FTP - File Transfer Protocol

lctseng / Liang-Chi Tseng

FTP

- ❑ FTP
  - ❑ File Transfer Protocol
  - ❑ Used to transfer data from one computer to another over the internet.
  - ❑ Client-Server Architecture.

- ❑ FTP connections
  - ❑ Control connection
    - ❑ Created when an FTP session is established
    - ❑ Only for passing control information
  - ❑ Data connection
    - ❑ Each time that data is sent, a distinct TCP data connect is established

- ❑ Data connection Modes:
  - ❑ Active Mode
  - ❑ Passive Mode

FTP
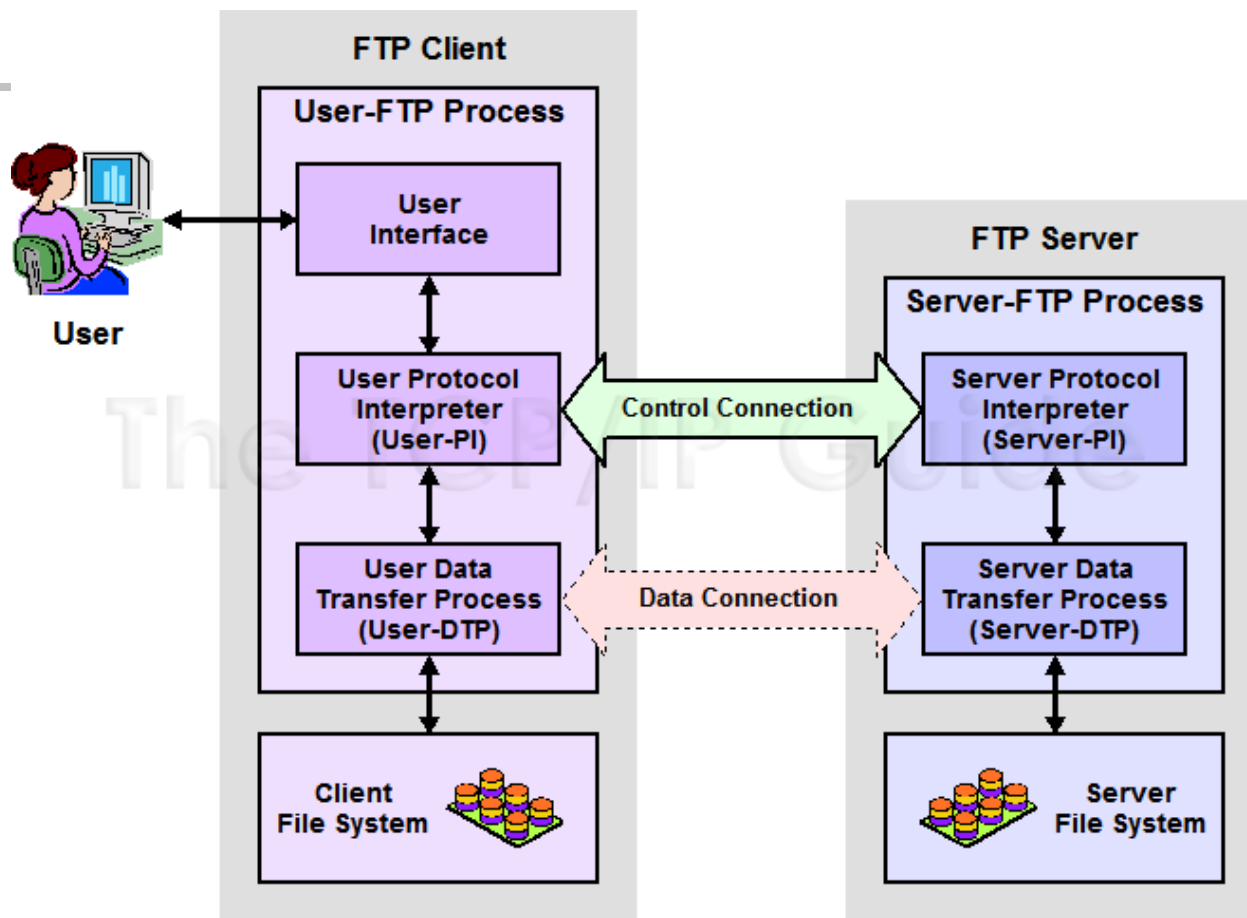
❑ FTP Request For Comments (RFCs):
- ❑ RFC 959 – File Transfer Protocol
- ❑ RFC 2228 – FTP Security Extensions
- ❑ RFC 2428 – FTP Extensions for IPv6 and NATs
- ❑ RFC 2640 – UTF-8 support for file name

