



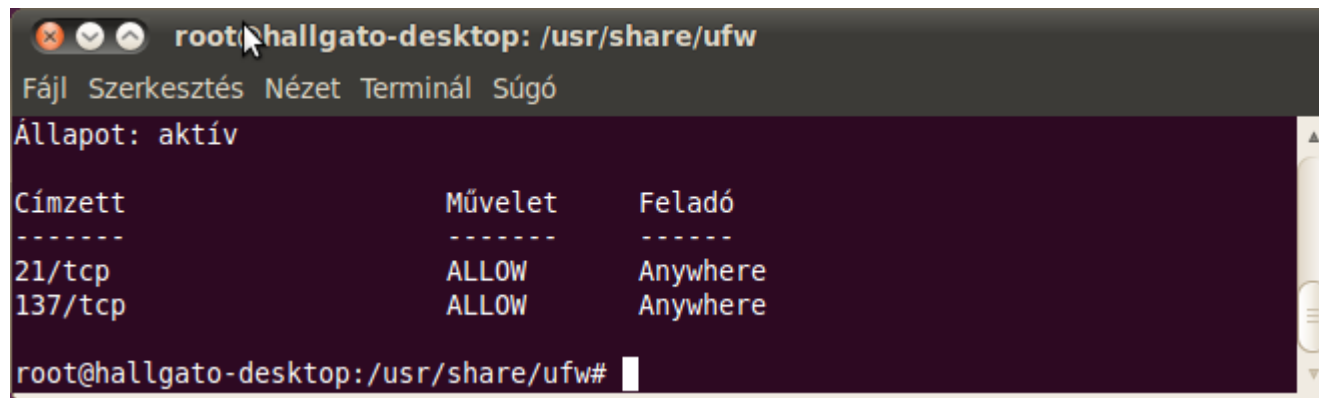
Tűzfal

Tűzfal

- ▶ Minden be | ki csomag a Netfilter alrendszerhez kerül. Ez dönti el: elfogad | módosít | visszautasít
- ▶ iptables
- ▶ Tűzfal konfiguráló, menedzselő eszközök
 - ▶ ufw - parancssor
 - ▶ Firestarter - GUI
 - ▶ Gufw - GUI

Uncomplicated Firewall

- ▶ Engedélyezés: `sudo ufw enable | disable`
- ▶ Állapot: `sudo ufw status [verbose]`
- ▶ Konfig. Állományok: `/etc/default/ufw`, `/etc/ufw/ufw.conf`
- ▶ Szabályok: `/lib/ufw/user.rules`
- ▶ Engedélyezés példák
- ▶ `sudo ufw allow szolgáltatásnév | port/protokoll`
 - ▶ `sudo ufw allow ftp`
 - ▶ `sudo ufw allow 137/tcp`



The screenshot shows a terminal window titled 'root@hallgato-desktop: /usr/share/ufw'. The window contains the output of the 'ufw status' command, which shows the firewall is active and lists two rules: '21/tcp' and '137/tcp', both set to 'ALLOW' and 'Anywhere'.

```
root@hallgato-desktop: /usr/share/ufw
Fájl Szerkesztés Nézet Terminál Súgó
Állapot: aktív

Címzett          Művelet      Feladó
-----
21/tcp           ALLOW        Anywhere
137/tcp          ALLOW        Anywhere

root@hallgato-desktop: /usr/share/ufw#
```

ufw - tiltás

- ▶ `sudo ufw deny proto tcp from 192.168.0.5 to any port 22`
- ▶ `sudo ufw deny 22`

The image shows two terminal windows from a Linux desktop environment. The left window displays the output of the `ufw status` command, showing a table of active rules. The right window shows the content of the `/etc/ufw/user.rules` file, which contains the configuration for the firewall rules.

