UFW tűzfal telepítése és konfigurálása az a Debian 11.05 rendszeren

https://hostpresto.com/community/tutorials/install-and-configure-ufw-firewall-on-ubuntu-16-04/
https://blog.cherryservers.com/how-to-configure-ubuntu-firewall-with-ufw
https://www.liquidweb.com/kb/installing-using-ufw-ubuntu-16-04-lts/
https://www.tutorialspoint.com/how-to-configure-and-set-up-a-firewall-on-ubuntu-16-04
https://www.cyberciti.biz/faq/howto-configure-setup-firewall-with-ufw-on-ubuntu-linux/
https://help.ubuntu.com/community/UFW
https://help.ubuntu.com/community/Firewall

A biztonság nagyon fontos szempont, amikor saját szervert futtat. Az **UFW (Uncomplicated Firewall, egyszerű tűzfal)** egy frontend a tűzfalszabályok kezelésére, és könnyen használható gazdagép alapú tűzfalakhoz. Az UFW a parancssori felületen keresztül használható, és célja a tűzfal konfigurálásának egyszerűsítése.

Az **Iptables** a rendszergazdák által használt egyik legnépszerűbb tűzfaleszköz. A bejövő és kimenő kapcsolatok kezelésére és védelmére szolgál a kiszolgálón, de az iptables konzol módban fut, és nagyon bonyolult a kezelése és konfigurálása. Az ufw egy alkalmazástűzfal, amely az Ubuntu iptables alapú tűzfalának kezelésére szolgál, és amely keretet ad a netfilter szabályok kezeléséhez, valamint parancssori felületet biztosít a tűzfalszabályok vezérléséhez.

Az **UFW tűzfal** segítségével különféle szolgáltatásokat engedélyezhet és blokkolhat port, hálózati interfész és forrás IP-cím szerint.

Ebben az anyagban megtanuljuk az UFW-parancsokat különböző opciókkal, hogy biztosítsa a különféle szolgáltatásokat az Ubuntu 16.04-en.

UFW telepítése

A szolgáltatást könnyen telepítheti a következő parancsok futtatásával:

```
sudo  apt-get  update
sudo  apt-get  install  ufw
```

Az UFW állapotát a következő parancs futtatásával is ellenőrizheti:

```
sudo  ufw  status
```

A következő kimenetet kell látnia:

```
tanulo@debian:~$ sudo ufw status
Status: inactive
tanulo@debian:~$
```

Ha a fenti kimenetet látja, az azt jelenti, hogy nem aktív. A következő parancs futtatásával engedélyezheti:

```
sudo  ufw  enable
```

```
tanulo@debian:~$ sudo ufw enable
Firewall is active and enabled on system startup
tanulo@debian:~$
```

Magyarul:

```
A tűzfal aktív és engedélyezett rendszerindításkor
```

Ha szeretné letiltani az tűzfalat, akkor futtassa a következő parancsot **(Most nem adja ki ezt a parancsot!)**:

```
sudo ufw disable
```

Az aktuális UFW-szabályok listázása

Az alapértelmezett tűzfalszabályokat a következő paranccsal listázhatja:

```
sudo ufw status verbose
```

A következő kimenetet kell látnia:

```
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), deny (routed)
New profiles: skip
```

Magyarul:

```
tanulo@server:~$ sudo ufw status verbose
Állapot: aktív
Naplózás: on (low)
Alapértelmezett: deny (bejövő), allow (kimenő), disabled (route-olt)
Új profilok: skip
```

Láthatja, hogy alapértelmezés szerint minden bejövő kapcsolat le van tiltva.

Bejövő kapcsolatok engedélyezése

Ha távoli gépről szeretné elérni a rendszert, akkor engedélyeznie kell az SSH-kapcsolatokat.

