

# T?zfalak elméletben és gyakorlatban

Kadlecsik József

KFKI RMKI

[kadlec@sunserv.kfki.hu](mailto:kadlec@sunserv.kfki.hu)

# Tartalom

- Tűzfalak és típusaik
- Netfilter
- A netfilter és iptables gyakorlati szempontból
- Nyitott problémák, megoldatlan kérdések
- Összefoglalás

# A tűzfalak definíciója

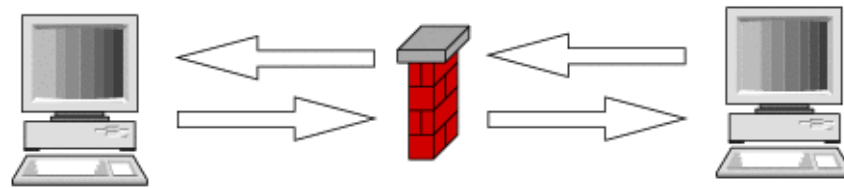
- Jól definiált kapcsolódási pont a védendő rendszer, hálózat és más rendszerek, hálózatok között
- A biztonsági rendszer részeként egy biztonsági szabályzatot valósít meg

# Biztonsági szabályzat

- Mit kell védeni
- Mi ellen
- Milyen mélységben
- Egyéb funkciók
- Üzemeltetési szabályok
- Katasztrófa-terv

# Csomagszűrő t?zfalak I.

- Átjáró a védett hálózat és a külvilág között

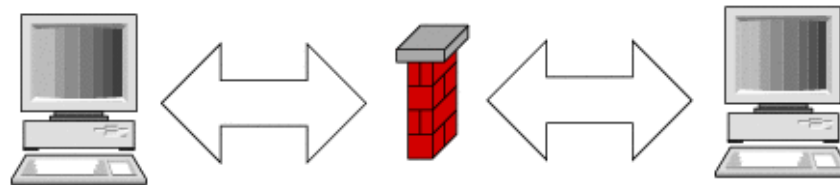


# Csomagszűrőzfalak II.

- Vagy átengedi a csomagot, vagy eldobja
- Csomagok IP, ICMP/TCP/UDP stb fejlécei, nem csomagtartalom alapján dönt
  - Csomagok alapján állapottábla
  - Egyéb kapcsolódó információk
  - Segéd-kapcsolatok
- Csomagot **nem** módosít
  - Címfordítás
  - Fejléc-módosítás

# Proxy t?zfalak I.

- Határozott fizikai szétválasztása a védett és védend? hálózatoknak



# Proxy t?zfalak II.

- Mindkét kommunikáló fél a t?zfallal építi ki a kapcsolatot
- Proxy t?zfalnak "beszélni kell" a használt alkalmazások nyelvét
- El?nyök és hátrányok



