IPv6 Biztonság: Ipv6 tűzfalak tesztelése és vizsgálata

Mohácsi János

Networkshop 2005

Mohácsi János, NIIF Iroda

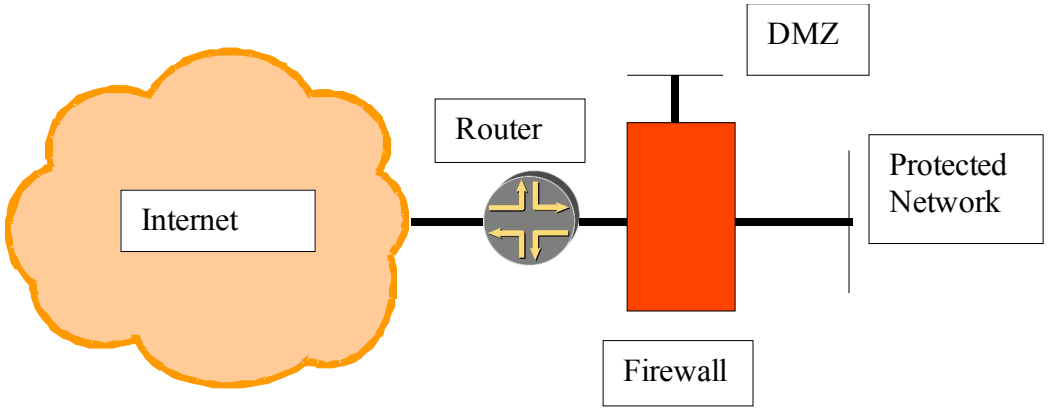
Tartalom

- Bevezetés
- IPv6 tűzfal követelmény analízis
- IPv6 tűzfal architektúra
- IPv6 tűzfalak alkalmazás támogatása
- IPv6 tűzfalak áttekintése
- Jövő

IPv6 Tűzfalak

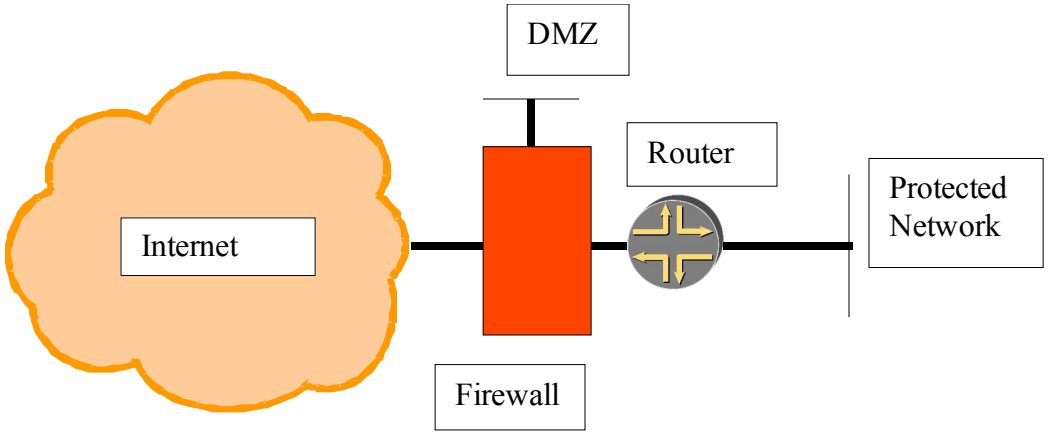
- IPv6:
  - IPv6 valóban biztonságosabb vagy ez csak vágyálom
- IPv6 tűzfal követelmények
  - Nincs szükség NAT-ra
    - Hálózat szekenelés gyakorlatilag lehetséges (/64)
    - A csomagszűrés gyengesége nem lehet NAT-al elfedni – egyre több szolgáltatás igényel publikus címet
  - Kiegészítő IPv6 fejlécek támogatása
  - IPv4/IPv6 együttmüködési megoldások támogatása
  - IPv4 biztonság megtartása

