Serwery FTP

Autorzy:
Mariusz Guz
Łukasz Sala
IV FDS

Rzeszów 15-01-2003

STRESZCZENIE

Jedną z palety usług świadczonych przez firmy specjalizujące się w „hostingu” jest udostępnianie swym klientom wirtualnych serwerów FTP. Polega to na uruchomieniu na jednym komputerze, spełniającym rolę serwera, odpowiednio skonfigurowanego demona FTP, który potrafi obsłużyć sesje transferu plików w sposób zależny od tego, na jaki adres IP są one skierowane. Serwer FTP jest bazą informacji dla innych komputerów znajdujących się w sieci lokalnej lub w sieci Internet. Użytkownicy połączeni z takim PC-tem mogą kopiować, przesuwać, wykonywać, usuwać pliki lub katalogi używając protokołu FTP (File Transfer Protocol).

Celem pracy jest omówienie instalacji, konfiguracji oraz wykorzystania i obsługi serwera FTP. Praca podzielona jest na dwie części, pierwsza część zajmuje się serwerem FTP na platformie systemowej Linux Debian. Opisany serwer to ProFTPD. Każda z kolejnych sekcji zawiera szereg informacji przygotowujących i określających działania administratora serwera. W kolejnych krokach poznajemy specjalizowane narzędzia zarządzania serwerem oraz problemy jakie mogą pojawić się podczas konfiguracji i administracji serwera. W niniejszej pracy można także odnaleźć rozwiązania najczęściej pojawiających się problemów podczas pracy serwera. Druga część pracy opisuje komercyjną dystrybucję serwera FTP Serv-U. Poszczególne sekcje przeprowadzają nas przez proces instalacji i konfiguracji serwera. Znajdziemy tu opis instalacji i procedur uruchomienia podstawowego serwera FTP dla użytkownika ‘anonymous’ oraz dla użytkowników określonych nazwą i hasłem. W tej części znajdziemy wyjaśnienia niemalże wszystkich dostępnych opcji w programie, dokonane są one w sposób przystępny i poparte przykładami oraz szczegółowymi wyjaśnieniami.

Treść pracy zawiera również dwa dodatki, w których można znaleźć listę kodów odpowiedzi serwera oraz ich wyjaśnienia oraz zestaw najważniejszych poleceń FTP na wypadek, gdy nie będzie wygodniejszego programu.

SPIS TREŚCI

ProFTPD

1. KOMPILACJA I INSTALACJA.

1.1. Informacje wstępne

1.1.1. Na jakich platformach program się kompiluje?

Użytkownicy zgłaszali, że ProFTPD kompiluje się na następujących platformach (i wersjach):

- Linux 2.0.x & 2.2.x (glibc 2.x only) & 2.4.x
- BSDI 3.1 & 4.0
- IRIX 6.2, 6.3, 6.4, 6.5
- Solaris 2.5.1, 2.6, 2.7, 8 (Sparc)
- AIX 3.2 & 4.2
- OpenBSD 2.2/2.3
- FreeBSD 2.2.7
- Digital UNIX 4.0A
- DEC OFS/1
- Cygwin

1.1.2. CVS

CVS (Concurrent Versions System) jest systemem zarządzania wersjami, który pozwala wielu programistom (rozrzuconym po pokoju albo po całym świecie) zachowanie podstawowego kodu tworzonego programu jak i na rejestrowanie wszystkich zmian w pracy.

Repozytorium CVS dla programu ProFTPD jest dostępne dla zwykłych użytkowników w trybie tylko do odczytu, jakkolwiek kod tam umieszczony nie gwarantuje nawet poprawnego skompilowania, nie mówiąc o poprawnej pracy. Dostęp do CVS został utworzony dla dostępu do ważnych patchów (poprawek) poprawiających bezpieczeństwo, oraz dla zainteresowanych użytkowników aby mieli możliwość przetestowania najnowszych zmian.

Najnowsze pliki CVS dostępne są na ftp.proftpd.org, umieszczane są około 1 rano czasu środkowo-europejskiego.

Zalecane ustawienia ~/.cvsrd:

```
cvs -z 3
update -Pd
diff -u
```

Gdzie można uzyskać informacje na temat cvs?

CVS został stworzony przez Cyclic Software (http://www.cyclic.com/) i szczegóły dotyczące CVS można znaleść na ich stronie. Dokumentacja CVS jest przejrzysta, szczegółowa i przede wszystkim ciężka po wydrukowaniu.

1.1.3. Używanie niestandardowych modułów

Aby użyć niestandardowych modułów należy skompilować ProFTPD w następujący sposób:

```
./configure --with-modules=mod_module1:mod_module2:mod_module3
make
make install
```

1.1.4. Uruchamianie w trybie debug

Można to wykonać poleceniem: `/usr/local/sbin/proftpd -d9 -n`
Ścieżka może być inna, jeśli nie zainstalowaliśmy programu w domyślnej lokalizacji. [2]

1.2. Instalacja

Instalacji możemy dokonać na kilka sposobów, najlepszym jest udanie się na stronę projektu ProFTPD (http://www.proftpd.org/) i ściągnięcie stamtąd programu. Pobrać program można np. z serwera ftp://ftp.proftpd.org/distrib/. W zależności od używanego systemu możemy ściągnąć odpowiednią wersję pakietową (rpm'y lub source rpm'y) – z katalogu packages/, lub wersje źródłowe (spakowane jako proftpd-****.tar.gz lub proftpd-****.tar.bz2) - katalog source/. W naszym przypadku oprzemy się na wersji źródłowej: *proftpd-1.2.7rc3.tar.gz*.

Po ściągnięciu tego pliku należy go rozpakować. Jeśli posługujemy się Midnight Commanderem to wystarczy wejść do pliku archiwum i skopiować jego zawartość w wybrane przez nas miejsce. Jeśli nie mamy Midnight Commandera należy rozpakować archiwum komendą:

```
tar -xzvf proftpd-1.2.7rc3.tar.gz
```

co spowoduje rozpakowanie naszego archiwum do katalogu "proftpd-1.2.7rc3". Po wejściu do tego katalogu (komendą `cd <nazwa katalogu>` o ile nie używamy MC) należy skompilować program. Robimy to w następujący sposób wpisując polecenia:

```
./configure
make
make install
```

Spowodowało to zainstalowanie ProFTPD z domyślnymi opcjami, umieszczając pliki programu w następujących katalogach:
proftpd i ftpshut w katalogu "/usr/local/sbin/"
ftpcount i ftpwho w katalogu "/usr/local/bin/"
plik konfiguracyjny *proftpd.conf* w katalogu "/usr/local/etc/"
oraz pliki pomocy (manual) w katalogu "/usr/local/man/man?/"

Jeśli będziemy chcieli dodać jakieś moduły do programu to należy ponownie skompilować program, przy czym należy pamiętać, aby najpierw wyczyścić katalog instalacyjny (jeśli używamy tego samego katalogu w którym kompilowaliśmy po raz pierwszy) poleceniem `make distclean`.

1.3. Kompatybilność i integracja

1. SQL

ProFTPD wspiera autentykację i logowanie poprzez bazy SQL'owe korzystając z modułu mod_sql dostarczanego z główną dystrybucją.

2. SSH

Pod adresem http://www.castaglia.org/proftpd/doc/ znajduje się mini-HOWTO dotyczące tunelowania połączeń ftp poprzez SSH.

3. IPv6

Aktualnie nie ma oficjalnego wsparcia dla IPv6 dla wersji 1.2x programu, jest ono przewidziane w wersjach 1.3x.

4. Uwzględnianie wielkości liter w nazwach plików (filename case sensitivity)

ProFTPD jest całkowicie zależny od systemu operacyjnego w kwestii uwzględniania wielkości liter w nazwach plików - jeśli system operacyjny je rozróżnia to robi to także ProFTPD. Jak narazie nie ma w planach modułu do obsługi tego zagadnienia. [2]

2. KONFIGURACJA:

2.1. Ustawienia wstępne

Ponieważ prawdopodobnie podczas procesu konfiguracji będziemy często wyłączać i włączać ProFTPD dobrze jest sobie utworzyć SymLink do programu (np. w katalogu /etc/). Za pomocą Midnight Commandera robimy to w następujący sposób: zaznaczamy *proftpd* (w katalogu "/usr/local/sbin") i z menu File wybieramy SymLink i wpisujemy w pierwszej linijce (do jakiego pliku ma być "skrót"): */usr/local/sbin/proftpd* (jeśli wywołaliśmy polecienie SymLink przy zaznaczonym programie *proftpd* to linijka ta będzie wpisana). Jeśli w drugim panelu MC mieliśmy otwarty katalog "/etc/" to następna linijka powinna wyglądać następująco: */proftpd*, jeśli nie mieliśmy otwartego tego katalogu to należy zastąpić tamten wpis następującym: */etc/proftpd*.

Aby nasz demon ftp nie działał na koncie root'a (ze względów bezpieczeństwa) dobrze jest utworzyć osobną grupę użytkowników na potrzeby obsługi ftp. Jeśli chcemy aby przy każdorazowym dodaniu użytkownika tworzony był dla niego katalog można zmodyfikować plik */etc/adduser.conf* zmieniając następujące zmienne:

DHOME=/<katalog> odpowiada za umiejscowienie katalogu domowego, domyślnie powinno być *DHOME==/home*

GROUPHOMES=<yes/no> odpowiada za tworzenie katalogów domowych każdego użytkownika wg schematu */home/nazwa_grupy/użytkownik.* Zmienną można ustawić na *yes.*

Następnie dodajemy grupę "ftp" i użytkownika "ftpdemon" na którym będzie działał nasz demon ftp. Robimy to następującymi komendami:

```
addgroup ftp
       Adding group ftp (102)...
       Done.
       Press any key to continue...
```

Co dodaje nam grupę "ftp". Następnie dodajemy do tej grupy użytkownika:

```
adduser --ingroup ftp ftpdemon
Adding user ftpdemon...
Adding new user ftpdemon (1000) with group ftp.
Creating home directory /home/ftp/ftpdemon.
Copying files from /etc/skel
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for ftpdemon
Enter the new value, or press return for the default
        Full Name []: demon ftp
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [y/n] y
```

Tak wykonane polecenie powinno utworzyć (o ile wcześniej zmieniliśmy plik "*/etc/adduser.conf*") katalogi "/ftp/ftpdemon/" w katalogu "/home/".

2.2. Konfiguracja ProFTPD

Następną czynnością będzie skonfigurowanie ProFTPD, w tym celu należy wyedytować plik */usr/local/etc/proftpd.conf*.

W chwili obecnej ProFTPD posiada siedem różnych kontekstów konfiguracyjnych: główny serwer, <Anonymous>, <Directory>, <Global>, <Limit>, <VirtualHosts> i pliki .ftpaccess.

Serwer główny

Kontekst ten kieruje wszystkim co nie jest zawarte w pozostałych kontekstach (np. każdą dyrektywą konfiguracyjną która nie jest wyraźnie zawarta w innym kontekście konfiguracyjnym.

<Anonymous>

Sekcja ta jest używana do skonfigurowania serwera z dostępem anonimowym. Po zalogowaniu użytkownik jest domyślnie przenoszony (*chroot*) do katalogu użytkowników anonimowych i wyłączone jest wymaganie poprawnego hasła - wymagane jest podanie adresu e-mail. W katalogu <Anonymous>'a nie powinno być plików systemowych ani innych ważnych plików.

Należy zwrócić uwagę na to, że sekcja <Anonymous> nie jest osobnym serwerem, lecz raczej "podzbiorem" serwera w którego konfiguracji jest uwzględniona. Jakiekolwiek dyrektywy konfiguracyjne ustawione dla tego serwera będą uwzględnione również w sekcji <Anonymous> chyba, że zostaną zmienione w tejże sekcji.

<Directory>

Kontekst ten jest przeznaczony do konfiguracji katalogów. Uwzględnia to wyświetlanie zawartości katalogu bazujące na loginie zalogowanego użytkownika lub jego przynależności do grupy lub też zależy od nazwy pliku (np. pliki ukryte w systemie Unix), plik *.ftpaccess* podlega temu kontekstowi z definicji. Często w tym kontekście występuje również sekcja <Limit>.

<Global>

Ten blok konfiguracyjny służy do tworzenia zestawów dyrektyw konfiguracyjnych, które odnoszą się uniwersalnie i do konfiguracji głównego serwera jak i do konfiguracji wirtualnych hostów. Można tworzyć wielokrotne bloki <Global>. Podczas uruchomienia programu wszystkie te bloki są łączone w jeden a następnie wstawiane w sekcje konfiguracyjne każdego z serwerów. Należy jednak pamiętać, że jeśli w tym bloku została użyta jakaś dyrektywa, a później w sekcji głównego serwera lub w <VirtualHost> została użyta ta sama dyrektywa, ale z innymi parametrami, to ta ostatnia ma pierwszeństwo nad dyrektywą z sekcji <Global>. Pozwala to na ujednolicenie konfiguracji dla wszystkich serwerów a następnie na dostrojenie każdego z nich osobno.

<Limit>

Kontekst ten jest używany do ustanawiania ograniczeń jak i które z poszczególnych komend i grup komend FTP mogą być użyte.

.ftpaccess

Pliki te są podobne do plików *.htaccess* serwera Apache, które są analizowanymi w locie plikami konfiguracyjnymi - z ograniczonymi deklaracjami - które użytkownik może umieszczać w odpowiednich katalogach. [1]

2.3. Przykładowy plik konfiguracyjny "/usr/local/etc/proftpd.conf"

```
# This is a ProFTPD configuration file
```

Po pierwsze ustawienia globalne

ServerName	"Moj Serwer FTP"	nazwa serwera
ServerAdmin	admin@moja.domena.pl	email administratora
ServerType	standalone	typ serwera
DeferWelcome	on	dyrektywa opóźniająca wyświetlanie nazwy i adresu serwera do momentu autentykacji użytkownika
DefaultServer	on	
DefaultRoot	~	ustawienie jako korzenia katalogu domowego użytkownika
Port	21	nr portu
Umask	002	maska ustawiana nowo tworzonym plikom i katalogom

Ustawienia użytkownika i grupy serwera

User	ftpdemon	użytkownik na jakim uruchomiony jest serwer FTP
Group	ftp	grupa do której należy ten użytkownik (przypuszczalnie musisz ja sobie stworzyć)

Timeouty - różne

TimeoutIdle	300
TimeoutStalled	300
TimeoutLogin	60
TimeoutNoTransfer	300

Logi

ExtendedLog	/var/log/proftp.log	miejsce składowania logów
ExtendedLog	/dev/tty11	konsola na której są wyświetlane logi

DisplayLogin	.welcome.msg	wiadomość powitalna
MaxInstances	20	maksymalna ilość procesów potomnych, tylko dla trybu standalone
MaxLoginAttempts	2	maksymalna ilość prób logowania

Ograniczenia obciążenia serwera

MaxClients 20 ">>> Za duzo uzytkownikow <<<"
maksymalna liczba użytkowników zalogowanych w danej chwili i w cudzysłowie wiadomość

MaxClientsPerHost 40 ">>> Za duzo polaczen z jednego IP <<<"
maksymalna liczba połączeń z jednego IP

Ograniczenia IP/hostów z których można się zalogować

Opcja a) Możesz zalogować się z każdego miejsca poza tymi, które są w polach > Deny from

```
 <Limit LOGIN>
   Order allow,deny
   Deny from host.domena1.pl
   Deny from w3cache.pwr.wroc.pl
   Deny from w3cache.tpnet.pl
   Deny from w3cache.
   Deny from   .cst.tpsa.pl
   Deny from   .gov.pl
   Deny from   .gov
#    Deny from   .pol.co.uk
 </Limit>
```

Opcja b) możesz zalogować się z każdego miejsca (poza .lame.net)

```
<Limit LOGIN>
Order deny,allow
Deny from .lame.net
 AllowAll
</Limit>
```

<u>Ustawienia dla poszczególnych użytkowników</u>

```
##########################
#      A N O N Y M O U S   #
##########################
```

Dotyczy np. użytkownika ftp czyli tzw. anonymousa

<Anonymous ~ftp>		początek ustawień użytkownika ftp
User	ftp	użytkownik
Group	ftp	grupa
AnonRequirePassword	off	logowanie bez hasła
UserAlias anonymous ftp		aliasy tego użytkownika, może się logować i ftp i anonymous
DisplayLogin .welcome.msg		powitalna wiadomość odczytywana z pliku
DisplayFirstChdir .message		wiadomość która pokazuje się po wejściu do katalogu
GroupOwner	ftp	
Umask	002	
HideUser	root	ukrywa przed użytkownikiem wszystkie katalogi/pliki użytkownika root
HideGroup	root	ukrywa przed użytkownikiem wszystkie katalogi/pliki grupy root

```
 HideNoAccess        on              ukrywa przed użytkownikiem wszystkie katalogi/pliki do
                                     których nie ma on dostępu
```

Ograniczenia obciążenia serwera (j.w)

```
 MaxClients   10 ">>> Za duzo uzytkownikow <<<"
 MaxClientsPerHost  5 ">>> Za duzo polaczen z jednego hosta <<<"
```

Ograniczenia mówiące o braku praw do uploadu

```
<Limit WRITE>                        ograniczenie zapisywania
   DenyAll                           zabroń jakiegokolwiek zapisywania
 </Limit>
 <Limit READ DIRS>                   ograniczenie odczytywania zawartości katalogów
   IgnoreHidden  on                  ignorowanie ukrytych plików/katalogów
 </Limit>
</Anonymous>                         to jest koniec ustawień dla tego użytkownika

######################
# DLA WYBRANYCH    #
######################
<Anonymous ~wybrany>                 użytkownik wybrany - należy go dodać do systemu
```

opis do tych opcji jak wyżej

```
 User                    wybrany
 Group                   ftp
 AnonRequirePassword     on
 DisplayLogin            .welcome.msg
 DisplayFirstChdir       .message
 GroupOwner              wybrany
 Umask                   002
 HideUser                root
 HideGroup               root
 HideNoAccess            on
 MaxClients   10 ">>> Za duzo uzytkownikow <<<"
 MaxClientsPerHost  5 ">>> Za duzo polaczen z jednego IP <<<"
```

Zezwalamy na logowanie się tylko z IP w polach Allow from i z domen *.pl - pozostałe zabronione

```
 <Limit LOGIN>
   Order allow,deny
   Allow from .pl
   Allow from 127.0.0.1
   Allow from 192.168.1.
   Allow from 212.160.79.
   Allow from  212.160.254.10
   Allow from  212.160.254.2
   DenyAll
 </Limit>
```

opcja a) bez prawa do UPLOADu

```
 <Limit WRITE>
   DenyAll
 </Limit>
 <Limit READ DIRS>
   IgnoreHidden  on
 </Limit>
```

opcja b) zezwala na UPLOAD

```
<Directory uploads/*>
  <Limit READ>
    DenyAll
  </Limit>
  <Limit STOR>          ograniczenia komendy STOR - załaduj - upload
    AllowAll            zezwalaj na wszystkie
  </Limit>
  <Limit MKD>           ograniczenia komendy MKD - tworzenie katalogu
    AllowAll            zezwalaj na wszystkie
  </Limit>
 </Directory>
</Anonymous>
```

3. PROBLEMY Z KONFIGURACJĄ

3.1. Jak dodać kolejne konto anonimowe?

Najlepiej sprawdzić w katalogu *sample-configurations/* w katalogu z wersją instalacyjną programu - znajdują się tam przykładowe pliki konfiguracyjne. Ogólnie mówiąc należy dodać kolejnego użytkownika systemowego (polecenie `adduser`). Katalog domowy użytkownika może, ale nie musi, być głównym katalogiem dla konta tego użytkownika na serwerze ftp. Po utworzeniu w systemie operacyjnym konta użytkownikowi należy dodać do pliku konfiguracyjnego coś podobnego do:

```
<Anonymous ~private>
       AnonRequirePassword off
       User private
       Group private
       RequireValidShell off
         <Directory *>
           <Limit WRITE>
             DenyAll
           </Limit>
         </Directory>
</Anonymous>
```

Pozwoli to klientom ftp połączenie się z twoim serwerem z loginem "private" i adresem e-mail jako hasło. Można zmienić dyrektywę *AnonRequirePassword* na "on" jeśli chcesz aby logujący się użytkownik podawał prawidłowe hasło dla użytkownika "private". Powyższa konfiguracja pozwala klientom wchodzić, wyświetlać i czytać wszystkie katalogi, zabrania jakiejkolwiek możliwości zapisu.

3.2. Jak skonfigurować bezpieczną możliwość uploadu?

Poniższy fragment pliku konfiguracyjnego ilustruje jak zabezpieczyć katalog uploadu (co jest dobrym pomysłem jeśli nie chcesz np. aby ludzie używali twojego serwera do przechowywania "warezu").

```
<Anonymous /home/ftp>
  User username
  Group usergroup
  UserAlias ftp username
  AuthAliasOnly on
  RequireValidShell off
```

```
  <Directory pub/incoming/>
     <Limit STOR CWD>
        AllowAll
     </Limit>
     <Limit READ RMD DELE MKD>
        DenyAll
     </Limit>
  </Directory>
</Anonymous>
```

Zabrania to wszystkich operacji zapisu do katalogu głównego i podkatalogów użytkownika anonymous, z wyjątkiem katalogu "incoming/" gdzie pozwolenia są odwrócone - klient może zapisywać ale nie może czytać (pobierać plików). Jeśli zamiast *<Limit STOR>* użyje się *<Limit WRITE>* na katalogu "incoming/" klienci będą mogli wykonywać wszystkie operacje zapisu w podkatalogu (wliczając usuwanie, zmianę nazwy i tworzenie katalogów)>

3.3. Jak schować katalog przed użytkownikami anonimowymi?

Należy użyć dyrektyw *HideUser* lub *HideGroup* w połączeniu z odpowiednim użytkownikiem/grupą. Na przykład, jeśli masz następujący katalog gdzieś w katalogu anonimowego użytkownika ftp:

```
drwxrwxr-x 3 ftp staff 6144 Apr 21 16:40 prywatny
```

Możesz użyć dyrektywy "*HideGroup staff*" aby katalog "prywatny" nie był wyświetlany w liście katalogów. Na przykład w ten sposób:

```
<Anonymous ~ftp>
...
       <Directory Private>
              HideGroup staff
       </Directory>
...
</Anonymous>
```

3.4. Ukrywanie plików/katalogów nie działa!

Musisz się upewnić, że grupa, którą ukrywasz nie jest podstawową grupą użytkownika anonimowego - jeśli tak nie jest dyrektywa *HideGroup* nie zadziała.

3.5. Jak zabronić użytkownikom wstępu do ukrytego katalogu?

Możesz albo zmienić prawa dostępu tego katalogu, aby zabronić anonimowym użytkownikom FTP dostępu do niego, lub jeśli chcesz żeby wyglądał on na niewidzialny (tak jakby go nie było) - użyj dyrektywy *IgnoreHidden* w środku bloku *<Limit>* dla jednego lub więcej poleceń które mają kompletnie ignorować ukryty katalog.

3.6. Jak postawić wirtualny serwer FTP?

Musisz skonfigurować swój komputer tak, aby mógł obsługiwać kilka adresów IP. Często jest to nazywane "aliasingiem", i ogólnie może być skonfigurowane poprzez alias IP lub fikcyjny interfejs, należy zapoznać się z dokumentacją systemu operacyjnego w celu dokonania tego. Jeśli masz już skonfigurowany komputer tak, aby akceptował dodatkowy adres IP, na którym chcesz mieć postawiony wirtualny serwer FTP, użyj dyrektywy konfiguracyjnej *<VirtualHost>* aby utworzyć ten wirtualny serwer:

```
<VirtualHost 10.0.0.1>
       ServerName "Moj wirtualny serwer FTP"
</VirtualHost>
```

Możesz dodać dodatkowe bloki dyrektyw do kontekstu *<VirtualHost>*, aby utworzyć konta użytkowników.

3.7. Chcę tylko anonimowy dostęp do wirtualnego serwera.

Użyj bloku *<Limit LOGIN>* aby zabronić dostępu na samym początku bloku *<VirtualHost>*, a następnie w bloku *<Anonymous>* użyj jej ponownie aby zezwolić na dostęp anonimowy. Pozwoli to logować się anonimowo i odrzuci wszystkie inne próby logowania. Przykładowy wycinek pliku konfiguracyjnego:

```
<VirtualHost 10.0.0.1>
       ServerName "Moj wirtualny serwer FTP"
       <Limit LOGIN>
              DenyAll
       </Limit>

       <Anonymous /usr/local/private>
              User private
              Group private
              UserAlias anonymous private # klient logujący się jako 'anonymous' jest
                                          # aliasowany jako 'private'
              <Limit LOGIN>
                     AllowAll
              </Limit>
              ...
       </Anonymous>
</VirtualHost>
```

3.8. Jak ograniczyć użytkowników do danego katalogu?

Dla ogólnego dostępu można użyć dyrektywy *<Anonymous>* w połączeniu z dyrektywą *User-Password/AnonRequirePassword*.
Jeśli jednak chcesz zamknąć grupę użytkowników (lub grupy) w danym katalogu możesz użyć dyrektywy *DefaultRoot*. Pozwala ona ustalić katalog główny (lub "~" żeby uwięzić użytkownika w jego katalogu domowym), a dodatkowe wyrażenie grupowe może być użyte do kontroli grup użytkowników, do których ograniczenie będzie się odnosiło. Na przykład:

```
<VirtualHost host.siec.foo>
       DefaultRoot ~
       ...
</VirtualHost>
```

Tworzy to konfigurację, w której każdy użytkownik logujący się do host.siec.foo jest ograniczony do swojego katalogu domowego (nie może użyć komendy `chdir` aby dostać się wyżej niż swój katalog domowy).
Można też użyć:

```
<VirtualHost myhost.mynet.foo>
       DefaultRoot /u2/public uzytkownicy,!zespol
       ...
</VirtualHost>
```

W tym przykładzie wszyscy użytkownicy będący członkami grupy "uzytkownicy", ale nie będący członkami grupy "zespol" są ograniczeni do katalogu /u2/public. Jeśli użytkownik nie spełnia warunku w dyrektywie *DefaultRoot* loguje się normalnie (nie jest uwięziony, domyślnym katalogiem jest jego katalog domowy). W jednym bloku konfiguracyjnym można wielokrotnie używać dyrektywy *DefaultRoot* aby tworzyć wielokrotne ograniczenia. Jeśli dwie dyrektywy *DefaultRoot* odnoszą się do tego samego użytkownika ProFTPD wybierze jedną z nich (bazując na tym jak była zanalizowana składnia).

3.9 Dlaczego anonimowy ftp nie działa (”550 login incorrect”)?

Należy sprawdzić następujące rzeczy:

- Upewnij się że użytkownik/grupa które podałeś wewnątrz bloku *<Anonymous>* istnieją w systemie. Musi istnieć prawdziwy użytkownika i grupa użytkowników, ponieważ jest to używane do autentykacji użytkowników.
- Jeśli dyrektywa *RequireValidShell* nie jest wyłączona, upewnij się, że użytkownik ftp (podany dyrektywą *User* wewnątrz bloku *<Anonymous>*) posiada ważną powłokę wymienioną w pliku */etc/shells*. Jeśli nie chcesz przyznawać użytkownikowi ważnego shella zawsze możesz użyć ”*RequireValidShell off*” aby wyłączyć sprawdzanie ważności powłoki.
- Jeśli *UseFtpUsers* nie jest ustawiona na *off*, upewnij się, że twój „użytkownik ftp” nie jest wymieniony w pliku */etc/ftpusers*.

Jeśli powyższe sposoby zawiodą powinieneś sprawdzić logi systemowe. Kiedy autentykacja zawiedzie z jakiegokolwiek powodu ProFTPD używa systemowego mechanizmu logów aby zapisać powód niepowodzenia.

3.10. Jak mogę ograniczyć rozmiar uploadowanych plików?

Służą do tego dwie dyrektywy: *MaxRetrieveFileSize* i *MaxStoreFileSize* przeznaczone do kontrolowania maksymalnego rozmiaru plików przesyłanych do i z serwera.

3.11. Jak mogę ograniczyć ilość połączeń przypadających na jednego użytkownika?

Służy do tego dyrektywa *MaxClientsPerUser*.

3.12. Jak skonfigurować ProFTPD aby obsługiwał wznawianie?

Aby pozwolić na wznawianie ściągania należy użyć dyrektywy konfiguracyjnej *AllowRetrieveRestart*.
Aby pozwolić na wznawianie wysyłania (uploadu) należy jednocześnie użyć dyrektyw *AllowOverwrite* i *AllowStoreRestart*. Spowodowane jest to tym, że restart/wznowienie wysyłania pliku jest formą zastępowania (nadpisywania) pliku.
Należy zwrócić uwagę na to, że dyrektywy *HiddenStor* i *AllowStoreRestart* nie są ze sobą kompatybilne.

3.13. Jak wyświetlić wiadomość przed zalogowaniem się użytkownika?

Należy użyć dyrektywy DisplayConnected wskazującej który plik zawiera wiadomość mającą się ukazać przed logowaniem.

```
DisplayConnect /ftp/ftp.virtualhost/login.msg
```

3.14. Jak wyświetlić wiadomość po zalogowaniu się użytkownika?

Należy użyć dyrektywy *DisplayLogin*, która wysyła określony plik w formacie ASCII do połączonego użytkownika. [1]

```
DisplayLogin        /etc/proftp.msg
```

4. NAJCZĘŚCIEJ SPOTYKANE PROBLEMY PODCZAS PRACY

4.1. ProFTPD nie działa

Podczas uruchamiania ProFTPD w trybie standalone nie widać procesu przy użyciu "`ps`". Może to być spowodowane wieloma czynnikami, prawdopodobnie czymś takim jak nie uruchamianie ProFTPD jako root (program musi być uruchomiony początkowo z konta root'a, ale później przełączy się na nie uprzywilejowanego użytkownika). Niezależnie ProFTPD zapisuje wszystkie błędy poprzez standardowy mechanizm zapisu błędów (syslog). Należy sprawdzić logi systemowe, aby ustalić gdzie tkwi problem.

To nie działa!

Wielokrotnie może się zdarzyć, że wystąpi całkowicie przypadkowy problem wydający się nierozwiązywalnym. Najlepszym miejscem by spytać o pomoc jest zdecydowanie lista mailingowa (proftpd-l) ale bezproduktywnym jest proszenie o pomoc bez podania wystarczającej ilości informacji na temat problemu.

Czy:

- sprawdziłeś logi systemowe?
- próbowałeś uruchomić serwer w trybie debugowania?
- przeczytałeś FAQ?
- sprawdziłeś archiwum listy mailingowej?
- używasz najnowszej wersji programu?

Jeśli wysyłasz zapytanie na listę mailingową spróbuj podać wystarczającą ilość informacji na temat problemu. Informacje te mogą zawierać (ale nie muszą być ograniczone do):

- system operacyjny i wersję serwera (proftpd -vv),
- listę zainstalowanych modułów (proftpd -l),
- odpowiednie wycinki z logów,
- wynik uruchomienia ProFTPD w trybie debug,
- fragment pliku konfiguracyjnego.

4.2. "inet_create_connection() failed: Operation not permitted"

Nie uruchamiasz ProFTPD jako root, albo masz inetd skonfigurowane do uruchamiania ProFTPD jako użytkownik inny niż root. Demon ProFTPD musi być uruchomiony jako root, aby mieć dostęp do portów tcp niższych niż 1024 lub, aby otworzyć plik z hasłami (shadow password file) podczas autentykacji użytkowników. Demon przełącza uid/gid (identyfikatory użytkowników/grup) na użytkowników i grupy podane w dyrektywie *`User/Group`* podczas normalnej pracy, tak więc polecenie "`ps`" pokaże że program działa na koncie jakie mu podałeś.

4.3. ”Unable to bind to port/Address already in use”

Komunikat "address in use" (adres jest już używany) normalnie oznacza, że ktoś (jakiś program) zajmuje dany adres (port).

Można to sprawdzić poleceniem: `fuser -n tcp 21`

```
debian:/# fuser -n tcp 21
21/tcp:              1042
```

W odpowiedzi otrzymujemy PID procesu używającego tego portu.

Następnie możemy sprawdzić jaki to proces:

```
debian:/# ps aux
USER       PID %CPU %MEM   VSZ  RSS TTY      STAT START   TIME COMMAND
ftpdemon  1042   0.0   0.4   2628 1076 ?          S     22:53    0:00 proftpd: (accepting
connections)
root      1048  0.0  0.6  3576 1612 pts/1    R    22:57   0:00 ps aux
```

W tym przypadku na porcie 21 działa akurat demon proftpd.

Najczęstszym powodem jest to, że ProFTPD jest w trybie *standalone* a *inetd* jest wciąż skonfigurowane dla portu 21. Należy skomentować linię zaczynającą się od "ftp" w pliku */etc/inetd.conf* i zrestartować (*killall -HUP inetd* lub coś podobnego powinno pomóc) i spróbować uruchomić ProFTPD jeszcze raz.

4.4. "(Login failed): Invalid shell"

Użytkownikowi próbującemu się połączyć przyznana została powłoka (shell) nie będąca wymienioną w pliku systemowym */etc/shells.* Domyślnie proftpd wymaga, aby logujący się użytkownicy mieli ważną (uwzględnioną w pliku *shells*) powłokę. Aby wyłączyć to wymaganie należy użyć następującej dyrektywy w pliku konfiguracyjnym:

```
RequireValidShell off
```

4.5. "Fatal: Socket operation on non-socket"

Twój ProFTPD jest skonfigurowany w trybie *inetd* zamiast w *standalone.* W tym trybie ProFTPD oczekuje, że będzie uruchomiony z super-serwera *inetd*, co implikuje że standardowe wejścia/wyjścia (stdin/stdout) będą gniazdami (socket) a nie terminalami. W wyniku czego operacje na gniazdach nie powiodą się i zostanie wypisany powyższy błąd. Jeśli chcesz uruchamiać ProFTPD z powłoki (shell'a), w trybie *standalone*, potrzebujesz zmodyfikować plik konfiguracyjny *proftpd.conf* i dodać (lub zmienić) w nim następującą dyrektywę:

```
ServerType standalone
```

4.6. " Fatal: unable to determine IP address of " nazwa_komputera

Komputer, na którym uruchomiony jest ProFTPD ma źle skonfigurowane ustawienia dotyczące identyfikacji komputera - biblioteka sprawdzająca (resolver) nie może ustalić adresu IP dla tej nazwy komputera. Rozwiązaniem może być poprawa wpisów DNS dla tej domeny, poprawa nazwy hosta, sprawdzenie i ewentualne poprawienie pliku */etc/hosts*. Które z tych rozwiązań zadziała zależy w głównej mierze od systemu operacyjnego i od rodzaju błędu.

4.7. Problemy z klientami ftp za ścianą ogniową (firewall'em)

Specyfikacja FTP określa, że do komunikacji powinny być użyte wyłącznie dwa gniazda (socket). Pierwsze działa na porcie 21 i jest kanałem kontrolnym, poprzez który przesyłane są wszystkie komendy i kody odpowiedzi. Jeśli istnieje potrzeba przesłania danych, na przykład ściągnięcie pliku, pobranie zawartości katalogu - jest tworzony na żądanie drugi kanał, to gniazdo może mieć jedną z dwóch form:

non-Passive (nie pasywne)
Końcówka gniazda (socket) znajdująca się w serwerze pracuje na porcie 20. W ten sposób łatwo można skonfigurować firewall'a

Passive (pasywne)
Port na obu końcach gniazda jest dynamicznie alokowany. Z tego powodu jest niemożliwe poprawne skonfigurowanie firewall'a ponieważ mapowanie (przypisanie) portów do ftp będzie inne za każdym razem, gdy nastąpi przesyłanie danych.

Rozwiązaniem jest zmuszenie użytkowników aby skonfigurowali swoje klienty ftp aby używały trybu nie-pasywnego (np. na porcie 20).

4.8. Czy mogę uruchomić więcej niż jeden VirtualHost na pojedynczym IP?

Nie, a przynajmniej nie w sposób obsługi wirtualnych hostów stosowanym w HTTP/1.1. To ograniczenie jest wprowadzone w dokumentacji RFC dla FTP, w przeciwieństwie do specyfikacji HTTP/1.1 nie ma mechanizmu porównywalnego do nagłówka HTTP "Host: foo.bar.com" specyfikującego do którego hosta odnosi się połączenie. Zatem jedyną metodą określenia do którego wirtualnego hosta odnosi się połączenie jest właśnie przez docelowy adres IP.

Jedynym wyjątkiem od tego jest, jeśli utrzymujesz kilka serwerów na jednym IP, używanie dla każdego z nich odrębnego portu, jakkolwiek wymaga to aby łączący się klienci używali niestandardowych portów - dlatego też prawdopodobnie nie jest dobrym rozwiązaniem przy większej ilości utrzymywanych serwerów.

4.9. Jak uruchomić ProFTPD z inetd?

Znajdź w pliku */etc/inetd.conf* linię wyglądającą mniej więcej tak (o ile wcześniej używany był *ftpd* lub inny serwer ftp):

```
ftp stream tcp nowait root in.ftpd in.ftpd
```

zastąp ją następującą

```
ftp stream tcp nowait root in.proftpd in.proftpd
```

Następnie znajdź numer procesu PID dla *inted*. Można to zrobić w następujący sposób używając polecenia `ps` i `grep`. Polecenie `grep` służy do wyszukiwania w strumieniu wyjściowym określonego ciągu znaków. Jeśli nie jesteś zalogowany na root'a to do polecenia `ps` należy dodać parametry `ax`:

```
debian:~# ps ax |grep inetd
  198  ??  IWs    0:00.00 inetd -wW
```

Tak więc PID *inetd* jest 884. Następnie należy *inetd* wysłać SIGHUP aby się zrekonfigurował - używamy do tego polecenia `kill`. Ponieważ *inetd* jest uruchomione jako root, a nie jesteś zalogowany jako root, trzeba być `su` (super user) aby móc użyć polecenia `kill`.

```
debian:~# /bin/kill -s HUP 198
```

Dlaczego `/bin/kill`? Ponieważ wiele powłok dostarcza polecenie `kill` jako wbudowane w powłokę, więc shell wyśle komendę bezpośrednio a nie używając systemowego `/bin/kill`. Może to być bardzo użyteczne, ale różne powłoki mają różną składnię dla określenia tego samego wysyłanego sygnału. Tak więc zamiast zapamiętywać wszystkie te sposoby łatwiej jest użyć bezpośrednio systemowego `/bin/kill`.

4.10. Czy istnieje możliwość użycia tcp-wrappers z ProFTPD?

Pakiet TCP Wrappers oferuje kontrolę dostępu do zdalnych usług opartą na dopasowaniu wzorca. Za jego pomocą udzielamy lub blokujemy dostęp do określonych usług przez określone zasoby. Pakiet TCP Wrappers to jakby połączenie zapory sieciowej i narzędzi wykrywania intruzów. Można z niego skorzystać używając ProFTPD. Jakkolwiek program posiada wbudowaną kontrolę dostępu na podstawie adresu IP (dyrektywy *`Deny`* i *`Allow`*), jednak wielu administratorów woli ujednolicić kontrolę dostępu korzystając, np. z *in.tcpd*. Jeśli chcesz korzystać z TCP wrappers skonfiguruj ProFTPD żeby działało w trybie inetd jak każdy inny demon współpracujący z tcp wrappers i dodaj odpowiednie linijki do plików *hosts.allow/deny*.
Jeśli używasz ProFTPD w trybie *standalone* moduł *mod_wrap* może być użyty do kierowania serwera do plików *hosts.allow/deny*.

4.11. Czy mogę uruchomić serwer FTP na nie standardowym porcie?

Tak. Użyj bloku *<VirtualHost>* wraz z FQDN (Fully Qualified Domain Name - w pełni uprawnioną nazwą domeny) dla twojego hosta (z DNS'u) lub jego adresem IP, oraz dyrektywy *Port* w bloku *<VirtualHost>*. Na przykład, jeśli twój host jest określony jako "moj_komputer.moja_domena.pl" i chcesz postawić dodatkowy serwer ftp na porcie 2001 plik konfiguracyjny może zawierać coś takiego:

```
<VirtualHost moj_komputer.moja_domena.pl>
      Port 2001
      ...
</VirtualHost>
```

4.12. Czy mogę kontrolować stosunek wysyłania/ściągania (upload/download ratio)?

Tak – umożliwia to moduł *mod_ratio*.
Dyrektywy ratio (stosunku) to cztery liczby: ratio pliku, początkowy kredyt dla plików, ratio bajtów (ilości bajtów), początkowy kredyt dla bajtów. Podanie 0 w którymś z miejsc wyłącza sprawdzanie tego warunku.
Dyrektywy ratio są następujące: *HostRatio* (ratio dla danego hosta: można użyć nazwy domeny, IP, możliwość użycia wzorca - wildcards), *AnonRatio* (sprawdza hasło podane przy logowaniu), *UserRatio* (można stosować "*" aby odnosiło się do każdego użytkownika) i *GroupRatio* (ratio dla grupy użytkowników).

```
Ratios on                              # włączenie modułu
UserRatio ftp 0 0 0 0                  # bez ratio dla użytkownika ftp
HostRatio master.debian.org 0 0 0 0    # bez ratio dla hosta master.debian.org
GroupRatio proftpd 100 10 5 100000     # ratio 100:1 dla plików, kredyt 10 plików,
                                       # 5:1 dla bajtów, kredyt 100k dla bajtów
AnonRatio billg@microsoft.com 1 0 1 0  # ratio 1:1, bez kredytów
```

Wersja 2.0 i wyższe tego modułu integrują się z modułem *mod_sql*. Ograniczeniem modułu mod_ratio jest to, że ratio jest utrzymywane tylko na jedną sesję i nie jest prowadzony zapis korzystania z ratio w wielu sesjach.

4.13. Zbyt wolne logowanie

Jest ono prawdopodobnie spowodowane przez firewall lub timeout (czas zwłoki) z DNS. Domyślnie ProFTPD spróbuje sprawdzić użytkownika korzystając z DNS i inetd - jeśli są one zablokowane lub zostanie przekroczony czas zwłoki spowoduje to wolniejsze niż normalnie logowanie. Aby wyłączyć sprawdzanie przez DNS i inetd należy w pliku konfiguracyjnym zmienić:

```
      UseReverseDNS       off
      IdentLookups        off
```

4.14. Jak mogę zobaczyć kto jest połączony?

Polecenie *ftpwho* pokazuje stan każdego połączenia z serwerem ftp oraz jaka jest jego aktualna aktywność.

4.15. Wiadomość "FTP server shut down ... please try again later."

Zostało wykonane polecenie *ftpshut*. Poszukaj pliku */etc/shutmsg* i usuń go.

4.16. Jak wyłączyć serwer bez zabijania procesu proftpd?

Polecenie *ftpshut* pozwala na odrzucanie wszystkich połączeń przez serwer wyświetlając wiadomość o niedostępności, bez wyłączania procesu proftpd. Wyłączenie to może być w harmonogramie lub natychmiastowe, istniejące połączenia mogą mieć zgodę na zakończenie lub przerwane natychmiastowo. Ponowne przyjmowanie połączeń uzyskuje się przez usunięcie pliku */etc/shutmsg*.

4.17. Czy istnieje możliwość wyłączenia pojedynczego wirtualnego hosta?

Nie, polecenie *ftpshut* działa tylko na poziomie demona a nie na poziomie wirtualnych hostów.

4.18. "Error 421"

Błąd ten oznacza, że "coś poszło źle".

- połączenie przekroczyło czas zwłoki,
- podany w pliku konfiguracyjnym DefaultRoot nie istnieje,
- proces-rodzic serwera został "zabity",
- należy sprawdzić */etc/services,*
- złe uprawnienia dla DefaultRoot.

4.19. proftpd nie ma w liście aktywnych procesów.

Dwa możliwe powody: pierwszy - najprostszy - proftpd po prostu nie został włączony, spróbuj wywołać polecenie `proftpd -n -d2` w trybie debugowania i zobacz, co się stanie. Drugim powodem może być to, że program jest uruchamiany z inetd a nie ma żadnych aktywnych sesji w danym momencie.

4.20. Jak zrestartować/uruchomić ponownie serwer?

Zależy to od trybu, w jakim jest włączony serwer:

inetd
Jeśli nie dokonano zmian w konfiguracji inetd nie trzeba nic robić. Serwer przeładowywuje konfigurację każdorazowo przy nowym połączeniu.

Standalone
Można wyłączyć (poleceniem `kill`) i włączyć serwer jeszcze raz lub wysłać sygnał SIGHUP do głównego procesu demona proftpd.

4.21. "451 append/restart not permitted, try again"

Dyrektywa konfiguracyjna *`AllowStoreRestart`* (pozwól na restart zapisu pliku) w pliku konfiguracyjnym domyślnie jest wyłączona, ponieważ pozwala ona na uszkodzenie każdego zapisywalnego pliku przez złośliwego użytkownika. Zaleca się włączyć tą opcję tylko dla wybranych (autentykowanych) użytkowników i tylko dla wybranych katalogów.

4.22. "501 REST not compatible with server configuration"

Komenda **REST** (RESTART) - ponów transfer. Pole argumentu reprezentuje miejsce, od którego ma być wznowiony transfer wskazanego pliku. Komenda ta nie powoduje transferu całego pliku ale skok do miejsca w którym transfer został przerwany.

Jak jest wspomniane w dokumentacji w opisie dyrektywy konfiguracyjnej *`HiddenStor`*, użycie tej dyrektywy jest niekompatybilne z komendą FTP - REST. Należy albo zabronić użycia komendy REST dyrektywami *`AllowRetrieveRestart`* i *`AllowStoreRestart`*, lub nie używać *`HiddenStor`*.

4.23. "No such group "nogroup"" (nie ma takiej grupy "nogroup")

Domyślnie plik konfiguracyjny ProFTPD używa użytkownika "nouser" i grupy "nogroup", niektóre systemy/dystrybucje nie mają zdefiniowanej grupy użytkowików "nogroup". Rozwiązaniem jest dodanie tej grupy do pliku */etc/groups* lub zmiana wpisu "nogroup" w pliku *proftpd.conf* na grupę która jest już utworzona. [1]

Serv-U

1. WSTĘP

Serv-U wersja 4.0 jest prostym serwerem FTP przeznaczonym pod takie platformy jak Windows 95/98/2000/ME/XP i Windows NT 4.0. Oznacza to, że w łatwy sposób zwykły komputer PC staje się bazą informacji dla innych komputerów znajdujących się w sieci lokalnej lub w sieci Internet. Użytkownicy połączeni z takim PC-tem mogą kopiować, przesuwać, wykonywać, usuwać pliki lub katalogi używając protokołu FTP (File Transfer Protocol).

Serv-U jest programem komercyjnym, co zmusza użytkownika do opłaty rejestracyjnej, jednak możemy bezpiecznie i zgodnie z prawem używać programu przez okres 30 dni bez ponoszenia jakichkolwiek kosztów.
Serv-U jest dostępne w trzech różnych wersjach z różnymi możliwościami:

1. Personal Edition stworzono dla indywidualnych użytkowników. Wersja ta jest całkowicie darmowa jednak wiąże się to z ograniczonymi możliwościami:
   - jedna domena z pojedynczym połączeniem konkurencyjnym,
   - nie więcej niż 5 kont użytkowników,
   - nie ma możliwości mapowania katalogów lub robienia linków,
   - nie dostępna ochrona SSL/TLS.

2. Standard Edition zaprojektowana dla biznesu jak i dla użytkowników indywidualnych. Wersja ta powiększa swoje możliwości w porównaniu z poprzednią, i zawiera:
   - jedna domena z maksymalnie 25-cioma konkurującymi połączeniami,
   - nie więcej niż 100 kont użytkowników,
   - możliwość mapowania i tworzenia linków do katalogów,
   - brak możliwości zdalnego zarządzania,
   - opcjonalnie możliwość ochrony SSL/TLS.

3. Professional Edition adresowana do wymagających i komercyjnych zastosowań. W tej wersji dostępne są następujące możliwości:
   - nieograniczona liczba domen z nielimitowaną liczbą konkurujących połączeń,
   - nieograniczona liczba kont użytkowników,
   - możliwość mapowania i tworzenia linków do katalogów,
   - możliwość zdalnego zarządzania,
   - ochrona SSL/TLS.

Wersja Professional jest dostępna w 30-dniowej wersji trial-owej. W tym czasie użytkownik ma prawo użytkowania i testowania wszystkich opcji bez ograniczeń. Po upływie 30 dni musisz zapłacić opłatę rejestracyjną. [3]

2. INSTALACJA

Po uruchomieniu instalatora zaczyna się proces instalacji, w którym:

- zapoznajemy się z warunkami licencji,
- określimy folder w którym dokonamy instalacji – standardowo będzie to C:\Program Files\Serv-U, możemy zmienić miejsce przeznaczenia klikając przycisk *Browse*
- określamy listę komponentów, jaką chcemy zainstalować:
  - serwer,
  - administratora,
  - plik pomocy,
  - pomoc internetową.

  Przy każdym z komponentów jest liczba określająca rozmiar pamięci, jaki dany komponent będzie zajmował po instalacji. Wybór komponentu zatwierdzamy zaznaczając dany komponent, poniżej listy wyświetlane są liczby reprezentujące całkowity rozmiar pamięci dyskowej potrzebnej do instalacji oraz rozmiar dostępnych zasobów dyskowych.
- określamy nazwę grupy, pod jaką będzie dostępne Serv-U w Menu Start – standardowo wpisane jest 'Serv-U FTP Server'
- instalator pyta nas czy wszystkie wprowadzone wcześniej informacje są poprawne, jeżeli nie to możemy cofnąć się do tyłu wciskając przycisk *Back*, jeżeli jesteśmy pewni wciskamy *Next*.
- instalator dokonuje instalacji, na ekranie możemy zaobserwować postęp w instalacji. Gdy instalacja powiedzie się ujrzymy okno informujące nas o tym
- kolejnym oknem, jakie pojawi się na naszym ekranie jest okno z zapytaniem czy chcemy zainstalować ikony na pulpicie i czy chcemy uruchomić program Serv-U Administrator (odpowiadamy wedle uznania). [3]

3. URUCHOMIENIE

3.1 Uruchomienie - pierwsza metoda

Aby uruchomić serwer korzystamy ze skrótu znajdującego się na pulpicie (o ile takowy utworzyliśmy), albo odszukujemy program Serv-U Administrator w Menu Start. Na początku administrator musi zdecydować czy serwer ma być automatycznie uruchamiany podczas startu komputera. Jeżeli nawet serwer nie będzie się włączał podczas startu komputera to i tak będzie go można włączyć w dowolnym momencie np. poprzez ikonę znajdującą się w tray-u.

Najszybszą drogą do ustawienia pierwszej domeny i konta użytkownika jest metoda kreatora. Kreator automatycznie jest wywoływany podczas pierwszego uruchomienia. Kreator zadaje serię pytań, na które należy udzielić odpowiedzi.

- określamy adres IP, możemy zostawić to pole puste w przypadku, gdy korzystamy z połączenia modemowego z Internetem (przy każdym połączeniu jest nam przyznawany inny adres IP)
- określamy nazwę domeny, może to być dowolna nazwa
- kolejne pytanie dotyczy anonimowego konta użytkownika tzn. możemy utworzyć specjalne konto o nazwie „Anonymous", które nie wymaga hasła. Jeżeli utworzymy konto Anonymous to kreator zapyta nas o ścieżkę dostępu do katalogu domowego. Ścieżkę możemy określić rozwijając pasek z drzewem katalogów zorganizowanych na dysku. Gdy już określimy katalog domowy możemy sprawić, aby nasz użytkownik anonimowy mógł się poruszać i widzieć tylko to, co znajduje się w katalogu domowym i nic poza tym ('Lock user In home directory').
- odpowiadając na kolejne pytanie YES stworzymy konto użytkownika z hasłem – podajemy nazwę użytkownika jego hasło oraz oczywiście katalog domowy.

- możemy również określić przywileje dla stworzonego użytkownika, do wyboru mamy
    - Bez przywilejów
    - Administrator grupy
    - Administrator domeny
    - Administrator systemu
    - Read-only Administrator
- ostatnie okno finalizuje nasze wszystkie powyższe ustawienia.

3.2 Uruchomienie - druga metoda

Jeśli nie skorzystamy z pomocy kreatora, możemy wszystkich ustawień dokonać ręcznie.

- klikamy podwójnie na '<<Local Server>>' po lewej stronie okna, powinien zastartować serwer i rozwinąć się drzewo dostępnych opcji,
- klikamy na 'Domain' w drzewie po lewej stronie okna,
- z menu wybieramy „Domains/New Domain",
- określamy adres IP, możemy zostawić to pole puste w przypadku, gdy korzystamy z połączenia modemowego z Internetem (przy każdym połączeniu jest nam przyznawany inny adres IP),
- określamy nazwę domeny, może to być dowolna nazwa,
- możemy zmienić port na którym będzie umieszczony nasz serwer, standardowo ustawiony jest port 21,
- stworzyliśmy nową domenę, w oknie po lewej stronie pojawiają się nowe pozycje w drzewie,
- klikamy na pozycję 'Users' w drzewie po lewej stronie okna,
- z menu wybieramy „Users/New User",
- wpisując użytkownika 'anonymous' i nie podają hasła tworzymy użytkownika anonimowego, który jest domyślnym i standardowym użytkownikiem we wszystkich programach FTP,
- określamy katalog domowy dla stworzonego użytkownika,
- blokujemy możliwość wyjścia poza katalog domowy zaznaczając pytanie 'Lock user In home directory',
- po wykonaniu powyżej opisanych czynności konto Anonymous jest gotowe do użycia.

4. ADMINISTRACJA

Serv-U Administrator jest programem, który umożliwia administratorowi konfigurować serwer: tworzyć domeny, definiować użytkowników, udostępniać zasoby plikowe. Najprostszą metodą uruchomienia programu Serv-U Administrator jest podwójne kliknięcie na ikonę znajdującą się w tray-u. Jeżeli nie ma tam ikony, program można uruchomić z Menu Start. Program Serv-U jest pojedynczą instancją aplikacji umożliwiającej uruchomienie wielu wirtualnych serwerów FTP. Każdy Serwer FTP jest nazywany domeną („domain"), każda domena posiada użytkowników, grupy oraz ustawienia unikalne dla każdej domeny (takie jak ograniczenia).

4.1 Serwer

4.1.1 Ustawienia serwera (Server Settings)

General – dokonujemy ustawień globalnych tzn. obowiązujących wszystkich użytkowników na danym serwerze:

Max. speed
Maksymalna prędkości przesyłu danych tzn. jaką szerokość pasma sieciowego będzie zajmował Serv-U. Jeżeli pozostawimy to pole puste to będzie wykorzystywana maksymalnie dostępna szerokość pasma.

Max. no. of users
Ta liczba określa maksymalną liczbę użytkowników jaka może jednocześnie być podłączona.

Check anonymous passwords
Zaznaczenie tej opcji powoduje że podczas logowania się użytkownika anonimowego będzie sprawdzane jego hasło i musi mieć ono formę adresu e-mail. Jeżeli pozostawimy tę opcję niezaznaczoną jako hasło można użyć dowolnego stringu.

Delete partially uploaded files
Zaznaczenie tej opcji spowoduje, że ściągnięte pliki nie do końca będą automatycznie usuwane. Standardowo ta opcja jest odznaczona, co powoduje że po wznowieniu przerwanego połączenia z serwerem częściowo ściągnięty plik będzie dociągany.

Block anti time-out schemes
Zaznaczenie tej opcji spowoduje, że nawet po długiej bezczynności użytkownika nie zostanie wylogowany wylosowany serwera

Block FTP_bounce attacks
Ta opcja powoduje że serwer zezwala jedynie na transfer pomiędzy klientem FTP a serwerem, i blokowane są wszystkie inne bezpośrednie próby transferu pomiędzy serwerami. Funkcja ta ogranicza możliwość złośliwych ataków.

Block users who connect more than XX times within YY seconds for ZZ minutes
Jeżeli użytkownik będzie próbował zalogować się więcej niż XX razy na YY sekund to jego konto zostanie zablokowane na ZZ minut.

Dir Cache - ta zakładka dostarcza nam opcji do ustawienia jaką długość i jaki czas ma być przechowywana lista w pamięci cache

Advanced – te opcje wpływają na ogólne zachowanie i funkcjonalność serwera. Domyślnie wszystkie opcje ustawione są optymalnie dla naszych potrzeb.

Serwer
Te ustawienia dotyczą ustawień serwera i odnosi się haseł, oraz zabezpieczeń przed zmianami z zewnątrz osobom nie mających uprawnień administratora.

Sockets
Te opcje pozwalają nam na konfigurowanie, jakie „wtyczki" są aktywne tzn. możemy np. rozkazać, aby co jakiś czas wysyłał pakiet wykrywający przerwane połączenia.

File Uploads
Określa, jakie prawa mają inni użytkownicy lub procesy podczas wysyłania danego pliku

File Downloads
określa, jakie prawa mają inni użytkownicy lub procesy podczas ściągania danego pliku

4.1.2 Działania (Activity)

Zakładka ta jest wielce pomocna administratorowi, gdyż może on na bieżąco śledzić cały ruch na serwerze. W oknie po prawej stronie dostępne są trzy zakładki, które mówią o podłączonych użytkownikach, zablokowanych adresach IP oraz zdarzeniach jakie miały miejsce podczas danej sesji.

Users (Użytkownicy)
to okno zawiera informacje o zalogowanych użytkownikach na serwerze, każdy z użytkowników dostaje numer identyfikacyjny. Przed numerem ID wyświetla się ikona informująca, jakie działanie przeprowadza użytkownik. Znajdują się tutaj informacje o adresie IP zalogowanego użytkownika, na jakie konto użytkownik załogował się, jakie wykonuje obecnie działanie, np. może ściągać jakieś pliki - wtedy podawany jest, jaki jest stopień zaawansowania ściąganego pliku (w procentach). Dodatkowa znajdują się tu informacje, w jakim katalogu obecnie przebywa użytkownik, oraz jego ostatnie polecenie (w kolumnie *Last Command*). Używając prawego przycisku myszki administrator może do użytkownika wysłać wiadomość, lub też usunąć użytkownika z serwera, może usunąć go i zablokować wejście na konto na określony czas lub usunąć użytkownika i zabronić wejście na konto całkowicie (ta zmiana jest również widoczna w opcji '*IP Access*' danego konta użytkownika). Najbardziej represyjną opcją jest wyrzucenie użytkownika z serwera i wyłączenie konta. Istotną właściwością w zakładce *Users* jest możliwość włączenia 'szpiegowania' (*Spy on user*) użytkownika. Po włączeniu tej opcji w menu pojawia się nowa zakładka z numerem użytkownika i nazwą konta, na jakie jest zalogowany. Śledzenie to dostarcza administratorowi serwera szczegółowych informacji na temat poczynań danego użytkownika. W dolnej części okna wyświetlane są statystyki dotyczące serwera oraz użytkownika. Są to min. czas, jaki użytkownik przebywa na serwerze, (data oraz godzina), czas bezczynności użytkownika, średnią szybkość transferu w obie strony, ilość transferowanych danych (w KB), oraz wykorzystanie zasobów dyskowych do robienia upload-ów. Ostatnią, choć jedną z ważniejszych możliwości w tym oknie jest opcja '*Auto reload*', która powoduje automatyczne odświeżanie wszystkich informacji dostępnych w tym oknie.

Blocked IPs
ta opcja pozwala na śledzenie jakie adresy IP nie mają dostępu do serwera i na jaki czas ich dostęp został zabroniony.

Session Log
w tej zakładce administrator znajduje informacje na temat aktualnej sesji. [3]

4.2 Domena

4.2.1 Ustawienia domeny (Domain Settings)

General - wszystkie dokonywane ustawienia w tej zakładce oraz w zakładkach znajdujących się na tym poziomie dotyczą ustawień danej domeny czyli wszystkich użytkowników znajdujących się w danej domenie.

Max. no. of users
określamy maksymalną liczbę użytkowników mogących się podłączyć w tym samym czasie. Jeżeli zostawimy to pole puste to nie będzie ograniczenia na liczbę użytkowników.

Virtual path mappings
ta opcja pozwala na mapowanie fizycznej ścieżki na inny katalog. Jest to wygodny sposób robienia wirtualnych odnośników do plików lub katalogów znajdujących się na innych dyskach lub komputerach. Klękając przycisk '*Add'* rozpoczynamy proces mapowania, najpierw ustalamy ścieżkę fizyczną katalogu który chcemy mapować. Następnie podajemy katalog na który mapujemy, będzie to katalog użytkownika lub katalog domowy. Podając katalog, na który mapujemy, oprócz podania konkretnej ścieżki możemy użyć wpisu: %HOME% - katalog domowy użytkownika.
Na końcu procedury mapowania określamy wirtualną nazwę, która będzie wyświetlana na ekranie monitora użytkownika serwera FTP. Po zakończonej procedurze możemy ją edytować w celu dokonania jakiś zmian (*Edit*) lub też usunąć (*Delete*). Stworzenie wirtualnego katalogu (mapowanie) nie spowoduje automatycznego dodania tego katalogu do listy dostępnych katalogów, jaką posiada użytkownik. Aby mapowany katalog był widoczny przez użytkownika serwera FTP należy określić jego prawa w ustawieniach użytkownika (*Domains/Users/Name_User*).

Links
to standardowa opcja tworzenia skrótów do katalogów.

IP Access – opcja ta pozwala na ustanowienie pewnych praw dla użytkowników, tzn. można komuś zezwolić na dostęp do serwera lub go mu zabronić. Dozwolone jest stosowanie pewnego rodzaju uogólniania, tzn. można zabronić lub zezwolić użytkownikom wejście na serwer, jeżeli jego IP spełnia pewne warunki np.

`192.168.11.xx`	dowolne IP o dwu cyfrowych końcówkach adresu
`192.168.11.34-201`	wszystkie IP z przedziału 34 - 201
`192.168.11.*`	w tym przypadku wszystkie adresy IP lokalne mają określone prawo
`?`	prawa są określone dla użytkownika o nazwie składającej się z jednego znaku.

Ważną sprawą jest zdanie sobie sprawy, że jeżeli nadamy jakieś ograniczenia tzn. np. pozwolimy, aby dostęp miał jakiś adres IP to nie będzie możliwe załogowanie się na to konto żadnemu innemu użytkownikowi z innym adresem IP.

Messages – ta opcja umożliwia wysyłanie komunikatów przez serwer do użytkownika podczas różnych zdarzeń np. podczas logowania.

Logging – opcja ta pozwala administratorowi na określenie czy informacje o zdarzeniach na serwerze mają być zapisywane do pliku, jeśli tak to, w jakiej formie i jakie informacje trafią do pliku. Oczywiście w linii ‘Log file name‘ należy podać ścieżkę dostępu do pliku – czyli wskazać konkretny plik na dysku. Administrator może również określić, jakie informacje będą wyświetlane w *Activity/Domain Log.*

UL/DL Ratios - ta opcja umożliwia, określenie plików które mogą być ściągane bez konieczności sprawdzenia prawa „współczynnika stosunku”. Można tu podawać konkretne ścieżki dostępu do plików lub samą nazwę pliku bez ścieżki dostępu – co będzie oznaczać że zasada ta będzie dotyczyła się wszystkich plików na dysku o takiej nazwie.

4.2.2 Działania (Activity)

Ta opcja ma podobne możliwości jak opisana powyżej (przy serwerze) jedynie różni się tym, że wszystkie te statystyki dotyczą danej domeny, a nie całego serwera. [3]

4.2.3 Użytkownicy (Users)

Ta opcja pozwala na stworzenie konta użytkownika, liczba stworzonych kont jak wiadomo zależy od wersji programu Serv-U. Po utworzeniu jakiegoś konta klikając na jego nazwę dostępne są kolejne zakładki w drzewie. Wszystkie dokonywane tutaj ograniczenia będą dotyczyły wyłącznie tego użytkownika.

Ustawienia użytkownika

Account – pozwala na ustawienie nazwy użytkownika, grupy - do jakiej należy oraz hasła. Jednym z koniecznych ustawień w tej zakładce jest podanie ścieżki dostępu do katalogu domowego. Kolejnym istotnym parametrem ustawianym w tej zakładce jest *Privilege* – przywileje tzn. jaki status ma użytkownik. Status wybieramy z listy dostępnych statusów. Można również ograniczyć prawo do poruszania się po katalogu domowym tzn. można zabronić wychodzenia powyżej katalogu domowego „*Lock user in home directory*”. Można również wyłączyć danego użytkownika, blokując jego konto poprzez zaznaczenie opcji ‘*Disable account*’

General – ta opcja pozwala na ustawienie podstawowych parametrów transferu oraz zasad obowiązujących na danym koncie. Ustawienia te są lokalne, czyli dotyczące danego użytkownika, jednak ustawienie jakiegoś parametru na wartość większą (np. transferu ściągania plików) od wartości, jaką wcześnie ustawiliśmy dla całej domeny spowoduje, że to ustawienie będzie ignorowane. Dzieje się tak, gdyż ustawienia dla domeny mają większy priorytet niż ustawienia dla użytkownika, tak samo jest przy ustawieniach dla serwera, one mają najwyższy priorytet.

Hide 'hidden' files
ta opcja pozwala na zezwolenie użytkownikowi oglądanie plików lub katalogów, które są ukryte. Jeżeli zaznaczymy tę opcję to pliki ukryte nie będą widoczne dla użytkownika. Opcja ta jest użyteczna, jeżeli w katalogu znajdują się jakieś linki do innych plików lub katalogów lub w danym katalogu zawarte są jakieś pliki zawierające komunikaty lub pliki, które rejestrują zdarzenia na koncie (Log file).

Always allow login
ta opcja pozwala na załogowanie się na konto nawet w przypadku, gdy na serwerze zalogowana jest już maksymalna liczba użytkowników. Opcja ta jest użyteczna szczególnie dla konta administratora.

Allow only X login(s) from the same IP address
zapobiega logowaniu na konto użytkownika więcej niż X razy z pod tego samego adresu IP. Niektóre programy przeglądające serwery FTP dla każdego ściąganego pliku nawiązują nowe połączenie np. Internet Explorer. Zaleca się, aby nie ustawiać mniej niż 2 połączenia z tego samego adresu IP, gdyż gwarantuje to bezproblemową pracę użytkowników na koncie.