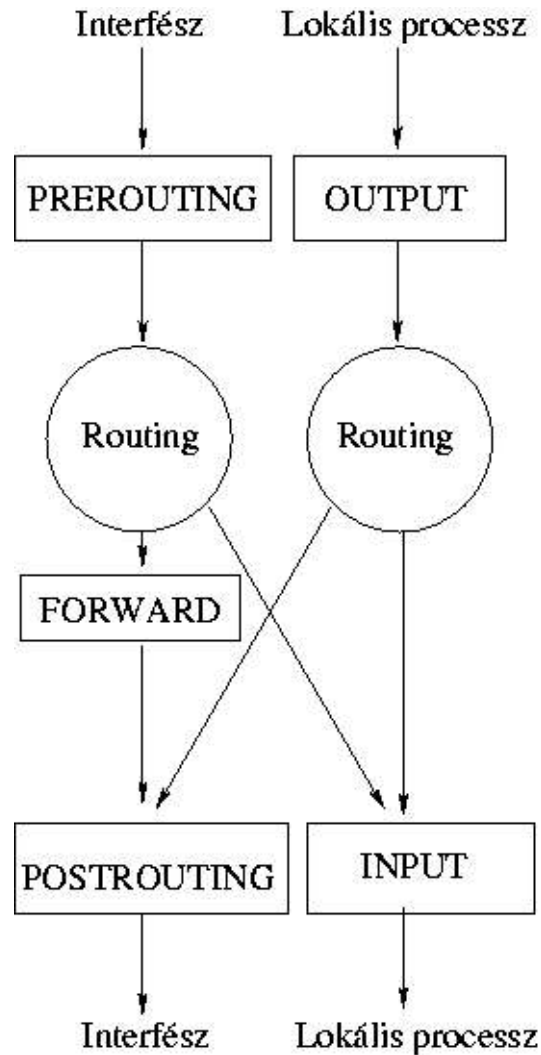
# Netfilter

- Linux 2.4-es kernel t?zfal szolgáltatása
- Állapottartó csomagsz?r?
- Támogat címfordítást (NAT) és csomag-módosítást (mangle)
- Modularizált keretrendszer

# Alrendszerek

- Jól definiált funkciók:
  - Conntrack: kapcsolat-nyomkövetés
  - Mangle: csomag-módosítás
  - NAT: IP cím fordítás
  - Filter: szűrés
- ACCEPT, DROP (, QUEUE, STOLEN)

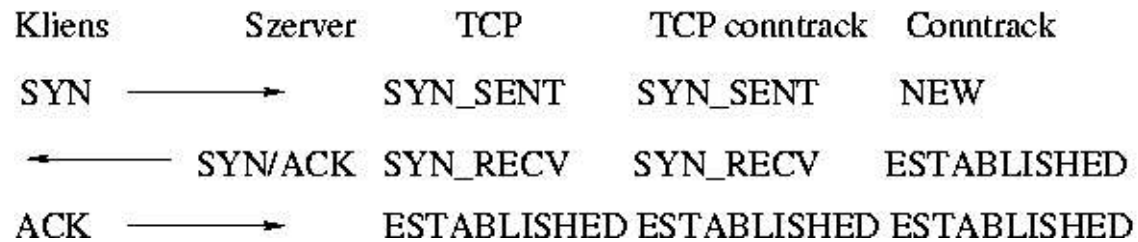
# Netfilter és az IP stack



# Kapcsolat-nyomkövetés (conntrack)

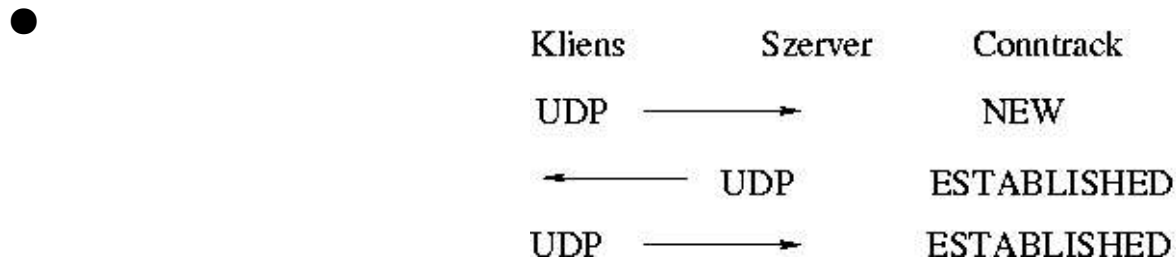
- Belépési pontok: PREROUTING, OUTPUT és POSTROUTING, INPUT
- Állapottér: NEW, ESTABLISHED, RELATED, INVALID
  - Filter alrendszer
- Nincs táblázat

# Kapcsolat-nyomkövetés: TCP



- Nem csak SYN csomag lehet NEW állapotú!

