Merre tovább, Linux tűzfalak?

Kadlecsik József
MTA Wigner Fizikai Kutatóközpont
kadlecsik.jozsef@wigner.mta.hu

Networkshop 2018, Eger

Tartalom

- Netfilter és conntrack
- Csomagszűrő tűzfal alternatívák
  - Iptables
  - Iptables + ipset
  - Nftables
  - Bpfilter
- Politika
- Jövő?

netfilter

- A tűzfal keretrendszer a Linux kernelben
  - Jól definiált pontok (hooks) a network stackben
  - Callback függvény(ek) prioritással regisztrálhatók ezekhez a pontokhoz
- Minimális igények: néhány kódsor!

Connection tracking

- A csomagok kapcsolatokhoz rendelése
- Egyszerű állapottér
- Kapcsolat-nyilvántartás (conntrack table)
  - Memória
  - Több CPU használata (locking)
  - NAT
- „Drága”

iptables

- Netfilterrel együtt született (1998)
  - iptables, ip6tables, arptables, ebtables
  - Táblák, láncok, szabályok
  - Több egyezési feltétel, egy target
  - Nem elhagyható egyezések: protokoll, forrás és cél cím, input és output interfész **neve**
- Rendkívül nagy számú kiterjesztés (match, target)

iptables problémák

- Bináris „protokoll” a user-kernel kommunikációban
- Egy tábla egy bináris blob a kernelben
  - Egy-egy szabály módosítása költséges (iptables-restore)
  - Konkurrens szabály-módosítás
  - Nincs backup tábla (iptables-apply)
- Egy target
- Lineáris feldolgozás
- Nem kikapcsolható counterek (per-CPU/match)

iptables + ipset

- Iptables
  - Statikus szabályok
  - Egyszerű szabály „módosítás”
  - Nemlineáris feldolgozás
- Ipset
  - Netlink interfész

nftables

- Programozási nyelv
- Táblák, láncok teljesen konfigurálhatók
- Nincs „match”, „target” szétválasztás
- Nincs beépített csomag/byte számláló
- Dinamikus szabály-módosítás
  - Láncolt listák a kernelben
- Generikus „set” és „map” támogatás
- Netlink interfész

Migráció nftables-re

- Szabály-transzláció iptables-ről nftables-re:
  - iptables-translate, iptables-restore-translate
- Iptables szintaxis használata nftables-el:
  - iptables-compat, iptables-compat-restore
- Ipset: nftables natív set
- Firewall tools (fail2ban, firewalld, stb)

- Még nem minden match, set típus támogatott
- Nyelv nem annyira olvasható

Debian migrációs tervek

- Most
  - nftables teljesen támogatott és ajánlott iptables helyett
- Következő release (opt-in)
  - Iptables-compat iptables helyett
- Következő utáni release (opt-in)
  - Csak nftables

bpfilter

- 2018 február, Daniel Borkmann: RFC
  - Iptables (ABI) kompatibilis interfész
  - XDP (express data path): network interfész driver futtatja

- BPF: Berkeley Packet Filter, Steven McCanne, Van Jacobson, 1993
  - Már használtátok :-)

BPF a Linuxnál

- Virtuális gép a kernelben
  - Interpreter
  - JIT
  - Maps
- Mire használják
  - Networking: socket filters (openswitch), tc
  - Tracing: kprobe (dtrace), syscalls analízis
  - In-kernel optimalizálás: TCP stack
  - Live kernel debugging

Bpfilter kérdések

- Miért iptables ABI?
- Hogyan kompatibilis?
  - Négy dekóder?
  - ~100 match/target?
- Mi van a komplex esetekkel?
- Mi van az iptables hibáival?

Politika

- Patrick McHardy írta az nftables-t…
  - Copyright perek Németországban: komoly összegek!
  - 2016: felfüggesztettük a coreteam tagságát, majd kizártuk
  - Legutóbbi perben visszalépett

Jövő?

- Iptables (+ipset) sokáig lesz még
- Nftables (lassan) terjedni fog
- Bpfilter ?

- Mi lenne jó: nftables + bpfilter
- Június: netfilter workshop