FTP

File Transfer Protocol

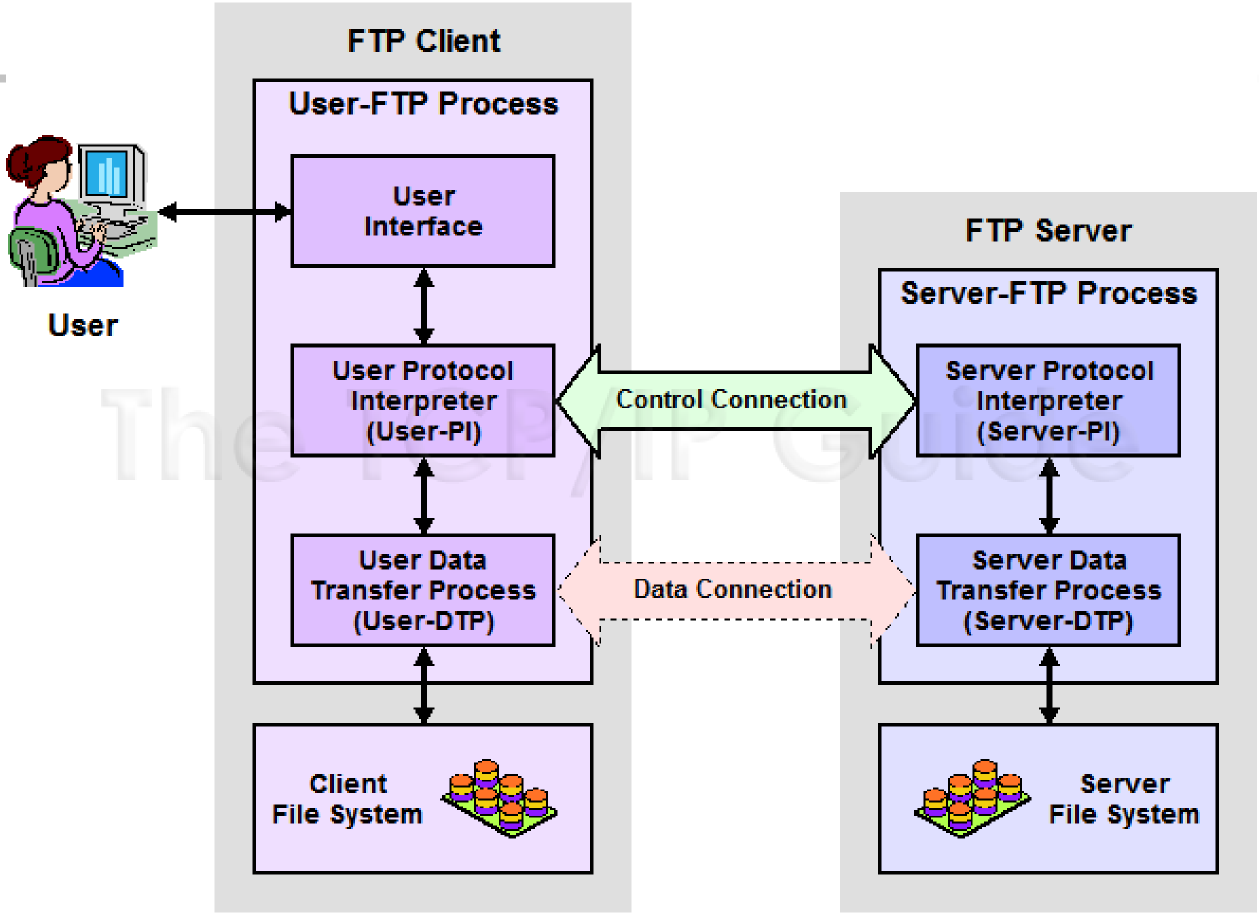
FTP

- ❑ 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 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	❑Server
	• Binding on port 21
• Connect to server port 21 from port A.	• Accepts connection from client, output welcome messages.
• USER ####	• 331 User name okay, need password.
• PASS *********	• 230 User logged in, proceed.
• EPRT |1|ip|portnum|	• 200 PORT Command successful.
• Send some requests get return data from portnum	• Binding source port 20, connect to client port portnum, send data.
• Quit	• …