Az SSH-t a következő parancs futtatásával engedélyezheti:

```
sudo ufw allow ssh
```

vagy

```
sudo ufw allow 22/tcp
```

Kimenet:

```
Rule added
Rule added (v6)
```

Magyarul:

```
tanulo@server:~$ sudo ufw allow ssh
Szabály hozzáadva
Szabály hozzáadva (v6)
```

vagy

```
tanulo@server:~$ sudo ufw allow 22/tcp
Szabály hozzáadva
Szabály hozzáadva (v6)
```

Most ellenőrizze az ufw állapotát:

```
sudo ufw status
```

A kimenetet így kell látnia:

```
Status: active

To                         Action      From
--                         ------      ----
22                         ALLOW       Anywhere
22/tcp                     ALLOW       Anywhere
22 (v6)                    ALLOW       Anywhere (v6)
22/tcp (v6)                ALLOW       Anywhere (v6)
```

Magyarul:

```
tanulo@server:~$ sudo ufw status
Állapot: aktív

Címzett                    Művelet     Feladó
-------                    -------     ------
22                         ALLOW       Anywhere
22/tcp                     ALLOW       Anywhere
22 (v6)                    ALLOW       Anywhere (v6)
22/tcp (v6)                ALLOW       Anywhere (v6)
```

Bejövő kapcsolatok megtagadása

Ha meg akarja tagadni a hozzáférést egy bizonyos porthoz, akkor a következő formátumot használhatja **(FIGYELEM! Ezt nem kell begépelnie!)**:

```
sudo ufw deny " Port/Protocol"
```

Például megtagadhatja a hozzáférést a 80-as porthoz a következő parancs futtatásával:

```
sudo ufw deny 80/tcp
```

```
tanulo@server:~$ sudo ufw deny 80/tcp
Szabály hozzáadva
Szabály hozzáadva (v6)
```

Porttartomáyok (Port Range) engedélyezése

Porttartományokat is hozzáadhat a szabályokhoz. Például, ha engedélyezni szeretné a 2100 és 2200 közötti portokat a tcp protokollal, akkor futtassa a következő parancsot:

```
sudo ufw allow 2100:2200/tcp
```

```
tanulo@server:~$ sudo ufw allow 2100:2200/tcp
Szabály hozzáadva
Szabály hozzáadva (v6)
```

Most ellenőrizze az ufw állapotát:

```
sudo ufw status
```

A következő kimenetet kell látnia:

```
Status: active

To                         Action   From
--                         ------   ----
22                         ALLOW    Anywhere
22/tcp                     ALLOW    Anywhere
80/tcp                     DENY     Anywhere
2100:2200/tcp              ALLOW    Anywhere
22 (v6)                    ALLOW    Anywhere (v6)
22/tcp (v6)                ALLOW    Anywhere (v6)
80/tcp (v6)                DENY     Anywhere (v6)
2100:2200/tcp (v6)         ALLOW    Anywhere (v6)
```

Magyarul:

```
tanulo@server:~$ sudo ufw status
Állapot: aktív

Címzett                    Művelet     Feladó
-------                    -------     ------
22                         ALLOW       Anywhere
22/tcp                     ALLOW       Anywhere
80/tcp                     DENY        Anywhere
2100:2200/tcp              ALLOW       Anywhere
22 (v6)                    ALLOW       Anywhere (v6)
22/tcp (v6)                ALLOW       Anywhere (v6)
80/tcp (v6)                DENY        Anywhere (v6)
2100:2200/tcp (v6)         ALLOW       Anywhere (v6)
```

Alkalmazásprofilok

Kilistázhatja a helyi rendszeren elérhető alkalmazásprofilokat. Ehhez futtassa a következő parancsot:

```
sudo ufw app list
```

Kimenet:

```
    Available applications:
      OpenSSH
      Samba
```

Magyarul:

```
tanulo@server:~$ sudo ufw app list
Elérhető alkalmazások:
  OpenSSH
  Samba
```

FIGYELEM! előfordulhat az is, hogy nincs a listában semmi, mivel még nincs telepítve alkalmazás (szolgáltatás).

A profillal és a benne foglalt szabályokkal kapcsolatos információk listázásához futtassa a következő parancsot **(FIGYELEM! Ezt nem kell begépelnie!)**:

```
sudo ufw app info "App Name"
```

Ha például az SSH-profilra vonatkozó információkat szeretne megtudni, futtassa a következő parancsot:

```
sudo ufw app info OpenSSH
```

Kimenet:

```
tanulo@server:~$ sudo ufw app info OpenSSH
Profil: OpenSSH
Cím: Secure shell server, an rshd replacement
Leírás: OpenSSH is a free implementation of the Secure Shell protocol.

Port:
  22/tcp
```

