© Kiskapu Kft. Minden jog fenntartva

A proftpd beállítása

Egy sokoldalú FTP-kiszolgáló Apache-szerű beállítóállománnyal.

Az FTP (File Transfer Protocol) egy igen régóta méltán népszerű protokoll, amelyet elsősorban hatékony állományátvitelre terveztek. Mind belső hálózaton, mind az Interneten rengeteg felhasználási területe létezik. Te is könnyedén felállíthatsz egy FTP-kiszolgálót, viszont biztonságos beállításához több kell egy deb-, vagy egy RPM-csomag telepítésénél. Az FTP igen összetett protokoll, ugyanakkor a vonatkozó rfc elolvasásával közelebb kerülhetsz a megismeréséhez. Ajánlom az rfc959-t, amely Debian alatt a `proftpd-doc` csomag része, és `/usr/share/doc/proftpd-doc/rfc/rfc0959.txt.gz` néven érhető el. Mint láthatod, a `proftpd` telepítését Debian Woody alatt mutatom be, 2.4.19-es rendszermaggal és a Netfilter használatával. A parancsok más terjesztésekben eltérhetnek ettől, de a telepítés menete nagy vonalakban ugyanaz.

Active és passive mód

A lustábbak kedvéért a fontosabb fogalmakat itt ismertetem, de ez nem jelenti azt, hogy felesleges lenne elolvasni a fellel-hető leírásokat. Ne felejtsd el, hogy a különböző fórumokon (levelezőlistákon, IRC-n stb.) nem szívesen foglalkoznak olyan kérdésekkel, amelyekre valahol már léteznek válaszok.
Egy jellemző FTP-kapcsolat a következőképpen fest: az ügyfél csatlakozik a kiszolgáló egy megadott kapujára (alapesetben ez a `21/tcp - ftp`). Ha a hitelesítés sikeres volt, a kapcsolat további része az eggyel alacsonyabb számú kapun folytatódik (`20/tcp - ftp-data`). Ezt követően kétféleképpen történhet a fájlátvitel. Active módban a kiszolgáló csatlakozik az ügyfél egyik kapujára, míg passive módban az ügyfél kapcsolódik a kiszolgálóhoz. A passive mód az alapértelmezett – ez a tűzfalazásnál nyerhet nagy jelentőséget. A témától elszakadva: egy szigorú tűzfal esetén jó ötlet lehet a belső hálóról active módban elérni egy FTP-kiszolgálót az Interneten, ha passive módban nem sikerül állományokat letölteni. Láthatod, hogy az active, illetve passive mód a kiszolgáló oldaláról nézve működő vagy tétlen.

A proftpd telepítése

A Debian Woodyban található `proftpd` csomag egy megbízható változatot tartalmaz (1.2.5), így szerény véleményem szerint a kiszolgálót felesleges forrásból telepíteni. Ha valakinek mégis ez a rigolyája, az 1.2.7 változatszámút az ➲ ftp://ftp.proftpd.org/distrib/source/proftpd-1.2.7.tar.bz2 címről töltheti le, illetve a 45. CD Magazin/Proftpd könyvtárában található. A deb-csomagot `dselect`-tel vagy egy hasonló `apt`-előtéttel célszerű telepíteni. A forrás lefordítása nem különösebben nehéz feladat:

```
# mv proftpd-1.2.7.tar.bz2 /usr/src
# cd /usr/src
# bzcat proftpd-1.2.7.tar.bz2 | tar xv
# cd proftpd-1.2.7
# ./configure --prefix=/usr
# make
# make install
```

A deb-csomag telepítése során a `debconf` felteszi azt a kérdést, hogyaz FTP-kiszolgálót ***standalone*** (önálló) vagy `inetd` módban szeretnéd-e futtatni. Önálló módban az `ftp` démon folyamatosan fut, és foglalja a számára kijelölt kaput, várva az ügyfelekre. Az `inetd` esetén az Internet Superserver fogja a kaput, és csak szükség esetén, azaz egy új ügyfél érkezésekor indítja el a démont. Az `inetd`-s megoldás kevesebb erőforrást emészt fel, ugyanakkor minden új ügyfelet megvárakoztatsz, hiszen türelmesnek kell lenniük, mire a démonfolyamat elindul. Általánosságban elmondható, hogy húsz felhasználó után már mindenképp érdemes önálló `ftp` démont futtatni. Ez a választás természetesen nem végleges, utólag könnyedén megváltoztathatod a döntésedet.
Debconf esetén további kérdést jelent, hogy szeretnéd-e engedélyezni az úgynevezett anonim elérést. Ez azt jelenti, hogy regisztrált felhasználónév, illetve jelszó nélkül is el lehessen-e elérni a kiszolgálót, vagy sem. Anonim eléréskor az ügyfél felhasználónévként anonimoust (névtelen) ad meg, jelszóként pedig többnyire egy elektronikus levélcímet. Érdemes nemmel válaszolni, s ezáltal kitiltani a vendégfelhasználókat. A döntés nem végleges, hiszen utólag könnyű őket engedélyezni, de legalább a kiszolgáló beállítása alatt nem érhető el jelszó nélkül a rendszer.

