

Chapter 5: Network services

FTP – File Transfer Protocol

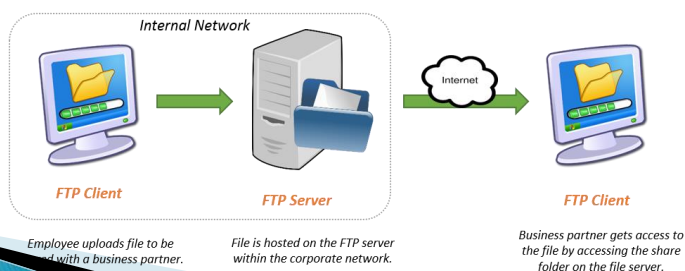
Lecturer: Nguyễn Thị Thanh Vân – FIT - HCMUTE

Nội dung

- I. TỔNG QUAN.
- II. MÔ HÌNH HOẠT ĐỘNG
 1. CƠ CHẾ ACTIVE,
 2. CƠ CHẾ PASSIVE
- III. FTP CLIENT, FTP SERVER
- IV. CÀI ĐẶT FTP
- V. CẤU HÌNH FTP
- VI. CẤU HÌNH VIRTUAL FTP SERVER.

I. Tổng quan

- ▶ **FTP (File Transfer Protocol)** là giao thức cung cấp cơ chế truyền tin dưới dạng tập tin (file) thông qua mạng TCP/IP
- ▶ FTP có hai thành phần :
 - FTP Server: chứa CSDL dùng chung
 - FTP Client: kết nối với server. Các OS đều hỗ trợ
- ▶ FTP Server sử dụng 2 port:
 - + **Port 20**: dùng để truyền dữ liệu (data port).
 - + **Port 21**: dùng để truyền lệnh (command port).
- ▶ Mô hình hoạt động: server/client



Thanh Vân - CNTT

3

Hoạt động

Có hai cơ chế :

❑ Active FTP:

- Bất cứ khi nào client yêu cầu dữ liệu qua kết nối điều khiển, thì **Server** khởi tạo một kết nối chuyển dữ liệu cho client
- Port nguồn luôn là 20, port đích luôn >1024

❑ Passive FTP :

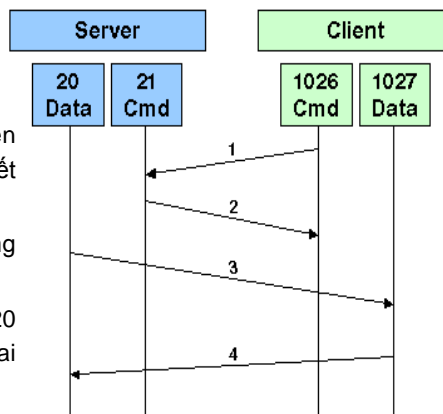
- Bất cứ khi nào client yêu cầu dữ liệu qua kết nối điều khiển thì **Client** khởi tạo một kết nối chuyển dữ liệu cho client.
- Port nguồn và port đích luôn lớn hơn 1024

Thanh Vân - CNTT

4

II.1. Cơ chế Active

- ▶ **Bước1:** client dùng một cổng ngẫu nhiên không dành riêng (port $N=1026 > 1024$) kết nối vào cổng 21 của FTP Server.
- ▶ **Bước2:** server gửi xác nhận ACK về cổng (port $N=1026$) của client.
- ▶ **Bước3:** server khởi tạo kết nối từ cổng 20 của mình đến cổng dữ liệu mà client đã khai báo (port $N+1=1027$).
- ▶ **Bước4:** client gửi ACK phản hồi cho server thông qua cổng dữ liệu 20.