FTP – Flow (2)

- ❑ 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
331 Any password will work
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

```
% 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

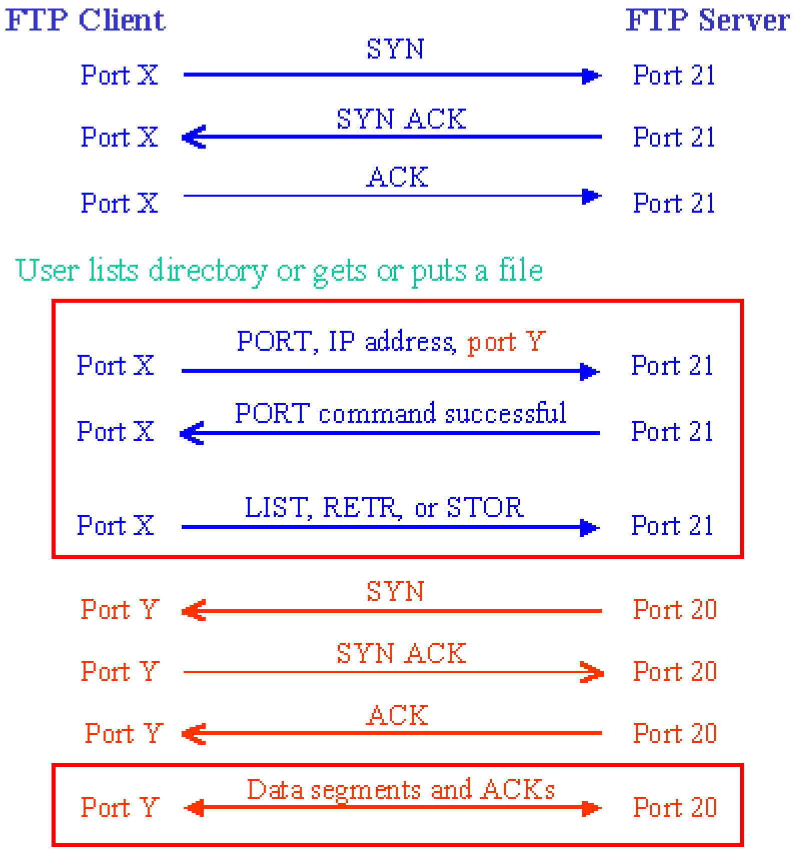
- FTP client sends "EPSV/PASV" command to the server, make the server bind a random port (>1023) and reply the random port back.
- When initializing the data connection, the FTP client connect to the FTP Server the random port, get data from that port.
- EPSV ➔ Server reply: 229 Entering Extended Passive Mode (|||1868|)
- 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



FTP Client — FTP Server

Port X → SYN → Port 21

Port X ← SYN ACK ← Port 21

Port X → ACK → Port 21

User lists directory or gets or puts a file

Port X → PORT, IP address, port Y → Port 21

