FTP Clients and Servers

FTP Clients:

ASCII		X-Programs	
prgm	(package,serie)	prgm	(package,serie)
`ftp`	(lukemftp,n)	`IglooFTP`	(iglooftp,xap)
`mc`	(mc,ap)	`gftp`	(gftp,gnm)
`ncftp`	(ncftp,n)	`kbear`	(kbear,k2de)
		`xftp`	(xftp,xap)
		`konqueror`	
		`firefox`	

and Browsers as users and anonymous ftp clients.
Best is `Konqueror` for user (upload/download)and anonymous.

FTP Servers:

INETD		STANDALONE	
`proftpd`	(proftpd,n)	`proftpd`	(proftpd,n)
`pure-ftpd`	(pure-ftpd,n)	`pure-ftpd`	(pure-ftpd,n)
`wu.ftpd`	(not in SuSE8.0)	`vsftpd`	(vsftpd,n)
`in.ftpd`	(ftpd,n)		
`vsftpd`	(vsftpd,n)		

ASCII FTP Clients commands:

```
ascii      cat      help     lpage    open     quote    site
bgget      cd       jobs     lpwd     page     rename   type
bgput      chmod    lcd      lrename  pdir     rhelp    umask
bgstart    close    lchmod   lrm      pls      rm       version
binary     debug    lls      lrmdir   put      rmdir
bookmark   dir      lmkdir   ls       pwd      set
bookmarks  get      lookup   mkdir    quit     show
```

FTP Clients connections:

system user: - User registered in system where the FTP server runs.
- Requires a valid system user password
- List of NOT allowed users to login as ftp client is in `/etc/ftpusers`
- Often can be configured to be `chrooted()` into their own directories.
- Are normally allowed to upload files and directories into the server.

ftp/anonymous:Normally set to be the `ftp` user in the system where FTP server runs.
- Normally with an empty password or an e-mail address (.....@....)
- Normally set to be `chrooted` in the home directory of the the `ftp` user (usually `/usr/local/ftp` or `/srv/ftp` directory)
- Browsers usually log in as anonymous or ftp user.
- FTP Server can be configured to allow uploads into it but not recommended. If do configured then the uploaded files will not be downloadable untill they are set to chmod 644 (they are normally set to 600 when uploaded).

gftp and SSH Server:

gftp can connect with the sftp subsysystem of sshd. Here are the settings:
Setting: Menu item: FTP ---> `Options` --->Tab SSH ---> Set '`Use SSH2 SFTP subsys`'
Host:*(normal)* Port: 22 User: *(normal)* Passwd:*(n/a)* Connection Type SSH2
- Start connection(click on double computer icon)

- Type yes if BlaBlaBla..... (yes/no) window appears and press <Enter>.
- Enter Password and press <Enter>

Very Secure FTP Server (vsftpd)

Description: Quick and Very secure FTP server loaded via inetd only

Files involved:

`/usr/sbin/vsftpd`	Main FTP server Daemon
`/etc/vsftpd.conf`	Its configuration file
`/etc/vsftpd.chroot_list`	Users who will/won't be chroot()'ed
`/etc/pam.d/vsftpd`	Pam modules config for `vsftpd` authentication

Things important to set in the config file before using it:

```
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES

...................................
#Set the general rule which decides if all of the system users will be chrooted()
chroot_local_user=YES

# The follwoing 2 lines sets exceptions to the above decided rule
# This means if all chroot_local_users=YES then the chroot_list_file lists the users that will not be chrooted().
But if the  chroot_local_users=NO the chroot_list_file lists the users that will be chrooted()
#chroot_list_enable=YES
# (default follows)
#chroot_list_file=/etc/vsftpd.chroot_list

# Allow some broken ftp clients("ncftp" and "mirror")  to do recursive  ls
ls_recurse_enable=YES
```