Hozzáférés engedélyezése adott IP-címekről

Egy adott porthoz való hozzáférést is engedélyezheti adott IP-címről. Például, ha azt szeretné, hogy az IP 192.168.0.2 csak a 22-es porthoz férhessen hozzá, futtassa a következő parancsot:

```
sudo ufw allow from 192.168.0.2 to any port 22
```

```
tanulo@server:~$ sudo ufw allow from 192.168.0.2 to any port 22
Szabály hozzáadva
tanulo@server:~$
```

Ellenőrzés:

```
tanulo@server:~$ sudo ufw status
Állapot: aktív

Címzett                    Művelet     Feladó
-------                    -------     ------
22                         ALLOW       Anywhere
22/tcp                     ALLOW       Anywhere
80/tcp                     DENY        Anywhere
2100:2200/tcp              ALLOW       Anywhere
22                         ALLOW       192.168.0.2
22 (v6)                    ALLOW       Anywhere (v6)
22/tcp (v6)                ALLOW       Anywhere (v6)
80/tcp (v6)                DENY        Anywhere (v6)
2100:2200/tcp (v6)         ALLOW       Anywhere (v6)
```

UFW szabályok törlése

Törölhet bizonyos ufw szabályokat. Először fel kell sorolnia az ufw szabályokat, majd ezeket eltávolíthatja.

Futtassa a következő parancsot az ufw szabályok listázásához:

```
sudo ufw status numbered
```

Kimenet:

```
Status: active

To                         Action      From
--                         ------      ----
[ 1] 22                    ALLOW IN    Anywhere
[ 2] 22/tcp                ALLOW IN    Anywhere
[ 3] 80/tcp                DENY IN     Anywhere
[ 4] 2100:2200/tcp         ALLOW IN    Anywhere
[ 5] 22                    ALLOW IN    192.168.0.2
[ 6] 22 (v6)               ALLOW IN    Anywhere (v6)
[ 7] 22/tcp (v6)           ALLOW IN    Anywhere (v6)
[ 8] 80/tcp (v6)           DENY IN     Anywhere (v6)
[ 9] 2100:2200/tcp (v6)    ALLOW IN    Anywhere (v6)
```

Magyarul:

```
tanulo@server:~$ sudo ufw status numbered
Állapot: aktív

     Címzett                    Művelet     Feladó
     -------                    -------     ------
[ 1] 22                         ALLOW IN    Anywhere
[ 2] 22/tcp                     ALLOW IN    Anywhere
[ 3] 80/tcp                     DENY IN     Anywhere
[ 4] 2100:2200/tcp              ALLOW IN    Anywhere
[ 5] 22                         ALLOW IN    192.168.0.2
[ 6] 22 (v6)                    ALLOW IN    Anywhere (v6)
[ 7] 22/tcp (v6)                ALLOW IN    Anywhere (v6)
[ 8] 80/tcp (v6)                DENY IN     Anywhere (v6)
[ 9] 2100:2200/tcp (v6)         ALLOW IN    Anywhere (v6)
```

A szabályok bármelyikének eltávolításához ezeket a számokat kell használnia. **(FIGYELEM! Ezt nem kell begépelnie!)**:

```
sudo ufw delete number
```

Például, ha el szeretné távolítani a harmadik számú szabályt, futtassa a következő parancsot:

```
sudo ufw delete 3
```

```
tanulo@server:~$ sudo ufw delete 3
Törlés:
 deny 80/tcp
Folytatja a műveletet (i|n)? i
Szabály törölve
tanulo@server:~$ _
```

Ellenőrzés:

```
tanulo@server:~$ sudo ufw status
[sudo] tanulo jelszava:
Állapot: aktív

Címzett                    Művelet     Feladó
-------                    -------     ------
22                         ALLOW       Anywhere
22/tcp                     ALLOW       Anywhere
2100:2200/tcp              ALLOW       Anywhere
22                         ALLOW       192.168.0.2
22 (v6)                    ALLOW       Anywhere (v6)
22/tcp (v6)                ALLOW       Anywhere (v6)
80/tcp (v6)                DENY        Anywhere (v6)
2100:2200/tcp (v6)         ALLOW       Anywhere (v6)
```

