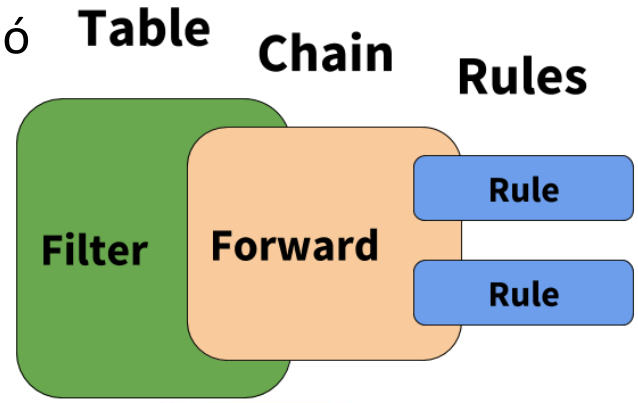
Számítógépes Hálózatok

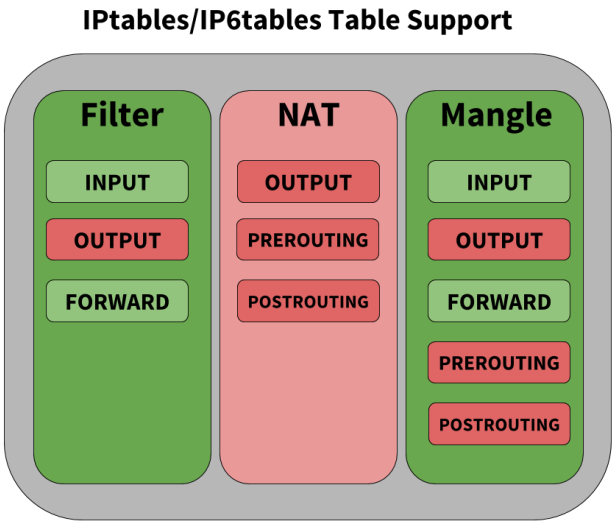
9. gyakorlat

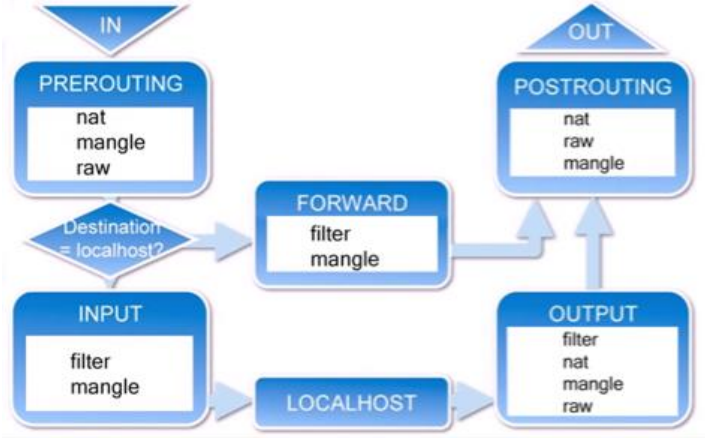
péntekieknek 7. gyakorlat

iptables

- Az iptables egy Linux alkalmazás, amellyel a felhasználó konfigurálni tud tűzfal funkcionalitást, ill. csomagszűrési/csomagtovábbítási szabályokra, NAT módosítására/lekérdezésére jó







iptables

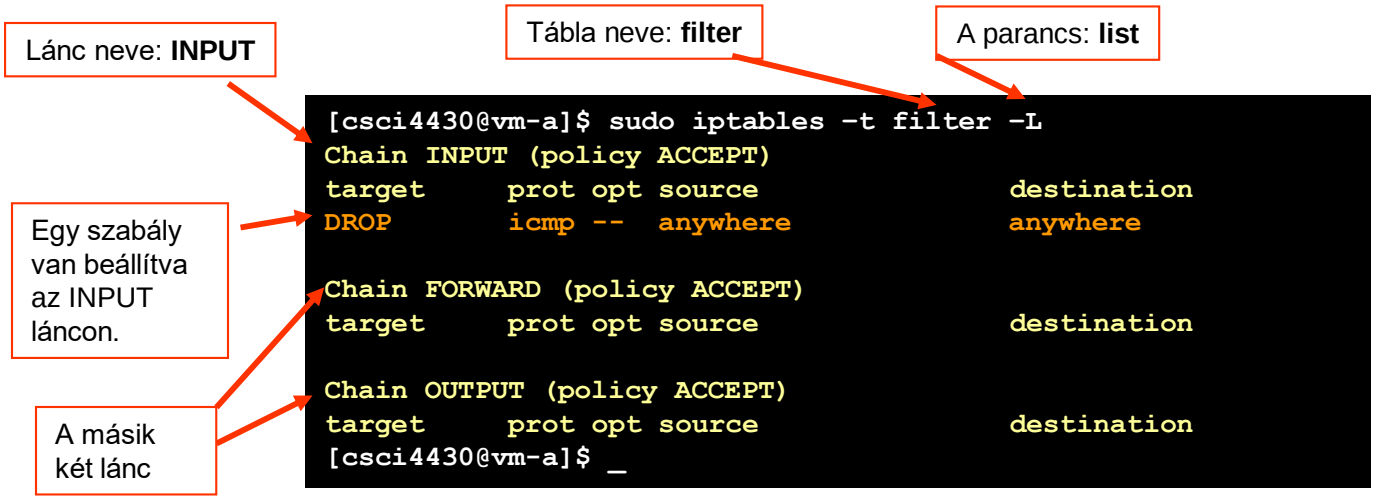
- Alapból három tábla van, amely szabályok halmazait tartalmazza
- A **filter** tábla a csomag szűrésre való
- A **nat** tábla a címfordításra való
- A **mangle** tábla a csomagok speciális célú feldolgozására való (megváltoztatja a csomagok tartalmát)
- Mindegyik táblában szabályok sorozata van, amelyeket láncoknak hívunk