# Example config file `/etc/vsftpd.conf`

```
#
# The default compiled in settings are very paranoid. This sample file
# loosens things up a bit, to make the ftp daemon more usable.
#
# Allow anonymous FTP?
anonymous_enable=YES
anon_root =/usr/local/ftp

# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
# Default umask for local users is 077. You may wish to change this to 022,
# if your users expect that (022 is used by most other ftpd's)
#local_umask=022
#
# Uncomment this to allow the anonymous FTP user to upload files. This only
# has an effect if the above global write enable is activated. Also, you will
# obviously need to create a directory writable by the FTP user.
#anon_upload_enable=YES
#
# Uncomment this if you want the anonymous FTP user to be able to create
# new directories.
#anon_mkdir_write_enable=YES
#
# Activate directory messages - messages given to remote users when they
# go into a certain directory.
dirmessage_enable=YES
#
# Activate logging of uploads/downloads.
xferlog_enable=YES
#
# Make sure PORT transfer connections originate from port 20 (ftp-data).
connect_from_port_20=YES
#
# If you want, you can arrange for uploaded anonymous files to be owned by
# a different user. Note! Using "root" for uploaded files is not recommended!
#chown_uploads=YES
#chown_username=whoever
#
# You may override where the log file goes if you like. The default is shown below.
#xferlog_file=/var/log/vsftpd.log
#
# If you want, you can have your log file in standard ftpd xferlog format
#xferlog_std_format=YES
#
# You may change the default value for timing out an idle session.
#idle_session_timeout=600
# You may change the default value for timing out a data connection.
#data_connection_timeout=120
```

```
# It is recommended that you define on your system a unique user which the
# ftp server can use as a totally isolated and unprivileged user.
# nopriv_user=ftpsecure
#
# Enable this and the server will recognise asynchronous ABOR requests. Not
# recommended for security (the code is non-trivial).
#Not enabling it, however, may confuse older FTP clients.
#async_abor_enable=YES
#
# By default the server will pretend to allow ASCII mode but in fact ignore
# the request. Turn on the below options to have the server actually do ASCII
# mangling on files when in ASCII mode.
# Beware that turning on ascii_download_enable enables malicious remote parties
# to consume your I/O resources, by issuing the command "SIZE /big/file" in ASCII mode
# These ASCII options are split into upload and download because you may wish
# to enable ASCII uploads (to prevent uploaded scripts etc. from breaking),
# without the DoS risk of SIZE and ASCII downloads. ASCII mangling should be
# on the client anyway..
#ascii_upload_enable=YES
#ascii_download_enable=YES
#
# You may fully customise the login banner string:
ftpd_banner=Welcome to FTP service.
#
# You may specify a file of disallowed anonymous e-mail addresses. Apparently
# useful for combatting certain DoS attacks.
#deny_email_enable=YES
#banned_email_file=/etc/vsftpd.banned_emails
#
# You may specify an explicit list of local users to chroot() to their home
# directory. If chroot_local_user is YES, then this list becomes a list of
# users to NOT chroot().
chroot_local_user=YES
#chroot_list_enable=YES
#chroot_list_file=/etc/vsftpd.chroot_list
#
# You may activate the "-R" option to the builtin ls. This is disabled by
# default to avoid remote users being able to cause excessive I/O on large
# sites. However, some broken FTP clients such as "ncftp" and "mirror" assume
# the presence of the "-R" option, so there is a strong case for enabling it.
ls_recurse_enable=YES

pam_service_name=vsftpd
```

SFTP Server Installation with vsftpd(Debian)

- Install the Debian `vsftpd` binary package and its sources.

```
apt-get install vsftpd
cd /root
mkdir vsftpd-source
cd vsftpd-source
apt-get source vsftpd
```

- Extract the `.tar.gz` file into `/usr/local/vsftpd-2.0.3`

```
cd /usr/local
tar fvxz /root/vsftpd-source/vsftpd_2.0.3.orig.tar.gz
```

- To enable the SSL support, edit the file `builddefs.h`

```
cd vsftpd-2.0.3
vi builddefs.h
```

change the line:

```
#undef VSF_BUILD_SSL
```

to

```
#define VSF_BUILD_SSL
```

- Compile the binary daemon

```
make
```

- Rename the original installed binary file:

```
mv /usr/sbin/vsftpd /usr/sbin/vsftpd.orig
```

- Copy the new binary file to its regular location

```
cp vsftpd /usr/sbin/
```

- Create an SSL certificate for vsftpd

```
make-ssl-cert /usr/share/ssl-cert/ssleay.cnf /etc/ssl/certs/vsftpd.pem
```

and answer all the questions as appropriate.