A /etc/proftpd.conf állomány

Mint említettem, a `proftpd` beállítóállománya az Apache ***httpd.conf*** mintáit követi. Ennek megfelelően álljon itt egy lista a fontosabb irányelvekről:

- `ServerName {string}`
  A kiszolgáló nevét határozza meg. A kapcsolódást követően alapértelmezésben ezt a szövegfüzért látják a parancssori `ftp`-t használók:
  `"ProFTPD 1.2.5rc1 Server (Debian) [inter.net]"`
  Itt a Debian a `ServerName` által meghatározott név, míg az `inter.net` a számítógép úgynevezett FQDN-je (Fully Qualified Domain Name), vagyis a tartománynév.
- `ServerType {"inetd" | "standalone"}`
  Itt a kiszolgálófolyamat futtatásának módját határozod meg. Az `inetd`, illetve `standalone` közötti különbség leírását lásd fentebb.
- `User {string}`
  Annak a felhasználónak a neve, aki a démon tulajdonosa. Debian alatt alapértelmezésben ez ***nobody***, viszont ezt a felhasználót más folyamatok is használják, így érdemes egy külön ***ftpd*** nevű felhasználót létrehozni `/bin/false` héjjal, és azt adni meg itt.
- `Group {string}`
  Annak a csoportnak a neve, aki a démon tulajdonosa. Szintén ajánlott a ***nogroup*** helyett egy ***ftpd*** nevű felhasználó létrehozása.

- `DefaultRoot {string} [string]`
  Ez a parancs az angol szakszókincs szerint egy ***jail root***-ot hoz létre, ami valójában egy ketrec a felhasználóidnak. Az első értékként megadott könyvtárból nem tudnak feljebb lépni, vagyis számukra ez az új gyökér. A könyvtárnév az egyes felhasználókra nézve lehet relatív. A második érték nem kötelező, ezzel egy vagy több csoportra engedélyezheted avagy tilthatod ezt a megszorítást. Például:
  `"DefaultRoot ~ download,!upload"`
  Ennek a segítségével eléred, hogy minden felhasználó, aki tagja a ***download*** csoportnak, de nem tagja az ***upload*** csoportnak, be legyen szorítva a saját könyvtárába (~).
- `AllowForeignAddress {"on" | "off"}`
  Engedélyezi az ügyfélnek, hogy a `PORT ftp` parancs használatakor a sajátján kívül más címét is használhassa. Ha nem érted, hogy ez mit jelent, akkor nem olvastad el az rfc-t, erre viszont most nem térnék ki. A lényeg, hogy ha ezt bekapcsolod (alapértelmezésben tiltva van), akkor a felhasználók igénybe vehetik az FXP nyújtotta lehetőségeket. Az FXP egy olyan módszer (nem külön protokoll), amellyel két kiszolgáló között anélkül mozgathatsz állományokat, hogy a saját gépedre letöltenéd őket.
- `AuthUserFile {string}`
  Lehetőség van a `proftpd`-ben más forrásokból is meríteni a felhasználói adatbázist, nem kötelező a */etc/passwd*-t használni. Ez azért remek, mert az FTP-felhasználóknak nem kell feltétlenül létezniük a rendszerben. E források között szerepel az LDAP-, az SQL-kiszolgálók, illetve egy másik ***passwd*** állomány. Ezt az utóbbi forrást használja ez az irányelv, ami már elég nagyfokú biztonságot tesz lehetővé. Gondolj csak arra, hogy így könnyen megakadályozhatod az FTP-felhasználók távoli belépését `telnet`-en vagy `ssh`-n keresztül. Mivel azonban itt nem létezik az árnyékjelszó fogalma, óvatosan állítsd be a jogosultságokat arra az állományra, amit itt értékként megadsz. A legjobb, ha a tulajdonosa és a csoportja az, amit a ***User***, illetve a ***Group*** meghatározásnál megadtál, és csak a tulajdonos és a csoport tudja írni és olvasni, a többieknek pedig semmilyen jogosultságuk nincs. Az állományt az `ftpasswd` parancs segítségével lehet létrehozni, illetve karbantartani, közvetlen írása nem ajánlott.
- `AuthGroupFile {string}`
  A hasonló nevű `AuthUserFile`-hoz hasonló, csak ez a */etc/group* állományt helyettesíti. Szintén az `ftpasswd` paranccsal illik írni.