FTP
– Flow (1)

- Client

  - Connect to server port 21 from port A.

  - USER ####

  - PASS ********

  - EPRT |1|ip|portnum|

  - Send some requests
    get return data from portnum

  - Quit

- Server

  - Binding on port 21

  - Accepts connection from client, output welcome messages.

  - 331 User name okay, need password.

  - 230 User logged in, proceed.

  - 200 PORT Command successful.

  - Binding source port 20, connect to client port portnum, send data.

  - …

FTP
– Flow (2)

ftp user must exist before doing this!

❑ Example
  ❑ Control Connection

```
% telnet freebsd.cs.nctu.edu.tw 21
Trying 140.113.17.209...
Connected to freebsd.cs.nctu.edu.tw.
Escape character is '^]'.
220---------- Welcome to Pure-FTPd [privsep] ----------
220-You are user number 7 of 1000 allowed.
220-Local time is now 16:25. Server port: 21.
220-Only anonymous FTP is allowed here
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
USER ftp
230 Anonymous user logged in
PASS ftp
230 Any password will work
EPRT |1|140.113.235.135|65000|
200 PORT command successful
list
150 Connecting to port 65000
226-Options: -l
226 2 matches total
quit
221-Goodbye. You uploaded 0 and downloaded 0 kbytes.
221 Logout.
Connection closed by foreign host.
```

FTP
– Flow (3)

❑ Example (contd.)

    ❑ Retrieving Data

        ❑ Client must bind the random port

        ❑ Files info under /home/ftp is sent to client through this port

```
% nc -l 65000
drwxr-xr-x  852 888         2010              80328 Mar 28 11:39 distfiles
drwxr-xr-x   16 888         2010                 34 May 11  2008 pub
```

FTP

– commands, responses

- Commands
  - USER username
  - PASS password
  - LIST
    - Return list of file in current dir.
  - CWD dirname
    - Change working directory
  - RETR filename
    - Retrieves (gets) file.
  - STOR filename
    - Stores (puts) file onto server.
  - EPRT |1|ip|port|
    - Set to active mode
  - PASV(EPSV)
    - Set to passive mode
  - DELE
    - Remove file on the server.
  - QUIT

- ❑Return Codes
  - First code
    - 1: Positive Preliminary reply
    - 2: Positive Completion reply
    - 3: Positive Intermediate reply
    - 4: Transient Negative Completion reply
    - 5: Permanent Negative Completion reply
  - Second code
    - 0: The failure was due to a syntax error
    - 1: A reply to a request for information.
    - 2: A reply relating to connection information
    - 3: A reply relating to accounting and authorization.
    - 5: The status of the Server file system

FTP
– Active Mode vs. Passive Mode (1)

❑ Active Mode

- FTP client bind a random port (>1023) and sends the random port to FTP server using "EPRT" command.
- When the FTP server initiates the data connection to the FTP client, it binds the source port 20 and connect to the FTP client the random port sent by client.
- EPRT |1|ip|port|
- EPRT |2|ipv6|port|

❑ Passive Mode

- FTP client sends "EPSV/PASV" command to the server, make the server bind a random port (>1023) and reply the random port back.
- When initializing the data connection, the FTP client connect to the FTP Server the random port, get data from that port.
- EPSV ➔ Server reply: 229 Entering Extended Passive Mode (|||41868|)
- PASV ➔ Server reply: 227 Entering Passive Mode (h1,h2,h3,h4,p1,p2)