Ha vissza kell térnie az alapértelmezett beállításokhoz, egyszerűen írja be a következő parancsot. Ezzel minden módosítást visszaállít.

```
sudo  ufw  reset
```

```
tanulo@server:~$ sudo ufw reset
Az összes szabály visszaállítása a telepített alapértelmezésekre. Folytatja
a műveletet (i|n)? i
„user6.rules” biztonsági mentése ide: „/etc/ufw/user6.rules.20220129_115451”
„user.rules” biztonsági mentése ide: „/etc/ufw/user.rules.20220129_115451”
„before.rules” biztonsági mentése ide: „/etc/ufw/before.rules.20220129_115451”
„before6.rules” biztonsági mentése ide: „/etc/ufw/before6.rules.20220129_115451”
„after.rules” biztonsági mentése ide: „/etc/ufw/after.rules.20220129_115451”
„after6.rules” biztonsági mentése ide: „/etc/ufw/after6.rules.20220129_115451”

tanulo@server:~$ _
```

Ellenőrzés:

```
tanulo@server:~$ sudo ufw status
Állapot: inaktív
tanulo@server:~$
```

UFW tűzfalesemények naplózása

A tűzfalnaplók szükségesek a tűzfalszabályok hibaelhárításához és a hálózaton zajló szokatlan tevékenységek értesítéséhez. Tehát naplózási szabályokat kell hozzáadnia a tűzfalához. Az ufw naplófájl a **/var/log/ufw.log** címen található.

A naplózást a következő parancs futtatásával kapcsolhatja be:

```
sudo  ufw  logging  on
```

```
tanulo@server:~$ sudo ufw logging on
Naplózás bekapcsolva
```

A naplózást a következő parancs futtatásával kapcsolhatja ki:

```
sudo ufw logging off
```

```
tanulo@server:~$ sudo ufw logging off
Naplózás kikapcsolva
```

Az UFW több **alacsony**, **közepes** és **magas** naplózási szintet támogat. Az alapértelmezett ufw naplózási szint **alacsony**.

Különböző naplózási szinteket állíthat be a következő parancs futtatásával **(FIGYELEM! Ezt nem kell begépelnie!)**:

```
sudo  ufw  logging  low|medium|high
```

- **Alacsony:** naplózza az összes blokkolt csomagot, amely nem felel meg az alapértelmezett házirendnek, valamint az előre beállított szabályoknak megfelelő csomagokat.
- **Közepes:** ugyanaz, mint fent, plusz az összes engedélyezett csomag, amely nem egyezik a meghatározott házirenddel, minden érvénytelen csomag és minden új kapcsolat.
- **Magas:** ugyanaz, mint fent, csak sebességkorlátozás nélkül, plusz az összes csomag sebességkorlátozással.

Például, ha szeretnénk beállítani közepes szintet, akkor futtassuk az alábbi parancsot:

```
sudo  ufw  logging  medium
```

```
tanulo@server:~$ sudo ufw logging medium
Naplózás bekapcsolva
```

Speciális UFW szabályok

Az **ufw**-val mindent megtehet, amire az **iptables** képes. A parancssor használatával csak egyszerű szabályokat adhat hozzá. Ha további speciális szabályokat szeretne hozzáadni, akkor ezt több ufw konfigurációs fájl szerkesztésével érheti el.

- **/etc/default/ufw** : Ez az alapértelmezett házirend- és kernelmodulok fő ufw konfigurációs fájlja.
- **/etc/ufw/before.rules** : Ezekben a fájlokban a szabályok az ufw paranccsal hozzáadott szabályok előtt kerülnek feldolgozásra.
- **/etc/ufw/after.rules** : Az ezekben a fájlokban lévő szabályok az ufw paranccsal hozzáadott szabályok után kerülnek feldolgozásra.

Az UFW alapértelmezés szerint engedélyezi a DHCP-t, a ping-et és a visszacsatolást (loopback). Ezt letilthatja a **before.rules** fájl szerkesztésével.

```
sudo  nano  /etc/ufw/before.rules
```

Helyezze kommentbe (azaz írjon az első sorba # karaktert) a következő sorokat:

```
# allow all on loopback
#-A ufw-before-input -i lo -j ACCEPT
#-A ufw-before-output -o lo -j ACCEPT

# ok icmp codes for INPUT
#-A ufw-before-input -p icmp --icmp-type destination-unreachable -j ACCEPT
#-A ufw-before-input -p icmp --icmp-type source-quench -j ACCEPT
#-A ufw-before-input -p icmp --icmp-type time-exceeded -j ACCEPT
#-A ufw-before-input -p icmp --icmp-type parameter-problem -j ACCEPT
#-A ufw-before-input -p icmp --icmp-type echo-request -j ACCEPT

# allow dhcp client to work
#-A ufw-before-input -p udp --sport 67 --dport 68 -j ACCEPT
```

