OpenBSD hálózat és NAT64

Répás Sándor

2014.11.27.

Bemutatkozás

Hálózatok biztonsága

Hálózati beállítások

- /etc/hostname.* állományok
- A * helyén a hálózati kártya típus (driver) azonosító
- Tartalmazza az adott kártya/interfész IPv4 és IPv6 címét, valamint a szükséges routing bejegyzést is
- Pl:
  - inet 10.1.1.1 255.255.255.0
  - inet6 alias 2001:738:2c01:8001::1 64
  - !route add -inet6 default 2001:738:2c01:8000::99
- Hol van ez a Linuxban, és hogyan néz ki?

Debian Linuxon

- /etc/network/interfaces

  iface eth0 inet static
  address 10.1.1.1
  netmask 255.255.255.0
  iface eth0 inet6 static
  address 2001:738:2c01:8001::1
  netmask 64
  gateway 2001:738:2c01:8000::99

- Több interfész?

Hálózat újrakonfigurálása

Debian

/etc/init.d/networking restart

OpenBSD

sh /etc/netstart

Routing/forwarding engedélyezése

Debian

/etc/sysctl.conf állományban

net.ipv4.ip_forward=1

net.ipv6.conf.all.forwarding=1

Parancssorból

sysctl net.ipv4.ip_forward=1

sysctl net.ipv6.conf.all.forwarding=1

OpenBSD

/etc/sysctl.conf álományban

net.inet.ip.forwarding=1

net.inet6.ip6.forwarding=1

Parancssorból

sysctl net.inet.ip.forwarding=1

sysctl net.inet6.ip6.forwarding=1

Névfeloldás és interfészek

- Mint Debian Linuxon
- Tehát?

Packet Filter

- OpenBSD csomagszűrő és NAT eszköze
- Különböző verziói megtalálhatóak a NetBSD és FreeBSD rendszerekben is
- Képes stateful és stateless működésre is

Konfigurálás

- /etc/pf.conf állományban
- Konfiguráció beolvasása

  pfctl -f /etc/pf.conf
- Konfiguráció szintaxisának ellenőrzése

  pfctl -nf /etc/pf.conf
- PF letiltása/engedélyezése

  pfctl -d/pfctl -e
- Permanens PF letiltása/engedélyezése

  /etc/rc.conf-ban: pf=NO/YES

Konfigurálás

- Aktuális szabályok kiíratása

  pfctl -sr
- Állapottábla kiíratása

  pfctl -ss
- Filter statisztikák és számlálók kiíratása

  pfctl -si
- Maximum értékek kiíratása

  pfctl -sm

/etc/pf.conf öt része

- Macros: Felhasználó által megadott változók. Pl: IP cím, interfész név
- Tables: IP címeket tartalmazó struktúra
- Options: PF működését befolyásoló beállítások
- Queueing: Sávszélesség korlátozás és prioritizálás
- Filter Rules: Csomagokra szűrés, NAT (Ez kell nekünk.)

Példák

- Macro:

block out on fxp0 from { 192.168.0.1, 10.5.32.6 } to any

- Table:

table <goodguys> { 192.0.2.0/24 }

pass in on fxp0 from <goodguys> to any

- Options:

set limit states 40000

Filter rule szintaxis

action [direction] [log] [quick] [on interface] [af] \
[proto protocol] [from src_addr [port src_port]] \
[to dst_addr [port dst_port]] [flags tcp_flags] [state]

Filter rule példák

pass in on sk0

block in on sk1 from 192.168.0.1

pass in on sk1 proto udp from any to any no state

pass out on sk1 from sk0 to any nat-to sk1

DNS64

- A DNS szolgáltatás kiterjesztése.
- Ha a kért névhez tartozik IPv6-os cím, azaz AAAA rekord, normál működés történik.
- Ha a kért névhez csak IPv4-es cím, azaz csak A rekord van, akkor szintetizál egy AAAA rekordot, melynek utolsó 32 bitje az IPv4-es cím, majd válaszként ezt a szintetizált címet adja vissza. Ez az IPv4-embedded IPv6 cím.