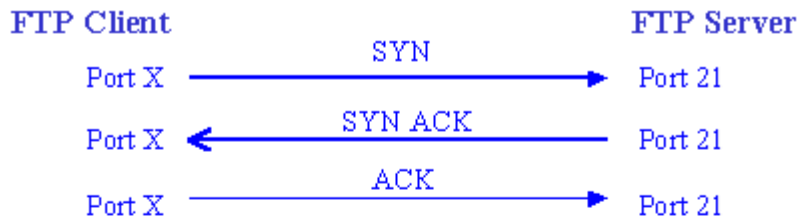※ IP:port (6bytes) ➔ h1,h2,h3,h4,p1,p2
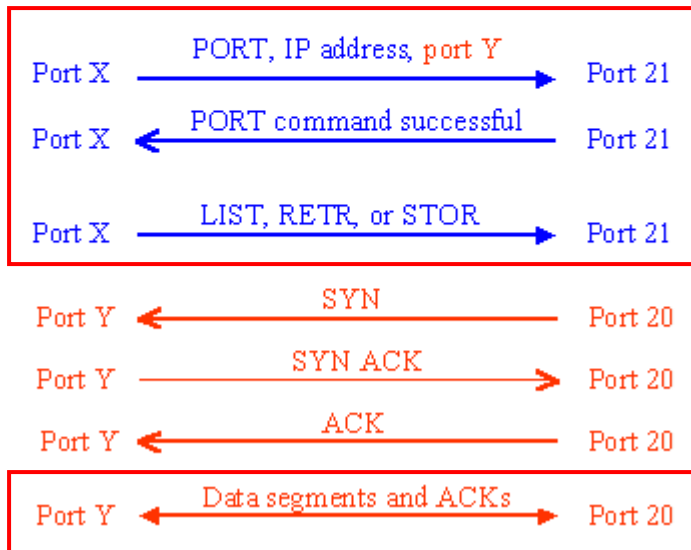Ex. 140.113.17.215:45678 ➔ 140,113,17,215,178,110

FTP
– Active Mode vs. Passive Mode (2)

Active mode
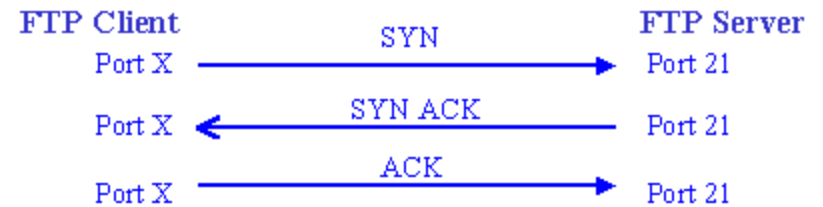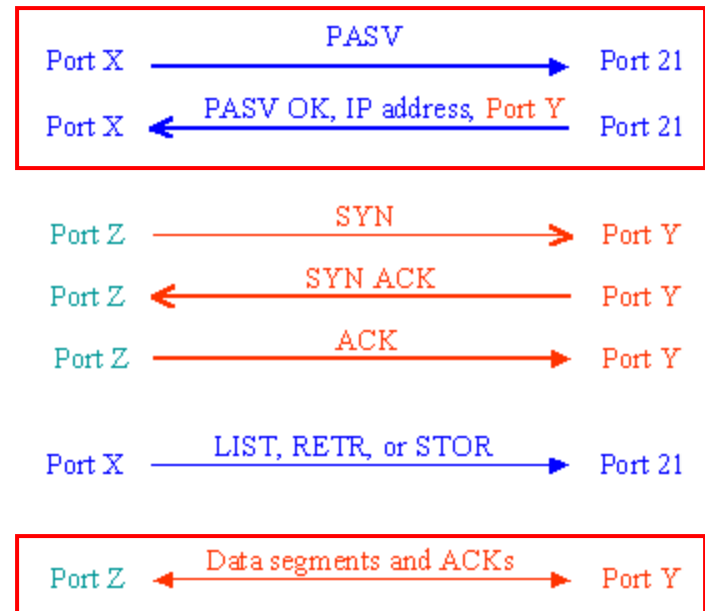
Passive mode

FTP
– When FTP meets NAT/Firewall (1)

❑ Active mode, NAT/Firewall on client side.