iptables – filter tábla

- Itt három lánc van:
- Az INPUT láncot (az ott megadott szabályok sorozatát) bármely rendszerhez beérkező csomagra használja az alkalmazás
- Az OUTPUT láncot bármely olyan csomagra, amely a rendszerből kilép
- A FORWARD láncot pedig azokra a csomagokra, amelyek továbbítódnak a rendszeren keresztül (tehát ezeket nem a rendszernek szánták)

Forrás: The Chinese University of Hong Kong (CUHK), CSCI4430 Data Communication and Computer Networks
https://millyz.github.io/ta/csci4430_2017/Lab%20on%20iptables.ppt

iptables – filter tábla

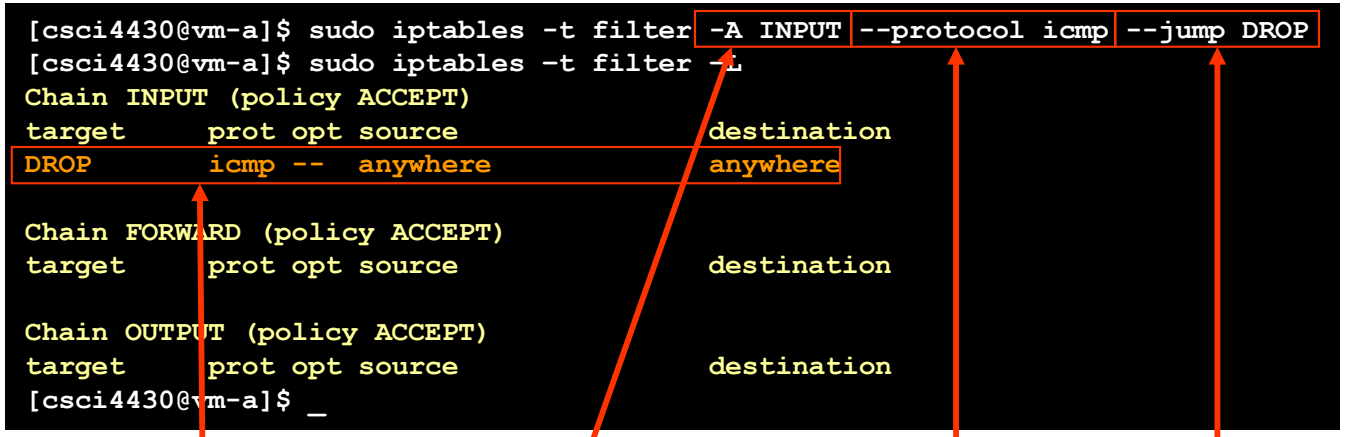


Az INPUT láncban lévő szabály jelentése:

Amikor egy ICMP hasznos teherrel rendelkező csomag áthalad az INPUT-on, DROP-olja ezt a csomagot függetlenül attól, hogy honnan jött, és hova megy.

Forrás: The Chinese University of Hong Kong (CUHK), CSCI4430 Data Communication and Computer Networks
https://millyz.github.io/ta/csci4430_2017/Lab%20on%20iptables.ppt

iptables – filter tábla



Ez a bejegyzés mutatja, hogy egy új szabály sikeresen hozzá lett adva a filter tábla INPUT láncához.

Egy új szabály hozzáadása az INPUT lánchoz.

Az ICMP protokollú csomagok lesznek érdekesek ennél a szabálynál.

Ha egy csomag áthalad az INPUT-on, és egy ICMP csomagról van szó, akkor DROP-olva lesz a csomag.

iptables – nat tábla

- Itt is három lánc van:
- Az OUTPUT lánc itt is van, de kevésbé érdekes
- A PREROUTING lánc még az előtt megváltoztatja a csomagokat mielőtt elérnék az INPUT láncot (pl. porttovábbítást szeretnénk alkalmazni)
- A POSTROUTING lánc pedig azután fogja megváltoztatni a csomagokat miután az OUTPUT láncot elhagyták (pl. a hálózati címfordítás első, egyszerűbb esete)

iptables – nat tábla

- Például szeretnénk a 192.168.1.10 IP címhez és 80-as porthoz jövő csomagot a 192.168.1.20 IP című géphez küldeni a 80-as portjához, akkor az alábbi parancsok (is) kelleni fognak:

```
iptables -t nat -A PREROUTING -p tcp –dport 80 -j DNAT –to-destination 192.168.1.20:80
```

```
iptables -t nat -A POSTROUTING -p tcp -d 192.168.12.20 –dport 80 -j SNAT –to-source 192.168.12.10
```