NAT64

- Ha egy IPv6-os kliens egy IPv4-es kiszolgálót szeretne elérni, akkor a kiszolgálót a DNS64-től kapott IPv4-embedded IPv6 címmel címzi meg.
- A routing az IPv4-embedded IPv6 címre küldött csomagokat a NAT64 gateway felé irányítja.
- A NAT64 gateway végzi az IPv6 és IPv4 protokollok közti átalakítást.

DNS64+NAT64

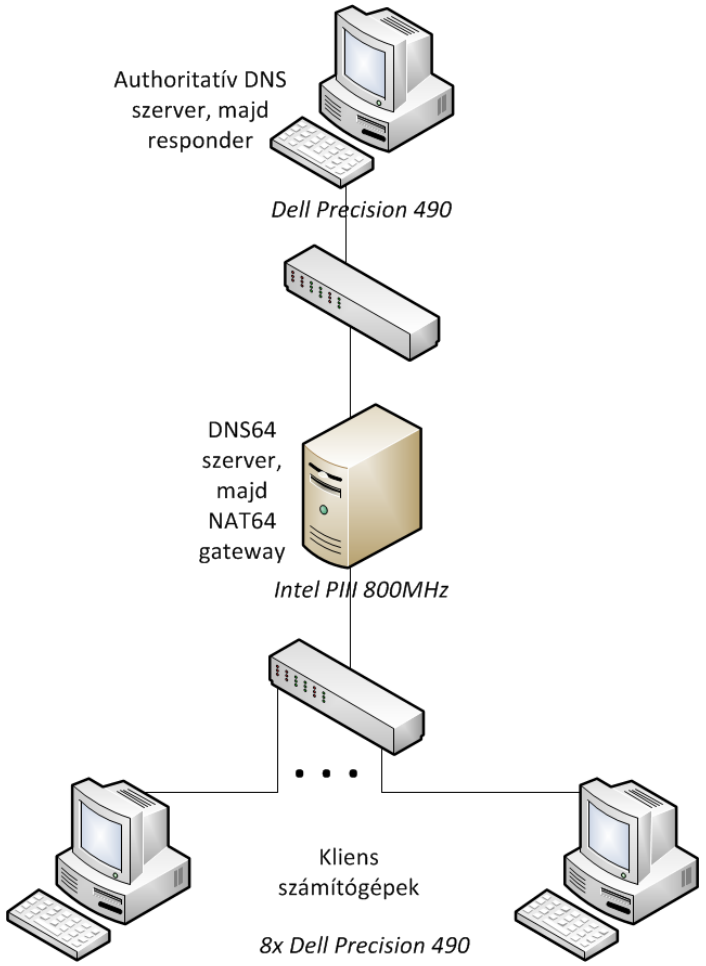
- A két szolgáltatás együttes alkalmazásával megoldható, hogy a csak IPv6-os IP címmel rendelkező kliens elérhesse a csak IPv4-es címmel rendelkező szervert.
- IPv4-es címet a szolgáltatók a viszonylag kevés új szervernek még tudnak biztosítani, azonban a sok új kliensnek már csak IPv6-os címet képesek allokálni.
- A meglévő szervereknek csak kis része érhető el IPv6 protokollal is.
- Így a DNS64/NAT64 ideális megoldás lehet az IPv6 bevezetésének jelenlegi szakaszában.

Miért érdemes OpenBSD-vel foglalkozni?

- Lényegesen gyorsabban továbbítja NAT64 segítségével a csomagokat, mint a Linux alapú TAYGA
- Lényegesen több csomagot továbbít nála

