**HỌC VIỆN KỸ THUẬT QUÂN SỰ**

**KHOA CÔNG NGHỆ THÔNG TIN**

**BÁO CÁO MÔN HỌC**

**QUẢN TRỊ MẠNG**

**ĐỀ TÀI**

**THIẾT KẾ VÀ QUẢN LÝ FTP SERVER SỬ DỤNG VSFTPD CHO MỘT DOANH NGHIỆP**

|  |  |
| --- | --- |
| Nhóm 5: | Nguyễn Thu Phương - CNTT1  Nguyễn Huy Tuân - CNTT2 |

*Hà Nội, 11/2022*

MỤC LỤC

[MỤC LỤC 1](#_Toc120010174)

[DANH MỤC HÌNH ẢNH 3](#_Toc120010175)

[DANH MỤC BẢNG BIỂU 4](#_Toc120010176)

[I. Tổng quan về FTP 5](#_Toc120010177)

[1. FTP là gì? 5](#_Toc120010178)

[2. FTP Server là gì? 5](#_Toc120010179)

[3. Mục đích, chức năng của FTP Server 5](#_Toc120010180)

[*3.1. Mục đích* 5](#_Toc120010181)

[*3.2. Chức năng* 6](#_Toc120010182)

[*3.3. Lợi ích khi doanh nghiệp sử dụng FTP Server* 6](#_Toc120010183)

[4. Ưu, nhược điểm của FTP 7](#_Toc120010184)

[*4.1. Ưu điểm* 7](#_Toc120010185)

[*4.2. Nhược điểm* 7](#_Toc120010186)

[II. Nguyên lý hoạt động của FTP 7](#_Toc120010187)

[1. Mô hình cơ bản FTP 7](#_Toc120010188)

[*1.1. Kết nối TCP trong FTP* 7](#_Toc120010189)

[*1.2. Mô hình FTP* 8](#_Toc120010190)

[*1.3. Chức năng từng phần trong mô hình FTP* 9](#_Toc120010191)

[2. Nguyên lý hoạt động của FTP 9](#_Toc120010192)

[3. Một số lệnh command sử dụng trên FTP 10](#_Toc120010193)

[4. FTP reply 11](#_Toc120010194)

[5. Phương thức tạo kết nối và truyền dữ liệu trong FTP 12](#_Toc120010195)

[*5.1. Phương thức tạo kết nối dữ liệu* 12](#_Toc120010196)

[*5.2. Phương thức truyền dữ liệu* 13](#_Toc120010197)

[6. Dữ liệu trong FTP 14](#_Toc120010198)

[*6.1. FTP Data Types* 14](#_Toc120010199)

[*6.2. FTP Data Structures* 14](#_Toc120010200)

[7. Mã hóa kết nối FTP với SSL/TLS 15](#_Toc120010201)

[III. Cài đặt hệ thống FTP server 16](#_Toc120010202)

[1. Cài đặt và cấu hình vsftpd 16](#_Toc120010203)

[2. Demo kết nối máy chủ FTP server bằng Windown client 19](#_Toc120010204)

[3. Demo kết nối máy chủ FTP server bằng Ubuntu client 23](#_Toc120010205)

[4. Mã hóa kết nối FTP với SSL/TLS 25](#_Toc120010206)

[TÀI LIỆU THAM KHẢO 28](#_Toc120010207)