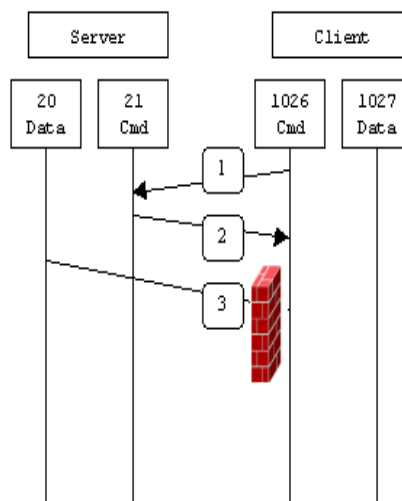


II.1. Cơ chế Active

- Để FTP Server hỗ trợ chế độ Active các kênh truyền sau phải mở:
 - Cổng 21 phải được mở cho bất cứ nguồn gửi nào (để Client khởi tạo kết nối)
 - FTP Server's port 21 to ports > 1024 của client (Server trả lời về cổng điều khiển của Client)
 - Cho kết nối từ cổng 20 của FTP Server đến các cổng > 1024 (Server khởi tạo kết nối vào cổng dữ liệu của Client)
 - Nhận kết nối hướng đến cổng 20 của FTP Server từ các cổng > 1024 (Client gửi xác nhận ACKs đến cổng data của Server)

II.1. Cơ chế Active

- Firewall phía client là nguyên nhân của việc không thể tạo ra một kết nối FTP hoàn chỉnh.
- Cho phép các hacker dễ dàng dùng các công cụ scan để dò tìm các cổng đang mở trên máy

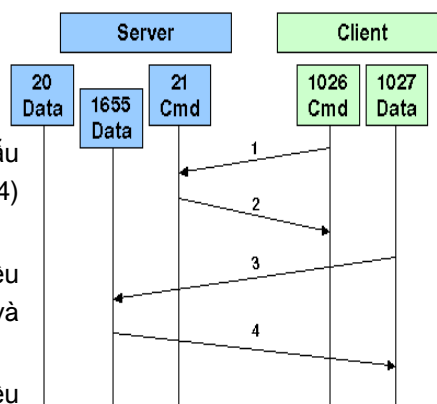


Thanh Vân - CNTT

7

II.2. Cơ chế Passive

- ▶ **Bước 1:** client dùng một cổng lệnh ngẫu nhiên không dành riêng (port $N > 1024$) kết nối vào cổng 21 của FTP Server.
- ▶ **Bước 2:** server sẽ mở cổng dữ liệu không dành riêng bất kỳ $P (P > 1024)$ và gửi lệnh Port P cho client.
- ▶ **Bước 3:** client tạo kết nối truyền dữ liệu từ cổng dữ liệu của nó (port $N+1$) đến cổng dữ liệu P của server.
- ▶ **Bước 4:** server trả lời bằng xác nhận ACK về cho cổng dữ liệu của client.



Thanh Vân - CNTT

8

II.2. Cơ chế Passive

- ▶ Để hỗ trợ FTP chế độ passive, các kênh truyền sau phải được mở:
 - Cổng FTP 21 của Server nhận kết nối từ bất nguồn nào (cho Client khởi tạo kết nối)
 - Cho phép trả lời từ cổng 21 FTP Server đến cổng bất kỳ trên 1024 (Server trả lời cho cổng control của Client)
 - Nhận kết nối trên cổng FTP server > 1024 từ bất cứ nguồn nào (Client tạo kết nối để truyền dữ liệu)
 - Cho phép trả lời từ cổng FTP Server > 1024 đến các cổng > 1024 (Server gửi xác nhận ACKs đến cổng dữ liệu của Client)

II.2. Cơ chế Passive

- ▶ Ở chế độ thụ động, FTP Client tạo kết nối đến Server, tránh vấn đề Firewall lọc kết nối từ Server đến cổng của máy bên trong
- ▶ Hạn chế ở phía Server:
 - Cho phép máy ở xa kết nối vào cổng bất kỳ > 1024 của Server.
 - > Khả năng nguy hiểm trừ khi FTP cho phép mô tả dãy các cổng >= 1024 mà FTP Server sẽ dùng (ví dụ WU-FTP Daemon).
 - Một số FTP Client lại không hỗ trợ chế độ thụ động.

Active-Passive

- ▶ IIS hỗ trợ cả hai chế độ kết nối Active và Passive, do đó việc kết nối theo phương thức Active hay Passive tùy thuộc vào từng Client.
- ▶ IIS không hỗ trợ cơ chế vô hiệu hóa (disable) chế độ kết nối Active hay Passive.
- ▶ Khi hệ thống có firewall (chỉ cho phép kết nối TCP theo cổng dịch vụ 21) thì những hệ thống này phải mở TCP port 20 (để truyền dữ liệu với các lệnh của FTP).
- ▶ Hỗ trợ Active: Command line , < IE 5.0
- ▶ Hỗ trợ Passive: >IE 5.0

III.1. Chương trình FTP client.