A fájl mentése után, tiltsa le, majd engedélyezze újra az ufw-t a módosítások befrissítéséhez:

```
sudo  ufw  disable
sudo  ufw  enable
```

```
tanulo@server:~$ sudo ufw disable
A tűzfal leállítva és elindulása letiltva a rendszer elindulásakor
tanulo@server:~$ sudo ufw enable
A tűzfal aktív és engedélyezett rendszerindításkor
tanulo@server:~$ _
```

Ellenőrzés:

```
tanulo@server:~$ ping 192.168.0.1
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.
^C
--- 192.168.0.1 ping statistics ---
41 packets transmitted, 0 received, 100% packet loss, time 40318ms

tanulo@server:~$ _
```

Végül adja ki a következő parancsot:

```
sudo  ufw  disable
```

UFW Súgó

Az ufw összes elérhető kapcsolójának listázásához futtassa a következő parancsot:

```
sudo ufw -h
```

Kimenet:

```
Usage: ufw COMMAND

Commands:
 enable                          enables the firewall
 disable                         disables the firewall
 default ARG                     set default policy
 logging LEVEL                   set logging to LEVEL
 allow ARGS                      add allow rule
 deny ARGS                       add deny rule
 reject ARGS                     add reject rule
 limit ARGS                      add limit rule
 delete RULE|NUM                 delete RULE
 insert NUM RULE                 insert RULE at NUM
 route RULE                      add route RULE
 route delete RULE|NUM           delete route RULE
 route insert NUM RULE           insert route RULE at NUM
 reload                          reload firewall
 reset                           reset firewall
 status                          show firewall status
 status numbered                 show firewall status as numbered list of RULES
 status verbose                  show verbose firewall status
 show ARG                        show firewall report
 version                         display version information

Application profile commands:
 app list                        list application profiles
 app info PROFILE                show information on PROFILE
 app update PROFILE              update PROFILE
 app default ARG                 set default application policy
```

UFW grafikus interfész kilensre

A GUFW egy grafikus felület az ufw számára.
A GUFW-t telepítheti a következő parancsok futtatásával:

```
sudo apt-get update
```

```
sudo apt-get install gufw
```

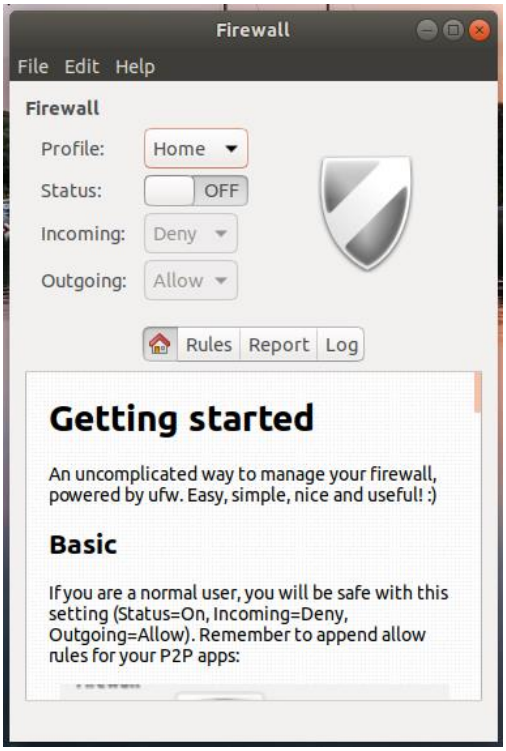
FIGYELEM! A feladatot az Ubuntu vagy az Xubuntu kliensen végezze el a Terminalban!

```
tanulo@ubuntu-kliens:~$ sudo apt-get update
```

```
tanulo@ubuntu-kliens:~$ sudo apt-get install gufw
```

Az alkalmazás elindítása:

```
tanulo@ubuntu-kliens:~$ gufw
```


Firewall
File Edit Help
Firewall
Profile: Home
Status: OFF
Incoming: Deny
Outgoing: Allow
Rules Report Log
Getting started
An uncomplicated way to manage your firewall, powered by ufw. Easy, simple, nice and useful! :)
Basic
If you are a normal user, you will be safe with this setting (Status=On, Incoming=Deny, Outgoing=Allow). Remember to append allow rules for your P2P apps: