouze zaregistrované

Napadené weby a co s tím?

Webhostingy

- Přes 130.000 aktivních webů, většina na opensource CMS = možné problémy
- Přetížené servery versus nudící se servery
- Denně až desítky napadených webů versus jednotky za měsíc
- Moc práce a hodně klientů, kteří to nechtěli pochopit

Co s tím?

- IDS/IPS ochrana
- IDS – detekce problémů a průniků
- IPS – reálná ochrana před průniky

IDS a IPS neboli IDS/IPS

IDS - Intrusion Detection System

- Monitoring sítě a hledání podezřelého provozu

IPS - Intrusion Prevention System = ochrana před:

- Přirozeně vypadajícími DoS, které naše DDoS ochrana nemůže detekovat (například zneužití XML-RPC).
- SQLi útoky
- Brute force útoky na přihlašovací formuláře.
- Roboty, kteří schválně přetěžují vaše stránky
- Roboty, kteří vkládají do komentářů škodlivý kód (XSS)
- Viry v emailech a i běžném HTML (FTP) provozu
- Zranitelnostmi ve známých open source CMS a eshopech
- Útoky zneužívající zero-day exploit (známé i potenciální)
- Různým skenováním aplikací

(Opět) Slepé uličky u IDS/IPS

Sliby

- Filtrace až 60 Gbps provozu
- Při DDoS útoku nespadne
- Možnost vlastních pravidel
- Rychlé zpracování
- IPv6 není problém

Realita

- **Maximálně 2 Gbps**
- Spadlo téměř při každém útoku
- Pravidla nemají logiku
- Zpracování pomalé
- IPv6 se učili „na nás“

Opět řešení v linuxu - opensource

Suricata

Open Source IDS / IPS / NSM engine

- Vysoký výkon a stabilita
- 9 měsíců příprav a testů (nejprve jako IDS)
- PF_RING (stejně jako u DDoS) a AF_PACKET a INTEL síťovky

Testovali jsme i další

- Distribuce IDS/IPS založené na Suricatě
- Snort, různé placené verze
- Výsledek je čistá Suricata + Evebox + Logstash + Elasticsearch
- 384 GB RAM a 40 vláken CPU
- 300 GB logů/den
  (logujeme 1 útok za 300 sec)

WEDOS

Co zvládne IDS/IPS Suricata u WEDOS

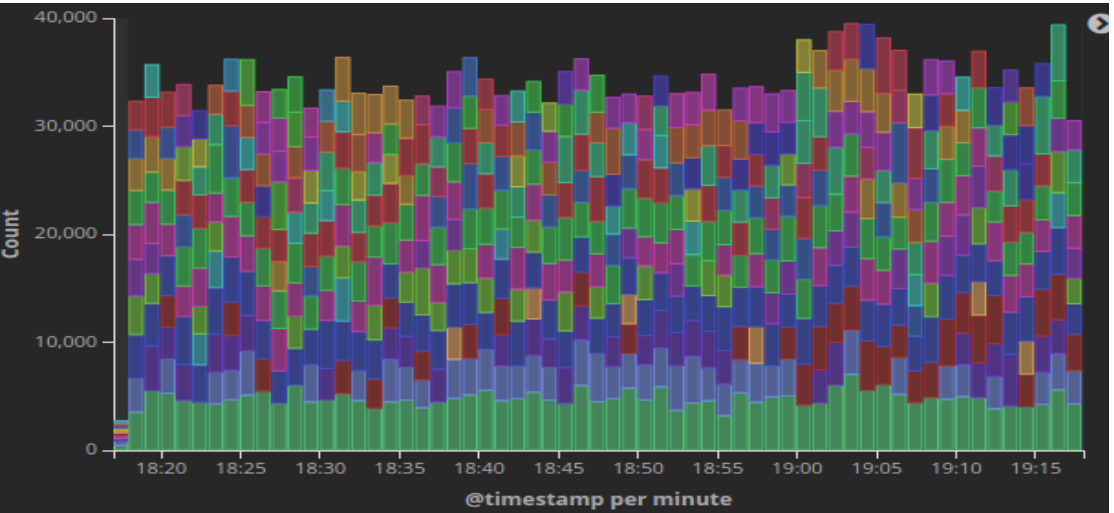
- přes 37.000 útoků na prolomení hesla ve WordPressu, přes 10 pokusů za sekundu

- zhruba stejný počet pokusů byl o prolomení dalších hesel (maily nebo jiné redakční systémy)

- průměrně přes 1.000.000 různých bezpečnostních problémů, což je přes 279 pokusů za sekundu

- z toho přes 183.000 mělo kritickou úroveň, tj. nešlo o varování nebo nízkou úroveň, což je cca 51 pokusů za sekundu, které jsou nebezpečné pro klienty

- ze zhruba 100 IP rozsahů z celého světa přicházelo cca 73% závadného provozu



IDS a IPS

- Monitoring a statistiky
- Zablokovat 40% provozu, který nikomu nechybí
- Chrání weby před známými hrozbami
- Používá přes 21.500 pra
- Hodinové aktualizace
- Chytrá pravidla
- Skutečně online
- Zpoždění 3-7 ms

WEDOS

Co chceme ještě nabídnout?

Individuální řešení

- Filtrace dle zemí a regionů (zdroj/cíl) a ASN
- Filtrace dle protokolů
- Whitelist a blacklist
- Individuální pravidla u IDS/IPS
- IDS/IPS u VPS a Cloudu
- Filtrace na zakázku pro třetí strany

Individuální statistiky

- DDoS útoků
- z IDS/IPS

WEDOS

Co řešíme u DDoS a IDS/IPS ochran

DDoS

- Nové hrozby
- Navyšování výkonu dle potřeby (včetně možné virtualizace)
- Chytré řešení
- Nesourodost HW (to u nás není zvykem a bojujeme s tím)
- Jak to řešit pro 2 budovy

IDS/IPS

- Distribuované řešení versus cluster
- HTTPS a SSL
- Jak to řešit pro 2 budovy

WEDOS

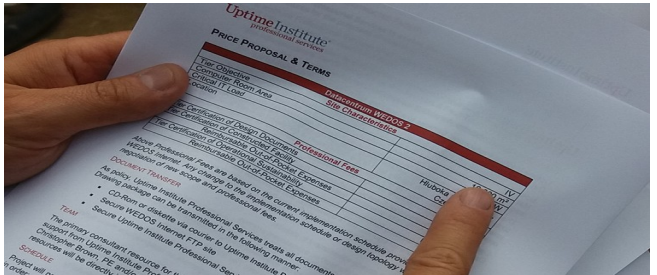
Je reálné filtrovat 100 Gbps?

Věříme, že ano ...

- 2 datacentra již letos
- 3x100 Gbps na Hluboké již letos
- Filtrace přímo na Hluboké
- Chceme testovat filtraci spolu s CESNET, z.s.p.o.

Síť na 100 Gbps

- Roky řešíme návrh
- Testujeme HW
- Letos spustíme – navenek 1 budova, služby s vysokou dostupností ve 2 datacentrech
- Živé migrace
- Řešíme TIER IV (podepsána smlouva s Uptime Institute)



WEDOS

Děkuji za pozornost

Dotazy: datacentrum@wedos.com

Nevěříte? Chcete se přesvědčit na vlastní oči?Přijeďte!

Detaily na:

https://datacentrum.wedos.com

http://dc.wedos.cz/

Chcete se podílet na projektu?
Ozvěte se!