**DANH MỤC HÌNH ẢNH**

*Hình 1. Minh họa về FTP 5*

*Hình 2. Minh họa việc trao đổi dữ liệu giữa các thiết bị 6*

*Hình 3. Các kết nối trong FTP 7*

*Hình 4. Mô hình hoạt động của FTP 8*

*Hình 5. Minh họa phương thức tạo kết nối của FTP 13*

*Hình 6. Cơ chế mã hóa của SSL/TLS 15*

*Hình 7. Minh họa FTPS 16*

*Hình 8. Kiểm tra phiên bản của vsftpd 16*

*Hình 9. Kết quả sau khi cấu hình tường lửa 17*

*Hình 10. Tạo người dùng mới 18*

*Hình 11. Kiểm tra thư mục vừa tạo 19*

*Hình 12. Giao diện của FileZilla 19*

*Hình 13. Thêm tên miền 20*

*Hình 14. Tạo kết nối tới Server 21*

*Hình 15. Kết quả khi truy cập thành công vào Server 21*

*Hình 16. Kết quả khi thực hiện sửa tập tin 22*

*Hình 17. Gửi tập tin đã sửa về Server 22*

*Hình 18. Kiểm tra tập tin tại Server 22*

*Hình 19. Thêm tên miền vào file hosts 23*

*Hình 20. Kết nối với Server bằng tên miền 23*

*Hình 21. Kết quả kiểm tra đường dẫn hiện đang truy cập 23*

*Hình 22. Kết quả hiển thị danh sách các tệp 24*

*Hình 23. Kết quả tải về tập tin 24*

*Hình 24. Kết quả upload tệp lên Server 24*

*Hình 25. Thay đổi quyền người dùng 24*

*Hình 26. Kiểm tra sự thay đổi về quyền 25*

*Hình 27. Tạo chứng chỉ SSL 25*

*Hình 28. Cấu hình file config 26*

*Hình 29. Kết quả sau khi mã hóa kết nối 27*

# DANH MỤC BẢNG BIỂU

*Bảng 1: Một số lệnh command trên FTP 10*

*Bảng 2: Ý nghĩa của tham số X trong FTP reply code 12*

*Bảng 3: Ý nghĩa của tham số y trong reply code 12*

# I. Tổng quan về FTP

## *1. FTP là gì?*

Diagram

Description automatically generated

Hình 1. Minh họa về FTP

- FTP viết tắt từ *File Transfer Protocol*, là một giao thức truyền tải tập tin từ máy tính này đến máy tính khác thông qua mạng lưới truyền thông dùng giao thức TCP/IP (chẳng hạn như mạng Internet hoặc mạng nội bộ,…)

- Thông qua giao thức FTP, người dùng có thể truyền tải dữ liệu đa dạng như hình ảnh, văn bản, video, âm thanh… Các dữ liệu được truyền từ máy tính cá nhân lên máy chủ đang đặt ở một nơi khác hoặc tải các tập tin có trên máy chủ về máy tính cá nhân.

## *2. FTP Server là gì?*

- Máy chủ FTP là một chương trình máy tính được xây dựng để xử lý việc truyền dữ liệu giữa các máy tính. Máy chủ đợi các máy khách kết nối với nó và đưa ra các lệnh yêu cầu máy chủ tải lên, tải xuống hoặc liệt kê các thư mục. Giao thức FTP là các lệnh mà máy chủ FTP sử dụng để thực hiện điều này.

- Máy chủ FTP cho phép các thao tác tải xuống, tải lên, xem, sửa, xóa, sao chép các tệp và gán quyền cho người dùng. Quản trị viên của máy chủ FTP có thể hạn chế quyền truy cập để tải xuống các tệp khác nhau và từ các thư mục khác nhau nằm trong máy chủ FTP.

## 3. Mục đích, chức năng của FTP Server

### *3.1. Mục đích*

- Khuyến khích việc dùng chung các tập tin (như là các chương trình ứng dụng hoặc dữ liệu)

- Khuyến khích việc sử dụng máy tính từ xa một cách gián tiếp.

- Xóa nhòa sự khác biệt về hệ thống lưu trữ tập tin giữa các máy chủ, giúp cho người dùng hầu như không phải quan tâm đến những sự khác biệt của chúng.

- Truyền tải dữ liệu một cách đáng tin cậy và có hiệu quả cao.

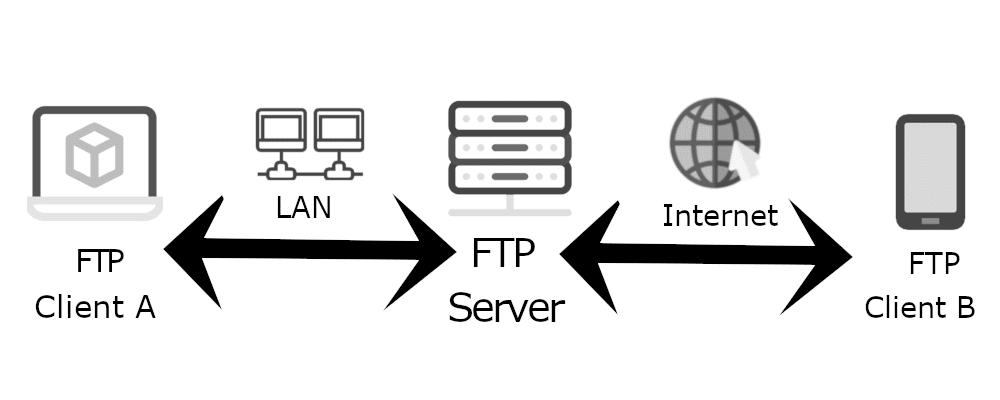
### *3.2. Chức năng*

- Truyền tải dữ liệu website lên máy chủ:

Bộ phận IT của doanh nghiệp có thể quản lý toàn bộ dữ liệu dạng thư mục và tập tin thông qua tài khoản FTP. Nghĩa là người dùng có thể tải tập tin với dung lượng lớn hoặc nhỏ từ máy tính cá nhân lên server.

- Truyền tải dữ liệu giữa các máy tính:

Chức năng nổi bật của FTP là truyền tải dữ liệu giữa các máy tính với nhau. Người dùng thường bị động về mặt thời gian khi sao chép lượng lớn tập tin nếu sử dụng phương thức gửi mail hay sao chép vật lý thủ công (CD, USB flash,…). Tuy nhiên, với FTP người dùng có thể chủ động khi sao chép và truyền tập tin với dung lượng lớn một cách nhanh chóng.



Hình 2. Minh họa việc trao đổi dữ liệu giữa các thiết bị

### *3.3. Lợi ích khi doanh nghiệp sử dụng FTP Server*

*- Cho phép tải về tập tin trong trang web:*

Khi khách hàng của bạn nhấn chuột vào một liên kết cho phép tải về tệp tin trong trang web thì trình duyệt sẽ thực hiện các thao tác truyền FTP. Điều cần quan tâm là tập tin đó sẽ được lưu trữ ở đâu để khách hàng có thể tải về bất cứ lúc nào họ muốn.

*- Có thể nhập vào địa chỉ của máy chủ cần truy xuất tới:*

Một số tổ chức cung cấp dịch vụ FTP thông dụng (có thu phí) giúp bạn có thể nhập vào địa chỉ của máy chủ cần truy xuất tới. Bao gồm tên, mật khẩu đăng nhập (nếu có) và các giao diện để bạn có thể dễ dàng tải về hoặc đưa lên các tệp tin của mình. Đó là các tổ chức như: Rapidshare, Megaupload, File Host, v.v… với chi phí đăng ký tài khoản khá cao tính bằng USD.

*- Các đối tượng có thể cùng truy cập:*

Khi sở hữu một máy chủ FTP server, bạn có khả năng tự cho phép các đối tượng có thể cùng truy cập, sử dụng, và thao tác trên một vùng dữ liệu chung do chính bạn quyết định. Bên cạnh đó, bạn có khả năng phân quyền và cung cấp tài khoản truy cập cho nhiều đối tượng sử dụng dữ liệu. Đảm bảo mức độ bảo mật cao và tốc độ truy cập nhanh không phụ thuộc khoảng cách về địa lý.

## *4. Ưu, nhược điểm của FTP*

### *4.1. Ưu điểm*

- Cho phép truyền nhiều tin cùng 1 lúc.

- Cho phép chuyển tệp tin nếu không may mất kết nối.

- Tự động chuyển tập tin bằng các Script.

- Cho phép thêm dữ liệu vào khung chờ, và lên lịch truyền.

- Khả năng đồng bộ hoá tệp tin.

### *4.2. Nhược điểm*

- Khả năng bảo mật kém. Tên người dùng, mật khẩu và tệp đều được gửi bằng văn bản thuần túy, do đó tin tặc có thể dễ dàng truy cập thông tin của bạn.

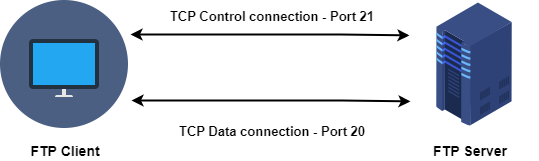
- Không phù hợp cho các tổ chức, do yêu cầu phải tạo cổng kết nối khi truyền.

- Máy chủ có khả năng bị qua mặt, gửi thông tin đến các cổng ngẫu nhiên trên một máy tính không chính xác.

# II. Nguyên lý hoạt động của FTP

## *1. Mô hình cơ bản FTP*

### *1.1. Kết nối TCP trong FTP*



Hình 3. Các kết nối trong FTP

Dựa trên mô hình cơ bản của chuyển đổi dữ liệu, giao thức FTP hoạt động bằng hai hướng là nhận và truyền dữ liệu giữa máy chủ Server và máy khách Client. Data Connection và Control Connection chính là hai tiến trình TCP (Transmission Control Protocol) tạo ra quy trình nhận cũng như truyền dữ liệu của Server và Client.

* **Control connection (sử dụng port 21 – trên server):** Đây là phiên làm việc TCP logic đầu tiên được tạo ra khi quá trình truyền dữ liệu bắt đầu. Tuy nhiên, tiến trình này chỉ kiểm soát các thông tin điều khiển đi qua nó, ví dụ như các tập lệnh hoặc các reponse (phản hồi). Quá trình này sẽ được duy trì trong suốt quá trình phiên làm việc diễn ra.
* **Data connection (sử dụng port 20 – trên server):** Là một kết nối dữ liệu TCP được tạo ra với mục đích chuyên biệt là truyền tải dữ liệu giữa máy Client và máy Server. Kết nối sẽ tự động ngắt khi quá trình truyền tải dữ liệu hoàn tất.

### *1.2. Mô hình FTP*

Diagram

Description automatically generated

Hình 4. Mô hình hoạt động của FTP

Do chức năng điều khiển và dữ liệu được truyền tải bằng cách sử dụng các kênh riêng biệt nên mô hình FTP chia mỗi thiết bị thành 2 phần giao thức logic chịu trách nhiệm cho mỗi kết nối ở trên:

* **Protocol interpreter (PI)**: Là thành phần quản lý kênh điều khiển, phát và nhận lệnh và trả lời.
* **Data transfer process (DTP)**: Chịu trách nhiệm gửi và nhận dữ liệu giữa client và server.

### *1.3. Chức năng từng phần trong mô hình FTP*

***Phía Server***

* **Server Protocol Interpreter (Server-PI)**: Chịu trách nhiệm quản lí Control Connection trên Server. Nó lắng nghe yêu cầu kết nối hướng từ User trên cổng 21. Khi kết nối được thiết lập, nó nhận lệnh từ User-PI, gửi phản hồi và quản lí tiến trình truyền dữ liệu trên Server.
* **Server Data Transfer Process (Server-DTP)**: chịu trách nhiệm nhận và gửi file từ User-DTP. Server-DTP vừa làm nhiệm vụ thiết lập Data Connection và lắng nghe Data Connection của User thông qua cổng 20. Nó tương tác với Server File System trên hệ thống cục bộ để đọc và chép file.

***Phía Client***

* **User Interface**: Đây là chương trình được chạy trên máy tính, nó cung cấp giao diện xử lí cho người dùng, chỉ có trên phía Client. Nó cho phép người dùng sử dụng những lệnh đơn giản để điều khiển các session FTP, từ đó có thể theo dõi được các thông tin và kết quả xảy ra trong quá trình.
* **User Protocol Interpreter (User-PI)**: Chịu trách nhiệm quản lí Control Connection phía Client. Nó khởi tạo phiên kết nối FTP bằng việc gửi Request tới Server-PI. Sau khi kết nối được thiết lập, nó xử lí các lệnh nhận được trên User Interface, gửi chúng tới Server-PI rồi đợi nhận Response trở lại. Nó cũng quản lí các tiến trình trên Client.
* **User Data Transfer Process (User-DTP)**: Có nhiệm vụ gửi hoặc nhận dữ liệu từ Server-DTP. User-DTP có thể thiết lập hoặc lắng nghe DataConnection từ Server thông qua cổng 20. Nó tương tác với Client File System trên Client để lưu trữ file.

## *2. Nguyên lý hoạt động của FTP*

- Cần có 2 kết nối TCP trong phiên làm việc của FTP: ***TCP Data connection*** trên cổng 20, ***TCP Control connection*** trên cổng 21.