Mérési topológia

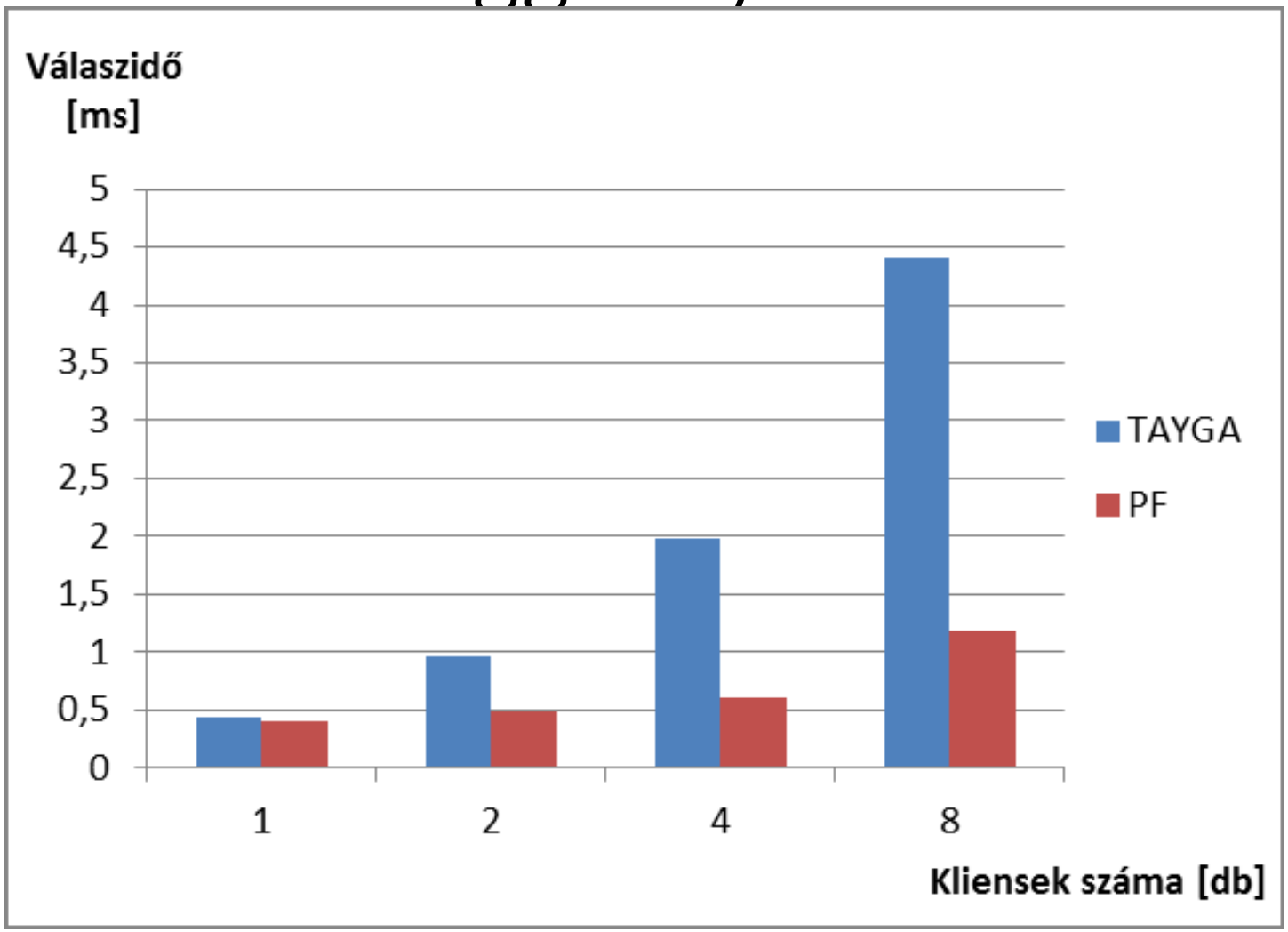
- Vizsgált eszközök:
  - DNS64 szerver és NAT64 gateway implementációk
  - egy kis teljesítményű számítógépen futtatva
- További eszközök:
  - 8+1 darab nagyteljesítményű Dell Precision munkaállomás
  - 2 darab 1000BASE-TX switch