- (-t kapcsolóval a táblát határozzuk meg, -A PREROUTING : a szabályt a PREROUTING lánc végére szúrja be, -j a csomagcél megadására (SNAT: Source NAT, DNAT: Destination NAT))

iptables

- További példák itt:
- http://linux-training.be/networking/ch14.html
- (a forráskódok között is megvan: Chapter%A014.%A0iptables firewall.pdf)

Feladat 1: Egyszerű TCP proxy

Készítsünk egy egyszerű TCP alapú proxyt (átjátszó). A proxy a kliensek felé szerverként látszik, azaz a kliensek csatlakozhatnak hozzá. A proxy a csatlakozás után kapcsolatot nyit egy szerver felé (parancssori argumentum), majd minden a klienstől jövő kérést továbbítja a szerver felé és a szervertől jövő válaszokat pedig a kliens felé.

Pl: python netProxy.py szalaigj.web.elte.hu 9000

Webböngészőbe írjuk be: localhost:9000

Nézzük meg a megoldást!

msvcrt

- Az **msvcrt** modulnak számos olyan függvénye van, amelyek a Windows platformon hasznosak lehetnek:
  - msvcrt.**kbhit**(): *True*-val tér vissza, ha egy billentyűleütés beolvasásra vár
  - msvcrt.**getche**():
    - beolvas egy billentyűleütést,
    - visszatér az eredményül kapott karakterrel,
    - és kiírja a konzolra, ha nyomtatható karakter
    - blokkol, ha nincs billentyűleütés
    - (A *Ctrl*-*C*-t nem tudja beolvasni)

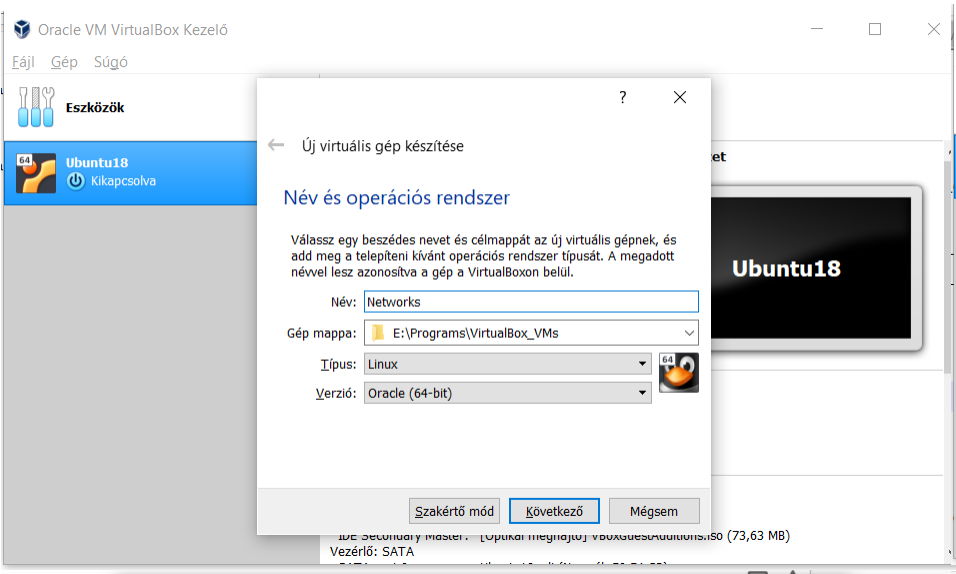
Feladat 2: Chat

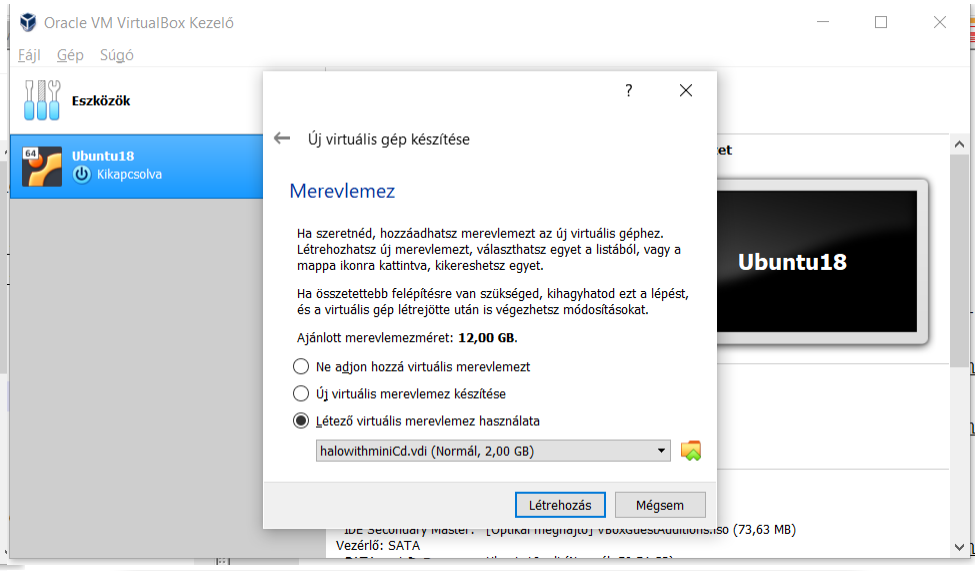
- Készítsünk egy chat alkalmazást, amelyen a chat szerverhez csatlakozott kliensek képes beszélni egymással!
- A szerver szerepe, hogy a kliensektől jövő üzenetet minden más kliensnek továbbítja névvel együtt: [<név>] <üzenet> ; pl. [Józsi] Kék az ég!
- A kliensek a szervertől jövő üzeneteket kiírják a képernyőre.
- Nézzük meg a megoldást!