- Edit `/etc/vsftpd.conf` and make sure the SSL parameters are set as follows:

```
ssl_enable=YES
rsa_cert_file=/etc/ssl/certs/vsftpd.pem
```

- Activate the ftp server either as `inetd` or `xinetd` service or standalone. For standalone operation the following parameter need to be set in the configuration file `/etc/vsftpd.conf`:

```
listen=YES
```

Note: I recommend using free <u>Filezilla</u> client program under Windows and set the `Servertype` to:

```
FTP over SSL (explicit encryption)
```

in the Menu: `File --> Site Manager` Window.

<u>Filezilla</u> can be found at:

```
http://www.filezilla.de
```

Note: Unfortunately till now I could not make the WinSCP work with this server.

Proftp

Intro: The server proftpd and its configuration below can be used for:

- anonymous ftp
  - name is `anonymous` or `ftp` and password can be anything
  - the client is limited (chroot) to the directory `/usr/local/ftp`

- Normal system ftp user
  - users are from the group `users`
  - login name uses normal *system user* and *password*
  - the user is free to move through the entire system

- Web client ftp user
  - users are from the group `www`
  - login name uses normal *system user* and *password*
  - the user is restricted (chroot) to his home directory web page area eg. `~/public_html`

Configuration file: `/etc/proftpd.conf`

Notes:

- Contrary to the `wu.ftpd` the `proftpd` does not need to have the directories `/lib` and `/bin` to work on normal (long) directory listings.
- If you want users to login with ftp but not with telnet or ssh then:
  - Make sure that the shell of the concerned users is set to `/bin/false` (in `/etc/passwd`)
  - Make sue that the shell /bin/false is listed in the file `/etc/shells`.

