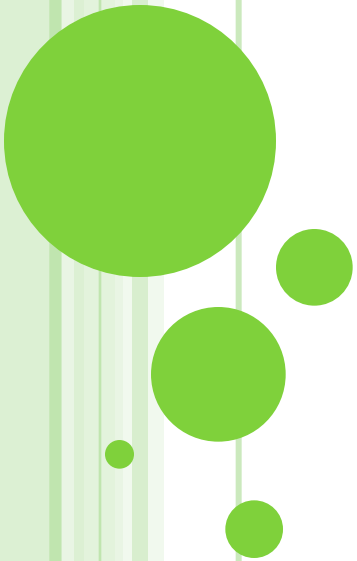


FTP –
File Transfer Protocol

FTP

- FTP
  - File Transfer Protocol
  - Used to transfer data from one computer to another over the internet.
  - Client-Server Architecture.
  - Separated control/data connections.
  - Modes:
    - Active Mode, Passive Mode
  - RFCs:
    - RFC 959 – File Transfer Protocol
    - RFC 2228 – FTP Security Extensions
    - RFC 2640 – UTF-8 support for file name

FTP – Flow (1)

Client	Server
	• Binding on port 21
• Connect to server port 21 using port A.	
	• Accepts connection from client, output welcome messages.
• USER ####	
	• 331 User name okay, need password.
• PASS ********	
	• 230 User logged in, proceed.
• PORT h1,h2,h3,h4,p1,p2	
	• 200 PORT Command successful.
• Send some requests get return data from p1*256+p2	
	• Binding source port 20, connect to client port p1*256+p2, send data.
• Quit	
	• …

FTP – Flow (2)

- Example
  - Control Connection

```
lwbsd:~ -lwhsu- telnet ftp.tw.freebsd.org 21
Trying 140.113.17.209...
Connected to freebsd.cs.nctu.edu.tw.
Escape character is '^]'.
220-FTP server ready.
220 Only anonymous FTP is allowed here
USER anonymous
331 Any password will work
PASS lwhsu@cs.nctu.edu.tw
230 Any password will work
PORT 140,113,17,197,39,19
200 PORT command successful
CWD pub
250-If you're looking for one of the FreeBSD releases, please look in the
250-releases/${ARCH}/${RELNAME} directory, where ARCH = "i386" or "alpha"
250-for Intel and DEC Alpha architecture machines and RELNAME = the release
250-you're interested in, e.g. "3.5.1-RELEASE" or "4.2-RELEASE".
250-
250 OK. Current directory is /pub
LIST
150 Connecting to port 10003
226-Options: -l
226 30 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

```
$ cat server.pl
#!/usr/bin/perl -w

package MyPackage;
use strict;
use base qw(Net::Server::PreFork);
MyPackage->run(port => $ARGV[0]);

sub process_request {
    while (<STDIN>) {
        s/\r?\n$//;
        print STDERR "$_\n";
    }
}
```