* *Control connection*: luôn được mở ở mọi thời điểm khi dữ liệu hoặc lệnh được gửi.
* *Data connection*: chỉ được mở khi có trao đổi dữ liệu thực.

**- Trình tự chung của FTP hoạt động như sau:**

(1) FTP Client mở Control connection đến FTP server (trên port 21) và chỉ định 1 cổng trên Client để Server gửi lại phản hồi. Đường kết nối này dùng để truyền lệnh và không phải là dữ liệu. Control connection sẽ mở trong suốt thời gian của phiên làm việc (telnet giữa 2 hệ thống)

(2) Client chuyển tiếp thông tin như username, password tới Server để thực hiện xác thực (authentication). Server sẽ trả lời bằng mã chấp nhận hay từ chối của các request.

(3) Client gửi thêm các lệnh với tên tệp, kiểu dữ liệu, … để vận chuyển, thêm luồng dữ liệu (tức là chuyển tập tin từ máy khách đến máy chủ hoặc ngược lại). Server sẽ phản hồi với mã (reply code) chấp nhận hoặc từ chối.

(4) Khi dữ liệu đã sẵn sàng, 2 bên sẽ mở kết nối TCP trên cổng 20.

(5) Dữ liệu có thể được vận chuyển giữa Client và Server trên cổng 20. Dữ liệu vận chuyển được mã hóa theo 1 số định dạng bao gồm NVT-ASCII hoặc nhị phân(binary)

(6) Khi quá trình vận chuyển dữ liệu được hoàn thành, phiên làm việc của FTP Server sẽ đóng lại Data Connection trên cổng 20. Nhưng vẫn giữ Control Connection trên công 21.

(7) Control connection có thể được sử dụng để thiết lập truyền dữ liệu khác hoặc đóng liên kết.

## *3. Một số lệnh command sử dụng trên FTP*

Bảng 1: Một số lệnh command trên FTP

|  |  |  |
| --- | --- | --- |
| **Lệnh Command** | **Đối số (Argument)** | **Mô tả (Description)** |
| USER | username | Username |
| PASS | password | Password |
| ACCT | account info | User account |
| CWD | pathname | Thay đổi thư mục làm việc |
| CDUP | none | Thay đổi thư mục cha |
| SMNT | pathname | Kết cấu |
| REIN | none | Dừng và khởi động lại |
| QUIT | none | Đăng xuất khỏi FTP |
| RETR | pathname | Lấy tập tin từ máy chủ |
| STOR | pathname | Lưu trữ dữ liệu trên máy chủ |
| RNFR | pathname | Đổi tên từ … |
| RNTO | pathname | Đổi tên thành … |
| DELE | pathname | Xóa file |
| RMD | pathname | Xóa thư mục |
| MKD | pathname | Tạo thư mục |
| LIST | pathname | Liệt kê tệp tin hoặc văn bản |
| STAT | pathname | Status |
| HELP | subject | Hiện màn hình trợ giúp |
| PORT | host-port | Chỉ định cổng vận chuyển (không mặc định) |
| TYPE | type code | Kiểu vận chuyển (ASCII, image,…) |
| MODE | mode code | Chế độ truyền (stream, block,…) |

## *4. FTP reply*

- Mỗi lần User-PI gửi lệnh đến Server-PI qua Control connection, server sẽ gửi lại phản hồi dưới dạng các code. Code reply nhằm các mục đích sau:

* Xác nhận máy chủ đã nhận được lệnh.
* Cho biết lệnh từ phía người dùng có được chấp nhận hay không, nếu xảy ra lỗi thì đó là lỗi gì.
* Cho biết nhiều thông tin khác nhau cho người dùng về phiên, ví dụ như là: tình trạng truyền file, …

- Cấu trúc của FTP reply code: Xyz.

- Ý nghĩa của X trong FTP reply code:

Bảng 2: Ý nghĩa của tham số X trong FTP reply code

|  |  |
| --- | --- |
| **Reply code Format** | **Mô tả** |
| 1yz | Đã khởi tạo hành động. Chờ 1 reply trước khi gửi 1 lệnh khác |
| 2yz | Hành động hoàn thành. Có thể gửi lệnh mới |
| 3yz | Lệnh được chấp nhận. Nhưng bị giữ do thiếu thông tin |
| 4yz | Lệnh không được chấp nhận hoặc không hoàn thành. Tình trạng lỗi tồn tại tạm thời. Lệnh có thể được ban hanh lại |
| 5yz | Lệnh không được chấp nhận hoặc đã hoàn thành. Không ban hành lại lệnh, ban hành lại lệnh sẽ dẫn đến cùng một lỗi |

- Tham số y cung cấp thêm thông tin như bảng dưới. z cũng cung cấp thêm thông tin nhưng ý nghĩa chính xác có thể khác nhau giữa các cài đặt.