- ▶ Giao tiếp với FTP Server, hầu hết các hệ điều hành đều hỗ trợ FTP Client,
- ▶ Để thiết lập một phiên giao dịch, ta cần phải có địa chỉ IP (hoặc tên máy tính), một tài khoản (FTP hỗ trợ)
 - User: anonymous
 - Password: rỗng.

Ví dụ ftp client bằng command line

```

C:\Windows\system32\cmd.exe - ftp 192.168.90.3
C:\Users\vannt>ftp 192.168.90.3
Connected to 192.168.90.3.
220 Microsoft FTP Service
User (192.168.90.3:(none)): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 Anonymous user logged in.
ftp> ls
200 PORT command successful.
150 Opening ASCII mode data connection for file list.
th1
th2
226 Transfer complete.
ftp: 10 bytes received in 0.00Seconds 3.33Kbytes/sec.
ftp>
  
```

Thanh Vân - CNTT

13

Tập lệnh của ftp client

Cd	cd remote-directory	Thay đổi đường dẫn thư mục trên FTP Server .
delete	delete remote-file	Xóa file trên FTP Server .
Dir	dir remote-directory	Liệt kê danh sách tập tin.
Get	get remote-file [local-file]	Download tập tin từ FTP Server về máy cục bộ.
Lcd	lcd [directory]	Thay đổi thư mục trên máy cục bộ.
Ls	ls [remote-directory] [local-file]	Liệt kê các tập tin và thư mục.
mdelete	mdelete remote-files [...]	Xóa nhiều tập tin.
Mget	mget remote-files [...]	Download nhiều tập tin.
Mkdir	mkdir directory	Tạo thư mục.
Put	put local-file [remote-file]	Upload tập tin.
Mput	mput local-files [...]	Upload nhiều tập tin.
Open	open computer [port]	Kết nối tới ftp server .

14

III.2. FTP server

- ▶ Là máy chủ lưu trữ tập trung dữ liệu, cung cấp dịch vụ FTP để hỗ trợ cho người dùng có thể cung cấp, truy xuất tài nguyên qua mạng TCP/IP.
- ▶ Cài đặt FTP server
 - Để cài đặt FTP trên hệ điều hành windows server yêu cầu server đã cài đặt IIS (Internet Information Services).
 - Vào “Server Manager” chọn “Roles” \ “Web Server(IIS)” \ phải chuột chọn “Add Role Services”...\Finish

V. Cấu hình dịch vụ FTP.

- ▶ Giao diện quản lý:
Administrative Tools | Internet Information Services(IIS) Manager | Computer name | FTP sites
1. Tạo mới FTP site.
 2. Tạo Virtual Directory.
 3. Cấu hình chứng thực FTP - Authentication
 4. Cấu hình cho phép dùng FTP - Authorization
 5. Cấu hình FTP User Isolate
 6. Theo dõi các user login vào FTP Server
 7. Tạo nhiều FTP Site.
 8. Theo dõi và cấu hình nhật ký cho FTP. ..
 9. Khởi động và tắt dịch vụ FTP.
 10. Lưu trữ và phục hồi thông tin cấu hình.

1. Tạo mới FTP site.

- ❖ Create a folder at "%SystemDrive%\inetpub\ftproot"
- ❖ Set the permissions to allow anonymous access:
 - Type the following command:
`ICACLS "%SystemDrive%\inetpub\ftproot" /Grant IUSR:R /T`
- ❖ FTP Sites | Add FTP Site:
- ❖ Nhập thông số cần thiết:
 - ❖ Site Information: FTP Site Name, Content Directory (nơi lưu tài nguyên)
 - ❖ Binding and setting SSL:
 - ❖ Enable Virtual Host Names : tick này cho phép ta tạo nhiều site trên cùng 1 địa chỉ IP
 - ❖ Start FTP Site automatically : tự kích hoạt FTP server sau khi hoàn tất
 - ❖ SSL : Thêm tính năng bảo mật
 - ❖ Chọn thêm phương thức chứng thực
 - Finish
- ❖ Kiểm tra tại client: ftp://IP