IPv6 tűzfal - metodus1



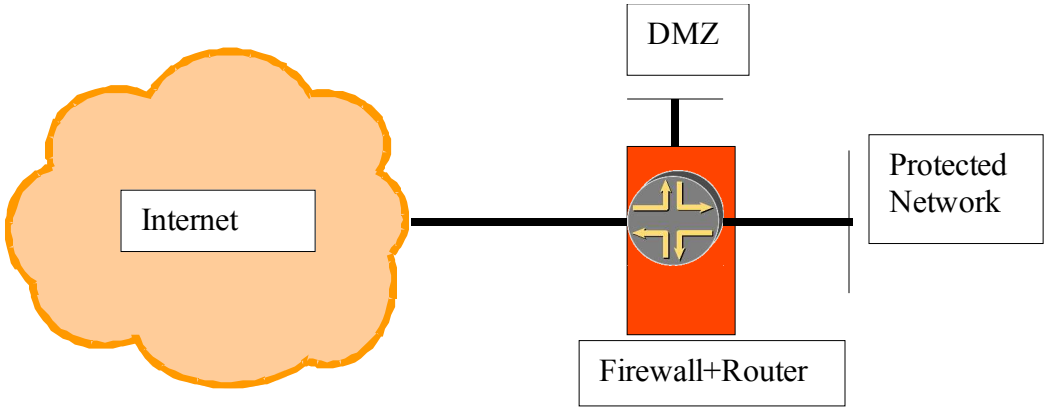
- Internet router firewall net architektúra
- Követelmények:
  - Tűzfal-nak támogatnia kell ND(NS/NA) üzeneteket
  - Tűzfal-nak támogatnia kell (RS/RA) üzeneteket ha SLAAC-t használunk
  - Tűzfal-nak támogatnia kell MLD üzeneteket ha multicastot használunk

IPv6 tűzfal – metódus 2



- Internet firewall router net architektúra
- Követelmények:
  - Tűzfalnak támogatnia kell ND (NS/NA)
  - Tűzfalnak támogatnia dinamikus routing protokollok szűrését
  - Tűzfalnak mindenféle interfész típust támogatnia kell

IPv6 tűzfal – metódus 3



- Internet firewall/router(edge device) net architektúra
- Követelmények:
  - Hatékony lehet – egyetlen pont routing és biztonsági politika bevezetésére – nagyon gyakori SOHO (DSL/cable) routereken
  - Mindazt támogatnia kell routereknek ÉS tűzfalaknak

Tűzfal követelmények

- Nem lehet vakon kiszűrni ICMPv6-t:

IPv6 specifikus	Echo request/reply	Debug
	No route to destination	Debug – jobb hiba indikáció mint ICMPv4 esetén
	TTL exceeded	Hiba jelentés
	Parameter problem	Hiba jelentés
szükséges	NS/NA	Szükséges a helyes müködéshez – kivéve statikus ND bejegyzések esetén
szükséges	RS/RA	Stateless Address Autoconfigration esetén szükséges
szükséges	Packet too big	Path MTU discovery
	MLD	Requirements in for multicast in architecture 1

Tűzfal követelmények 2

- Nem lehet vakon kiszűrni az IP opciókat (extension Header):

Hop-by-hop header	Mit kell tenni jumbogram-okkal és router alert opcióval? – multicast join üzenetekhez szükséges...
Routing header	Source routing – IPv4 esetén kártékonynak minősített, de szükséges IPv6 mobilitáshoz – csak a Home Agent-en szükséges engedélyezni
ESP header	Biztonsági policy szerinti feldolgozás
AH header	Biztonsági policy szerinti feldolgozás
Fragment header	Minden fregmens kivéve az utolsót 1280 octetnél hoszabb kell, hogy legyen