Port X ← PORT command successful ← Port 21

Port X → LIST, RETR, or STOR → Port 21

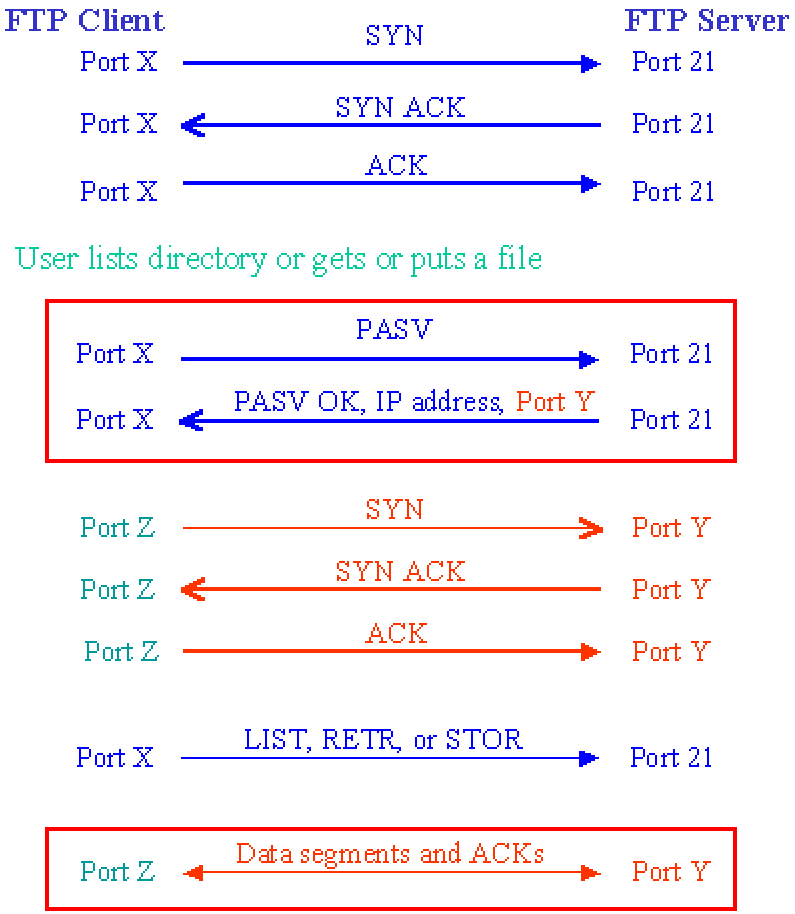
Port Y ← SYN ← Port 20

Port Y → SYN ACK → Port 20

Port Y ← ACK ← Port 20

Port Y ↔ Data segments and ACKs ↔ Port 20

Passive mode



FTP Client — FTP Server

Port X → SYN → Port 21

Port X ← SYN ACK ← Port 21

Port X → ACK → Port 21

User lists directory or gets or puts a file

Port X → PASV → Port 21

Port X ← PASV OK, IP address, Port Y ← Port 21

Port Z → SYN → Port Y

Port Z ← SYN ACK ← Port Y

Port Z → ACK → Port Y

Port X → LIST, RETR, or STOR → Port 21

Port Z ↔ Data segments and ACKs ↔ Port Y

FTP – When FTP meets NAT/Firewall (1)

□ Firewall behavior

- Generally, the NAT/Firewall permits all outgoing connection from internal network, and denies all incoming connection from external network.