# Kapcsolat-nyomkövetés: UDP



- Belső időzítések

# Kapcsolat-nyomkövetés: ICMP

- ICMP hibaüzenetek: RELATED vagy INVALID
  - Destination unreachable, Source quench, Time exceeded, Parameter problem, Redirect
- ICMP kérdés-válasz: NEW, ESTABLISHED
  - Echo, Timestamp, Info, Address mask

# Kapcsolat-nyomkövetés: protokoll helper

- Egy protokoll több TCP/UDP kapcsolaton épül:
  - Parancs csatorna
  - Segéd csatornák
- Klasszikus példa: FTP
  - PORT parancs: aktív mód
  - PASV parancs: passzív mód
- Netfilter: conntrack helper modulok



# Mangle alrendszer

- Csomag-módosítás:
  - Csomag fejében (IP/TCP) paraméterek módosítása: ToS, MSS, ECN, stb: szolgáltatások közti különbségtétel, hibás rendszerekkel való együttműködés
  - Lokálisan a csomag megjelölése (mark): komplex routing szabályok felállításához

# NAT alrendszer

- SNAT, MASQUERADE
- DNAT, REDIRECT
- Egyedi IP címre vagy tartományra
- Ameddig csak lehetséges, megőrzi az eredeti portokat
  - 0-511
  - 512-1023
  - 1024-65535
- Conntrack alrendszerre épül

# Filter alrendszer

- Csomagszűrés
- A kapcsolat-nyomkövetéssel állapotartó (stateful) csomagszűrő tífal

# Netfilter és iptables

- Netfilter: a kernel része
  - Kernel forráskódjában található
  - Statikus vagy moduláris
- Iptables: a program, amellyel a netfilter (egyres) részeit konfigurálhatjuk
  - <http://www.netfilter.org>

# Netfilter fordítása

- CONFIG\_NETFILTER
- CONFIG\_IP\_NF\_CONNTRACK, FTP, ...
- CONFIG\_IP\_NF\_IPTABLES
- CONFIG\_IP\_NF\_FILTER, NAT, MANGLE
- CONFIG\_IP\_NF\_MATCH\_\*
- CONFIG\_IP\_NF\_TARGET\_\*
- CONFIG\_IP\_NF\_COMPAT\_\*

# Patch-o-matic

- Netfilter javítások, bővítések gyűjteménye
- Kategóriák: submitted, pending, base, extra, userspace
- *runme* script
- Új funkciót megvalósító patch installálása után:  
*make oldconfig*

# Conntrack modulok

- Kapcsolatok maximális száma
  - /proc/sys/net/ipv4/ip\_conntrack\_max
  - ip\_conntrack modul hashsize paramétere
$$\text{ip\_conntrack\_max} = 8 * \text{hashsize}$$
- Conntrack & NAT helper modulok nem töltődnek be automatikusan:

```
# modprobe ip_conntrack_ftp ports=21,1121
```

```
# modprobe ip_nat_ftp ports=21,1121
```

# Iptables fordítása

- `make; make install` :-)
- ```
# make KERNEL_DIR=... BINDIR=... \  
LIBDIR=... MANDIR=...
```
- ```
# make KERNEL_DIR=... BINDIR=... \  
LIBDIR=... MANDIR=... install
```
- Disztribúcióból vagy kézzel telepített változat



# Iptables-save és restore

- Iptables nagy szabálygyűjtemény esetén lassú

```
# iptables-save [-c] > /etc/iptables_rules
```

```
# iptables-restore [-c] < /etc/iptables_rules
```

# Iptables használata

iptables [-t táblázat] parancs [egyezés(ek)]  
[cselekvés/ugrás láncra]

# iptables -L -n

# iptables -h

# iptables -m tcpmss -h

# iptables -j TCPMSS -h

# Iptables parancsok

- A(ppend)
- D(elete)
- I(nsert)
- R(eplace)
- N(ew)
- L(ist)
- P(olicy)

Névkonvenciók

# Általános egyezési feltételek

- -p [!] protokoll
- -s [!] cím/maszk
- -d [!] cím/maszk
- -i [!] interfész
- -o [!] interfész
  
- [!] -f

# Implicit egyezési feltételek

- A *-p protokoll* használatához köt?dnek:  
*-p tcp/udp/icmp*
- Nem önálló kernel modul részei
- UDP: *-p udp*
  - *--sport [!] port[:port]*
  - *--dport [!] port[:port]*
- ICMP: *-p icmp*
  - *--icmp-type [!] típusnév*