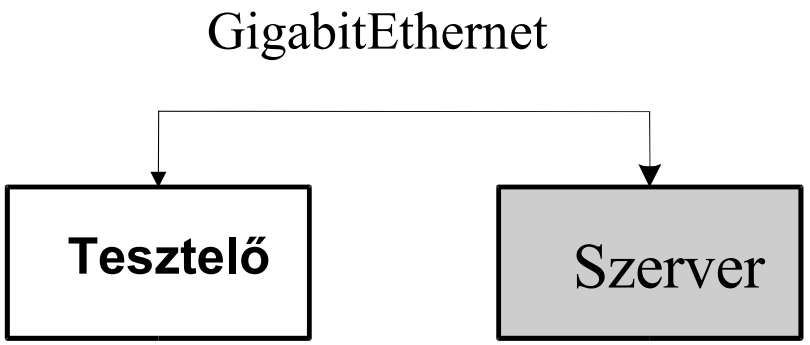
IPv6 tűzfalak alkalmazás támogatása

- FTP:
  - Elég komplex: PORT, LPRT, EPRT, PSV, EPSV, LPSV (RFC 1639, RFC 2428)
  - IPv6 tűzfalakban alig van támogatás
  - HTTP tűnik a következő generációs fájltranszfer protokollnak különösen WEBDAV és DELTA kiegészítéssel
- Egyéb nem triviálisan proxyzható protokoll pl. H.323:
  - Nincs támogatás

