



# Az én váram

## Tűzfal és VPN

BRKK::Békéscsaba  
Linux rendszergazda képzés  
2008



# Tűzfal



- Tervezd meg, az összehajigált menet közben alakuló rendszerek átláthatatlanok és nehezen kezelhetők, ebből adódóan sérülékenyek.
- Rajzold le, a rajz segít, hogy jobban átlásd, az esetleges hibákat könnyebben megtaláld.
- Ellenőrizd le!!!

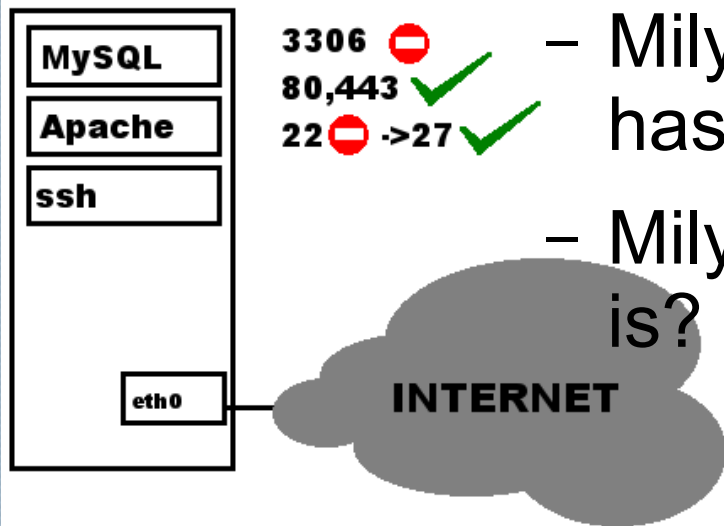


# Védd magad



- Először nézzünk egy egyszerű feladatot, adott szolgáltatásokat nyújtó rendszer biztonságossá tétele:

- MINDEN TILOS ami nem kifejezetten megengedett.



- Milyen szolgáltatás, milyen kapukat használ?

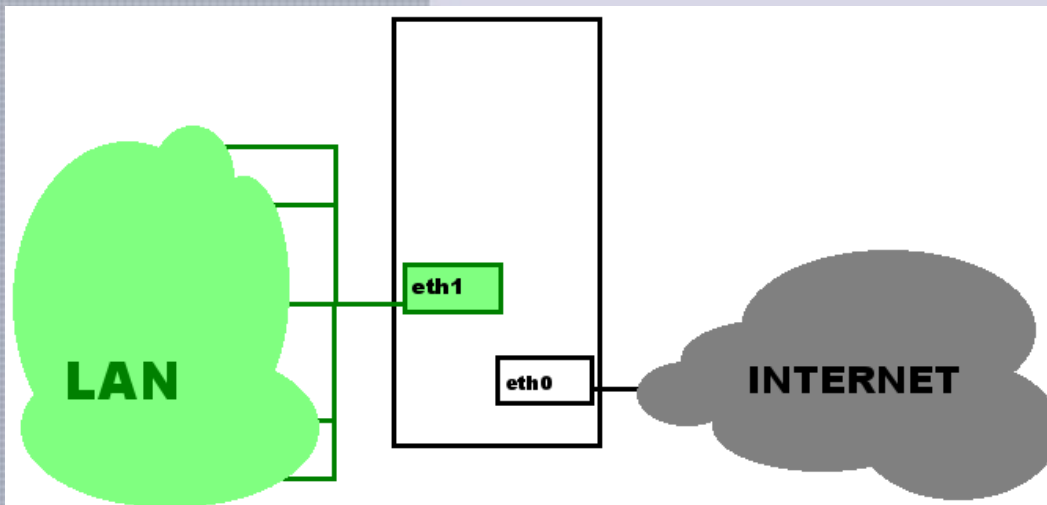
- Milyen szolgáltatás használható kívülről is?



# Átjáró

Az előző filozófia itt is érvényes, apró adalék csupán, hogy gépünk átjáró a LAN és az INTERNET között.

- Különböző szabályok kint és bent
- Címfordítás szükséges





# Alapszabályok

Bentről ki bármi, kintről befele csak ami bentről indult:

– Alapszabályok:

```
EXTIF="eth0"  
INTIF="eth1" vagy esetleg INTIF="vbnf0"  
iptables -P INPUT DROP  
iptables -F INPUT  
iptables -P OUTPUT ACCEPT  
iptables -F OUTPUT  
iptables -P FORWARD DROP  
iptables -F FORWARD  
iptables -t nat -F
```

– Bentről ki:

```
iptables -A FORWARD -i $INTIF -o $EXTIF -j ACCEPT
```

– Kintről befele:

```
iptables -A FORWARD -i $EXTIF -o $INTIF -m state  
--state ESTABLISHED,RELATED -j ACCEPT
```



# NAT

Ha szeretnénk, hogy a belső gépek használhassák az INTERNET szolgáltatásait, akkor címfordítást kell használnunk

```
iptables -t nat -A POSTROUTING -o $EXTIF -j MASQUERADE
```

Ahhoz, hogy a FORWARD tábla szabályai működjenek, be kell kapcsolnunk a kernelben az ip-forward opciót

```
echo "1" > /proc/sys/net/ipv4/ip_forward
```

és ha mindezt nem akarjuk minden egyes újrainduláskor begépelni, akkor a /etc/sysctl.conf -ban

```
# Uncomment the next line to enable packet forwarding for Ipv4  
net.ipv4.ip_forward=1
```



# A titkos alagút várunkba



## OpenVPN:

- biztonságos kapcsolat
- nincs szükség kernel szintű támogatásra, illetve ami kell az modulként bármikor telepíthető, ezért majdnem minden átjuttatható
- gépenként / kapcsolatonként állítható

## Telepítés:

[http://wiki.hup.hu/index.php/Az\\_OpenVPN\\_finomhangol%C3%A1sa](http://wiki.hup.hu/index.php/Az_OpenVPN_finomhangol%C3%A1sa)

**RSA-DH HOWTO sajna ENGLISH**

<http://openvpn.net/index.php/documentation/howto.html#pki>