Címzett	Művelet	Fel
21/tcp	ALLOW	Any
137/tcp	ALLOW	Any
22/tcp	DENY	192.168.0.5

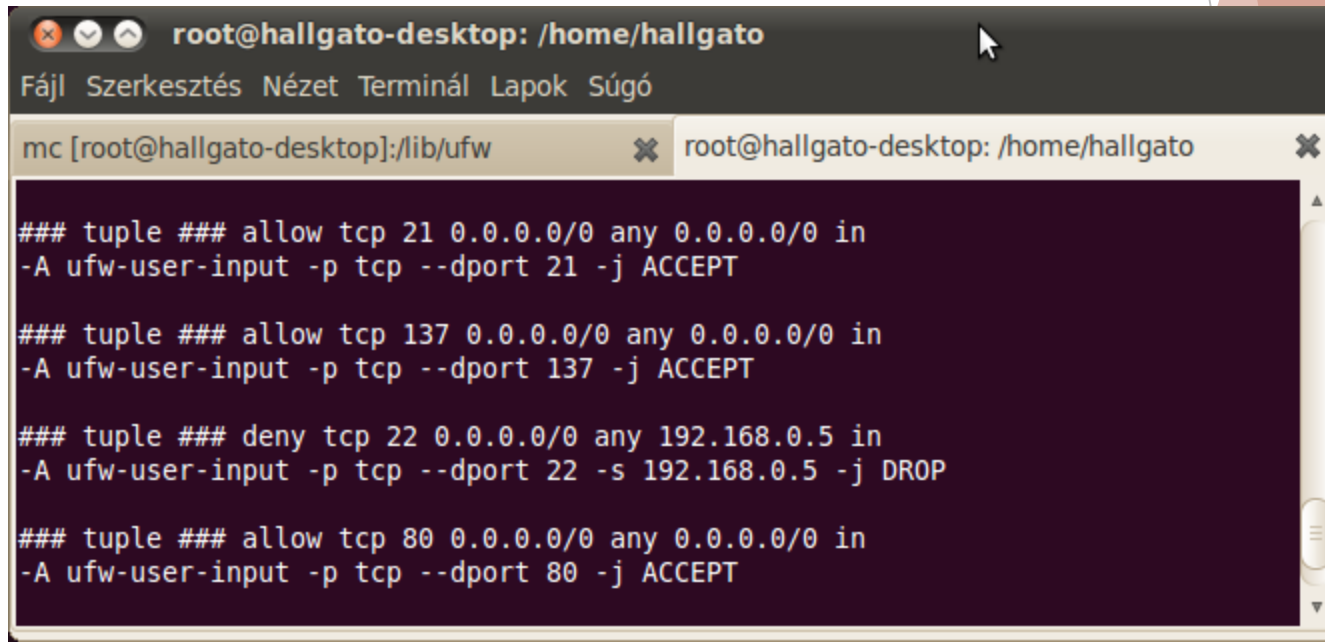
```
### tuple ### allow tcp 21 0.0.0.0/0 any 0.0.0.0/0 in
-A ufw-user-input -p tcp --dport 21 -j ACCEPT

### tuple ### allow tcp 137 0.0.0.0/0 any 0.0.0.0/0 in
-A ufw-user-input -p tcp --dport 137 -j ACCEPT

### tuple ### deny tcp 22 0.0.0.0/0 any 192.168.0.5 in
-A ufw-user-input -p tcp --dport 22 -s 192.168.0.5 -j DROP
```

Utasítások

- ▶ Szabály törlése
 - ▶ `sudo ufw delete allow 137/tcp`
- ▶ Milyen iptables utasítások keletkeznek egy ufw utasítás eredményeképpen?
 - ▶ `sudo ufw -dry-run allow http`



```
root@hallgato-desktop: /home/hallgato
Fájl Szerkesztés Nézet Terminál Lapok Súgó
mc [root@hallgato-desktop]:/lib/ufw root@hallgato-desktop: /home/hallgato

### tuple ### allow tcp 21 0.0.0.0/0 any 0.0.0.0/0 in
-A ufw-user-input -p tcp --dport 21 -j ACCEPT

### tuple ### allow tcp 137 0.0.0.0/0 any 0.0.0.0/0 in
-A ufw-user-input -p tcp --dport 137 -j ACCEPT

### tuple ### deny tcp 22 0.0.0.0/0 any 192.168.0.5 in
-A ufw-user-input -p tcp --dport 22 -s 192.168.0.5 -j DROP

### tuple ### allow tcp 80 0.0.0.0/0 any 0.0.0.0/0 in
-A ufw-user-input -p tcp --dport 80 -j ACCEPT
```