sample of `/etc/proftpd.conf`

```
# This is a basic ProFTPD configuration file. It establishes a single
# server and a single anonymous login. It assumes that you have a
# user/group "nobody"/"nogroup" for normal operation and anon.

#    !!! PLEASE read the documentation of proftpd !!!
#
# You can find the documentation in /usr/doc/packages/proftpd/,
# http://www.proftpd.org/ and don't forget to read carefully
# and _follow_ hints on http://www.proftpd.net/security.html.

ServerName               "powered by SuSE Linux"
ServerType               inetd
ServerAdmin              ftpadm@localhost
#
# uncomment, if you want to hide the servers name:
#
ServerIdent              on    "Michel's Laptop FTP Server ready"
DeferWelcome                   off
DefaultServer                  on

# Enable PAM for authentication...
#
AuthPAM                        on
```

```
# Setting this directive to on will cause authentication to fail
# if PAM authentication fails. The default setting, off, allows
# other modules and directives such as AuthUserFile and friends
# to authenticate users.
#
#AuthPAMAuthoritative         off

# This directive allows you to specify the PAM service name used
# in authentication (default is "proftpd" on SuSE Linux).
# You have to setup the service in the /etc/pam.d/<other_name>.
#
AuthPAMConfig                 proftpd

# Port 21 is the standard FTP port.
Port                    21

# disable listen on 0.0.0.0:21 - the port (and IP) should
# be specified explicitly in each VirtualHost definition
#
#Port                           0

# listen for each (additional) address explicitly that is
# specified (via Bind and Port) in a VirtualHost definition
#
#SocketBindTight                        on


# Umask 022 is a good standard umask to prevent new dirs
# and files from being group and world writable.
Umask                   022

# Set the user and group that the server normally runs at.
User                    nobody
Group                   nogroup

# Normally, we want files to be overwriteable.
<Directory /*>
  AllowOverwrite        on
  HiddenStor                  on
  #HideNoAccess               on
</Directory>

# protect .ftpaccess and similar - see also PathDenyFilter
#<Directory /*.ftp*>
#  <Limit ALL>
#    DenyAll
#    IgnoreHidden       on
#  </Limit>
#</Directory>

# It is a very good idea to allow only filenames containing normal
# alphanumeric characters for uploads (and not shell code...)
#PathAllowFilter "^[a-zA-Z0-9_.-]+$"
#PathAllowFilter "^[a-zA-Z0-9~ \*\/,_.-]+$"

# We don't want .ftpaccess or .htaccess files to be uploaded
#PathDenyFilter "(\.ftp)|(\.ht)[a-z]+$"
#PathDenyFilter "\.ftp[a-z]+$"

# Do not allow to pass printf-Formats (security! see documentation!):
#AllowFilter "^[a-zA-Z0-9@~' \*\/,_.-]*$"
```

```
DenyFilter  "%"

# To prevent DoS attacks, set the maximum number of child processes
# to 30.  If you need to allow more than 30 concurrent connections
# at once, simply increase this value.  Note that this ONLY works
# in standalone mode, in inetd mode you should use an inetd server
# that allows you to limit maximum number of processes per service
# (such as xinetd)
MaxInstances                   30

# Performance: skip DNS resolution when we process the logs...
#UseReverseDNS        off

# Turn off Ident lookups
IdentLookups         off
# Set the maximum number of seconds a data connection is allowed
# to "stall" before being aborted.
#TimeoutStalled                  300

# Where do we put the pid files?
ScoreboardPath       /var/run/proftpd

# Logging options
#
TransferLog          /var/log/xferlog

# Some logging formats
#
#LogFormat            default "%h %l %u %t \"%r\" %s %b"
#LogFormat            auth    "%v [%P] %h %t \"%r\" %s"
#LogFormat            write   "%h %l %u %t \"%r\" %s %b"

# Log file/dir access
#ExtendedLog          /var/log/proftpd.access_log    WRITE,READ write

# Record all logins
#ExtendedLog          /var/log/proftpd.auth_log      AUTH auth

# Paranoia logging level....
##ExtendedLog          /var/log/proftpd.paranoid_log  ALL default

# Do a chroot for web-users (i.e. public or www group), but
# do not change root if the user is also in the users group...
#
DefaultRoot ~/public_html     www
DefaultRoot ~                 ftpuser

# Limit login attempts
#MaxLoginAttempts                3

# Users needs a valid shell
#RequireValidShell               yes

# Use special Auth files instead....
#AuthUserFile                    /var/proftpd/authfiles/passwd
#AuthGroupFile                   /var/proftpd/authfiles/group

# Use LDAP server - see README.LDAP
#
#LDAPServer         "localhost"
#LDAPPrefix         "dc=your,dc=domain,dc=top"
```

```
#LDAPDN             "cn=YourDNUser,dc=your,dc=domain,dc=top"
#LDAPDNPass         "YourDNUserPassword"

# The ratio directives take four numbers: file ratio, initial file
# credit, byte ratio, and initial byte credit.  Setting either ratio
# to 0 disables that check.
#
# The directives are HostRatio (matches FQDN -- wildcards are allowed
# in this one), AnonRatio (matches password entered in an anon login,
# usually an email address), UserRatio (accepts "*" for 'any user'),
# and GroupRatio.  Matches are looked for in that order.
# Some examples:
#
# Ratios     on                                  # enable module
# UserRatio  ftp 0 0 0 0
# HostRatio  anyhost.domain.top 0 0 0 0          # leech access (default)
# GroupRatio proftpd 100 10 5 100000             # 100:1 files, 10 file cred
# AnonRatio  auser@domain.top 1 0 1 0            # 1:1 ratio, no credits
# UserRatio  * 5 5 5 50000                       # special default case

# Setting "Ratios on" without configuring anything else will enable
# leech mode: it logs activity and sends status messages to the ftp
# client, but doesn't restrict traffic.
```