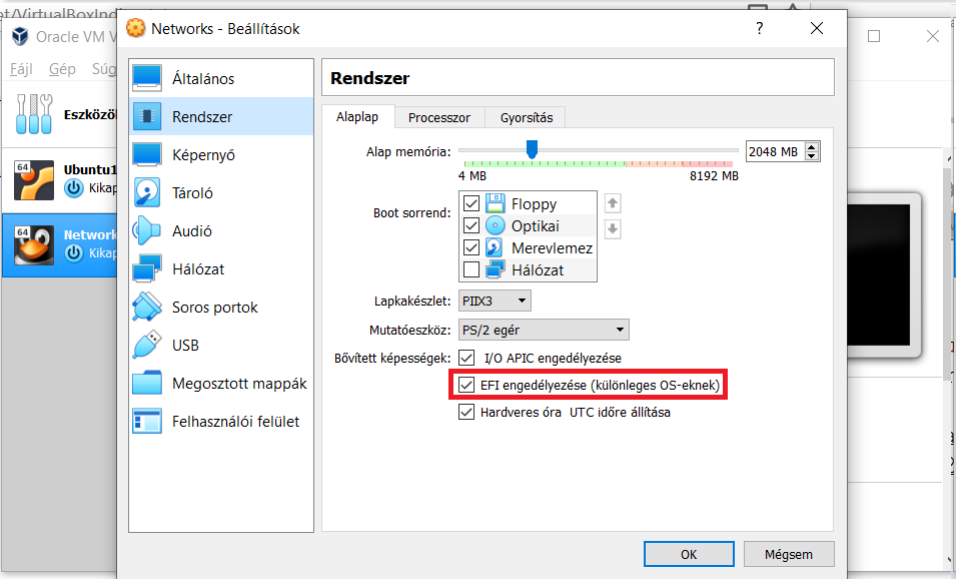
Mininet

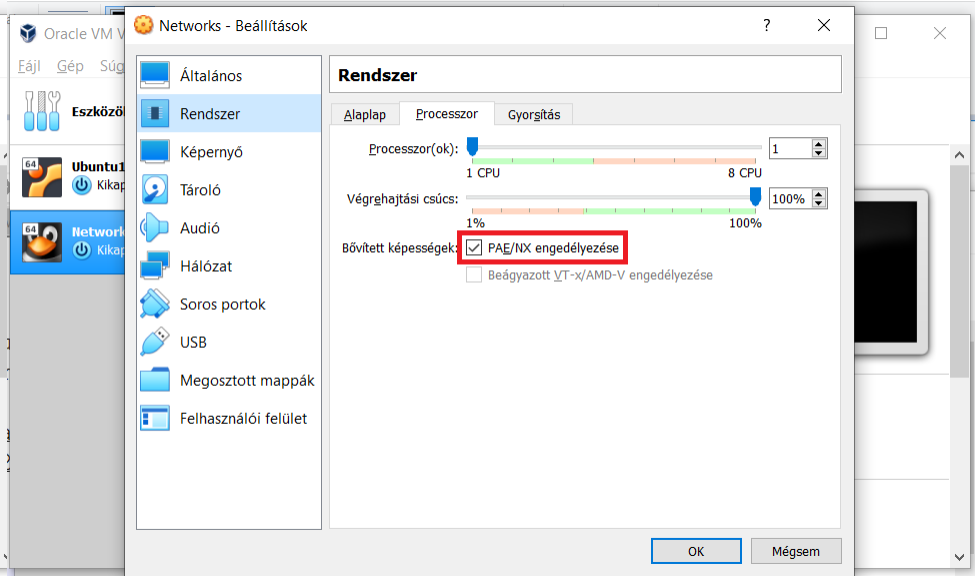
- Előfeltétel: VirtualBox telepítése: https://www.virtualbox.org/wiki/Downloads
- Töltsük le és csomagoljuk ki a tömörített lemezképet a VirtualBox-hoz: http://ggombos.web.elte.hu/oktatas/SzamHalo/mininet/halowithminiCdVirtualBox.7z
- A VirtualBox-ban készítsünk egy új VM-t úgy, hogy a kicsomagolt lemezt használja!
- Mielőtt elindítanánk:
  - Engedélyezzük az EFI-t
  - Engedélyezzük PAE/NX-t
  - A csatolt diszket a SATA-ból át kell rakni az IDE vezérlő alá
  - Network interfészt cseréljük le: Host-only-ra
- (Lásd a következő diák ábráit)