```
lwbsd:~ -lwhsu- perl server.pl 10003
2009/04/08-16:40:38 MyPackage (type Net::Server::PreFork) starting! pid(70673
Binding to TCP port 10003 on host *
Group Not Defined.  Defaulting to EGID '20 20 0 80'
User Not Defined.  Defaulting to EUID '1001'
drwxrwxr-x    6 888      2010           11 Oct 25  2007 CERT
lrwxr-xr-x    1 888      2010           15 Jun  1  2005 CTM -> development/CTM
lrwxr-xr-x    1 888      2010           17 Jun  1  2005 CVSup -> development/CVSup
drwxrwxr-x    4 888      2010            4 Jun 10  2005 ERRATA
lrwxr-xr-x    1 888      2010            1 Jun 10  2005 FreeBSD -> .
lrwxr-xr-x    1 888      2010           17 Jun  1  2005 FreeBSD-current -> branches/-current
lrwxr-xr-x    1 888      2010           19 Jun  1  2005 FreeBSD-stable -> branches/4.0-stable
lrwxr-xr-x    1 888      2010           25 Jun  1  2005 ISO-IMAGES-alpha -> releases/alpha/ISO-IMAGES
lrwxr-xr-x    1 888      2010           25 Jun  1  2005 ISO-IMAGES-amd64 -> releases/amd64/ISO-IMAGES
lrwxr-xr-x    1 888      2010           24 Jun  1  2005 ISO-IMAGES-i386 -> releases/i386/ISO-IMAGES