Bảng 3: Ý nghĩa của tham số y trong reply code

|  |  |
| --- | --- |
| **Reply code Format** | **Mô tả** |
| X0z | Lỗi cú pháp hoặc lệnh bất hợp pháp |
| X1z | Trả lời Request thông tin |
| X2z | Trả lời đề cập đến Connection management |
| X3z | Trả lời lệnh xác thực |
| X4z | Trả lời trạng thái máy chủ |

## *5. Phương thức tạo kết nối và truyền dữ liệu trong FTP*

### *5.1. Phương thức tạo kết nối dữ liệu*

**Normal (Active) Data Connections**:

* Phương thức đầu tiên được gọi là tạo kết nối dữ liệu bình thường (vì đây là phương pháp mặc định) hay còn gọi là kết nối kênh dữ liệu ở dạng chủ động.
* Phía Server-DTP tạo kênh dữ liệu bằng cách mở một cổng kết nối tới User-DTP
* Server sử dụng cổng đặc biệt được dành riêng cho kết nối dữ liệu là cổng số 20.

**Passive Data Connections**:

* Phương thức tạo kết nối bị động.
* Server sẽ chấp nhận 1 yêu cầu kết nối dữ liệu được khởi tạo từ Client.
* Server trả lời lại phía client với địa chỉ IP cũng như địa chỉ cổng mà nó sẽ sử dụng. Sau đó phía Server-DTP lắng nghe trên cổng này một kết nối TCP đến từ User-DTP.



Hình 5. Minh họa phương thức tạo kết nối của FTP

### *5.2. Phương thức truyền dữ liệu*

Để có thể truyền dữ liệu trong FTP server, dữ liệu đó cần được thiết lập xong giữa Server-FTP với User-FTP. Từ đó, các tập dữ liệu sẽ được truyền trực tiếp từ phía client tới phía Server, hoặc ngược lại tùy theo nhu cầu và mong muốn của bạn.

Do thông tin điều khiển được gửi đi trên kênh điều khiển, nên toàn bộ kênh dữ liệu có thể được sử dụng để truyền dữ liệu.

Có ba phương thức truyền dữ liệu:

* **Block mode:**  Là phương thức truyền dữ liệu mang tính quy chuẩn hơn. Với phương thức này, các dữ liệu sẽ gửi đi được chia thành nhiều khối nhỏ và được gộp vào thành các FTP Blocks. Trong đó, mỗi Block sẽ có một trường header 3 byte báo hiệu độ dài và cùng với thông tin về tập tin được gửi đi.
* **Stream mode:** Là phương thức truyền tập tin không có cấu trúc dạng header, dữ liệu được truyền đi dưới dạng các byte không cấu trúc liên tiếp. Dựa vào tính tin cậy trong việc truyền dữ liệu và thông qua kết nối TCP tới phía nhận nên chỉ ngắt kết nối là dữ liệu cũng kết thúc.
* **Compressed mode:**Là phương thức truyền dữ liệu kỹ thuật nén dữ liệu khá đơn giản run-length encoding. Các đoạn dữ liệu bị lặp sẽ được phát hiện và loại bỏ để giảm chiều dài của toàn bộ thông điệp.

## 6. Dữ liệu trong FTP

### *6.1. FTP Data Types*

- Có 4 kiểu dữ liệu khác nhau được quy định trong chuẩn của FTP:

* **ASCII**: File văn bản ASCII
* **EBCDIC**: tương tự ASCII, nhưng sử dụng kiểu kí tự EBCDIC do IBM đặt.
* **Image**: Các tập tin không có cấu trúc nội bộ chính thức.
* **Local**: Kiểu dữ liệu này được sử dụng để xử lí các tập tin có thể lưu trữ dữ liệu trong byte logic. Cách xác định loại này cùng với cách dữ liệu có cấu trúc cho phép dữ liệu được lưu trữ trên hệ thống đích một cách phù hợp với đại diện local của nó.