Mininet

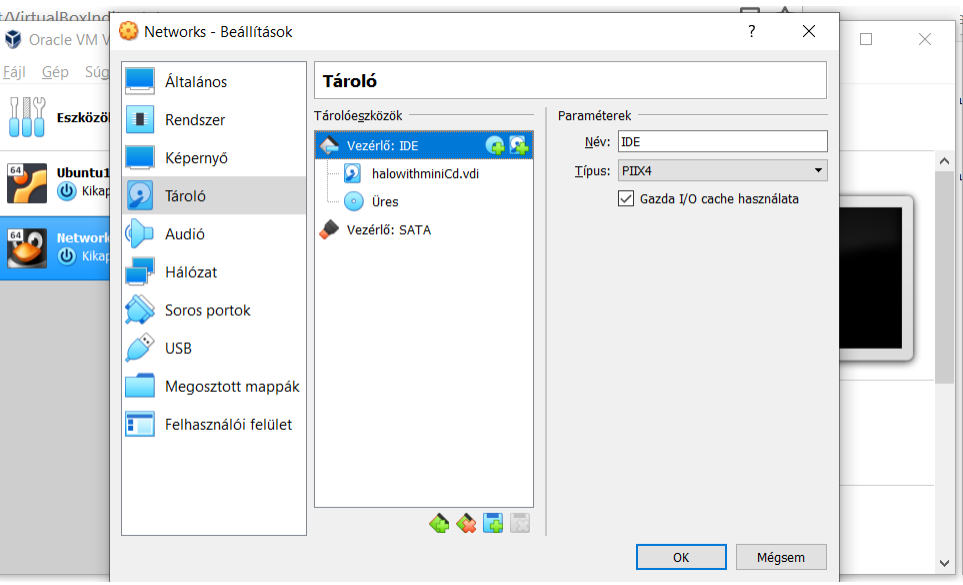

Oracle VM VirtualBox Kezelő
Fájl Gép Súgó
Eszközök
Ubuntu18
Kikapcsolva
Új virtuális gép készítése
Név és operációs rendszer
Válassz egy beszédes nevet és célmappát az új virtuális gépnek, és add meg a telepíteni kívánt operációs rendszer típusát. A megadott névvel lesz azonosítva a gép a VirtualBoxon belül.
Név: Networks
Gép mappa: E:\Programs\VirtualBox_VMs
Típus: Linux
Verzió: Oracle (64-bit)
Szakértő mód
Következő
Mégsem
Ubuntu18
Vezérlő: SATA

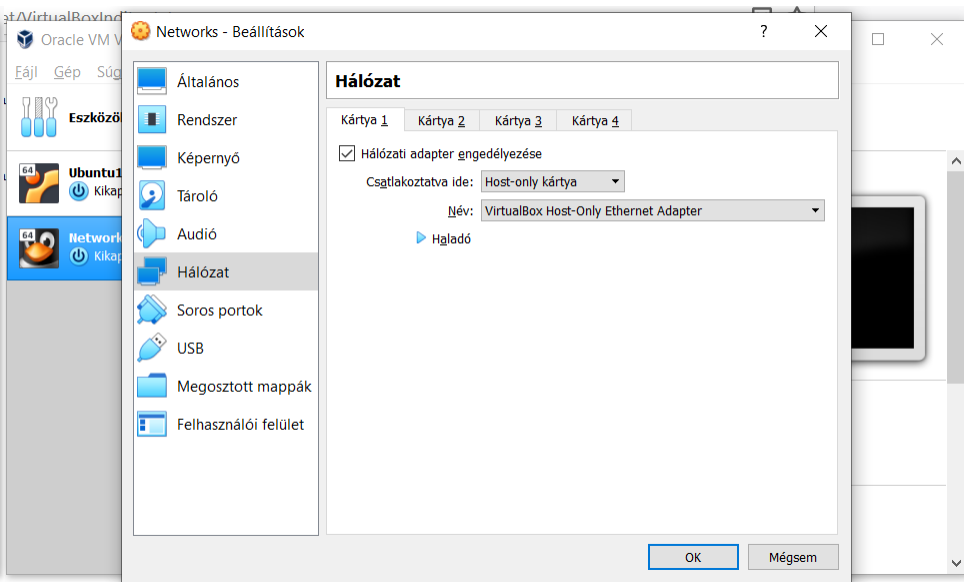

Oracle VM VirtualBox Kezelő
Fájl Gép Súgó
Eszközök
Ubuntu18
Kikapcsolva
Új virtuális gép készítése
Merevlemez
Ha szeretnéd, hozzáadhatsz merevlemezt az új virtuális géphez. Létrehozhatsz új merevlemezt, választhatsz egyet a listából, vagy a mappa ikonra kattintva, kikereshetsz egyet.
Ha összetettebb felépítésre van szükséged, kihagyhatod ezt a lépést, és a virtuális gép létrejötte után is végezhetsz módosításokat.
Ajánlott merevlemezméret: 12,00 GB.
Ne adjon hozzá virtuális merevlemezt
Új virtuális merevlemez készítése
Létező virtuális merevlemez használata
halowithminiCd.vdi (Normál, 2,00 GB)
Létrehozás
Mégsem
Ubuntu18
Vezérlő: SATA