lrwxr-xr-x    1 888      2010           24 Jun  1  2005 ISO-IMAGES-ia64 -> releases/ia64/ISO-IMAGES
lrwxr-xr-x    1 888      2010           24 Jun  1  2005 ISO-IMAGES-pc98 -> releases/pc98/ISO-IMAGES
lrwxr-xr-x    1 888      2010           27 Feb 19  2008 ISO-IMAGES-powerpc -> releases/powerpc/ISO-IMAGES
lrwxr-xr-x    1 888      2010           27 Jan 15  2007 ISO-IMAGES-ppc -> releases/powerpc/ISO-IMAGES
lrwxr-xr-x    1 888      2010           27 Jun  1  2005 ISO-IMAGES-sparc64 -> releases/sparc64/ISO-IMAGES
-rw-rw-r--    1 888      2010         6430 Jun 19  2004 README.TXT
-rw-------    1 888      2010           11 May 10  2008 TIMESTAMP
drwxrwxr-x    2 888      2010            3 Jun 10  2005 TrustedBSD
drwxrwxr-x    9 888      2010            9 Mar 11  2008 branches
drwxrwxr-x    8 888      2010            8 Jun 10  2005 development
lrwxr-xr-x    1 888      2010           15 Jun  1  2005 distfiles -> ports/distfiles
(...)
```

FTP

– COMMANDS, RESPONSES

- Commands
  - USER username
  - PASS password
  - LIST
    - Return list of file in current dir.
  - RETR filename
    - Retrieves (gets) file.