□ Problem when FTP meets NAT/Firewall

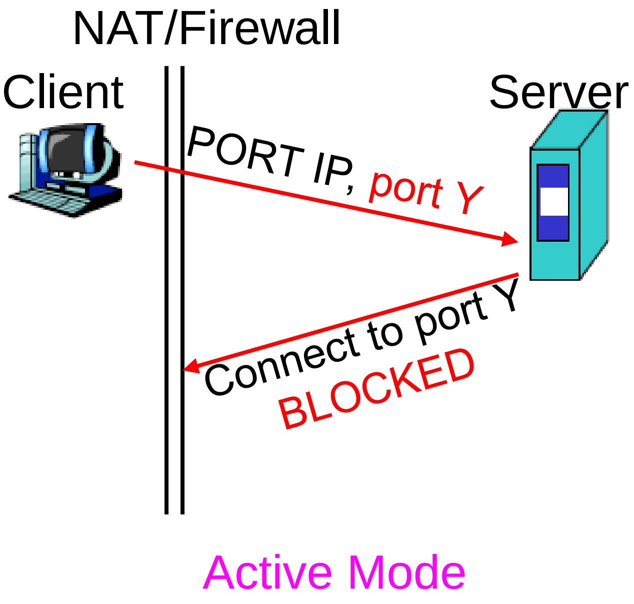
- Due to the separated command/data connection, the data connections are easily blocked by the NAT/Firewall.

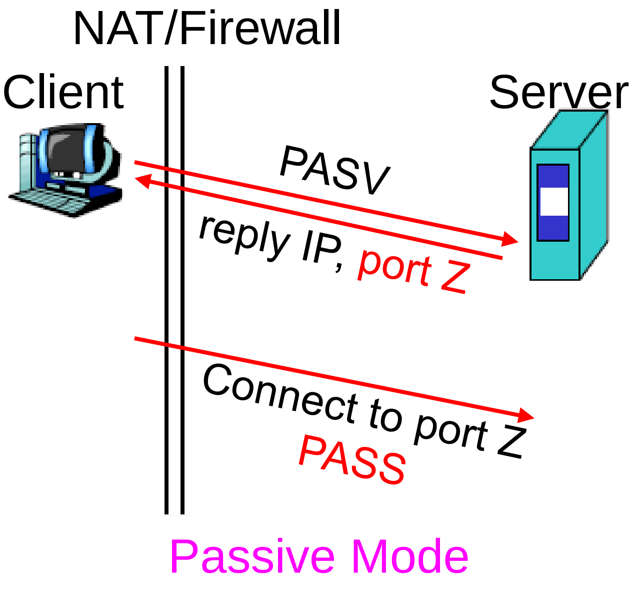
□ Problem Cases:

- Active mode, NAT/Firewall on client side.
  - ➢ Passive mode can solve this problem.
- Passive mode, NAT/Firewall on server side.
  - ➢ Active mode can solve this problem.
- Both client side and server side have NAT/Firewall
  - ➢ The real problem.

FTP – When FTP meets NAT/Firewall (2)

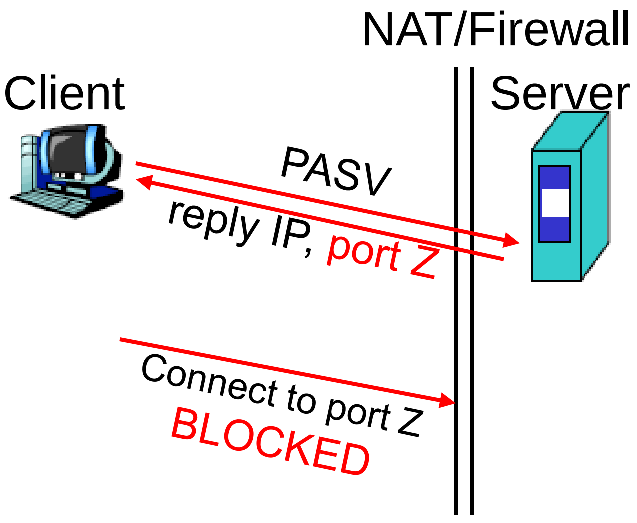
- ❑ Active mode, NAT/Firewall on client side.
  - Passive mode can solve this problem.



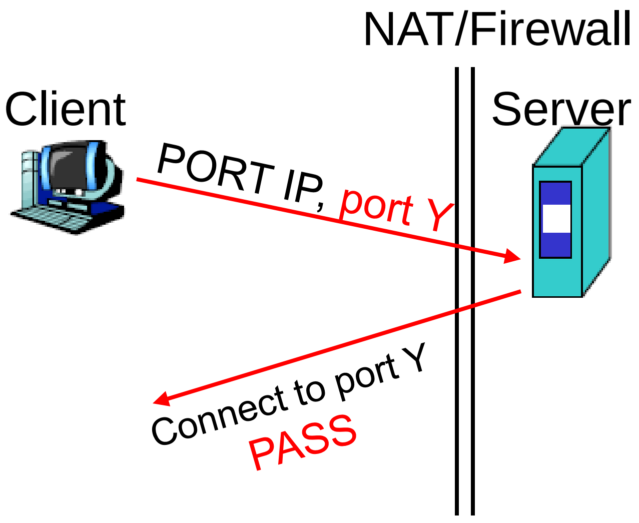


FTP – When FTP meets NAT/Firewall (3)

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