Networks - Beállítások
Általános
Rendszer
Képernyő
Tároló
Audió
Hálózat
Soros portok
USB
Megosztott mappák
Felhasználói felület
Rendszer
Alaplap
Processzor
Gyorsítás
Alap memória:
2048 MB
4 MB
8192 MB
Boot sorrend:
Floppy
Optikai
Merevlemez
Hálózat
Lapkakészlet:
PIIX3
Mutatóeszköz:
PS/2 egér
Bővített képességek:
I/O APIC engedélyezése
EFI engedélyezése (különleges OS-eknek)
Hardveres óra UTC időre állítása
OK
Mégsem


Networks - Beállítások
Általános
Rendszer
Képernyő
Tároló
Audió
Hálózat
Soros portok
USB
Megosztott mappák
Felhasználói felület
Rendszer
Alaplap
Processzor
Gyorsítás
Processzor(ok):
1
1 CPU
8 CPU
Végrehajtási csúcs:
100%
1%
100%
Bővített képességek:
PAE/NX engedélyezése
Beágyazott VT-x/AMD-V engedélyezése
OK
Mégsem

Mininet

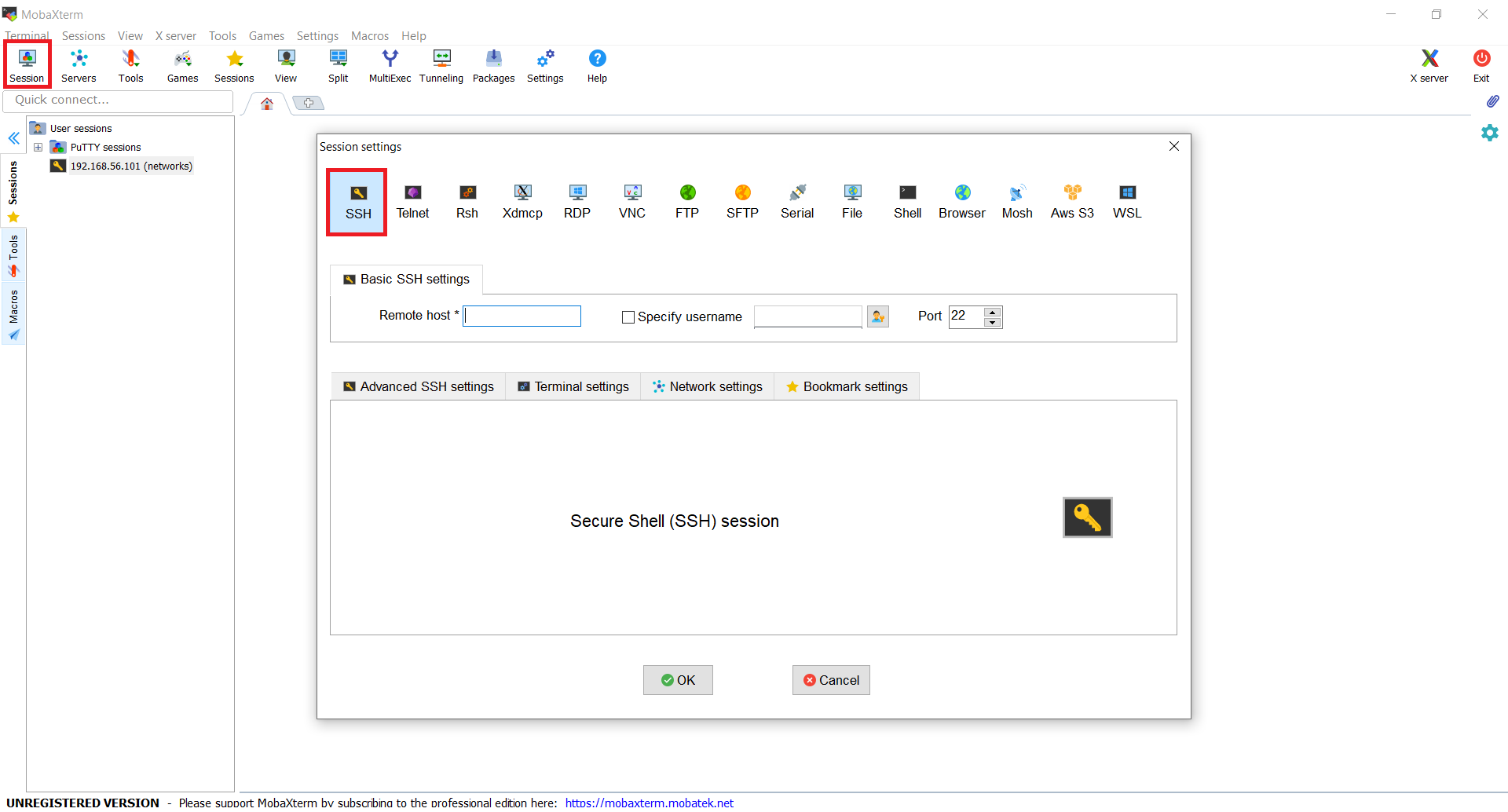

Networks - Beállítások
Általános
Rendszer
Képernyő
Tároló
Audió
Hálózat
Soros portok
USB
Megosztott mappák
Felhasználói felület
Tároló
Tárolóeszközök
Vezérlő: IDE
halowithminiCd.vdi
Üres
Vezérlő: SATA
Paraméterek
Név: IDE
Típus: PIIX4
Gazda I/O cache használata
OK
Mégsem