Alkalmazásprofil

```
[Samba]
title=LanManager-like file and
description=The Samba software
lements the SMB/CIFS protocol
es and printers to Windows, NT
ometimes also referred to as th
ports=137,138/udp|139,445/tcp
```

- ▶ Egyes alkalmazások saját profilokat telepítenek, amiben szerepel, hogy milyen portokat kell megnyitni a számukra
- ▶ `/etc/ufw/applications.d` könyvtár

```
mc [root@hallgato-desktop]:/etc/ufw/applications.d
Fájl Szerkesztés Nézet Terminál Lapok Súgó

mc [root@hallgato-desktop]:/etc/ufw/applications.d  root@hallgato-desktop: /home/hallgato

Fájl: cups      Sor 1 Oszl 0      152 bájt      100%
[CUPS]
title=Common UNIX Printing System server
description=CUPS is a printing system with support for IPP, samba, lpd, and other protocols.
ports=631

1Súgó 2NemTör 3Kilép 4Hex 5UgrSor 6 7Keres 8Nyers 9Formáz 10Kilép
```

Profilok

- ▶ Profil beállításainak megtekintése
 - ▶ `sudo ufw app info ALKALMAZÁS`

```
root@ubuntu-server:/etc/ufw# ufw app info Samba
Profile: Samba
Title: LanManager-like file and printer server for Unix
Description: The Samba software suite is a collection of programs that
implements the SMB/CIFS protocol for unix systems, allowing you to serve
files and printers to Windows, NT, OS/2 and DOS clients. This protocol is
sometimes also referred to as the LanManager or NetBIOS protocol.

Ports:
  137,138/udp
  139,445/tcp
```

Profil használata

- ▶ Telepített profilok listája
 - ▶ `sudo ufw app list`
- ▶ Az alkalmazáshoz kapcsolódó forgalom engedélyezése
 - ▶ `sudo ufw allow|deny ALKALMAZÁSNÉV`
 - ▶ `sudo ufw allow Samba`
 - ▶ `sudo ufw from 192.168.1.0/24 app Samba`
- ▶ Eredmény (`/lib/ufw/user.rules`)

```
### tuple ### allow udp any 0.0.0.0/0 137,138 192.168.1.0/24 - Samba in
-A ufw-user-input -p udp -m multiport --sports 137,138 -s 192.168.1.0/24
-j ACCEPT -m comment --comment 'sapp_Samba'
```

```
### tuple ### allow tcp any 0.0.0.0/0 139,445 192.168.1.0/24 - Samba in
-A ufw-user-input -p tcp -m multiport --sports 139,445 -s 192.168.1.0/24
-j ACCEPT -m comment --comment 'sapp_Samba'
```