Anonymous FTP

```
<Anonymous ~ftp>
      # Using '~ftp' the client will land in the home directory of ftp user.
      # just the same as in Apache (http://myserver.com/~username)

     # After anonymous login, daemon runs as:
     User               ftp
     Group              daemon

     # We want clients to be able to login with "anonymous" as well as "ftp"
     UserAlias          anonymous ftp

     # Limit the maximum number of anonymous logins
     MaxClients         10

     # We want 'welcome.msg' displayed at login, and '.message' displayed
     # in each newly chdired directory.
     DisplayLogin       msgs/welcome.msg
     DisplayFirstChdir        .message

     # Deny write operations to all directories, underneath root-dir
     # Default is to allow, so we don't need a <Limit> for read operations.
     <Directory *>
          <Limit WRITE>
               DenyAll
          </Limit>
     </Directory>
     #
     # Only uploads into incomming directory are allowed...
     #<Directory incoming>
     #
     #     Umask  017
     #
     #     # ... so deny read/write
     #     <Limit READ WRITE DIRS>
     #          DenyAll
     #     </Limit>
     #
     #     # ... allow file storing, but not other writes
     #     <Limit STOR CWD CDUP>
     #          AllowAll
     #     </Limit>
     #
     #</Directory>

</Anonymous>
```

wu.ftpd FTP Server for WWW clients.

1 - Install **`wuftpd`** and **`ftpdir`** on CD series '**n**'
2 - Comment the **`in.ftpd`** and activate the **`wu.ftpd -l -a`**
3 - Create a new user for each www client
- The home pages should all be stored in **`/home/<user>/www/`**
- The Virtual Host setting of Apache should point to the users www directory (/home/<user>/www)

eg.
```
<VirtualHost xx.yy.zz.34>
    DocumentRoot /home/michel/www/MyWebSpace.de
    .........
</VirtualHost>
```

4 - In each Client's directory (/home/<user>/) create the following setting

```
/home-
     |---drwxr-xr-x <username>
     |    |-- drwx--x--x bin  (files from /usr/local/ftp/bin)
     |    |    |-- ---x--x--x ls
     |    |    |-- ---x--x--x compress
     |    |    |-- ---x--x--x gzip
     |    |    |-- ---x--x--x tar
     |    |
     |    |-- drwx--x--x etc  (needed only to convert uid/guid in ls -la results)
     |    |    |-- -rw-r--r-- group
     |    |    |-- -rw-r--r-- passwd
     |    |
     |    |-- drwx--x--x lib  (files from /usr/local/ftp/lib)
     |    |    |-- ---x--x--x ld-linux.so.2
     |    |    |-- ---x--x--x libc.so.6
     |    |    |-- ---x--x--x libnss_files.so.2
     |    |
     |    |-- drwx--x--x msgs (needed only for messages display)
     |    |    |-- -rw-r--r-- cd_message.msg
     |    |    |-- -rw-r--r-- welcome.msg
     |    |
     |    |
     |    |-- drwxr-xr-x www (users home page area)
     |         |-- -Homepage Files and subdirs(upload area)
     |
     |---drwxr-xr-x msgs (general messages for all users)
     |    |-- -rw-r--r-- connections_limit.msg
     |    |-- -rw-r--r-- no_localhost.msg
     |    |-- -rw-r--r-- shutdown.msg
```

5 - All the file and directories (bin, etc, lib, msgs) belong to root
The directory **`/home/<user>/www`** belongs to the user.

6 - Fill in the global and individual messages files as desired
They are located in **`/home/msgs/`** and **`/home/<user>/www/`**

7 - Change the landing path of the user in `/etc/passwd` (the real system passwd) to
`username:x:110:501:WWW Client:/home/<user>/./www/:`
to land in `/home/username/www` and his '/' dir will be `/home/`*`username`* (real)
This is done through the function `chroot()` provoked by the directive:
`guestgroup users` in the **`/etc/ftpaccess`** file.
This user is then restricted to the `/home/`*`username`* directory as its '/' dir.

- Step 8 and 9 are only for UID and GID translation for directories listings:

8 - Enter the root and user name in the `/home/`*`username`*`/etc/passwd` file:
`root:*:0:0:::`
`<user>:*:<uid>:100:::`

9 - Enter the root and users groups in the `/home/`*`username`*`/etc/group` file:
`root::0:`
`users::100:`

10 - Script to add restricted users to the ftp server:
Name of the script: **`ftpuseradd`**
Use format: **`ftpuseradd <username>`**
Note: This user will also be allowed to do a telnet using the same name and password.
To prevent that, disallow the telnet to start in the inetd.conf for all users. Or
take out the `/bin/bash` shell at the end of the users's line in `/etc/passwd` file.

```
------------------------------------
 useradd -d /home/$1/./www/ -c $1 -g users $1
 mkdir /home/$1
 mkdir /home/$1/www
 chmod 755 /home/$1/ /home/$1/www
 chown $1.users /home/$1/ /home/$1/www
 cp -r /usr/local/ftp/bin/ /home/$1/
 cp -r /usr/local/ftp/lib/ /home/$1/
 chmod 711 /home/$1/bin/ /home/$1/lib/
 passwd $1
------------------------------------
```

11 - To add annonymous access to ftp server at another place than the default (/usr/local/ftp) do the following steps(as root user):

1 - Create a new ftp group and take note of the new group ID
2 - Look for the ftp user in `/etc/password`
- Erase its shell (`/bin/bash`)
- Change its home directory to `/home/ftp`
- Change its group number to the ftp group ID

3 - Create a /home/ftp and make the 'ftp' its owner and group with mode 755.
4 - Copy all subdirectories of `/usr/local/ftp` to `/home/ftp (mode 744)`
5 - Create a `/home/ftp/download` directory and make it chmod 755
6 - Modify `/home/ftp/etc/passwd` file to include only `ftp` and `root` users
7 - Modify `/home/ftp/etc/group` file to include only `ftp` and `root` groups
8 - Edit the `/etc/ftpaccess` file to reflect the proper anonymous settings.