  ❑ Wireless AP

  ❑ Passive mode can solve this problem.

NAT/Firewall   NAT/Firewall

Client   Server   Client   Server

PORT IP, *port Y*   PASV

                                   reply IP, *port Z*

Connect to port Y   Connect to port Z
BLOCKED   PASS

Active Mode   Passive Mode
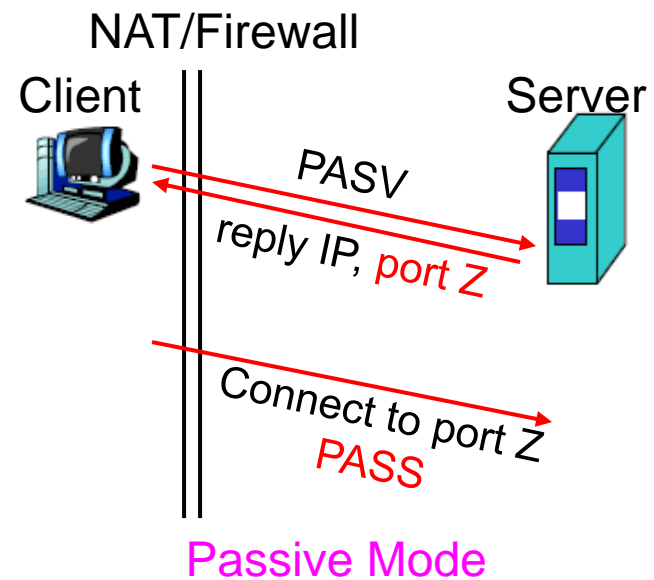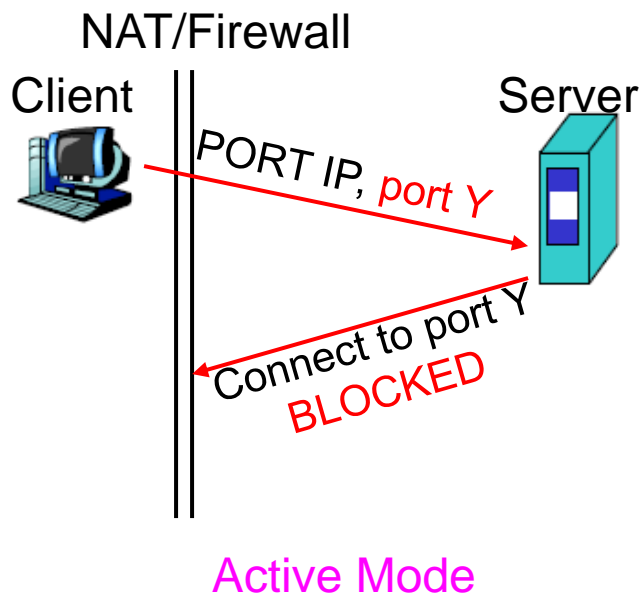
FTP
– When FTP meets NAT/Firewall (2)

❑ Passive mode, NAT/Firewall on Server side.
- Active mode can solve this problem.