# Implicit egyezési feltételek: TCP

- --sport, --dport
  - --tcp-flags [!] maszk beállított
- ... *-p tcp --tcp-flags SYN,RST,ACK SYN ...*
- [!] --syn
  - --tcp-option [!] opció-azonosító
  - --mss érték[:érték]

# Egyezési feltétel-kiterjesztések

- Támogatásukat be **kell** fordítani a kernelbe
- A kiterjesztésre explicit hivatkozi **kell**:  
*-m <kiterjesztés-modulnév>*
- B?ség zavara :-)

# State match

- A legfontosabbak egyike

*-m state --state állapot-lista*

- NEW, ESTABLISHED, RELATED, INVALID

*# iptables -A FORWARD -o eth0 -j ACCEPT*

*# iptables -A FORWARD -o eth1 -m state \*

*--state ESTABLISHED,RELATED -j ACCEPT*



# Unclean match

- Csomag-ellenőrzés: nem sérült-e, nem tartalmaz-e illegális paramétereket vagy paraméterkombinációt az IP, TCP, UDP, ICMP fejlécekben

```
# iptables -A FORWARD -m unclean -j DROP
```

# Limit match

- Kettős visszacsatolású határérték-vizsgálat:

*--limit-burst n*

*--limit m[/second/minute/hour/day]*

- Default: *--limit 3/hour --limit-burst 5*

# Egyéb 2.4.20-ban található match-ek

- `-m mac --mac-source XX:XX:XX:XX:XX:XX`
- `-p tcp|udp -m multiport --[s|d]ports port[,port,...]`
- `-m length --length hossz[:hossz]`
- `-m helper --helper helper-név`
- ....

# Targetek

- Általános típusok:
  - ACCEPT, DROP, RETURN (, QUEUE)
  - Ugrás láncra: -j láncnév
- Target-kiterjesztések:
  - Be **kell** fordítani a kernelbe
  - Termináló és nem-termináló targetek

# LOG target

- Naplózásra szolgál (syslogd, konzol, dmesg)
- `-j LOG --log-prefix "szöveg" ...`

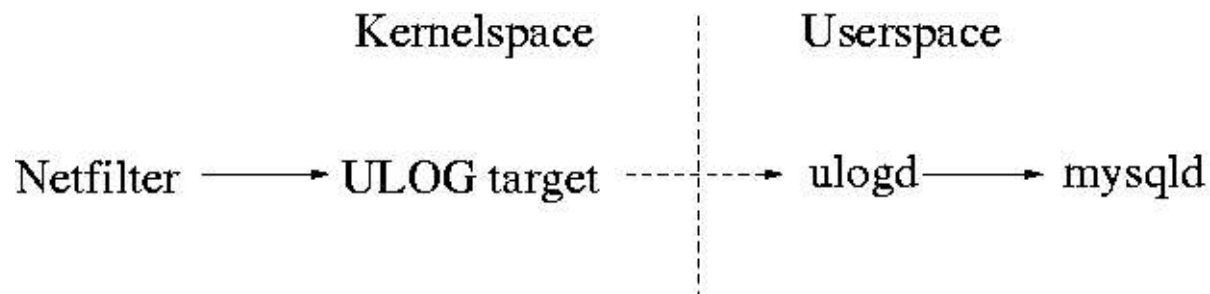
*# iptables -N logdrop*

*# iptables -A logdrop -m limit -j LOG \  
--log-prefix "Dropped: "*

*# iptables -A logdrop -j DROP*

# ULOG target

- Naplóüzenetek és csomagok felhasználói programmal való naplózásához
- Netlink socket



# REJECT target

- Csomageldobás ICMP Unreachable, Prohibited vagy TCP RST csomag visszaküldésével
- Ident kérések blokkolása (SMTP)

```
# iptables -A FORWARD -p tcp --dport 113 \  
-j REJECT --reject-with tcp-reset
```