Naplózás

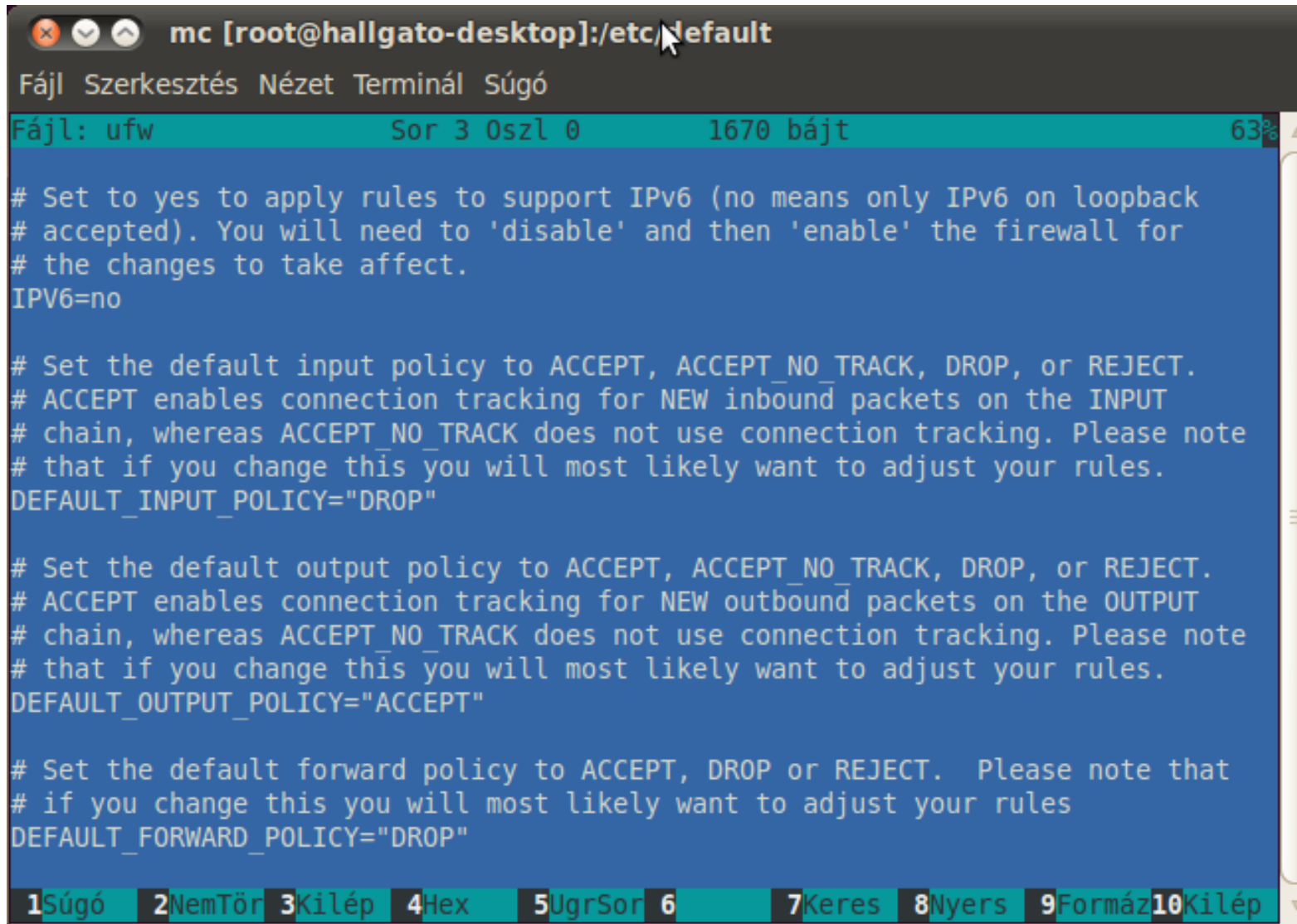
- ▶ `sudo ufw logging off | low | medium | high | full`
- ▶ Hova kerül?
- ▶ `/var/log/messages`
- ▶ `/var/log/syslog`
- ▶ `/var/log/kern.log`

IP álcázás

NAT

- ▶ Csomagtovábbítás engedélyezése
 - ▶ `/etc/default/ufw` → `DEFAULT_FORWARD_POLICY="ACCEPT"`
 - ▶ `/etc/ufw/sysctl.conf` → `net/ipv4/ip_forward=1`
- ▶ NAT tábla konfigurálása
 - ▶ `/etc/ufw/before.rules` az állomány elejére a fejléc után →
 - ▶ `# nat Table rules`
 - ▶ `*nat`
 - ▶ `:POSTROUTING ACCEPT [0:0]`
 - ▶ `# Forward traffic from eth1 through eth0.`
 - ▶ `-A POSTROUTING -s 192.168.0.0/24 -o eth0 -j MASQUERADE`
 - ▶ `COMMIT`
- ▶ Változások érvényesítése
 - ▶ `sudo ufw disable && sudo ufw enable`