Passive Mode
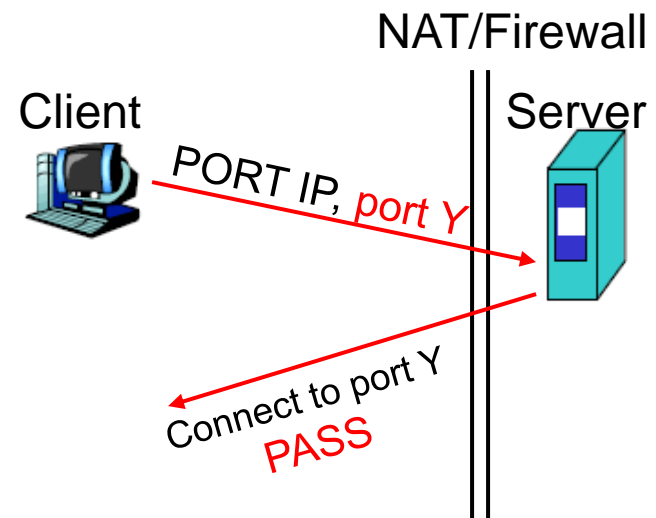
Active Mode

FTP
– When FTP meets NAT/Firewall (3)
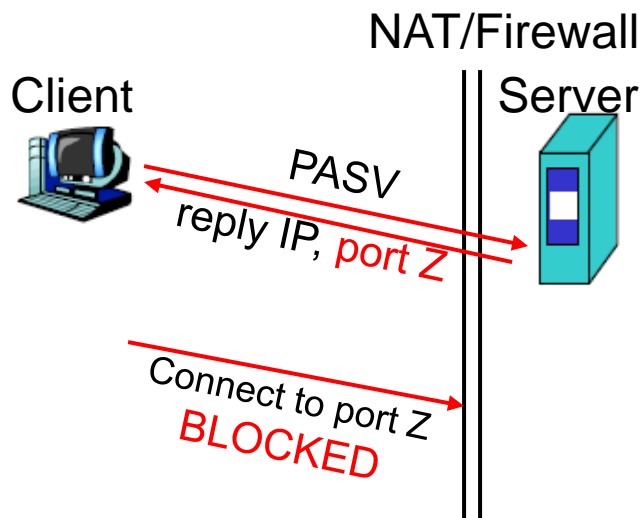
❑ Real Problem: Firewall on both sides.

Active Mode

Passive Mode
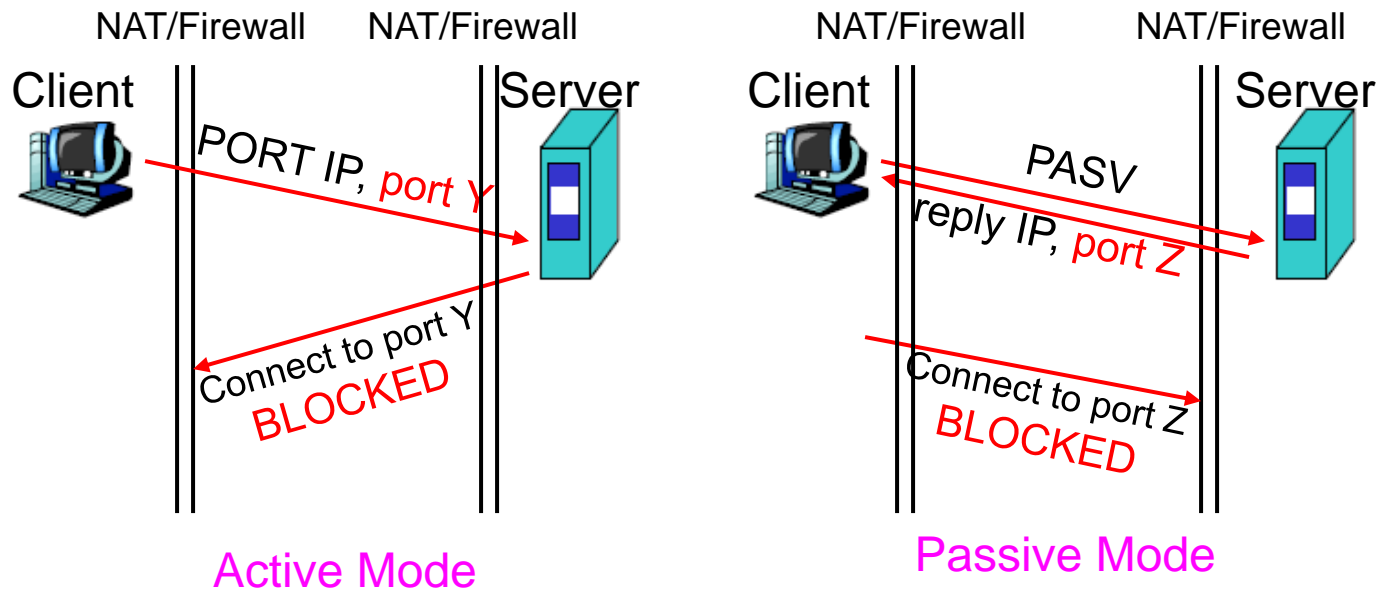
- Solution: ftp-proxy running on NAT/Firewall
  ➢ To be explain in firewall course (NA)

FTP
- Security

❑ Security concern

- As we seen, FTP connections (both command and data) are transmitted in clear text.

- What if somebody sniffing the network?

  ➢ We need encryption.

❑ Solutions

- FTP over TLS (FTPS、FTPES)

  ➢ Only commands are encrypted while transmitting.

  ➢ Better performance.

- FTP over SSH

  ➢ Tunneling a normal FTP session over an SSH connection.

- SSH File Transfer Protocol (SFTP)

  ➢ Both commands and data are encrypted while transmitting.

  ➢ One connection, but poor performance.

Pure-FTPd
- Intro (1)

❑ Introduction

- A small, easy to set up, fast and secure FTP server

- Support chroot

- Restrictions on clients, and system-wide.

- Verbose logging with syslog

- Anonymous FTP with more restrictions

- Virtual Users, and Unix authentication

- FXP (File eXchange Protocol)

- FTP over TLS

- UTF-8 support for filenames

Pure-FTPd
- Intro (2)

❑ Installation

- Ports: /usr/ports/ftp/pure-ftpd

- Package is also available

- Options

```
┌─────────────────── pure-ftpd-1.0.36_3 ───────────────────┐
│                                                          │
│  +[ ] ANONDELETE    Allow anonymous user to delete files │
│  +[ ] ANONRENAME    Allow anonymous user to rename files │
│  +[ ] ANONRESUME    Allow anonymous user to resume file upload │
│  +[x] DOCS          Build and/or install documentation   │
│  +[x] EXAMPLES      Build and/or install examples        │
│  +[ ] LARGEFILE     2GB+ file download                   │
│  +[ ] LDAP          User accounts in LDAP directories    │
│  +[ ] MYSQL         User accounts in MySQL database      │
│  +[x] PAM           PAM authentication                   │
│  +[ ] PERUSERLIMITS Per-user concurrency limits          │
│  +[ ] PGSQL         User accounts in PostgreSQL database  │
│  +[x] PRIVSEP       Privilege separation (recommended)   │
│  +[x] SENDFILE      Sendfile syscall                     │
│  +[ ] THROTTLING    Bandwidth throttling                 │
│  +[x] TLS           Secure network connection support via TLS │
│  +[ ] UPLOADSCRIPT  Uploadscript daemon support          │
│  +[ ] UTF8          UTF-8 filenames                      │
│  +[x] VIRTUALCHROOT Follow symlinks outside a chroot jail │
│                                                          │
└──────────────────────────────────────────────────────────┘
```

Pure-FTPd
- Intro (3)

- Other options

```
===>   Found saved configuration for pure-ftpd-1.0.36_3
===>    pure-ftpd-1.0.36_3 depends on file: /usr/local/sbin/pkg - found
You can use the following additional options:

LANG=lang (default: english)
- Enable compilation of one language support
  available lang: brazilian-portuguese, catalan, czech, danish, dutch,
  english, french, french-funny, german, hungarian, italian, korean,
  norwegian, polish, romanian, russian, simplified-chinese, slovak,
  spanish, swedish, traditional-chinese, turkish

TLS_CERTFILE=/path/to/file (default: /etc/ssl/private/pure-ftpd.pem)
- Custom location of certificate file for TLS
```