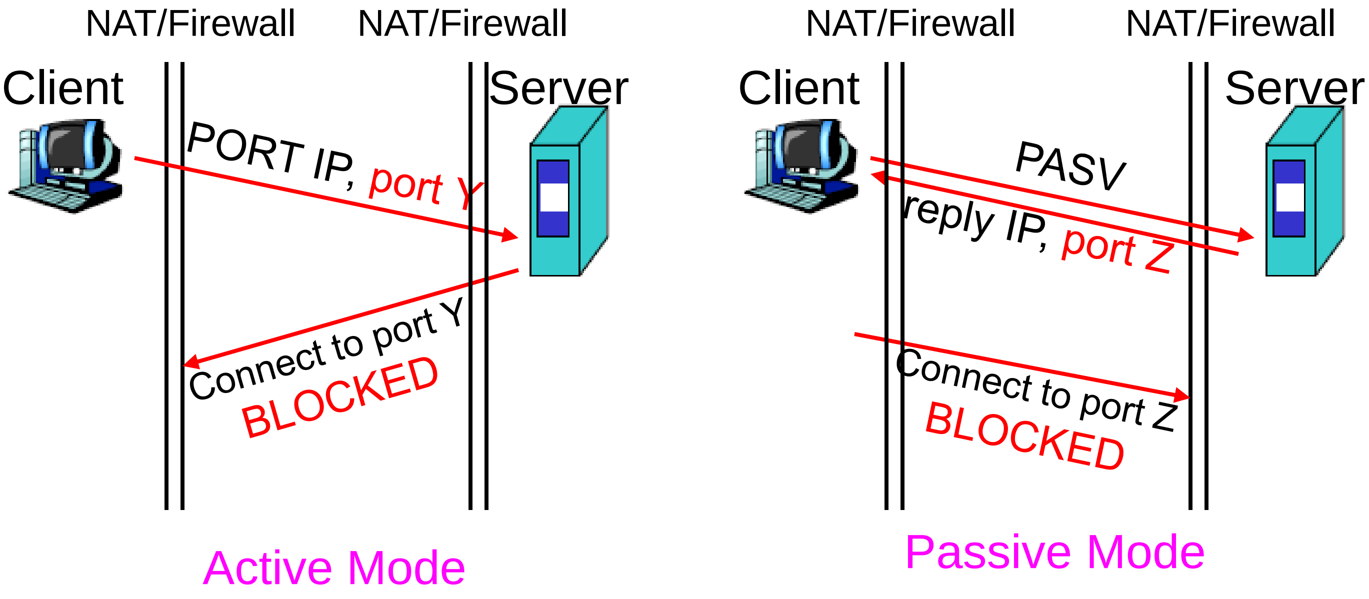
Passive Mode



Active Mode

FTP – When FTP meets NAT/Firewall (4)

❑ Real Problem: Firewall on both sides.



- Solution: ftp-proxy running on NAT/Firewall

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.

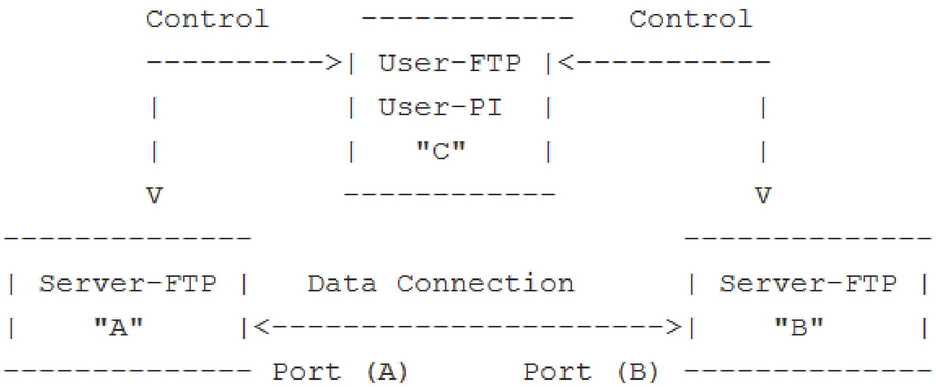
❑ Solutions

- FTP over SSH
  - So called secure-FTP(sftp).
  - Both commands and data are encrypted while transmitting.
  - One connection, but poor performance.
- FTP over TLS
  - Only commands are encrypted while transmitting.
  - Better performance.

FXP

❑ FXP

- File eXchange Protocol/Proxy FTP
- A user on one host performs a file transfer from one server to another
- Two control connections
  - ➢ One each from User-PI to the two Server-PI
- One data connections
  - ➢ Server-DTPs are invoked on each server to send data