/etc/default/ufw



The screenshot shows a terminal window with a dark background. The title bar reads "mc [root@hallgato-desktop]:/etc/default". Below the title bar is a menu bar with options: "Fájl", "Szerkesztés", "Nézet", "Terminál", and "Súgó". The status bar at the top of the editor shows "Fájl: ufw", "Sor 3 Oszl 0", "1670 bájt", and "63%". The main text area is blue and contains the following content:

```
# Set to yes to apply rules to support IPv6 (no means only IPv6 on loopback
# accepted). You will need to 'disable' and then 'enable' the firewall for
# the changes to take affect.
IPV6=no

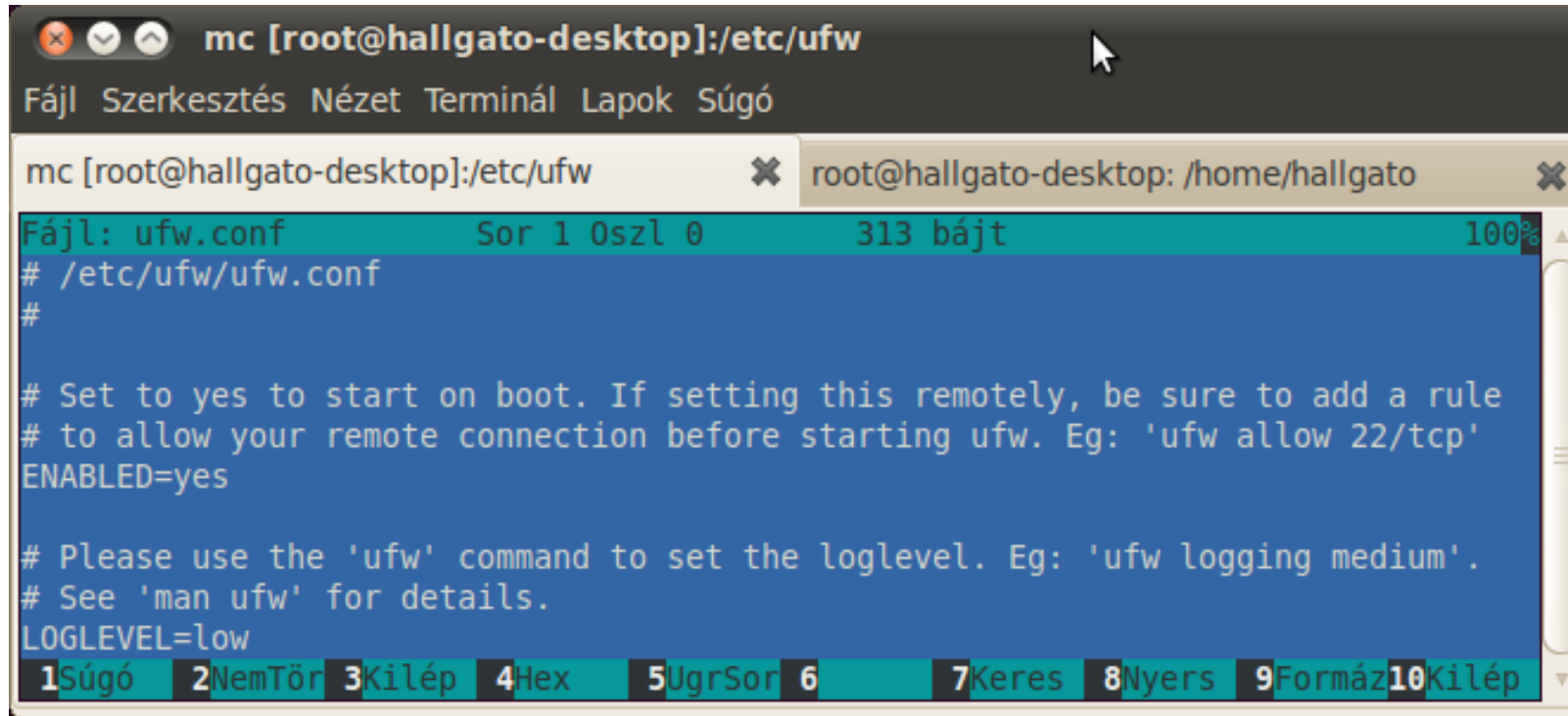
# Set the default input policy to ACCEPT, ACCEPT_NO_TRACK, DROP, or REJECT.
# ACCEPT enables connection tracking for NEW inbound packets on the INPUT
# chain, whereas ACCEPT_NO_TRACK does not use connection tracking. Please note
# that if you change this you will most likely want to adjust your rules.
DEFAULT_INPUT_POLICY="DROP"

# Set the default output policy to ACCEPT, ACCEPT_NO_TRACK, DROP, or REJECT.
# ACCEPT enables connection tracking for NEW outbound packets on the OUTPUT
# chain, whereas ACCEPT_NO_TRACK does not use connection tracking. Please note
# that if you change this you will most likely want to adjust your rules.
DEFAULT_OUTPUT_POLICY="ACCEPT"

# Set the default forward policy to ACCEPT, DROP or REJECT. Please note that
# if you change this you will most likely want to adjust your rules
DEFAULT_FORWARD_POLICY="DROP"
```