Thanh Vân - CNTT

17

2. Tạo Virtual Directory

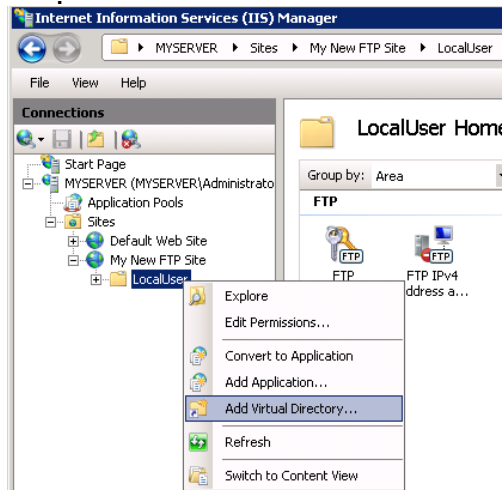
- ▶ Các thư mục con của FTP root đều có thể truy xuất :
`ftp://<IP_FTP_server>/<subDir_name>`
 - ▶ Virtual directory: để cho phép người dùng có thể truy xuất một tài nguyên bên ngoài FTP root .
 - ▶ Thực hiện:
 - Tạo một thư mục ảo bên trong FTP Site,
 - ánh xạ vào bất kỳ một thư mục nào đó trên ổ đĩa cục bộ hoặc ánh xạ vào một tài nguyên chia sẻ trên mạng.
 - ánh xạ xong ta có thể truy xuất:
- `"ftp://<địa_chỉ_của_FTP_server>/<tên_thư_mục_ảo >`

Thanh Vân - CNTT

18

2. Tạo Virtual Directory

Thực hiện:



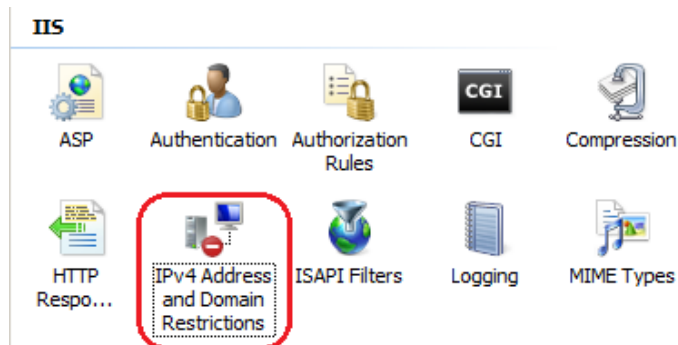
Kiểm tra trên client: ftp:// <IP>/<alias>

vd: ftp:// 192.168.90.2/share

Thanh Vân - CNTT

19

Hạn chế truy nhập FTP



20

3. Cấu hình Authentication

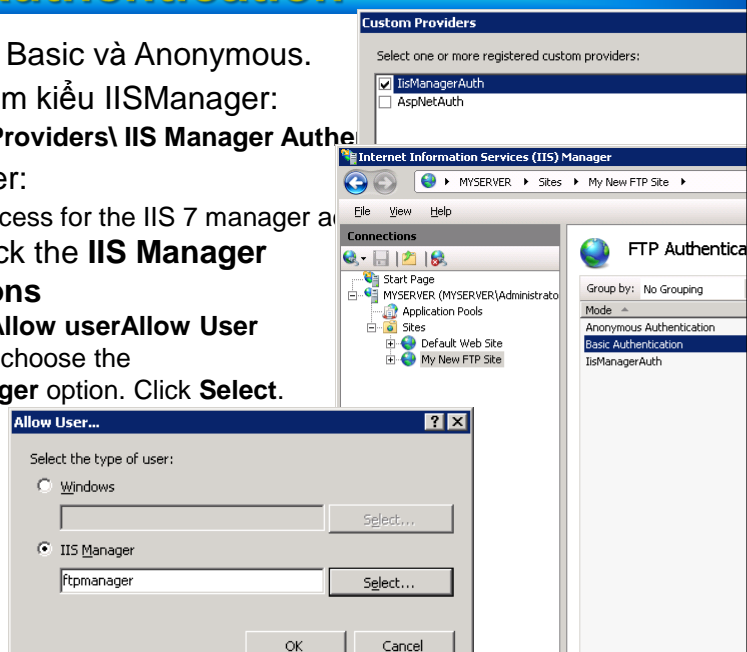
- ▶ Bước 1: Chọn kiểu chứng thực Authentication
- ▶ Bước 2: Cấu hình 1 kiểu chứng thực xác định ex, IISManager Permission