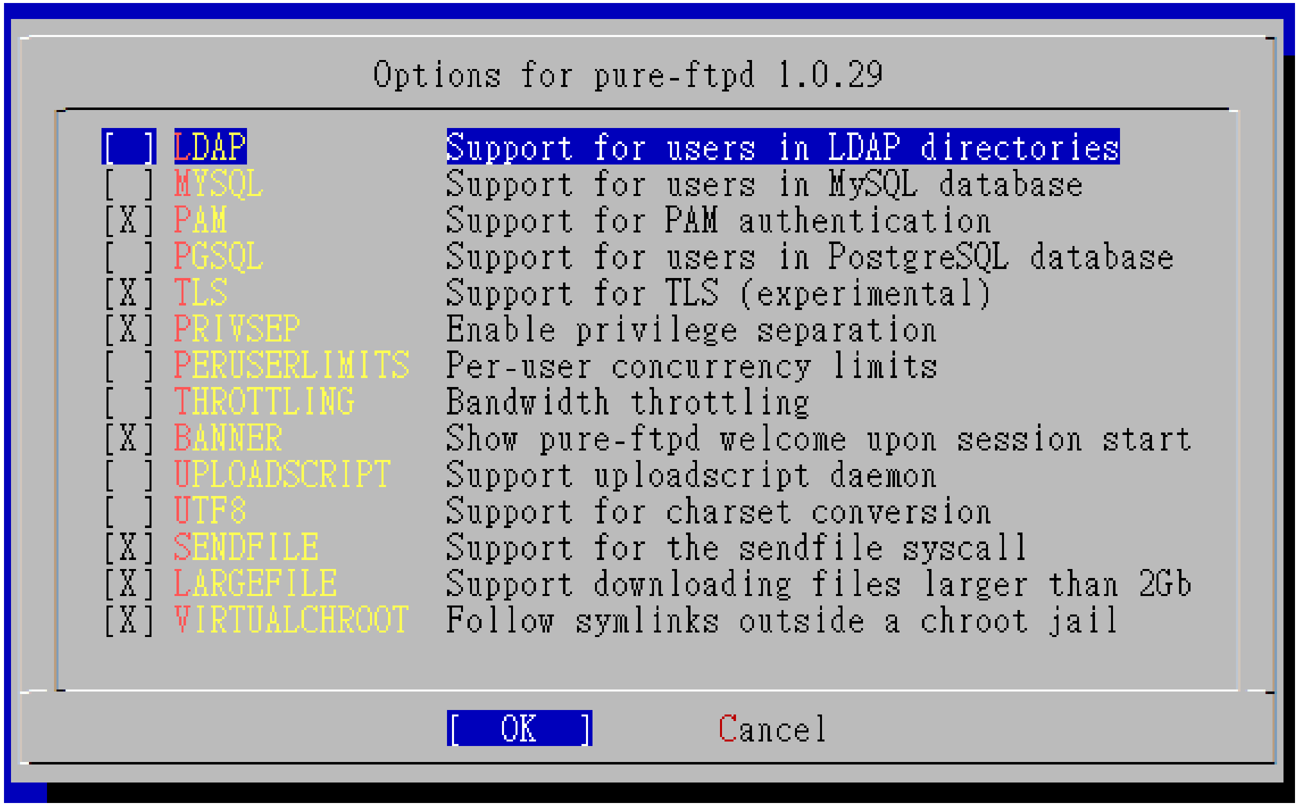
```
              Control     ------------   Control
              ---------->| User-FTP |<-----------
              |          | User-PI  |           |
              |          |   "C"    |           |
              V          ------------           V
      --------------                        --------------
      | Server-FTP |   Data Connection      | Server-FTP |
      |    "A"     |<---------------------->|    "B"     |
      -------------- Port (A)      Port (B) --------------
```

FTP
– Pure-FTPd (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

FTP
– Pure-FTPd (2)

- ❑ Installation
  - Ports: /usr/ports/ftp/pure-ftpd
  - Options



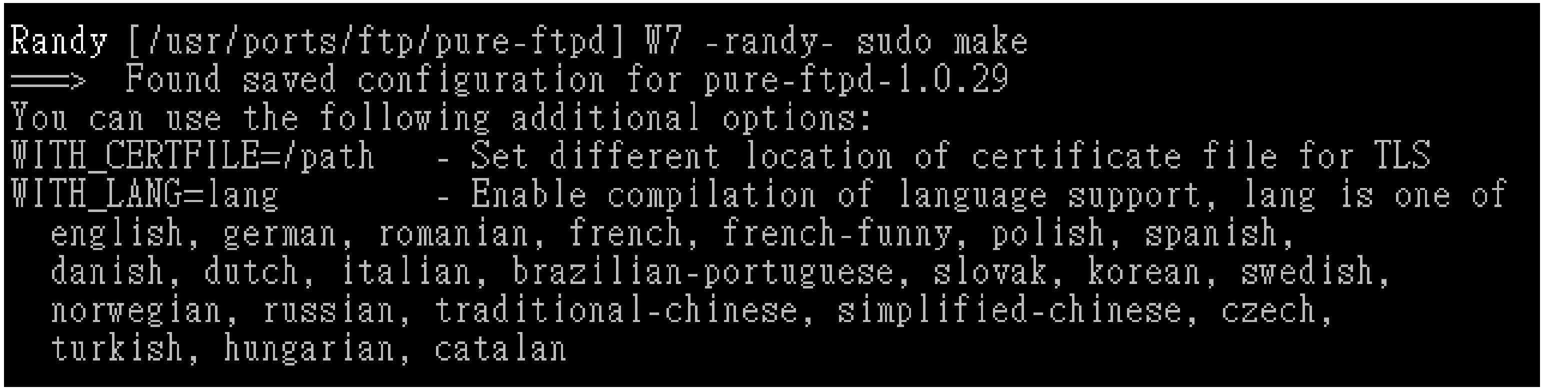
```
                    Options for pure-ftpd 1.0.29