At the bottom of the window is a status bar with a menu: "1Súgó", "2NemTör", "3Kilép", "4Hex", "5UgrSor", "6", "7Keres", "8Nyers", "9Formáz", "10Kilép".

/etc/ufw/ufw.conf



The image shows a terminal window titled "mc [root@hallgato-desktop]:/etc/ufw". The window has a menu bar with "Fájl", "Szerkesztés", "Nézet", "Terminál", "Lapok", and "Súgó". Below the menu bar, there are two tabs: "mc [root@hallgato-desktop]:/etc/ufw" and "root@hallgato-desktop: /home/hallgato". The main content area displays the contents of the file "ufw.conf". The text is as follows:

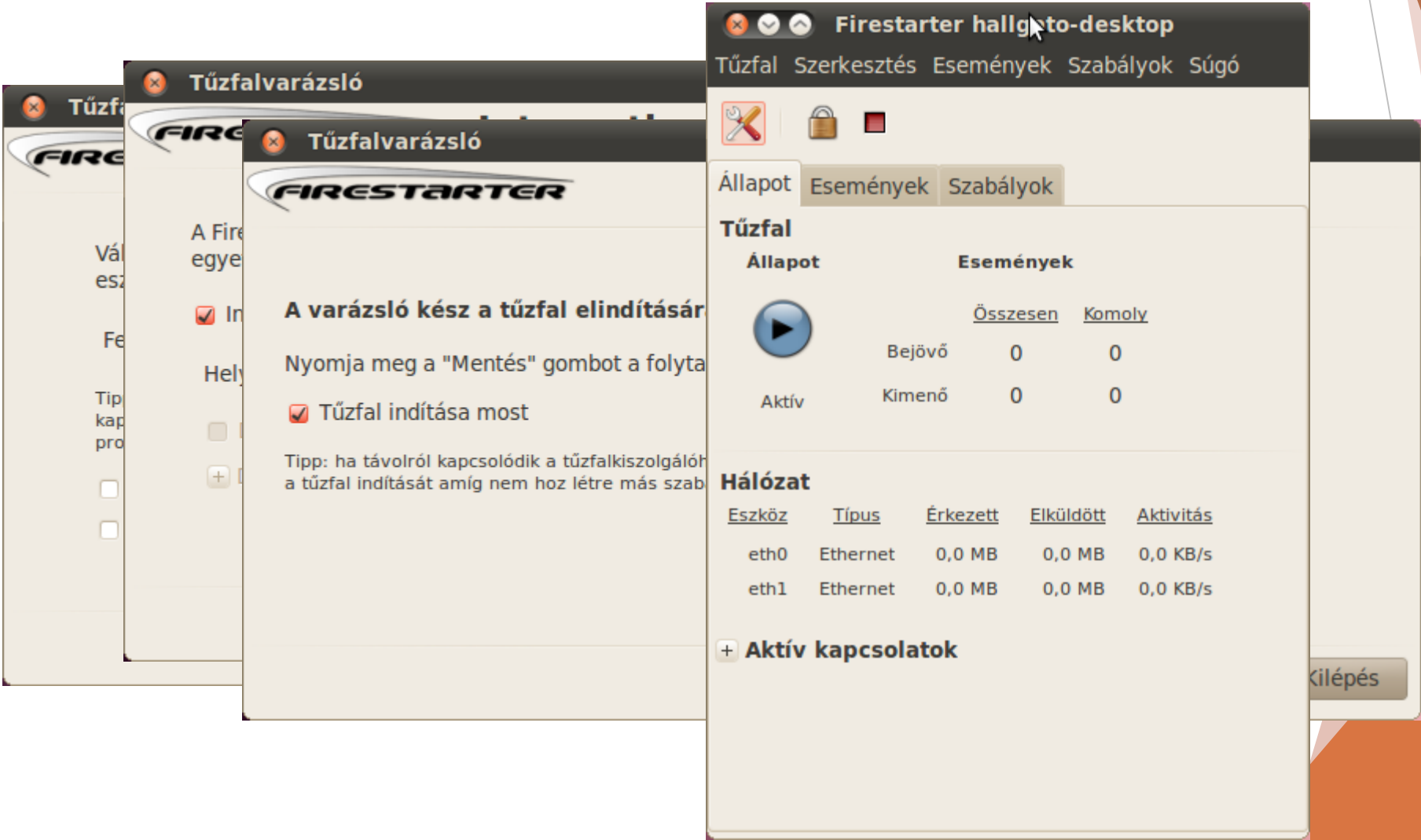
```
Fájl: ufw.conf      Sor 1 Oszl 0      313 bájt      100%
# /etc/ufw/ufw.conf
#
# Set to yes to start on boot. If setting this remotely, be sure to add a rule
# to allow your remote connection before starting ufw. Eg: 'ufw allow 22/tcp'
ENABLED=yes
# Please use the 'ufw' command to set the loglevel. Eg: 'ufw logging medium'.
# See 'man ufw' for details.
LOGLEVEL=low
```

