NPF: A NetBSD új tűzfala

Nagy Zoltán Arnold
The NetBSD Foundation
zoltan@netbsd.org

2011. szeptember 24.

Google Summer of Code

- A cél a szabad szoftverek támogatása
- Idén 7 éves a program
- Nyitott minden egyetemi hallgató számára
- A NetBSD minden évben ott volt, idén 9 projekt

Tűzfalkörkép

- IPFilter
- ipfw
- pf
- npf

Az NPF-ről

- A NetBSD Foundation által szponzorált projekt
- Az eredeti kódot Mindaugas Rasiukevicius (rmind@) írta
- Idén kiegészítettem illetve bekapcsolódtam a fejlesztésbe
- A NetBSD 6.0 -ban lesz széles körben elérhető
- Az első állomás a NetBSD hálózati kódjának javításában

Motiváció és célok

- A mostani tűzfalkódok többségét tervezés nélkül bővítették
- A mi tervezési céljaink:
  - minél inkább lockless kód
  - ebből adódó SMP skálázódás
  - állapottartó szűrés
  - modularitás és bővíthetőség
  - általános bytecode motor

Mit tud jelenleg?

- Tetszőleges definíciók (ext_if = "wm0")
- Csoportok (group (name "external", interface $ext_if)
- Rule procedures (csomagtranszformációk egy kapcsolatra)
  - IP ID randomizálás
  - TCP minimum TTL betartatás
  - TCP Maximum Segment Size (MSS) betartatás
  - Loggolás
- Tábla támogatás

Belülről

N-code engine:

- Általános célú bytecode engine, 32-bit minden szó, 4 regiszter
- A tűzfalszabályok erre a bytecodera fordulnak le
- CISC és RISC szerű utasítások
- Maga a csomag nem kerül értelmezésre, csak mint bytefolyam

Okos ábrázolási módok

- in6_addr (128-bit) a címekhez (első 32 bit ha IPv4)
- uint8_t a maszkokhoz

Fejlesztési célok

- Piros-fekete fa -> Radix fa a táblákhoz
- Maszkokat előre legenerálni
- Szabályonkénti statisztikák támogatása
- Dinamikus interfészkövetés
- Plugin támogatás bevezetése

Kérdések?