Networks - Beállítások
Általános
Rendszer
Képernyő
Tároló
Audió
Hálózat
Soros portok
USB
Megosztott mappák
Felhasználói felület
Hálózat
Kártya 1
Kártya 2
Kártya 3
Kártya 4
Hálózati adapter engedélyezése
Csatlakoztatva ide: Host-only kártya
Név: VirtualBox Host-Only Ethernet Adapter
Haladó
OK
Mégsem

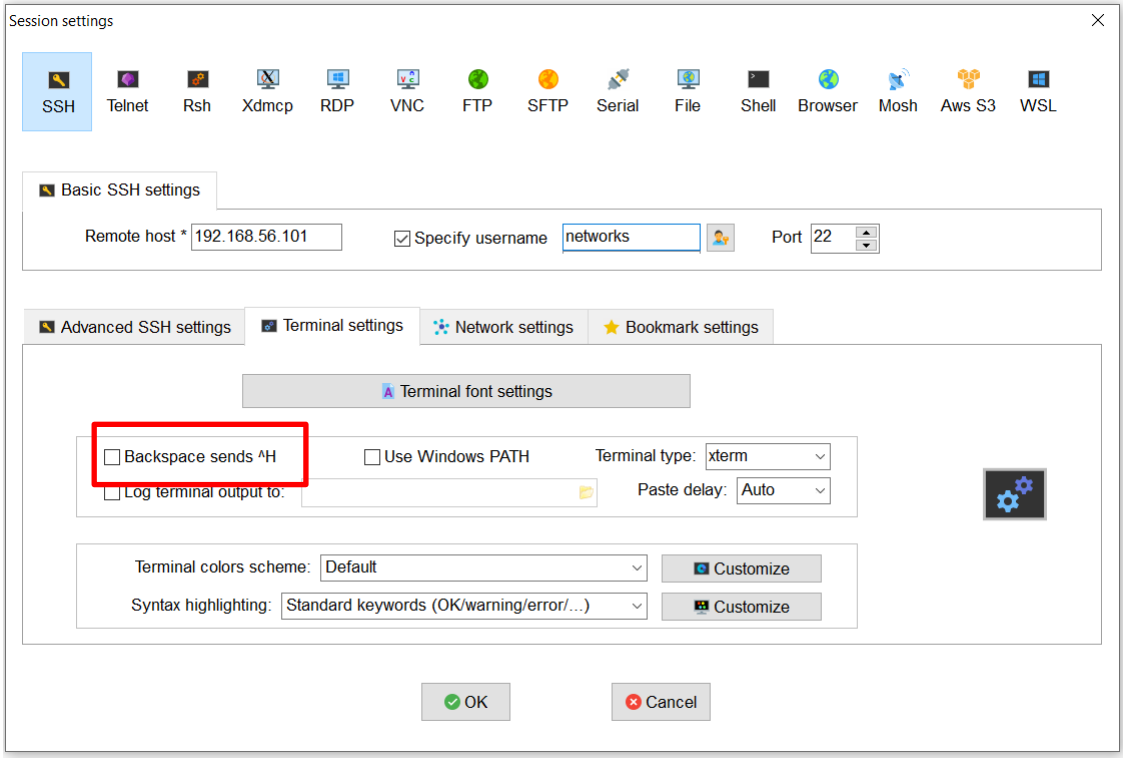
Mininet

- Ha kész, akkor indítsuk el a virtuális gépet!
  - Belépési adatok: `networks/networks`
- Ha nem kapott IP címet a gép (`ifconfig`), akkor futtassuk a `sudo dhclient` parancsot!
- Utána jegyezzük fel az IP címet (`ifconfig`)!
- Töltsük le a MobaXterm eszközt: http://ggombos.web.elte.hu/oktatas/SzamHalo/mininet/MobaXterm_Portable_v12.4.zip
- Adjuk meg a session-höz az adatokat:
  - Start a new remote session → SSH
  - Remote host: <a feljegyzett IP cím>
  - Specify username: networks
  - Port: 22

Mininet


MobaXterm
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
User sessions
PuTTY sessions
192.168.56.101 (networks)
Sessions
Tools
Macros
Session settings
SSH Telnet Rsh Xdmcp RDP VNC FTP SFTP Serial File Shell Browser Mosh Aws S3 WSL
Basic SSH settings
Remote host *
Specify username
Port 22
Advanced SSH settings
Terminal settings
Network settings
Bookmark settings
Secure Shell (SSH) session
OK
Cancel
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net