At the bottom of the terminal window, there is a status bar with the following text: "1Súgó 2NemTör 3Kilép 4Hex 5UgrSor 6 7Keres 8Nyers 9Formáz10Kilép".

Firestarter

- ▶ `sudo apt-get install firestarter`
- ▶ `sudo /usr/sbin/firestarter`
- ▶ Varázsló
 - ▶ Eszköz kiválasztása listából (ethx)
 - ▶ Internet kapcsolat megosztás engedélyezése (NAT)
 - ▶ Tűzfal indítása

Firestarter varázsló



Firestarter

- ▶ Szabályok
 - ▶ Bejövő forgalomra
 - ▶ Kimenő forgalomra
(alapból engedélyező | alapból tiltó)
- ▶ Engedélyezés | Tiltás
 - ▶ Gépről
 - ▶ Szolgáltatás
 - ▶ Átirányítás

Bejövő forgalom szabályai

Firestarter hallgato-desktop

Tűzfal Szerkesztés Események Szabályok

Új bejövő szabály

Szolgáltatás engedélyezése

Név HTTP

Port 80

Ha a forrás

☐ Bárki ☒ LAN kliens

☐ IP, kiszolgáló vagy

Megjegyzés

Firestarter hallgato-desktop

Tűzfal Szerkesztés

Új bejövő szabály

Szolgáltatás átirányítás

Név HTTPS

Port 443

A belső kiszolgálóra

IP vagy gép 192.168.1.50

Port 443

Megjegyzés

Mégse

Firestarter hallgato-desktop

Tűzfal Szerkesztés Események Szabályok Súgó

Szabályok

Szerkesztés Bejövő forgalom szabályai

Kapcsolatok engedélyezése erről a gépről:

Szolgáltatás engedélyezése	Port	Ennek:
HTTP	80	lan

Szolgáltatás átirányítása	Tűzfal port	Ennek:	Port
HTTPS	443	192.168.1.50	443