  - STOR filename
    - Stores (puts) file onto server.
  - PORT h1,h2,h3,h4,p1,p2
    - Set to active mode
  - PASV
    - 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 “PORT” 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.
  - PORT h1,h2,h3,h4,p1,p2
- Passive Mode
  - FTP client sends “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.
  - PASV ➔ Server reply: 227 Entering Passive Mode (h1,h2,h3,h4,p1,p2)

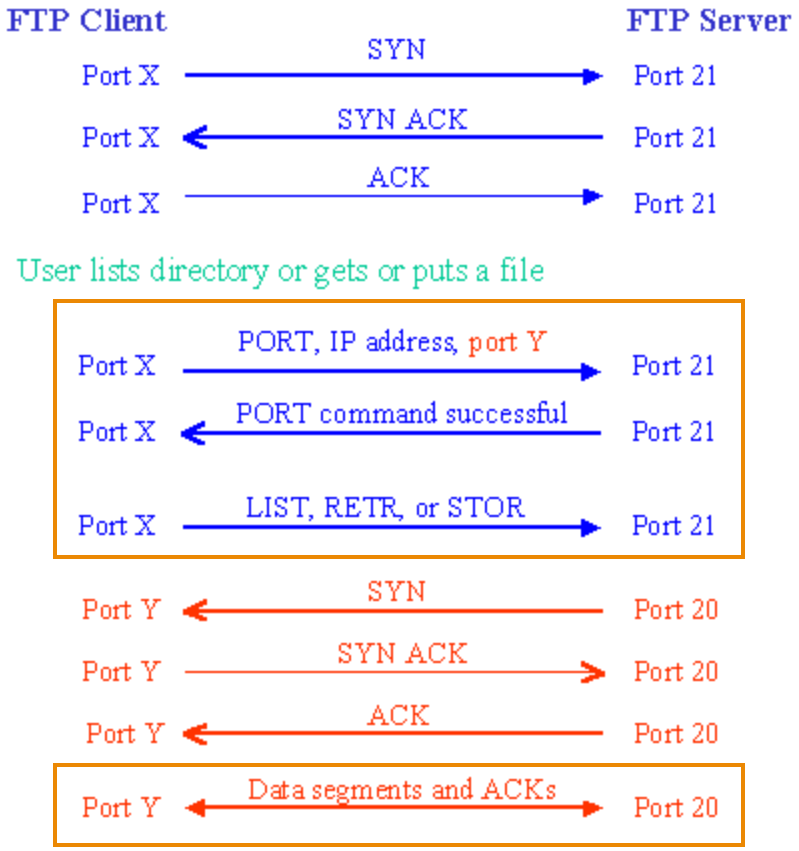
※ IP:port (6bytes) → h1,h2,h3,h4,p1,p2

Ex. 140.113.17.215:45678 → 140,113,17,215,178,110

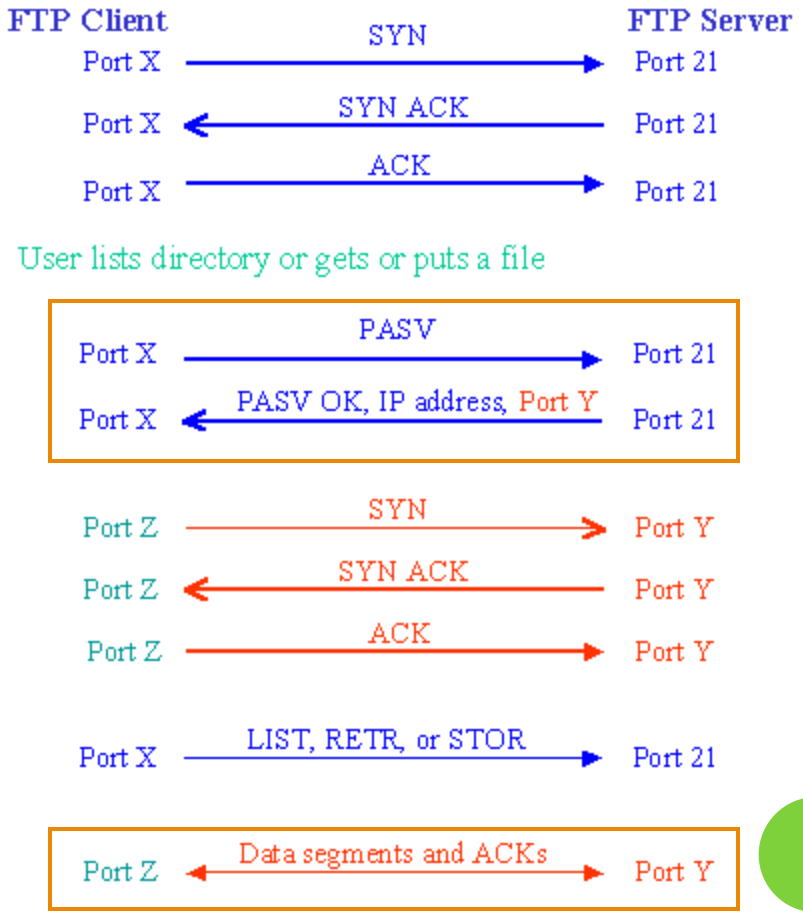
FTP

– Active Mode vs. Passive Mode (2)

Active mode



Passive mode

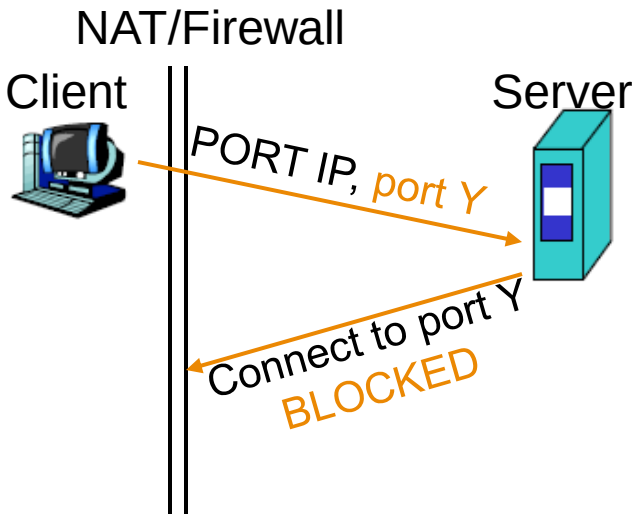


FTP
– When FTP meets NAT/Firewall (1)

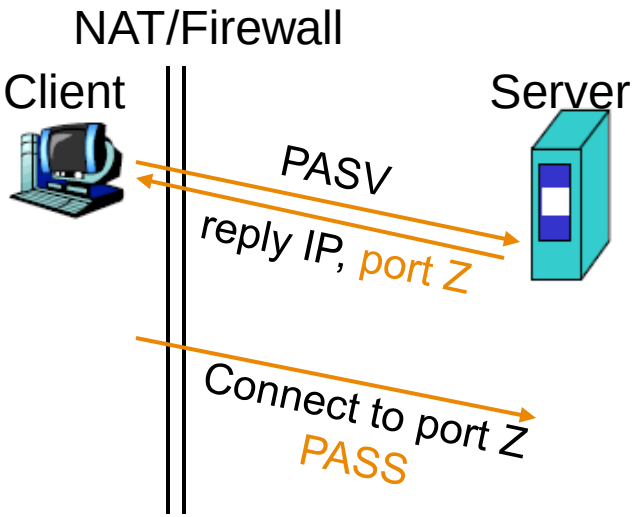
- Firewall behavior
  - Generally, the NAT/Firewall permits all outgoing connection from internal network, and denies all incoming connection from external network.
- Problem when FTP meets NAT/Firewall
  - Due to the separated command/data connection, the data connections are easily blocked by the NAT/Firewall.