/etc/ftpaccess

example and description

```
# ----- email of the responsible person when the %E is used in any message text --
email root@localhost

#---------- Declare all the accepted classes and their components ------------
# Enter a range of hosts allowed to be considered as this class instead of the '*'
# eg. *.mycompany.com
class   local      real,guest         *
class  remote      anonymous          *

#---------- Do not check password for anonymous clients ----------------------
# This directive is only meant for the anonymous clients!!!
# Format : paswd-check <none|trivial|rfc822> <enforce|warn>
# Meaning:   none   = No password is asked
#            trivial = The password must contain at least a '@' in it
#            rfc822 = The user must have a proper rfc822 compliant address
#            -------- Error handling types ----------
#            warn    = The user is warned of bad password but alllowed to login
#            enforce= The user is warned of bad password and is then disconnected
passwd-check none

# --------- Deny FTP connection from localhost (example only) here the messages path
are system relative -----------------
deny  localhost          /home/msgs/no_localhost.msg
#deny  *.michel.home       /msgs/no_localhost.msg

# --------- Limit the number of simultaneous connections ------
# Here the messages path are system relative
# limits all possible ftp conections to 20 on Saturday and sunday or
# Any Day from 18:00 hrs to 06:00 hrs.
# When limit occurs then send the message
limit  local  2      SaSu|Any1800-0600   /home/msgs/connections_limit.msg
limit  remote 3      Any                 /home/msgs/connections_limit.msg
#limit all    2      Any                 /home/msgs/connections_limit.msg


# ----------- Message invitating user to read the file README after Logging in
# and at each change of directories
# if the file README* exists in the current directory
readme   README*         login
readme   README*         cwd=*

# ----------- shutdown message sent when the ftp server shuts down.
# Here the messages path are system relative----------------------
shutdown     /home/msgs/shutdown.msg

# ----------- Allow all users to work on their files default (yes)----------------
# except the annonymous ones.

compress     no    anonymous
delete       no    anonymous
overwrite    no    anonymous
rename       no    anonymous
chmod        no    anonymous
umask        no    anonymous

#------- Banner is the message sent to user before login------------------------
# IMPORTANT:       It is recomended to limit the banner file content to one line
#            since not all ftp client software can handle multiline responses
# The message file path is system relative
banner /home/msgs/banner.msg

# ----------- Location of the welcome message sent after login.--------------------
# The message file path is user relative
message      /msgs/welcome.msg               login
```

```
# ------------ Location of the message sent after a change of directory .-----------
# The cwd=Path is the path of the relative directory that will provoke the sending
# of this message if changed to it. '*' means all directories
# The message file path and trigger directory (cwd) is user relative
message      /msgs/cd_message.msg            cwd=/www/test3
#message     /msgs/cd_message.msg            cwd=*


#  ------------- Log the consecutive failed Login attempt after 3 attempt
# and disconnect the user--------
loginfails 3

# ------- Don't allow extra functions (SITE GROUP and SITE GPASS)-----------------
private no

# ----- Allow only the /www directory to accept uploads from user ----------------
# Format:
#upload      Rootdir             RelDir yes|no user   group  mode   dirs|nodirs

upload /home/%U     *      no
upload /home/%U     /bin   no
upload /home/%U     /etc   no
upload /home/%U     /usr   no
upload /home/%U     /lib   no
upload /home/%U     /www   yes    %U     users  0755   dirs

# ----------- Allow only to a special /upload directory to have files
# uploaded from anonymous users -----(commented out!!! for security
# The user will also be allowed to make subdirectories as well
# The files will have the owner as nobody, group as nogroup and
# the access rights as 755

upload /home/ftp    *      no
upload /home/ftp    /bin   no
upload /home/ftp    /etc   no
upload /home/ftp    /usr   no
upload /home/ftp    /lib   no
upload /home/ftp    /download no
upload /home/ftp    /upload no

#upload      /home/ftp    /upload      yes    nobody nogroup      0755   dirs

#--- This path filter disallow filenames with unallowed characters --------------
# Format:
# path-filter clientTypeList ErrorMessagePath&Filename RegularExpression...!

path-filter anonymous,guest /home/msgs/badfilename.msg ^[-A-Za-z0-9_\.]*$ ^\. ^-

#--- Allow the use of tar and compress to all ------------------------------------
# Format:
# compress   yes|no       class1 [classX .......]
compress     yes             local     remote
tar          yes             local     remote

#----------- List of groups that will be restricted (considered like guests)--------
# This feature allows to restrict the users to their directories and not any further
# by issuing a chroot() to their home directories wich will be seen as the
# root directory(/)
# The /etc/passwd file must have the path to eg. /home/michel/./www/ to have the
# chroot()set the / to /home/michel and the ftp server to start the connection
# with the user logged at /home/michel/www/ (which has become /www/ directory)

guestgroup users

#--- log commands and transfers of users to syslog -------------------------------
log    commands     anonymous
log    transfers    anonymous,real,guest      inbound,outbound

# -- do not give any of the following files contained in any directory------------
noretrieve shadow passwd pap-secrets ftpaccess ftpusers ftphosts group ftpgroups
```

Pure FTP Serverr(pureftd)

Description: FTP server started as Daemon

Files involved:

`/etc/init.d/pure-ftpd`	Start/Stop script for `/usr/sbin/pure-ftpd`
`/etc/pam.d/pure-ftpd`	Pam modules config for `pure-tpd` authentication
`/etc/pure-ftpd.conf`	Config file for `pure-tpd`
`/usr/sbin/rcpure-ftpd`	Link to Start/Stop script `/etc/init.d/pure-ftpd`
`/usr/sbin/pure-ftpd`	Mail `pure-ftpd` FTP server Daemon

```
/usr/bin/pure-pw
/usr/bin/pure-pwconvert
/usr/bin/pure-statsdecode

/usr/sbin/pure-authd
/usr/sbin/pure-config-args
/usr/sbin/pure-config.pl
/usr/sbin/pure-ftpwho
/usr/sbin/pure-mrtginfo
/usr/sbin/pure-quotacheck
/usr/sbin/pure-uploadscript
```