Allow user to change password
zamarkowanie tej opcji pozwoli użytkownikowi konta na zmianę hasła dostępowego do konta zdalnie. Używając programów takich jak FTP Voyager użytkownik ma możliwość zmiany hasła do konta. Opcja ta jest użyteczna gdy konto użytkownika jest przeznaczone tylko dla jednego użytkownika, w przypadku, gdy z konta korzysta kilku użytkowników nie zaleca się markowania tej opcji.

Max. upload and download speed
określa jaka szerokość pasma będzie dostępna dla danego użytkownika, dotyczy się to zarówno ściągania jak i wysyłania plików na serwera. Wartość ta powinna być mniejsza od tej ustawionej w ustawieniach transferu domeny jak i serwera.

Idle time-out
za pomocą tej opcji określa się czas, po jakim połączenie zostanie przerwane gdy użytkownik nie będzie wykazywał żadnej aktywności. Zaleca się nie ustawianie czasu mniejszego niż 5 min, gdyż użytkownicy, którzy mają dostęp do Internetu poprzez słabe łącza, będą mogli spokojnie dokończyć transfer plików.

Session time-out
określa czas, po jakim połączenie zostanie zerwane, nie ważne jest czy użytkownik zakończył transfer plików czy nie. Połączenie jest natychmiast zrywane a kontynuowanie połączenia jest możliwe po odczekaniu 1 min. Ta opcja jest wygodna, gdy serwer jest oblegany przez wielu użytkowników, a kolejka oczekujących na połączenie użytkowników jest duża. Określenie czasu sesji daje szanse innym użytkownikom na zalogowanie się na serwer.

Max. no. of users
liczba określa maksymalną liczbę użytkowników zalogowanych na dane konto.

Login message file
określa plik z którego serwer odczyta wiadomość i wyśle do użytkownika podczas logowania się na dane konto.

Password type
pozwala na wybranie typu haseł

Dir Access – konfiguruje prawa do katalogów i plików dla danego użytkownika. Użytkownikowi można nadać min. następujące prawa:

Do pliku:
- czytania
- zapisywania
- dodawania
- usuwania
- wykonywania

Do katalogów:
- wyświetlania zawartości
- tworzenia
- przenoszenia

Dziedziczenie praw przez podkatalogi

IP Access – podobnie jak w ustawieniach dla domeny z tą różnicą, że nadane prawa będą dotyczyły wyłącznie danego konta, a nie jak tam wszystkich użytkowników znajdujących się w domenie. Należy pamiętać, że wprowadzone ograniczenia w domenie mają wyższy priorytet niż ograniczenia wprowadzone dla konta.

UL/DL Ratios – pozwala na określenie praw dotyczących „pożyteczności" użytkownika tzn. można zażądać od użytkownika aby w zamian za ściągnięte pliki z serwera pozostawił na nim jakieś swoje pliki. Niekoniecznie musi to być plik za plik, można ustalić jakiś stosunek np. 1/10 tzn. za 1 plik pozostawiony na serwerze użytkownik może pobrać 10 plików. Stosunek ten może odnosić się również do rozmiaru plików tzn. za pozostawione 100Mb na serwerze, użytkownik może pobrać 1Gb informacji. Dodatkowo kontrola tej zasady może odbywać się w ciągu jednej sesji lub też może dotyczyć wielu sesji. Użytkownik może również dostać tzw. bonusa tzn. pobrać określoną liczbę plików lub określony rozmiar danych „za darmo"- nie pozostawiając na serwerze nic ('Preset/Current').

Quota – określa, jakie zasoby dyskowe zostały posiada dany użytkownika. Opcja ta dotyczy przestrzeni dyskowej, jaka została przyznana użytkownikowi do pozostawiania na dysku serwera plików.

Enable disk quota
włączamy ograniczanie przestrzeni dyskowej.

Current X KB
ta opcja pokazuje obecne zasoby konta użytkownika tzn. ile danych użytkownik pozostawił na serwerze (w KB).

Maximum X KB
ta opcja pokazuje ile miejsca zostało przeznaczone na dane użytkownika, jest to wartość maksymalna. Gdy użytkownik pozostawi na dysku tyle danych ile jest określone w tym polu to próba dalszego wgrywania danych na dysk serwera zakończy się niepowodzeniem (serwer odmówi dostępu użytkownikowi).

Calculate current
wciśnięcie tego przycisku spowoduje obliczenie wolnej przestrzeni dyskowej dla danego użytkownika.

4.2.4 Grupy

Serv-U umożliwia grupowania pewnej liczby użytkowników w grupy którymi jest łatwiej zarządzać. Nową grupę tworzymy klikając prawym przyciskiem myszy na zakładkę *Groups* w drzewie po lewej stronie okna lub wybierając z górnego menu ikonę *New Group* Po nadaniu nazwy grupie po prawej stronie ekranu pojawiają się kolejne opcje:

Account - umożliwia zmianę nazwy grupy, oraz zrobienie notatki która ułatwia rozpoznawanie jakiego typu to jest grupa i po co została stworzona (notatkę wykonuje administrator). Opcja ta jest szczególnie przydatna przy bardzo rozbudowanych serwerach.

Dir Access - określa prawa do katalogów i plików w danej grupie.

IP Access - podobnie jak przy ustawieniach dla domeny. [3]

LITERATURA

[1] http://www.proftpd.org/docs/faq/faq_full.html
[2] http://proftpd.linux.co.uk/localsite/Userguide/other/userguide_full.html
[3] http://www.serv-u.com/
[4] RFC 959

DODATEK 1: KODY ODPOWIEDZI SERWERA FTP.

Odpowiedzi serwera składają się z trzycyfrowego kodu odpowiedzi i z tekstu komentarza. Cyfry kodu odpowiedzi mają ściśle określone znaczenie. Pierwsza cyfra określa generalnie czy odpowiedź jest dobra, zła, niekompletna:

- **`1xx`** - odpowiedź poprawna wstępna - oznacza zainicjowanie operacji, klient powinien poczekać na zakończenie operacji, co zostanie potwierdzone kolejną odpowiedzią od serwera,
- **`2xx`** - odpowiedź poprawna kompletna,
- **`3xx`** - odpowiedź częściowo poprawna, serwer oczekuje na dodatkowe dane,
- **`4xx`** - odpowiedź chwilowo niepoprawna, serwer w tej chwili nie może przeprowadzić żądanej akcji,
- **`5xx`** - odpowiedź jednoznacznie negatywna, błędna.

Druga cyfra przyporządkowuje odpowiedź do określonej kategorii odpowiedzi lub błędu:

- **`x0x`** - błąd składniowy polecenia,
- **`x1x`** - odpowiedź informacyjna,
- **`x2x`** - odpowiedź dotycząca połączenia lub sesji,
- **`x3x`** - odpowiedź dotycząca procesu autoryzacji,
- **`x4x`** - nie określono,
- **`x5x`** - odpowiedź dotycząca systemu plików serwera.

Znaczenie trzeciej cyfry nie jest wyspecyfikowane. Pełni ona rolę uściślającą dla dwóch poprzednich cyfr. Przedstawimy teraz dokładne znaczenie poszczególnych kodów trzycyfrowych używanych w protokole FTP (w kolejności liczbowej):

- **110** - odpowiedź na polecenie REST,
- **120** - usługa będzie gotowa za nnn minut,
- **125** - połączenie danych już otwarte; transfer rozpoczęty,
- **150** - plik poprawny; połączenie danych zostanie otwarte,
- **200** - poprawne polecenie,
- **202** - polecenie niezaimplementowane, zbyteczne,
- **211** - status systemu lub tekst pomoc,
- **212** - status katalogu,
- **213** - status pliku,
- **214** - tekst pomocy,
- **215** - nazwa systemu,
- **220** - serwer gotowy na przyjęcie nowego użytkownika,
- **221** - serwer zamknął połączenie sterujące,
- **225** - otwarto połączenie danych; nie rozpoczęto żadnego transferu,
- **226** - zamknięto połączenie danych, poprawnie zakończony transfer,
- **227** - serwer ustawił gniazdo nasłuchujące dla połączenia danych;

Odpowiedź zawiera dane w postaci (hl,h2,h3,h4,pl,p2), gdzie hl-h4 i pl-p2 to liczby dziesiętne, które określają adres IP i numer portu gniazda:

- **230** - użytkownik zalogowany,
- **250** - żądana operacja na pliku poprawna, zakończona,
- **257** - plik lub katalog utworzony,
- **331** - nazwa użytkownika zaakceptowana, serwer oczekuje na polecenie PASS,
- **332** - serwer żąda polecenia ACCT,
- **350** - żądana operacja na pliku wymaga dalszych danych,
- **421** - usługa niedostępna, zamknięto połączenie sterujące,
- **425** - nie można otworzyć połączenia danych,
- **426** - połączenie zerwane; transfer przerwany (AGOR),

- **450** - żądana operacja na pliku nie może być wykonana, plik niedostępny,
- **451** - akcja przerwana; lokalny błąd przetwarzania na serwerze,
- **452** - żądana akcja nie może być wykonana, za mało miejsca w systemie plików serwem,
- **500** - błąd składni; polecenie nierozpoznane,
- **501** - błąd składni w parametrach,
- **502** - polecenie niezaimplementowane,
- **503** - niepoprawna sekwencja poleceń,
- **504** - polecenie niezaimplementowana dla tego parametru,
- **530** - użytkownik niezalogowany,
- **532** - brak uprawnień do zapisu plików,
- **550** - żądana operacja nie może być wykonana, plik niedostępny,
- **551** - operacja przerwana; błąd stronicowania,
- **552** - żądana operacja na pliku przerwana; przekroczona alokacja,
- **553** - żądana operacja nie może być wykonana; nazwa pliku niedostępna. [4]

DODATEK 2: KOMENDY FTP

Chociaż dzisiaj coraz rzadziej już używa się do połączeń FTP klientów pracujących w trybie tekstowym, możemy nieraz spotkać się z sytuacją, w której będziemy musieli z nich skorzystać - np. gdy pod ręką nie będzie wygodniejszego programu. Wówczas pomocny może okazać się prezentowany poniżej zestaw najważniejszych poleceń FTP. Na początek można również wpisać komendę help, która przedstawia listę dostępnych poleceń wraz z ich składnią.

1. Komendy kontroli dostępu

Następujące komendy określają kontrole dostępu (nazwy komend podane są w nawiasach okrągłych):

USER NAME (USER) - logowanie
Argumentem tej komendy jest ciąg znaków identyfikujących logującego się użytkownika. Ta komenda jest przeważnie pierwszą wysłaną do serwera komendą zaraz po nawiązaniu połączenia z serwerem. Dodatkowymi informacjami identyfikującymi są komenda ***PASSword*** i/lub komenda ***ACCounT*** która jest wymagana przez niektóre serwery.

PASSWORD (PASS) - hasło
Argumentem tej komendy jest ciąg znaków będących hasłem logującego się uzytkownika. Komenda ta musi zostać bezzwłocznie wprowadzona po komendzie ***USERname***.