# SNAT target

- NAT: forrás IP cím átírás
- Statikus privát IP címek esetén használatos

*--to-source cím[-cím][:port-port]*

- Több is megadható - routing!

```
# iptables -t nat -A POSTROUTING -o ippp0 \  
-j SNAT --to-source x.y.z.w
```



# MASQUERADE target

- SNAT speciális esete
- Dinamikus privát IP cím esetén használatos
- Kimen? interfész IP címét használja

*--to-ports port[-port]*

```
# iptables -t nat -A POSTROUTING -o ippp0 \  
-j MASQUERADE
```

# DNAT target

- NAT: cél IP cím átírása
- Privát IP cím? szerver elérhet?ségének a biztosítása, terhelésmegosztás, proxy
- Hasonló szintaxis mint az SNAT esetén

```
# iptables -t nat -A PREROUTING -d x.y.z.w \  
-p tcp --dport 80 -j DNAT \  
--to-destination 192.168.1.1
```

# REDIRECT target

- DNAT speciális esete
- (Transzparens) proxy szolgáltatásokhoz

```
# iptables -t nat -A PREROUTING -p tcp \  
  --dport 80 -j REDIRECT --to-ports 3128
```

# TCPMSS target

- ICMP **kell** a TCP/IP m?ködéséhez
- Hibásan konfigurált t?zfalak nem engedik át az ICMP Fragmentation Needed csomagokat: TCP nagy csomagok esetén nem m?ködik

*--clamp-mss-to-pmtu*

*--set-mss érték*

# Egyéb targetek

- -j MARK --set-mark érték
- -j TOS --set-tos név
- -j ECN --ecn-tcp-remove
- ...

# B?vítések patch-o-matic-ban

- Helperek
- Új feltételek
- Új targetek
- Új szolgáltatások

# Helperek

- Submitted:
  - Tftp conntrack és NAT helper
  - Amanda conntrack és NAT helper
- Extra:
  - Eggdrop bot, CuSeeMee, (primitív) H.323, Microsoft Streaming Media, PPTP, RPC, rsh, Quake III Arena, talk

# Condition match

*# iptables ... -m condition --condition foo\_ok ...*

*# echo 1 > /proc/net/ipt\_condition/foo\_ok*

*# echo 0 > /proc/net/ipt\_condition/foo\_ok*



# Time match

```
# iptables -A FORWARD -o eth0 -p tcp --dport 21 \  
-m time --timestart 8:00 --timestop 16:00 \  
--days Mon,Tue,Wed,Thu,Fri -j DROP
```

# Iplimit match

- TCP/UDP kapcsolatok limitálása

```
# iptables -A FORWARD -p tcp --dport 80 --syn \  
-m iplimit --iplimit-above 16 --iplimit-mask 24 \  
-j DROP
```

# Fuzzy match

- Takagi-Sugeno-Kang Fuzzy Logic Controller
- Csomagok másodpercenkénti számára
- Minimális elfogadási arány 1%

```
# iptables -A FORWARD -p icmp \  
  --icmp-type echo-request \  
  -m fuzzy --upper-limit 10 --lower-limit 1 \  
  -j DROP
```

# Recent match

- Feltételek "mostanában" látott IP címekre

```
# iptables -A FORWARD -m recent --rcheck \  
    --seconds 60 -j DROP
```

```
# iptables -A FORWARD -i eth0 -d 127.0.0.0/8 \  
    -m recent --set -j DROP
```

- *--rcheck* helyett állhat akár *--update*

# Raw patch

- Új táblázat: raw
  - PREROUTING, OUTPUT
  - Legels?
- Új targetek:
  - TRACE  
TRACE: táblanév/láncnév/szabályszám <csomag>
  - NOTRACK
- State match kiterjesztése: UNTRACKED

# Nyitott problémák

- Iptables-save és iptables-restore kiküszöbölése
- IPv6 és conntrack (NAT)
- Netfilter-failover
- nfnetlink/ctnetlink
- User interfész és library
- ...

# Összefoglalás

- T?zfal-típusok közül a feladattól függ?en kell választani
- Netfilter egy lehetséges megoldás
- További fejlesztések várhatók

<http://www.netfilter.org>