Thanh Vân - CNTT

21

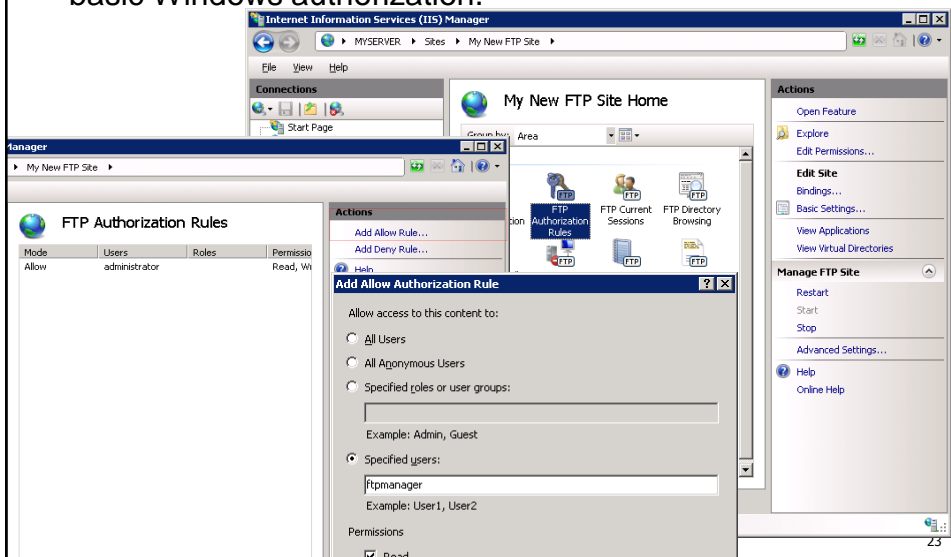
3. FTP Authentication

- ▶ Có 2 kiểu: Basic và Anonymous.
- ▶ Có thể thêm kiểu IISManager:
 - Custom Providers\ IIS Manager Authentication
- ▶ IISManager:
 - Enable access for the IIS 7 manager and
- ▶ Double-click the **IIS Manager Permissions**
 - Action\ Allow user Allow User displays, choose the IIS Manager option. Click **Select**.



4. FTP Authorization Rule

- ▶ This allows you to manage access to your ftp site through basic Windows authorization.



5. FTP User Isolation

- ❖ FTP User Isolation:
 - Do not isolate users: Không giới hạn truy xuất tài nguyên cho từng người dùng.
 - Isolate users: Giới hạn truy xuất tài nguyên FTP cho từng người dùng tới các thư mục:
 - **User name directory (disable global virtual directories)**
 - **User name physical directory (enable global virtual directories)**
 - **FTP home directory configured in Active Directory** : Dùng AD để giới hạn việc sử dụng tài nguyên cho từng người



FTP User
Isolation

5. FTP User Isolation

Here is how I use FTP user isolation and it works great.

- 1) Tạo FTPRoot folder
- 2) Tạo Master FTP site.
- 3) Tạo Virtual Directory
- 4) Trong Vdirectory, tạo user
- 5) Trong User Isolation: Chọn User name directory (disable global virtual directories)
- 6) Trong Authentication: enable basic authentication (dùng với account windows)
- 7) Trong Authorization, Hạn chế quyền user.
- 8) Cung cấp folder security cho user
- 9) Test