- TLS_CERTFILE   (Default: /etc/ssl/private/pure-ftpd.pem)

- LANG (Change the language of output messages)

❑ Startup:

- Add pureftpd_enable="YES" in /etc/rc.conf

Pure-FTPd
- Configurations (1)

❑ Configurations:

- File: /usr/local/etc/pure-ftpd.conf

- Documents

  ➢ Configuration sample: /usr/local/etc/pure-ftpd.conf.sample

    – All options are explained clearly in this file.

  ➢ Other documents

    – See /usr/local/share/doc/pure-ftpd/*

```
11:01am lctseng@lctseng(10.0.2.15)[/usr/local/share/doc/pure-ftpd]
[W1] > ls
AUTHORS                    README                            README.MySQL
CONTACT                    README.Authentication-Modules     README.PGSQL
COPYING                    README.Configuration-File         README.TLS
HISTORY                    README.Contrib                    README.Virtual-Users
NEWS                       README.LDAP                       THANKS
```

Pure-FTPd
- Configurations(2)

```
ChrootEveryone          yes
TrustedGID              0
AnonymousOnly           no
NoAnonymous             no
PureDB                  /usr/local/etc/pureftpd.pdb
UnixAuthentication      yes
AntiWarez               yes
Umask                   133:022
TrustedIP               140.113.0.0
CreateHomeDir           yes
TLS                     2
FileSystemCharset       UTF-8
ClientCharset           UTF-8
```

There are more configuration there!

Pure-FTPd
- Tools

❑ pure-*

```
> ls -1 /usr/local/sbin/pure-*
/usr/local/sbin/pure-authd
/usr/local/sbin/pure-config.pl
/usr/local/sbin/pure-ftpd
/usr/local/sbin/pure-ftpwho
/usr/local/sbin/pure-mrtginfo
/usr/local/sbin/pure-quotacheck
/usr/local/sbin/pure-uploadscript
> ls -1 /usr/local/bin/pure-*
/usr/local/bin/pure-pw
/usr/local/bin/pure-pwconvert
/usr/local/bin/pure-statsdecode
```

❑ pure-ftpwho

- List info of users who are currently connecting to the FTP server.

❑ pure-pw

- Manage Virtual Users in PureDB format

- pure-pw(8)

- See README.Virtual-Users

Pure-FTPd
- Anonymous Users and Virtual Users

❑ Anonymous Users

❑ Virtual Users

- FTP-only accounts without messing up your system accounts.

- Store individual quotas, ratios, bandwidth.

- Virtual users share the same system user.

- They are chrooted and have their own home directory.

Pure-FTPd
- Problem Shooting

❑ Logs Location

- In default, syslogd keeps ftp logs in /var/log/xferlog

❑ Most frequent problems

- pure-ftpd: (?@?) [ERROR] Unable to find the 'ftp' account

  ➢ It's ok, but you may need it for Anonymous FTP Account.

- pure-ftpd: (?@?) [ERROR] Sorry, but that file doesn't exist: [/etc/ssl/private/pure-ftpd.pem]

  ➢ If you set TLS = 2, then this file is needed.

- How to generate a pure-ftpd.pem?

  ➢ See README.TLS

FTP
- More Tools

❑ ftp/pureadmin

- Management utility for the PureFTPd

❑ ftp/lftp

- Shell-like command line ftp client, support TLS

❑ ftp/wget, ftp/curl

- Retrieve files from the Net via HTTP(S) and FTP

❑ ftp/mget

- Multithreaded commandline web-download manager

❑ FileZilla

- A graphical cross-platform FTP client, support TLS

❑ Pure-FTPd WebUI

- PHP based web interface for Pure-FTPd