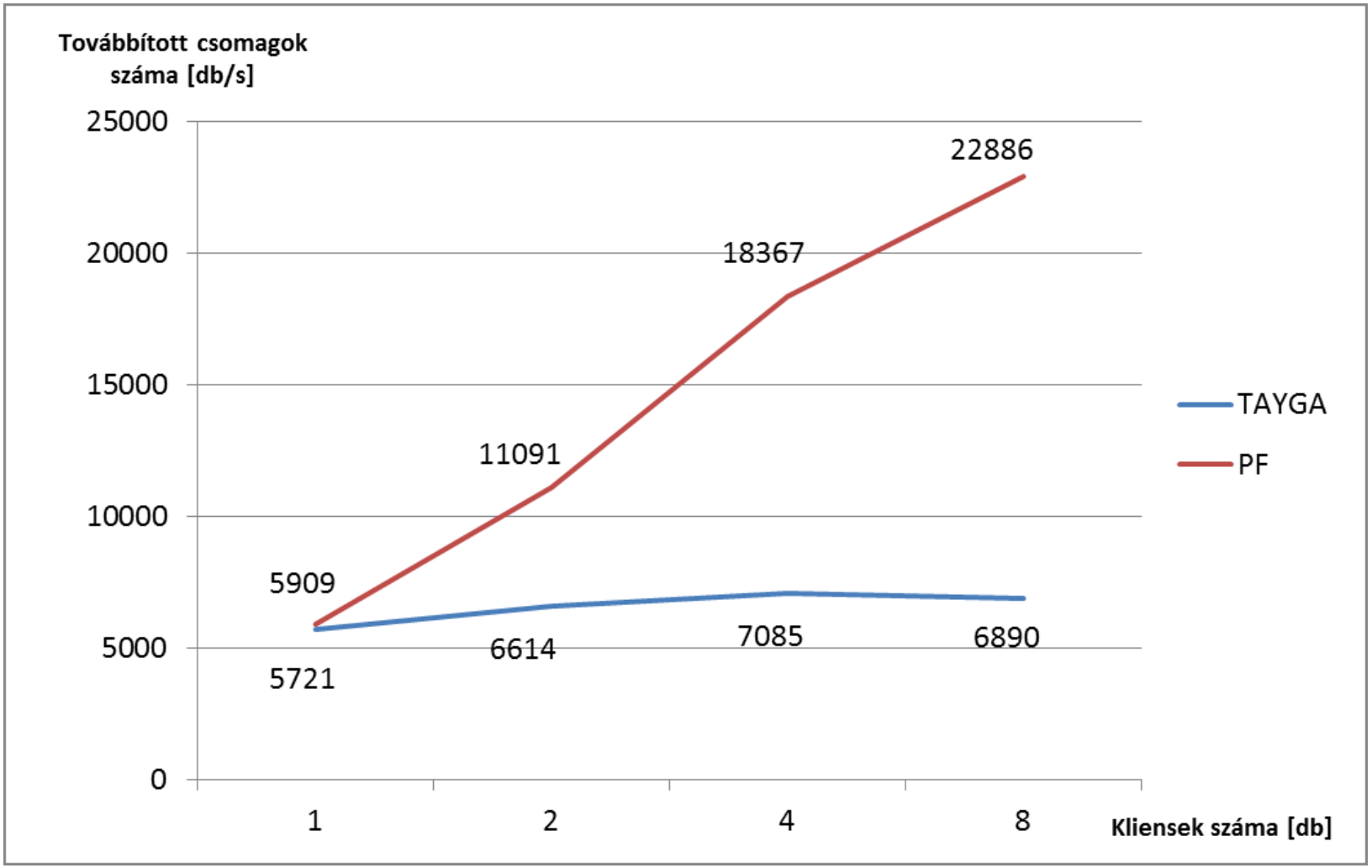
Mérés menete

- Előző ábra hálózati topológiája.
- Erre a célra készült scriptek segítségével történt.
- Minden mérési sorozat 1, 2, 4 és 8 klienssel került kivitelezésre, a terhelés mértékének megbízható beállításához.

Válaszidő [ms] a kliensek számának függvényében



Másodpercenként továbbított csomagok száma a kliensek számának függvényében



OpenBSD PF NAT64

- Az OpenBSD PF támogatja a NAT64-et „address family translation” néven
- Beállítása a /etc/pf.conf-ban:

```
pass in on sk1 inet6 from any to \
2001:738:2c01:8001:ffff:ffff::/96 af-to inet from \
193.225.151.75
```

Kérdések

repas.sandor@sze.hu