

[< Linux](#)

Szerver előkészítése

- **Szerző:** Sallai András
- Copyright © Sallai András, 2018
- [CC Attribution-Share Alike 4.0 International](#)
- Web: <http://szit.hu>

Bevezetés

Amikor telepítesz egy új Debian GNU/Linux szerveret, érdemes néhány beállítást elvégezni. Ezzel növeljük a rendszer biztonságát, megbízhatóságát.

Új felhasználó készítése

Készítsünk egy felhasználót a root helyet, akinek a nevében elvégezzük majd a rendszergazdai feladatokat.

Az új felhasználónak a sudoval adhatunk jogokat, ezért telepítenünk kell azt:

```
apt install sudo
```

Válasszunk egy tetszőleges adminisztrátori nevet. Legyen például admina. Vegyük fel a felhasználót:

```
adduser admina
```

Tegyük a sudo csoportba:

```
usermod -aG sudo admina
```

Alaptűzfal beállítása

Láncok ürítése:

```
iptables -F
```

Saját láncok törlése:

```
iptables -X
```

Számlálók nullázása:

iptables -Z

Nat tábla láncainak ürítése:

```
iptables -t nat -F
```

Alapértelmezett irányelvek, minden tiltva, kivéve kifelé:

```
iptables -P FORWARD DROP
iptables -P INPUT DROP
iptables -P OUTPUT ACCEPT
```

A már meglévő kapcsolatok engedélyezése:

```
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Helyi kapcsolatok engedélyezése:

```
iptables -A INPUT -s 127.0.0.0/8 -d 127.0.0.0/8 -i lo -j ACCEPT
```

SSH engedélyezése befele:

```
iptables -A INPUT -p tcp --dport 22 -m state --state NEW -j ACCEPT
```

A tűzfal perzisztensé tétele

A szükséges csomag telepítése:

```
apt install netfilter-persistent
```

Plugin telepítése:

```
apt install iptables-persistent
```

Igaz, ez utóbbi telepítésével fel kerül a netfilter-persistent csomag is.

A csomag konfiguráló rákérdez, hogy szeretnénk a meglévő tűzfal szabályokat menteni. Ezt megteszi IPv4 és IPv6 esetén:

Csomag konfiguráció

| iptables-persistent konfigurálása |

Current iptables rules can be saved to the configuration file /etc/iptables/rules.v4. These rules will then be loaded automatically during system startup.

Rules are only saved automatically during package installation. See the manual page of `iptables-save(8)` for instructions on keeping the rules file up-to-date.

Save current IPv4 rules?

<Igen>

<Nem>

Csomag konfiguráció

| iptables-persistent konfigurálása |

Current iptables rules can be saved to the configuration file `/etc/iptables/rules.v6`. These rules will then be loaded automatically during system startup.

Rules are only saved automatically during package installation. See the manual page of `ip6tables-save(8)` for instructions on keeping the rules file up-to-date.

Save current IPv6 rules?

<Igen>

<Nem>

Újrakonfigurálás:

```
dpkg-reconfigure iptables-persistent
```

De kézzel is elmenthetjük tűzfal-szabályokat:

```
iptables-save >/etc/iptables/rules.v4
ip6tables-save >/etc/iptables/rules.v6
```

A `iptables-persistent` csomag függőségként telepíti a `netfilter-persistent` csomagot. Ezzel a tűzfal perzisztenciája szabályozható:

```
netfilter-persistent flush
netfilter-persistent save
```

- A `flush` parancs az aktuális tűzfal szabályokat törli.
- A `save` parancs elmenti az aktuális tűzfal szabályokat, a visszaállításhoz.

Távoli hozzáférés engedélyezése

Távoli bejelentkezéshez használjunk SSH kulcsot.

A helyi gépen készítsük el a nyilvános kulcspárt.

```
ssh-keygen -t rsa
```

Létrejön egy `$HOME/.ssh/id_rsa` titkos kulcs, és egy `$HOME/.ssh/id_rsa.pub` nyilvános kulcs.

A nyilvános kulcsot másoljuk a távoli gépre. Ehhez adjuk ki a parancsot helyben:

```
scp $HOME/.ssh/id_rsa.pub janos@192.168.5.6:/tmp/id_rsa.pub
```

A távoli gépen tegyük a nyilvános kulcsot a helyére:

```
cat /tmp/id_rsa.pub >> /home/janos/.ssh/authorized_keys
```

Az alábbi helyen leírást talál a kulcsalapú hitelesítésről:

- [Kulcs alapú hitelesítés](#)

Függelék

Ufw tűzfal

Az ufw azt ígéri egyszerűbben állíthatjuk be a tűzfalat. Az ufw a telepítendő csomag neve, és a használható parancs is ez.

Telepítés:

```
apt install ufw
```

Az ufw gyorsan munkára bírható. Engedélyezzük a távoli SSH elérést:

```
ufw allow ssh
```

Engedélyezzük magát a tűzfalat:

```
ufw enable
```

Ellenőrizzük:

```
ufw status
```

Az ufw csomaggal kialakított tűzfal újraindítás után is működik, így nem kell külön gondoskodni róla.

Tűzfal szabályok automatizálása egyszerűen

Ebben a részben a tűzfal szabályokat egyszerűen egy fájlba mentjük, amit egy scripttel töltünk vissza az `/etc/network` könyvtár segítségével. A szükséges programok a `iptables-save` és `iptables-restore`, de ezek alapból telepítésre kerülnek, az `iptables` paranccsal együtt.

Mentsük el a tűzfal aktuális állapotát egy fájlba. Például:

```
iptables-save > /etc/iptables.up.rules
```

Hozzunk létre egy scriptet a /etc/network/if-pre-up.d/ könyvtárban:

```
nano /etc/network/if-pre-up.d/iptables
```

A tartalma a következő legyen:

```
#!/bin/sh  
/sbin/iptables-restore < /etc/iptables.up.rules
```

Adjunk futtatási jogot a scriptre:

```
chmod +x /etc/network/if-pre-up.d/iptables
```

Természetesen megoldás lenne, egy systemd script írása is.

Forrás

- <https://www.digitalocean.com/> (2018)
- <https://wiki.debian.org/DebianFirewall> (2018)
- <https://wiki.debian.org/iptables> (2018)

From:
<http://szit.hu/> - **SzitWiki**

Permanent link:
<http://szit.hu/doku.php?id=oktatas:linux:el%C5%91k%C3%A9sz%C3%ADt%C3%A9s>

Last update: **2018/08/07 13:39**