Mininet


Session settings
SSH
Telnet
Rsh
Xdmcp
RDP
VNC
FTP
SFTP
Serial
File
Shell
Browser
Mosh
Aws S3
WSL
Basic SSH settings
Remote host * 192.168.56.101
Specify username
networks
Port 22
Advanced SSH settings
Terminal settings
Network settings
Bookmark settings
Terminal font settings
Backspace sends ^H
Use Windows PATH
Terminal type: xterm
Log terminal output to:
Paste delay: Auto
Terminal colors scheme: Default
Customize
Syntax highlighting: Standard keywords (OK/warning/error/...)
Customize
OK
Cancel

Mininet

- Ubuntu 18 op. rendszer, felhasználó/jelszó: `networks/networks`
- Indítsunk egy MobaXterm session-t

Mininet

- Az alábbiakra még szükség van, hogy megfelelően működjön majd a mininet
- (Átmenetileg) át kell váltani a hálózatot „NAT”-ra vagy „bridge-elt kártya”-ra, hogy az alábbi telepítés sikeresen végrehajtódjon:

```
networks@networksELTE:~$ sudo apt install x11-xserver-utils iptables
```

- Ki kell törölni az alábbiakat:

```
networks@networksELTE:~$ rm .Xauthority
networks@networksELTE:~$ rm .Xauthority-*
networks@networksELTE:~$ exit
```

- Majd újra belépni

Mininet

- Belépés után:

```
networks@networksELTE:~$ xauth list
networksELTE:10  MIT-MAGIC-COOKIE-1  <egy alfanumerikus karaktersorozat, jelöljük S-sel>
networks@networksELTE:~$ xauth add networksELTE/unix:10 MIT-MAGIC-COOKIE-1 S
networks@networksELTE:~$ sudo xhost +
```

- Az előző dia tartalma és a mostani amiatt kell, hogy utána a mininet konzolon keresztül is működjön az xterm parancs…
- Egyébként az alábbi hiba jönne:

```
Warning: This program is an suid-root program or is being run by the root user.
The full text of the error or warning message cannot be safely formatted
in this environment. You may get a more descriptive message by running the
program as a non-root user or by removing the suid bit on the executable.
xterm: Xt error: Can't open display: %s
```

Mininet

- Indítsunk egy MobaXterm session-t
- Listázzuk az alábbi könyvtárt:

```
networks@networksELTE:~$ ls mininetScriptek/ComputerNetworks/L2-switching/
```

  - test1 topológia két fájlból áll:
  - `test1.mn`: meg lehet jeleníteni a miniedit segítségével
  - `test1.py`: egyből elindítja a hálózat emulátort

Mininet

- Indítsuk el a miniedit-et:

```
networks@networksELTE:~$ python mininet/examples/miniedit.py&
```

  - a *File* menüben meg tudjuk nyitni a `.mn` kiterjesztésű fájlokat
  - Nyissuk meg a `test1.mn` fájlt
  - A *File* menüben az „Export Level 2 Script”-tel lehet létrehozni python szkriptet

Mininet

- Nézzük meg a `test1.py`-t:

```
networks@networksELTE:~/mininetScriptek/ComputerNetworks/L2-switching$ vi test1.py
```

  - Egy `LinuxBridge`-et definiálunk, amellyel futtatni tudjuk a feszítőfa algoritmust (Spanning Tree Protocol, STP) hurkok kezelésére
  - Hozzáadunk hosztokat is, privát IP címekkel
  - Végül összekötjük ezeket a topológia alapján
  - A h1 és s1 kapcsolat sávszélessége: 10 Mbps (alapból elvileg nem limitált, a TCLink osztály azért kell, hogy limitálni tudjuk)
- Indítsuk el:

```
$ sudo python test1.py
mininet>
```

Mininet

- Elérhető csomópontok:

```
mininet> nodes
```

- Az s1 switchről infót kaphatunk
  - (brctl: ethernet bridge adminisztráció)

```
mininet> sh brctl show
```

  - Látszik, hogy nincs engedélyezve az STP
- A h1 h2 hostokon elindíthatunk egy-egy terminált:

```
mininet> xterm h1 h2
```

Mininet

- Itt lekérhetők az interface adatok, érdemes a mac címet megnézni!

```
# ifconfig
```

- Írassuk ki az ARP tábla aktuális tartalmát:

```
# arp
```

- Az s1 switch forwarding tábláját lekérdezhetjük a mininet konzolban:

```
mininet> sh brctl showmacs s1
```

Mininet

- Derítsük ki, hogy melyik interfésze van s1-nek a h2-vel összekötve (mininet konzol):

```
# mininet> links
h2-eth0<->s1-eth1 (OK OK)
...
```

- Figyeljük a forgalmat minden interfészen! mininet konzolba írva:

```
mininet> s1 tcpdump -n -i s1-eth1
```

Mininet

- Pingetés xterm ablakból: `h2` termináljából: (a `h1` `h2` nevek itt nem használhatók!)

```
# ping 10.0.0.1
```

- Írassuk ki az ARP tábla aktuális tartalmát:

```
# arp
```

Mininet

- Közben látjuk a mininet konzolban, hogy mentek ARP üzenetek
- Pingetés mininet konzolból, pl.:

```
mininet> h1 ping h2
```

- Kilépés:

```
mininet> exit
```

VÉGE
KÖSZÖNÖM A FIGYELMET!