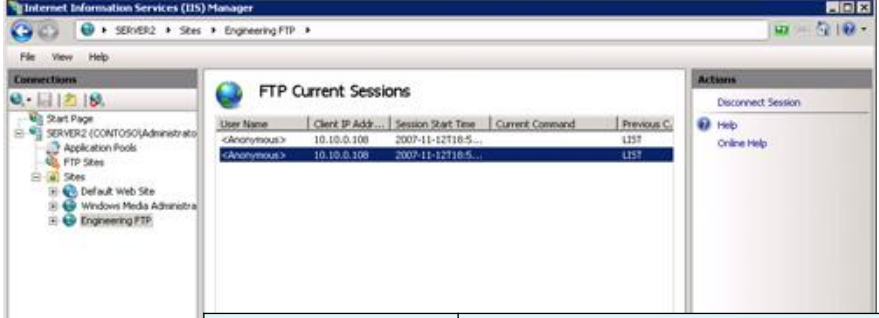
25

Isolation Mode

Isolation Mode	Chức năng
Do not isolate users	Đây là chế độ không sử dụng FTP User Isolation , ở mode này không giới hạn truy xuất của người dùng. Thông thường ta sử dụng mode này để tạo một public FTP Site .
Isolate users	Mode này chứng thực người dùng cục bộ (Local User) và người dùng miền (Domain User) truy xuất vào FTP Site . Đối với mode người quản trị phải tạo cho mỗi người dùng một thư mục con của thư mục FTP Root , với tên thư mục này là username của người dùng.
Isolate users using Active Directory	Sử dụng Active Directory để tách lập từng user truy xuất vào FTP Server .

26

6.Theo dõi các user login vào FTP Server



Element Name	Description
User name	Specifies the user name for this session.
Session start time	Specifies the start time for the current session.
Current command	Specifies the current command.
Previous command	Specifies the previous command.
Command start time	Specifies the start time for the command.
Bytes sent	Specifies the bytes sent.
Bytes received	Specifies the bytes received.
Session ID	Specifies the session ID.
Client IP	Specifies the client IP address.

Thanh Vân - CNTT

7. Tạo nhiều FTP Site

- ▶ Ta có thể tạo nhiều FTP Site trên một FTP Server bằng cách sử dụng **nhiều IP và nhiều FTP port.**
- ▶ Các bước thực hiện:
 - FTP Sites | New | FTP Site...:
 - Description
 - IP Address and Port Settings
 - FTP User Isolation
 - Home Directory cho FTP Site.
 - Chọn quyền hạn truy xuất cho FTP site, mặc định hệ thống chọn quyền Read,
 - Finish
 - Kiểm tra tại client: ftp://IP

8. Theo dõi và cấu hình nhật ký cho FTP

- ▶ Mặc định FTP lưu lại một số sự kiện như:
 - Địa chỉ của FTP Client truy xuất vào FTP Server,
 - Thời gian truy xuất của máy trạm,
 - Trạng thái hoạt động của dịch vụ,... để hỗ trợ cho
- ▶ Lưu trữ: %systemroot%\system32\LogFiles\MSFTPSVnnnnnnnn, trong đó nnnnnnnn là số ID của FTP Site.
- ▶ Hiệu chỉnh Nhật ký của dịch vụ
Tab FTP Site | Properties:
 - New log schedule: Chỉ định ghi nhận theo lịch biểu, kích thước file
 - Log file directory: Chỉ định thư mục lưu trữ log file.

9. Khởi động và tắt dịch vụ FTP

- ▶ Dùng trình tiện ích IIS: FTP Site:
 - Stop để dừng dịch vụ
 - Start để khởi động dịch vụ.
- ▶ Dùng dòng lệnh để khởi động và tắt dịch vụ FTP:
 - <command_prompt>net <stop/start> msftpsvc
 - Restart: < command_prompt >iisreset.

10. Lưu trữ và phục hồi thông tin cấu hình

- ▶ Lưu trữ thông tin cấu hình vào tập tin *.xml:
 - FTP Site \ All Task \ Save Configuration to a File
 - Chỉ định tên tập tin và thư mục lưu trữ thông tin cho FTP server.
 - Encrypt configuration using password: Sử dụng mật khẩu để mã hóa thông tin cấu hình
- ▶ Phục hồi thông tin hoặc tạo mới FTP site từ tập tin cấu hình *.xml:
 - FTP site\ New \ FTP site (from file)
 - Browse... để chọn tập tin cấu hình / Read File,
 - Chọn Location: tên mô tả
 - chọn OK.

THỰC HÀNH

- ▶ Theo yêu cầu