Az ftpasswd

Ez egy olyan könnyen használható segédeszköz, mely az `AuthUserFile` vagy az `AuthGroupFile` által megadott állományt módosítja. Kapcsolóit két egyszerű példán keresztül mutatom be. Létrehozok egy andras nevű felhasználót, és a ***download*** nevű csoportba teszem bele.

```
# ftpasswd --passwd --name andras --uid 1000
➥--gid 100 --home /home/andras --shell /bin/sh
```

A `--passwd` határozza meg, hogy a felhasználók adatbázisát szeretném módosítani, nem pedig a csoportokét. Lehetőség nyílik egy `--file` kapcsoló használatára, így meg lehet határozni az adatbázis nevét. Ha elhagyod, alapértelmezés szerint *./ftpd.passwd*, azaz a pillanatnyi könyvtárban egy ***ftpd.passwd*** nevű állomány. A többi kapcsoló magától értetődő. A `--gid`-et elhagyhatod, ekkor egy a `uid`-del megegyező csoportazonosítót vesz alapul. Senkit ne tévesszen meg, hogy létezik egy `--shell` kapcsoló, és egy valós héj van megadva utána! Ez nem jelenti azt, hogy az adott felhasználó be tudna lépni távolról `telnet`-en vagy `ssh`-n, hiszen nem is létezik a rendszerben. Mindössze a PAM (Pluggable Authentication Modules) miatt van itt szükség egy valós héj megadására. Többek közt így lehet egy FTP-felhasználót „hibernálni”: `/bin/false`-t adsz meg héjnak, legyen szó akár `AuthUserFile`-ról, akár nem. A felhasználó jelszavát ezután kétszer egymás után kell begépelned, akárcsak a `passwd` parancsnál. Ez a jelszó az adatbázisban titkosítva tárolódik.

```
# ftpasswd --group --name download --gid 100
```

A `--group` azt mondja meg, hogy a csoportok adatbázisát módosítom. A `--file` elhagyása miatt az állomány neve *./ftpd.group*. Paranoiások figyelmébe ajánlom a `--enable-group-passwd` kapcsolót, ami szerintem ebben az esetben teljesen felesleges.

A Netfilter beállítása

FTP-kiszolgálót tűzfallal ellátni eléggé összetett feladat. A Netfilter `ip_conntrack_ftp` modulja ugyanakkor jelentősen leegyszerűsíti ezt a feladatot. Ez nyomon követi az `ftp` csomagokat, így azt sem szükséges tudnod, mi az az `ftp-data` kapu. Ha van ilyen modulod, egy szempillantás alatt beállítható (lásd a 45. CD Magazin/proftpd könyvtárában).
Ha a tűzfaladnak nincs `ftp`-nyomkövető modulja, egy kicsit nehezebb lesz a dolgod. Először is engedélyezned kell az `ftp (21)`, az `ftp-data (20)` kapukat, illetve a passzív átvitelhez mindazokat a kapukat, amik szóba jöhetnek. Ez érthető, hiszen az ügyfélnek el kell tudna érni azt a kaput, ahol az átvitel folyik. A gond csak az, hogy a kapu az 1024-65 535 tartomány bármelyik eleme lehet. Ha ezt mind engedélyezni akarod, ne is telepíts tűzfalat a kiszolgálóra. Azzal lehet segíteni az ügyön, hogy megmondod a `proftpd`-nek, hogy egy szűk tartományból válasszon magának passzív kaput, és csak azt engedélyezed a tűzfalban. Az utóbbi varázslat a `PassivePorts` meghatározással hozható létre.

PassivePorts {int} {int}

Az első egész szám az intervallum alsó, míg a második a felső határát jelöli (közöttük csak szóköz van). Fontos, hogy ez a tartomány elég nagy legyen ahhoz, hogy az elvárt számú kapcsolatot ki tudja elégíteni. Ennek megfelelően egy `ip_conntrack_ftp`-t nem használó IP Tables tűzfalas FTP-kiszolgáló a 2. listán látható módon nézhet ki (lásd a 45. CD Magazin/proftpd könyvtárában).

Végezetül

A `proftpd` szolgáltatásait tekintve az egyik leggazdagabb FTP-kiszolgáló. A virtuális kiszolgálók létrehozásáról még szót sem ejtettünk. Sok szerencsét a kísérletezéshez, és írjatok bátran, ha valami kérdésetek van.

Fülöp Balázs (xut@freemail.hu)
18 éves, imádja a Túró Rudit, a Debian Linuxot és a teheneket. Az ELTE Radnóti Miklós Gyakorlóiskola tanulója immár ötödik éve. Kedvenc írója Slawomir Mro□ek. Leginkább a számítógépes hálózatok biztonsága érdekli.

© Kiskapu Kft. Minden jog fenntartva