

## I. Usługa FTP ([https://pl.wikipedia.org/wiki/Protok%C3%B3%C5%82\\_transferu\\_plik%C3%B3w](https://pl.wikipedia.org/wiki/Protok%C3%B3%C5%82_transferu_plik%C3%B3w))

**Protokół transferu plików, FTP** (od ang. *File Transfer Protocol*) – [protokół komunikacyjny](#) typu [klient-serwer](#) wykorzystujący [protokół sterowania transmisją](#) (TCP) według [modelu TCP/IP](#) (krótko: połączenie TCP), umożliwiający dwukierunkowy transfer plików w układzie [serwer FTP–klient FTP](#).

FTP jest zdefiniowany przez [IETF](#) w dokumencie [RFC 959](#) ↓.

FTP jest protokołem [8-bitowym](#) i dlatego nie wymaga kodowania danych do 7 bitów, tak jak w przypadku [poczty elektronicznej](#).

Do komunikacji wykorzystywane są dwa połączenia TCP. Jedno z nich jest połączeniem kontrolnym, za pomocą którego przesyłane są polecenia, a drugie służy do transmisji danych. Połączenie za pomocą protokołu FTP (krótko: połączenie FTP) może działać w dwóch trybach: aktywnym i pasywnym:

- jeżeli połączenie FTP działa w trybie aktywnym, używa [portu](#) 21 dla poleceń (zestawiane przez klienta) i portu 20 do przesyłu danych (zestawiane przez serwer)
- jeżeli połączenie FTP pracuje w trybie pasywnym, używa portu 21 dla poleceń i portu o numerze powyżej 1024 do transmisji danych (obydwa połączenia zestawiane są przez klienta).

W sieciach chronionych [zaporą sieciową](#) komunikacja z serwerami FTP wymaga zwolnienia odpowiednich portów na tej zaporze lub [routerze](#). Możliwe jest zainstalowanie wielu serwerów FTP na jednym routerze. Warunkiem jest rozdzielenie portów przez router dla każdego serwera.

Serwer FTP, zależnie od konfiguracji, może pozwalać na anonimowy, czyli bez podawania hasła [uwierzytelniającego](#), dostęp do jego zasobów. Najczęściej jednak serwer FTP [autoryzuje](#) każde połączenie za pomocą [loginu](#) i hasła.

## II. Opis programu PROFTPD

na podstawie strony internetowej:

<http://www.ulos.pl/proftpd-serwer-ftp-na-linuxa-wirtualni-uzytownicy->

**Proftpd** jest jednym z najpopularniejszych serwerów ftp dla Linuxa. Łatwy w konfiguracji, dość powiedzieć, że od razu po instalacji można z niego korzystać.

**UWAGA:** Po zainstalowaniu proftpd uzyskujemy pełny dostęp do plików i katalogów na serwerze!!! Dlatego odradzałbym pozostawienie proftpd w domyślnej konfiguracji.

Przed omówieniem podstawowej konfiguracji musimy sobie zadać pytanie: *"kogo ma obsługiwać nasz serwer plików i jakie zasoby udostępnić?"*

Mamy do wyboru:

- **użytkownicy systemowi** - użytkownicy mający dostęp do kont shell na naszym serwerze (zaufani)
- **użytkownicy ftp** - użytkownicy posiadający tylko dostęp do konta na ftp (mniej zaufani)

- **użytkownicy anonimowi** - użytkownicy posiadający dostęp to tzw. **anonymous FTP**, czyli przeważnie mogący ściągać pliki udostępnione przez administratora bez podawania loginu ani hasła

### III. Domyślna konfiguracja jest zorientowana na użytkowników systemowych i na razie skupię się na niej.

Edytujemy plik proftpd.conf:

```
# Dołączamy konfigi ewentualnie aktywowanych modułów.
Include /etc/proftpd/modules.conf

# Tryb pracy serwera, uruchamiamy jako samodzielny proces.
ServerType standalone
# Określamy konfigurację jako domyślną
DefaultServer on

# Jesli nie używamy IPv6.
UseIPv6 off

# Te 3 opcje znacznie skracają czas logowania.
UseReverseDNS off
IdentLookups off
ServerIdent off

# Określamy nazwę naszego serwera, nie podajemy jego nazwy ani wersji.
ServerName "ftp by ulos.pl"

# Komunikat powitalny.
DisplayLogin welcome.msg

# Zezwalamy na komunikat powitalny dopiero po zalogowaniu.
DeferWelcome on

MultilineRFC2228 on

# Zezwalamy na wyświetlanie dowiązań.
ShowSymlinks on

# Czas w jakim zostanie przerwane połączenie z serwerem.
TimeoutNoTransfer 600
TimeoutStalled 600
TimeoutIdle 1200

DisplayChdir .message true

DenyFilter \*.*

# Blokada logowania użytkownikowi root.
RootLogin off

# Uwięzienie użytkownika w wyznaczonym katalogu, z którego nie będzie mógł się wydostać.
# znak ~ katalog domowy w systemie Linux.
DefaultRoot ~

# Opcje do listowania plików w trybie binarnym:
# "-a"="ls -a" , "+a"=blokada parametru a czyli plików ukrytych(z kropką).
ListOptions "+a"
```

```

# Sprawdzamy czy dany użytkownik, który się loguje
# posiada przypisaną w /etc/shells powłokę (szybka metoda do zablokowania).
RequireValidShell          on

# Port na którym nasłuchuje proftpd.
Port                        21

# Konfiguracja portów trybu pasywnego używanego przez przeglądarki
# (ftp://host.pl).
# PassivePorts              49152 65534

# Użyteczna opcja jeśli nasz komputer stoi za NAT-em.
# MasqueradeAddress         1.2.3.4

# This is useful for masquerading address with dynamic IPs:
# refresh any configured MasqueradeAddress directives every 8 hours

# DynMasqRefresh 28800

# Maksymalna liczba procesów demona FTP.
# Dzięki tej dyrektywie możemy ustrzec się przed atakami typu DoS.
MaxInstances                30

# Użytkownik i grupa do których będzie należał proces serwera.
User                        proftpd
Group                       nogroup

# Ustawienie prawa dostępu właściciela do modyfikacji pliku i katalogów.
# 022 => 755 , 077 => 700 , 002 => 775
Umask                       022 022

# Pozwolenie na nadpisywanie plików.
AllowOverwrite              on

# Konfiguracja logów.
TransferLog /var/log/proftpd/xferlog
SystemLog   /var/log/proftpd/proftpd.log

```

Oczywiście po zmianie w pliku proftpd.conf restartujemy serwer.

Jest to przykład podstawowej konfiguracji proftpd z zachowaniem pewnych norm bezpieczeństwa dla użytkowników systemowych.

Należy wspomnieć o jeszcze jednej istotnej sprawie, protokół ftp przesyła **hasła i loginy w postaci niezaszyfrowanej**, jako tzw. plain text co daje możliwość podsłuchania tych dość ważnych informacji.