  [ ] LDAP           Support for users in LDAP directories
  [ ] MYSQL          Support for users in MySQL database
  [X] PAM            Support for PAM authentication
  [ ] PGSQL          Support for users in PostgreSQL database
  [X] TLS            Support for TLS (experimental)
  [X] PRIVSEP        Enable privilege separation
  [ ] PERUSERLIMITS  Per-user concurrency limits
  [ ] THROTTLING     Bandwidth throttling
  [X] BANNER         Show pure-ftpd welcome upon session start
  [ ] UPLOADSCRIPT   Support uploadscript daemon
  [ ] UTF8           Support for charset conversion
  [X] SENDFILE       Support for the sendfile syscall
  [X] LARGEFILE      Support downloading files larger than 2Gb
  [X] VIRTUALCHROOT  Follow symlinks outside a chroot jail

                   [  OK  ]       Cancel
```

FTP – Pure-FTPd (3)

- Other options



```
Randy [/usr/ports/ftp/pure-ftpd] W7 -randy- sudo make
===>  Found saved configuration for pure-ftpd-1.0.29
You can use the following additional options:
WITH_CERTFILE=/path    - Set different location of certificate file for TLS
WITH_LANG=lang         - Enable compilation of language support, lang is one of
  english, german, romanian, french, french-funny, polish, spanish,
  danish, dutch, italian, brazilian-portuguese, slovak, korean, swedish,
  norwegian, russian, traditional-chinese, simplified-chinese, czech,
  turkish, hungarian, catalan
```

- WITH_CERTFILE for TLS
  - ➢ Default: /etc/ssl/private/pure-ftpd.pem
- WITH_LANG
  - ➢ Change the language of output messages

❑ Startup:

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

FTP
– 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/*

```
Randy [/usr/local/share/doc/pure-ftpd] W7 -randy- ls
AUTHORS         README                          README.MySQL          pure-ftpd.png
CONTACT         README.Authentication-Modules   README.PGSQL          pureftpd.schema
COPYING         README.Configuration-File       README.TLS
HISTORY         README.Contrib                  README.Virtual-Users
NEWS            README.LDAP                     THANKS
```

FTP – Pure-FTPd Configurations(2)

```
# Cage in every user in his home directory
ChrootEveryone          yes

# If the previous option is set to "no", members of the following group
# won't be caged. Others will be. If you don't want chroot()ing anyone,
# just comment out ChrootEveryone and TrustedGID.
TrustedGID              0

# PureDB user database (see README.Virtual-Users)
PureDB                  /usr/local/etc/pureftpd.pdb

# If you want simple Unix (/etc/passwd) authentication, uncomment this
UnixAuthentication      yes

# Port range for passive connections replies. - for firewalling.
PassivePortRange        30000 50000

# This option can accept three values :
# 0 : disable SSL/TLS encryption layer (default).
# 1 : accept both traditional and encrypted sessions.
# 2 : refuse connections that don't use SSL/TLS security mechanisms,
#     including anonymous sessions.
# Do _not_ uncomment this blindly. Be sure that :
# 1) Your server has been compiled with SSL/TLS support (--with-tls),
# 2) A valid certificate is in place,
# 3) Only compatible clients will log in.
TLS 2