- 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.



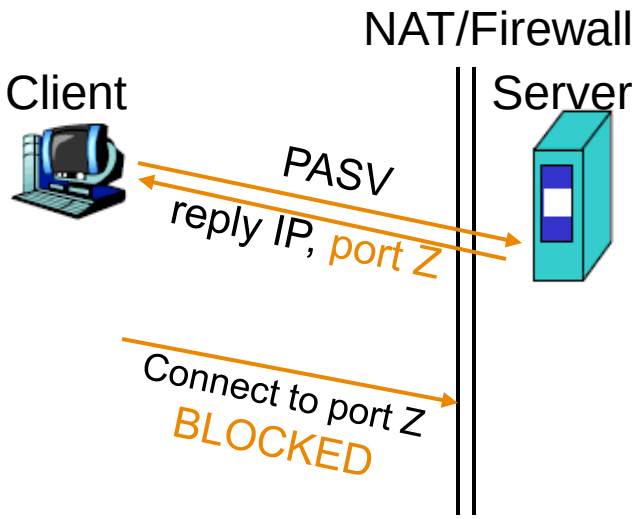
Active Mode



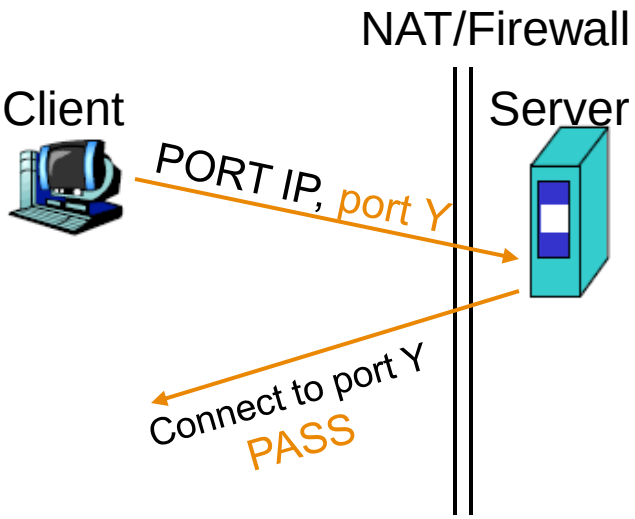
Passive Mode

FTP
– When FTP meets NAT/Firewall (3)

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



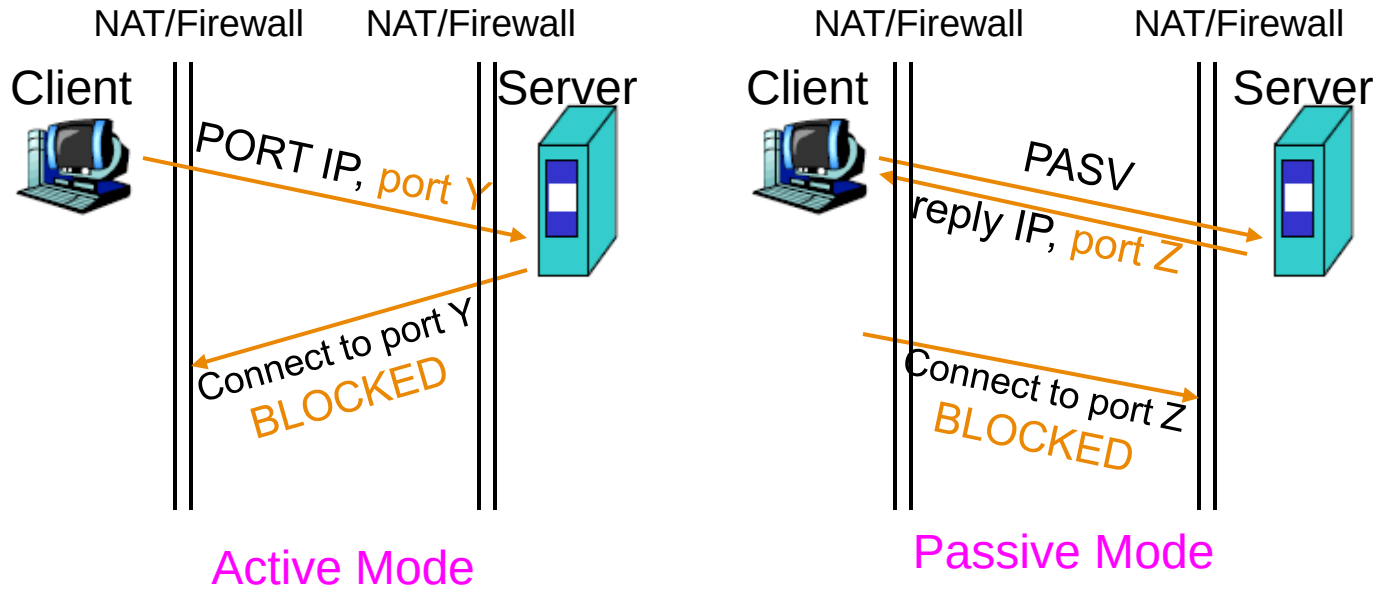
Passive Mode



Active Mode

FTP
– When FTP meets NAT/Firewall (4)

- Real Problem: Firewall on both sides.



- Solution: ftp-proxy running on NAT/Firewall

FTP – Security

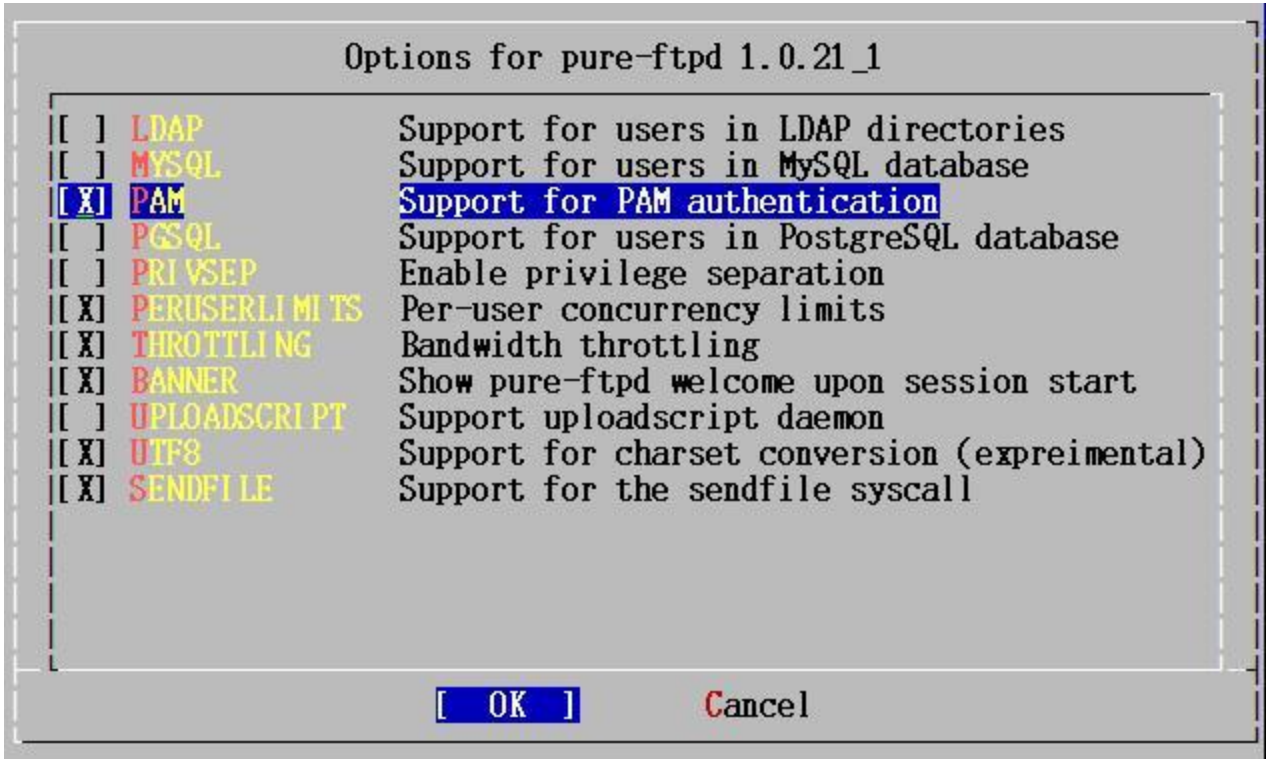
- Security concern
  - As we seen, FTP connections (both command and data) are transmitted in clear text.
  - What if somebody sniffing the network?
    - We need encryption.
- Solutions
  - FTP over SSH
    - So called secure-FTP.
    - Both commands and data are encrypted while transmitting.
    - Poor performance.
  - FTP over TLS
    - Only commands are encrypted while transmitting.
    - Better performance.

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 file names

FTP – PURE-FTPD (2)

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



FTP – Pure-FTPd (3)

- Other options

