



- Pomoc i obsługa techniczna
- Naprawa komputerów
- Programowanie
- Bazy danych
- Sieci komputerowe

Instalacja oraz konfiguracja serwera FTP na LINUX-ie.

Serwer FTP służy do udostępniania oraz wymiany plików a sieci. Mamy do wyboru wiele klientów FTP. Ja przedstawię instalację ProFTOPD na platformie UBUNTU 12.12 natomiast do testowania konfiguracji użyję klienta FileZilla. Ilość konfiguracji w/w oprogramowania jest ogromna: od podstawowego klienta oferującego nieszyfrowane połączenie bez ograniczeń po zaszyfrowane połączenie z prawami dostępu dla wybranych użytkowników.

Postaram się przedstawić cały proces krok po kroku przechodząc od najprostszej konfiguracji do bardziej zaawansowanych.

1. Instalacja ProFTPD.

- Logujemy się jako root

```
sudo su root
```

- Instalujemy ProFTPD

```
apt-get install proftpd
```

- Ustawiamy rodzaj serwera na Standalone
- W tym momencie każdy użytkownik posiadający konto na naszym serwerze będzie miał do niego dostęp. Po uruchomieniu programu FileZilla podajemy adres serwera, login i hasło.
- Nasz serwer FTP już działa. Należy pamiętać jednak, że zalogować może się każdy użytkownik posiadający konto w systemie. Ponadto będzie on miał dostęp do katalogów systemowych oraz kont innych użytkowników.

2. Podstawowa konfiguracja ProFTPD:

- Edytujemy plik konfiguracyjny

```
nano /etc/proftpd/proftpd.conf
```

- Uzupełniamy podstawowe dane

- ServerName „NazwaSerwera” - Zmiana nazwy Serwera
- ServerType standalone - Typ serwera
- DefaultServer on - Domyślna konfiguracja serwera
- DisplayLogin welcome.msg - Komunikat powitalny
- DeferWelcome on - Komunikat powitalny dopiero po zalogowaniu
- TimeoutNoTransfer 600
- TimeoutStalled 600
- TimeoutIdle 1200 - Czas po jakim nastąpi rozłączenie z serwerem
- Port 21 - Port nasłuchu
- MaxInstances 30 - Maksymalna liczba procesów
- Uniemożliwienie logowania dla administratora
 - RootLogin off
- Uniemożliwienie wyjścia użytkownika poza wyznaczony katalog
 - DefaultRoot ~ - „~” Uniemożliwia wyjście poza katalog domowy użytkownika systemu
- Aby zatwierdzić zmiany restartujemy usługę


```
service proftpd restart
```

3. Tworzymy wirtualnych użytkowników (posiadających uprawnienia tylko do ftp).

- Modyfikujemy plik /etc/proftpd/proftpd.conf


```
nano /etc/proftpd/proftpd.conf
```
- Dodajemy nowe linie kodu


```
AuthUserFile /etc/proftpd/ftpd.passwd
AuthGroupFile /etc/passwd/ftpd/ftpd.group
RequireValidShell off
```
- Zapisujemy plik konfiguracyjny
- Tworzymy katalog użytkownika


```
mkdir /home/ftp
```
- Nadajemy uprawnienia dla stworzonego katalogu dla odpowiednich osób i grup ftp


```
chown proftpd:nogroup /home/ftp
```

proftpd i nogroup muszą być takie same jak w pliku konfiguracyjnym wpisy:

User proftpd

Group nogroup

- Nadajemy uprawnienia do zapisu i odczytu w/w katalogu

```
chmod 777 /home/ftp
```

- Dodajemy nowego użytkownika ftp

```
ftpasswd --passwd --file /etc/proftpd/ftpd.passwd --name  
nazwa_użytkownika --home /home/ftp/nazwa_katalogu -p --uid  
Id_użytkownika_ftp --gid Id_grupy_użytkowników_ftp --shell /bin/false
```

- restartujemy Proftpd

```
service proftpd restart
```

4. TFTP - Zszyfrowanie danych za pomocą TLS.

- Aby możliwe było zszyfrowanie połączenia musimy zainstalować pakiet openssl

```
apt-get install openssl
```

- tworzymy katalog w którym będzie certyfikat serwera

```
mkdir /etc/proftpd/ssl
```

- Generujemy prosty certyfikat (więcej na temat certyfikatów w artykule poświęconym OpenSSL)

- Tworzymy klucz

```
openssl genrsa -des3 -out server.key 4096
```

- Tworzymy certyfikat podpisany wygenerowanym kluczem

```
openssl req -new -key server.key -out server.csr
```

- Odpowiadamy na pytania, które się pojawią

- Wydajemy polecenie

```
openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt
```

- Jeśli klucz serwera ma nie wymagać hasła tworzymy klucz serwera, który go nie wymaga

```
openssl rsa -in server.key -out server.key.insecure
```

```
mv server.key server.key.secure
```

```
mv server.key.insecure server.key
```

- Edytujemy plik /etc/proftpd/proftpd.conf

```
nano /etc/proftpd/proftpd.conf
```

- Dopisujemy w nim linijkę

Include /etc/proftpd/tls.conf

- Zapisujemy w/w plik i otwieramy *tls.conf*

nano /etc/proftpd/tls.conf

- Kasujemy wszystkie linijki i wpisujemy poniższą treść:

```
<IfModule mod_tls.c>
```

```
    TLSEngine on
```

```
    TLSLog          /var/log/proftpd/tls.log
```

```
    TLSProtocol     SSLv23
```

```
    TLSOptions      NoCertRequest
```

```
    TLSRSACertificateFile /etc/proftpd/ssl/server.crt
```

```
    TLSRSACertificateKeyFile /etc/proftpd/ssl/server.key
```

```
    TLSVerifyClient off
```

```
    TLSRequired     on
```

```
</IfModule>
```

- Uwaga jeśli linijka *TLSRequired* jest na „on” to do serwera mogą łączyć się tylko klienci z obsługą TLS. Jeśli na „off” będą mogli również połączyć się klienci bez obsługi TLS.
- Restartujemy serwer FTP
service proftpd restart
- Nasz serwer jest zabezpieczony i gotowy do pracy.

Artykuł pochodzi ze strony

www.einformatyka.com.pl