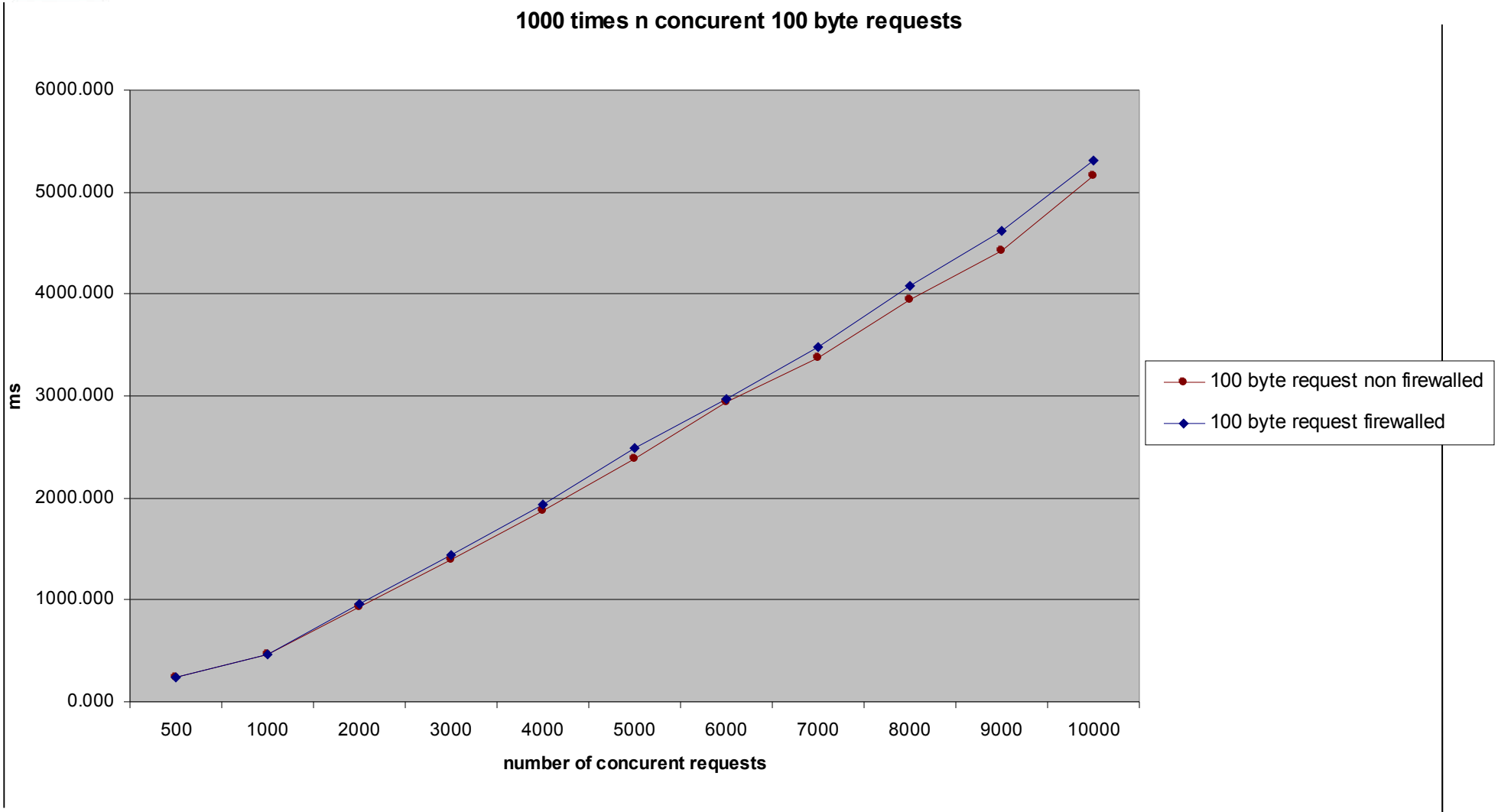
Áttekintés az IPv6 tűzfalakról

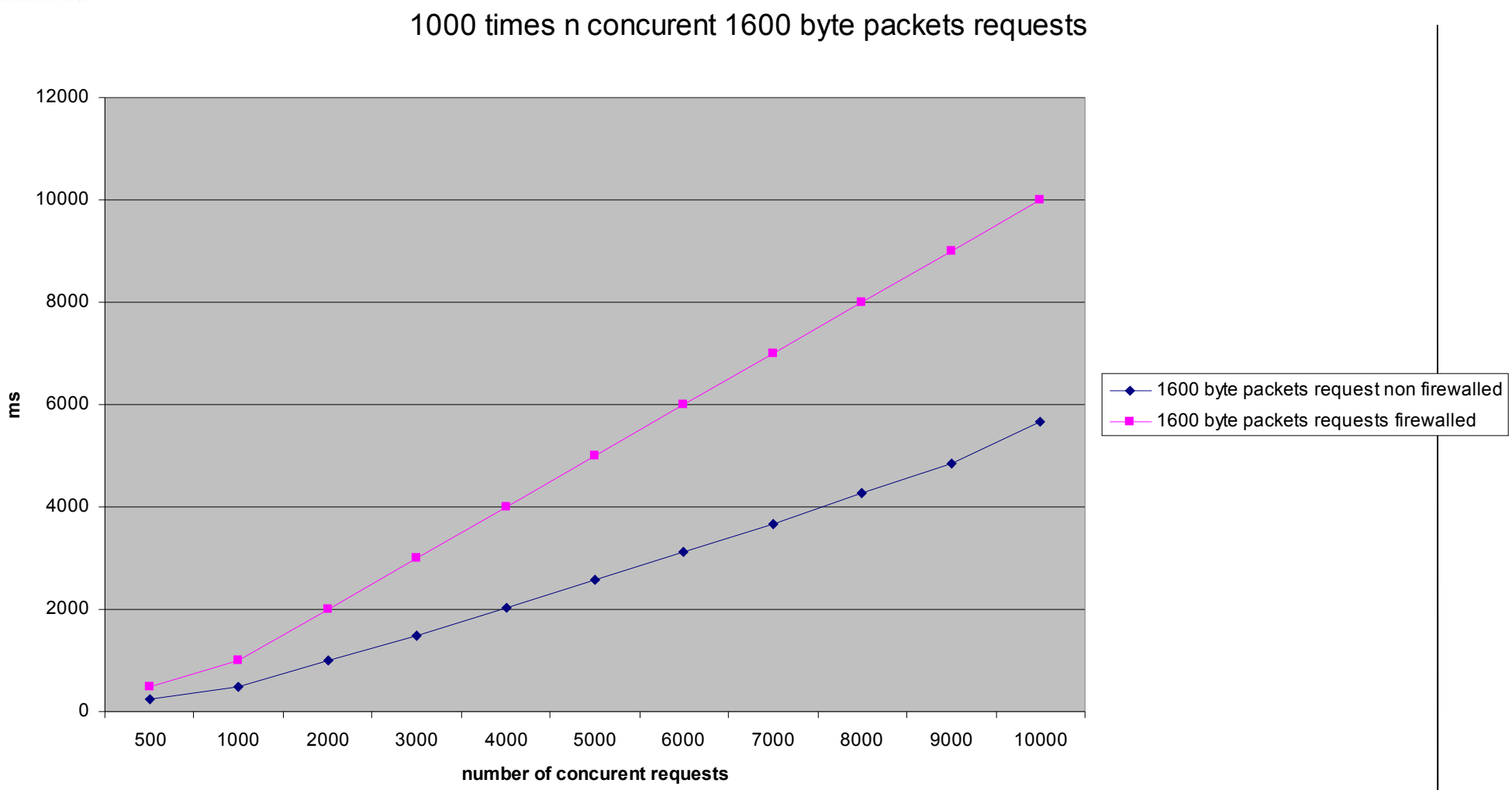
	IPFilter 4.1	PF 3.6	IP6fw	Iptables	Cisco ACL	Cisco PIX 7.0	Juniper firewall	Juniper NetScreen	Windows XP SP2
Hordozhatóság	Kiváló	Jó	Közepes	Gyenge	Gyenge	Gyenge	Gyenge	Gyenge	Gyenge
ICMPv6 támogatás	Jó	Jó	Jó	Jó	Jó	Jó	Jó	Jó	Jó
Neighbor Dissovery	Kiváló	Kiváló	Jó	Kiváló	Kiváló	Kiváló	Jó	Kiváló	Gyenge
RS /RA támogatás	Kiváló	Kiváló	Jó	Kiváló	Kiváló	Kiváló	Kiváló	Kiváló	Jó
Extension header támogatás	Jó	Jó	Jó	Kiváló	Jó	Jó	Jó	Jó	Gyenge
Fregmens támogatás	Gyenge	Teljes block	Gyenge	Jó	Gyenge	Közepes	Gyenge	Közepes	Gyenge
Stateful tűzfal	Igen	Igen	Nem	Csak USAGI	Reflexive firewall	Igen	ASP szükséges	Igen	Nem
FTP proxy	Nem	Következő változat	Nem	Nem	12.3(11)T-től	?	Nem	Nem	Nem
Egyéb	QOS támogatás	QoS támogatás, csomag validitás ellenőrzés	Előre definiált szabályok *BSD-ben	EUI64 check,	Idő alapú ACL		Nincs TCP flag támogatás jelenleg, HW alapú	IPSec VPN, routing támogatás	Grafikus konfiguráció