```
nabsd [/usr/ports/ftp/pure-ftpd] -liuyh- sudo make fetch
===>  Found saved configuration for pure-ftpd-1.0.21_1
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,
  dutch, italian, brazilian-portuguese, danish, slovak, korean,
  norwegian, swedish, russian, traditional-chinese, simplified-chinese,
  hungarian, catalan and czech.
```

  - WITH_CERTFILE for TLS
    - Default: /etc/ssl/private/pure-ftpd.pem
  - WITH_LANG
    - Change the language of output messages
- Startup:
  - Add pureftpd_enable="YES" into /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

```
mirror:/usr/local/share/doc/pure-ftpd -lwhsu- ls
AUTHORS                         README.Authentication-Modules  README.PGSQL
CONTACT                         README.Configuration-File      README.TLS
COPYING                         README.Contrib                 README.Virtual-Users
HISTORY                         README.LDAP                    THANKS
NEWS                            README.MySQL                   pure-ftpd.png
README                          README.Netfilter               pureftpd.schema
```

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                  /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
ClientCharset           big5
FileSystemCharset       utf-8
```

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
  - man pure-pw
  - See README.Virtual-Users

```
sudo pure-pw useradd testAC -f /usr/local/etc/pureftpd -u ftp -g users -d /ftp
sudo pure-pw mkdb /usr/local/etc/pureftpd.pdb -f /usr/local/etc/pureftpd
```

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
    - Use inetd to start ftp-proxy
    - man ftp-proxy
  - 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
    - Need some flags of ftp-proxy
    - man ftp-proxy
  - 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/*”

FTP – More Tools

- /usr/ports/ftp/pftpx
  - Another ftp proxy daemon
- /usr/ports/ftp/lftp
  - A powerful functional client
  - Support TLS
- /usr/ports/ftp/wget
  - Retrieve files from the Net via HTTP(S) and FTP
- /usr/ports/ftp/mget
  - Multithreaded commandline web-download manager
- FileZilla
  - An FTP Client for Windows
  - Support TLS