# UTF-8 support for file names (RFC 2640)
# Define charset of the server filesystem and optionnally the default charset
# for remote clients if they don't use UTF-8.
# Works only if pure-ftpd has been compiled with --with-rfc2640
FileSystemCharset       big5
# ClientCharset         big5
```

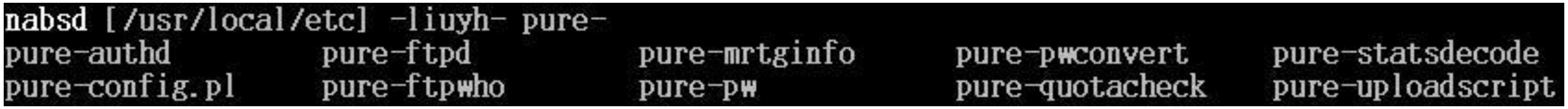
FTP
– Pure-FTPd Problem Shooting

❑ Logs Location

- In default, syslogd keeps ftp logs in /var/log/xferlog
- Most frequent problem
  - ➢ pure-ftpd: (?@?) [ERROR] Unable to find the 'ftp' account
    - – It’s ok, but you may need it for Virtual 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
– Pure-FTPd Tools

❑ pure-*



```
nabsd [/usr/local/etc] -liuyh- pure-
pure-authd           pure-ftpd            pure-mrtginfo        pure-pwconvert       pure-statsdecode
pure-config.pl       pure-ftpwho          pure-pw              pure-quotacheck      pure-uploadscript
```

❑ pure-ftpwho

- List information of users who use the FTP server now.

❑ pure-pw

- To create Virtual Users using PureDB
- pure-pw(8)
- See README.Virtual-Users

FTP
– More Tools

- ❑ ftp/pureadmin
  - Management utility for the PureFTPd
- ❑ ftp/lftp
  - A powerful functional client
  - Support TLS
- ❑ ftp/wget
  - Retrieve files from the Net via HTTP(S) and FTP
- ❑ ftp/mget
  - Multithreaded commandline web-download manager
- ❑ FileZilla
  - An FTP Client for Windows
  - Support TLS

FTP – PF: Issues with FTP (1)

- ❑ Reference: http://www.openbsd.org/faq/pf/ftp.html
- ❑ FTP Client Behind the Firewall
  - Problem
    - Clients cannot use active mode
  - Use ftp-proxy(8)
    - ftpproxy_enable="YES"
  - In pf.conf
    - nat-anchor "ftp-proxy/*"
    - rdr-anchor "ftp-proxy/*"
    - rdr on $int_if proto tcp from any to any port 21 -> 127.0.0.1 port 8021
    - anchor "ftp-proxy/*"

FTP
– PF: Issues with FTP (2)

❑ PF “Self-Protecting” an FTP Server

- Problem
  - ➢ Clients cannot use passive mode
- Open holes so that clients can connect into the data channel
- In pf.conf
  - ➢ pass in on $ext_if proto tcp from any to any port 21 keep state
  - ➢ pass in on $ext_if proto tcp from any to any port > 49151 keep state

FTP
– PF: Issues with FTP (3)

❑ FTP Server Protected by an External PF Firewall Running NAT

- Problem
  - ➢ Clients cannot use passive mode
- Use ftp-proxy(8)
  - ➢ Need some flags of ftp-proxy
  - ➢ ftpproxy_flags="-R 10.10.10.1 -p 21 -b 192.168.0.1"
- In pf.conf
  - ➢ nat-anchor “ftp-proxy/*”
  - ➢ nat on $ext_if inet from $int_if -> ($ext_if)
  - ➢ rdr-anchor “ftp-proxy/*”
  - ➢ pass in on $ext_if inet proto tcp to $ext_ip port 21 flags S/SA keep state
  - ➢ pass out on $int_if inet proto tcp to $ftp_ip port 21 user proxy flags S/SA keep state
  - ➢ anchor “ftp-proxy/*”