Ipfilter teljesítménye



- Szerver rendszer: FreeBSD 4.10 – MAXUSERS =1024 – thttpd szerver
- Tesztelő: Linux – erősen tuningolt – max openfiles hack – apachebench
- TCP stateful filtering különböző számú konkurens kérésekkel – IPv6 stateful filtering képességét


1000 times n concurent 100 byte requests
6000.000
5000.000
4000.000
3000.000
2000.000
1000.000
0.000
ms
500
1000
2000
3000
4000
5000
6000
7000
8000
9000
10000
number of concurent requests
100 byte request non firewalled
100 byte request firewalled


1000 times n concurent 1600 byte packets requests
12000
10000
8000
6000
4000
2000
0
ms
500
1000
2000
3000
4000
5000
6000
7000
8000
9000
10000
number of concurent requests
1600 byte packets request non firewalled
1600 byte packets requests firewalled

Konklúzió + Jövő

- Konklúzió:
  - IPv6 tűzfalak léteznek
  - Viszonylag jól használhatóak
  - Alkalmasak IPv6 hálózatok védelmére
  - Gyártói támogatás elérhető
- Jövő
  - Mobile IPv6 – problematikus lehet
  - Használhatóbbá tenni őket Campus IPv6 projektben
  - Egyéb tűzfal teljesítmény tesztek

Köszönet!

- Köszönet Patrick Grossetete, Stig Veenas, Ladislav Lhotka and Tim Chown-nak megjegyzéseikért
- Kérdések: mohacsi@niif.hu