ACCOUNT (ACCT) - konto
Argumentem tej komendy jest ciąg znaków określający konto użytkownika. Komenda ta nie jest bezpośrednio związana z komendą ***USERname*** lecz niektóre serwery jej wymagają w celu określenia dostępu. Każdej z sytuacji tzn. żądanie lub brak żądania komendy ***ACCounT*** ma swój określony kod zwrotny (wysłany przez serwer):
- komenda jest wymagana do zalogowania, po pomyślnym zalogowaniu wysyłany jest kod 332.
- gdy nie jest ona wymagana, po pomyślnym zalogowaniu wysyłany jest kod 230

CHANGE WORKING DIRECTORY (CWD) - zmiana folderu
Komenda ta pozwala użytkownikowi na zmianę folderu. Argumentem tej komendy jest ścieżka dostępu określająca folder, do którego żądamy dostępu.

CHANGE TO PARENT DIRECTORY (CDUP) - zmień folder na nadrzędny
Komenda ta jest specjalnym przypadkiem komendy ***CWD*** i została ona wprowadzona, aby ułatwić programom transferowanie drzewa katalogowego pomiędzy systemami mającymi różną składnie nazewnictwa dla folderu nadrzędnego.

STRUCTURE MOUNT (SMNT) - montowanie struktury
Komenda ta pozwala użytkownikowi na zamontowanie innego systemu plików bez ponownego logowania. (dotyczy systemów UNIX - Linux, ale planuje się je zaimplementować w klientach systemu Windows)

REINITIALIZE (REIN) - reinicjalizacja
Komenda ta rozłącza użytkownika, czyszcząc zajęte przez niego porty wejścia/wyjścia oraz pozwalają trwającemu już transferowy na jego dokończenie. Wszystkie parametry są resetowane do standardowych ustawień. Następnie połączenie zostaje nawiązane ponownie. Po tej komendzie następna w kolejności jest oczekiwana komenda ***USER***.

LOGOUT (QUIT) - wylogowanie
Komenda ta rozłącza użytkownika i jeżeli nie jest kopiowany żaden plik, serwer zamyka połączenie. Jeżeli transfer pliku jest w toku, połączenie pozostaje otwarte do momentu otrzymania odpowiedzi o przerwaniu transferu, a następnie serwer zamyka połączenie.
Nieoczekiwane zerwanie połączenie powoduje, że serwer wykonuje za użytkownika komendę ***ABORt*** oraz logout (***QUIT***). [4]

2. Komendy transferu

Wszystkie parametry transferu mają swoją standardową wartość, i w związku z tym komendy te są wysyłane razem z parametrami tylko i wyłącznie wtedy, gdy różnią się one od standardowych. Standardową wartością jest ostatnio ustawiona wartość, lub jeżeli żadna wartość nie została ustawiona to jest ona taka jak opisana poniżej. Powoduje to, że serwer musi "pamiętać" odpowiednie ustawienia. Następujące komendy ustalają parametry transferu:

DATA PORT (PORT)
Argumentem jest numer portu serwera dla data port'u użytego przy tworzeniu kanału data connection. Numery takich portów są już standardowo ustawione dla serwera i klienta, i normalnie użycie tej komendy nie jest potrzebne.

PASSIVE (PASV) - tryb pasywny
Komenda ta prosi serwer, aby ten słuchał na data port (który nie jest standardowym data port'em) i czekał na połączenie niż sam inicjował połączenie. Odpowiedz na tą komendę zawiera host'a i numer portu na którym serwer nasłuchuje.

REPRESENTATION TYPE (TYPE) - typ reprezentacji danych
Argument określa tryb reprezentacji szczegółowo opisany w RFC 959 w sekcji Data Representation and Storage.

Każdemu typowi przyporządkowano kod:
A - ASCII (N, T, C)
E - EBCDIC (N, T, C)
I - image

N - Non-print; T - Telnet format effectors; C - CarriageControl (ASA)

Standardowym ustawieniem jest typ ASCII Non-print.

FILE STRUCTURE (STRU) - struktura pliku
Argumentem jest pojedynczy znak określający strukturę pliku opisaną w RFC 959 w sekcji Data Representation and Storage.

Następujące kody zostały przypisane odpowiednim strukturom:
F - File (no record structure)
R - Record structure
P - Page structure

Standardowym ustawieniem jest File.
(dotyczy systemów UNIX - Linux, ale planuje się je zaimplementować w klientach systemu Windows)

TRANSFER MODE (MODE) - tryb transferu
Argumentem tej komendy jest pojedynczy znak określający tryb transferu opisany w RFC 959 w sekcji Transmition Modes.

Następujące kody zostały przypisane odpowiednim trybom:
S - Stream - Strumień
B - Block - Blok
C - Compressed - W postaci zkompresowanej

Standardowym ustawieniem jest Stream.

3. Komendy usług FTP

Komendy usług FTP definiują transfer pliku lub system plików zażądanych przez użytkownika. Argumentami tych komend będą przeważnie ścieżka dostępu do pliku. Składnia ścieżki dostępu musi odpowiadać regułom panującym na serwerze.
Do grupy tych komend należą:

RETRIVE (RETR) - pobierz - download
Komenda ta powoduje, iż serwer transferuje kopie pliku, sprecyzowanego w ścieżce dostępu, do innego serwera lub użytkownika na drugim końcu data connection. Status i zawartość pliku na serwerze powinna zostać niezmieniona.

STORE (STOR) - załaduj - upload
Ta komenda sprawia, że serwer zaakceptuje dane przesłane do niego za pomocą data connection i zapisze je na nim jako plik. Jeżeli plik o tej nazwie już na serwerze istnieje to użytkownik mając odpowiednie prawa może nadpisać istniejący plik. Jeżeli plik taki nie istnieje to tworzony jest nowy.

STORE UNIQUE (STOU) - załaduj unikalnie
Komenda ta zachowuje się podobnie do ***STORe*** z tą różnicą, że jeżeli na serwerze w danym folderze istnieje już plik o tej samej nazwie z jaką chcemy zapisać nowy plik, generowana jest nowa nazwa pod jaką zostaje ten plik zapisany. Odpowiedź zawiera ”250 Transfer started” wraz z wygenerowaną nazwą.

APPEND (with create) (APPE) - dodaj, dołącz

Ta komenda sprawia, że serwer zaakceptuje dane przesłane do niego za pomocą data connection i zapisze je na nim jako plik. Jeżeli plik sprecyzowany w ścieżce dostępu istnieje na serwerze, wtedy dane zostaną dodane do istniejących. W przeciwnym wypadku plik sprecyzowany w ścieżce dostępu zostanie stworzony od nowa.

ALLOCATE (ALLO) - przydziel

Komenda ta może być wymagana przez niektóre serwery do rezerwacji wystarczającej ilości miejsca do zapisania w całości transferowanego pliku. Argumentem tej komendy jest długość pliku, który ma być transferowany.

RESTART (REST) - ponów transfer

Pole argumentu reprezentuje miejsce, od którego ma być wznowiony transfer wskazanego pliku. Komenda ta nie powoduje transferu całego pliku, ale skok do miejsca w którym transfer został przerwany.

RENAME FROM (RNFR) - zmień nazwę ścieżki dostępu z…

Komenda określa starą ścieżkę dostępu do pliku która ma być zmieniona na nową. Po tej komendzie musi być wprowadzona komenda ***RENAME TO*** określająca nową ścieżkę dostępu.

RENAME TO (RNTO) - zmień nazwę ścieżki dostępu na

Komenda która musi wystąpić zaraz po ***RENAME FROM*** i która określa nową ścieżkę dostępu do pliku.

ABORT (ABOR) - przerwij ostatnią komendę

Komenda ta mówi serwerowi, aby ten przerwał poprzednią komendę usług FTP i każdy związany z nią transfer. Zamykany jest data connection, ale control connection nie, przez co można wykonywać inne operacje.

Istnieją dwa przypadki w których komenda ***ABORt*** zadziała:
- ostatnia komenda usług FTP została pomyślnie zakończona
- ostatnia komenda usług FTP jest w trakcie realizacji

W pierwszym przypadku serwer zamyka data connection (jeżeli jest on otwarty) i odpowiada kodem 226, która mówi, że komenda ***ABORt*** została pomyślnie wykonana.

W drugim przypadku serwer przerywa transfer i zamyka data connection zwracając kod 426 informując, że transfer się nie powiódł, a następnie wysyłając kod 226 który stwierdza poprawne wykonanie komendy ***ABORt***.

DELETE (DELE) - skasuj

Komenda ta powoduje, że plik określony ścieżką dostępu zostaje usunięty z serwera.

REMOVE DIRECTORY (RMD) - usuń folder

Komenda powoduje usunięcie folderu lub podfolderu określonego ścieżką dostępu.

MAKE DIRECTORY (MKD) - utwórz folder

A ta z kolei powoduje utworzenie folderu lub podfolderu w ścieżce dostępu.

PRINT WORKING DIRECTORY (PWD) - pokaż aktualny folder
Wyświetla nazwę folderu, w którym aktualnie się znajdujemy.

LIST (LIST) - wyświetla zawartość aktualnego folderu
Powoduje że serwer wysyła zawartość folderu określoną ścieżką dostępu. Dane zawierające zawartość folderu przesyłane są przez data connection jako typ ASCII lub EBCDIC. (użytkownik musi zadbać o ustawienie odpowiedniego trybu przed wysłaniem komendy LIST). Ponieważ przy transferze z jednego systemu do drugiego informacje o zawartości folderu mogą wyglądać różnie informacja ta może być trudna do wykorzystania w programach. Patrz dalej.

NAME LIST (NLST) - lista nazw
I dlatego też powstała ta komenda, która przesyła tylko i wyłącznie ścieżki i nazwy plików bez zbędnych informacji.

SITE PARAMETERS (SITE) - dodatkowe usługi
Komenda ta a raczej grupa komend pozwala na uruchomienie na serwerze dodatkowych usług takich jak np:

- **SITE CHAT <user> <message>** wysyła wiadomość do innego zalogowanego użytkownika,
- **SITE PSWD** pozwala na zdalną zmianę hasła,
- **SITE WHO** zwraca listę aktualnie zalogowanych osób w formacie *user name - connection date - IP/HostName - Transfer KBps,*
- **SITE ZONE** wyświetla strefę czasową, w jakiej jest uruchomiony serwer.

Oczywiście nie na wszystkich serwerach będzie można użyć tych komend.

SYSTEM (SYST)
Komenda ta pozwala na sprawdzenie na jakim systemie operacyjnym jest wystartowany serwer.

STATUS (STAT) - pokazuje status połączenia
Wyświetla status połączenia przesyłając tę informacje przez control connection w formie odpowiedzi. Komenda ta może być przesłana do serwera w trakcie transferu pliku lub podczas przerwy miedzy transferami. Użyta z parametrem w postaci ścieżki dostępu zwraca jej zawartość nie przez data connection lecze przez control connection zachowując się podobnie jak komenda ***LIST*** tylko używając innego kanału..

HELP (HELP) - pomoc
Powiadamia serwer, aby ten wysłał pełną informacje o swoim stanie i listę obsługiwanych komend. Specyfikacja zaleca również, aby komenda HELP mogła być dostępna jeszcze przed logowaniem czyli przed komenda USER.

NOOP (NOOP) - nic nie robię ale mnie nie rozłączaj
Komenda służy do podtrzymywania połączenia z serwerem mimo bezczynności użytkownika.[4]