- Trong thực tế, hai loại kiểu dữ liệu thường xuyên nhất được sử dụng là *ASCII* và *Image*.

+ Kiểu ASCII được sử dụng cho các tập tin văn bản và cho phép chúng được di chuyển giữa các hệ thống với dòng kết thúc mã chuyển đổi tự động.

+ Loại Image được sử dụng cho các tập tin nhị phân, chẳng hạn như đồ họa hình ảnh, tập tin ZIP và các dữ liệu khác.

### *6.2. FTP Data Structures*

- Ta có thể xác định cấu trúc tệp tin theo 3 cách:

* **File Structure**: Tệp là 1 luồng byte liền kề không có cấu trúc bên trong. Đây là cách mặc định và được sử dụng cho hầu hết các loại tệp.
* **Record Structure**: Tệp bao gồm một tập hợp các bản ghi, mỗi bản ghi được phân định bằng đánh dấu end-of-record. Cấu trúc bản ghi có thể sử dụng cho các tệp văn bản ASCII, nhưng chúng thường được gửi với cấu trúc tệp thông thường sử dụng kiểu dữ liệu ASCII.
* **Page Structure**: Tệp chứa 1 trang dữ liệu được lập chỉ mục đặc biệt. Cấu trúc này không được sử dụng phổ biến. Nó được tạo ra cho 1 máy tính cổ xưa được sử dụng trong ARPAnet đời đầu.

## *7. Mã hóa kết nối FTP với SSL/TLS*

- Hạn chế lớn nhất của FTP là vấn đề bảo mật. Tên người dùng, mật khẩu và tệp đều được gửi bằng văn bản thuần túy, do đó tin tặc có thể dễ dàng truy cập thông tin của bạn.

- Chính vì vậy, để tăng cường bảo mặt cho các kết nối FTP, ta mã hóa kết nối FTP với SSL/TLS.

Trong đó:

+ **SSL (*Secure Sockets Layer*) /TLS (*Transport Layer Security*)** là kỹ thuật mã hóa truyền tin trên internet. Sử dụng SSL/TLS, bằng việc mã hóa data truyền tin giữa máy tính và server thì có thể phòng tránh bên thứ ba nghe trộm hoặc giả mạo data.

+ *Cơ chế kỹ thuật của SSL/TLS:*

Diagram, text

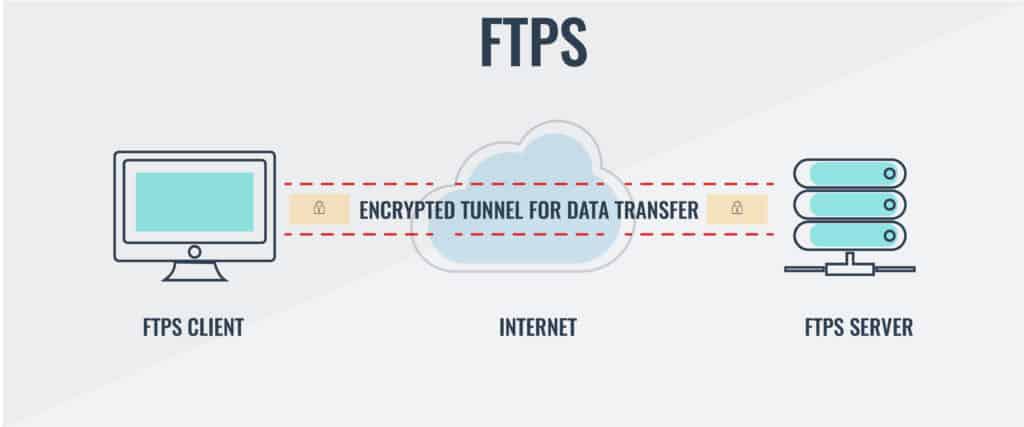
Description automatically generated

Hình 6. Cơ chế mã hóa của SSL/TLS

Chúng ta chú ý đến phần kiểm chứng certificate. Chứng chỉ không được các tổ chức đáng tin cậy chứng nhận thì không thể xác minh bằng root certificate. Nhiều người sử dụng Internet khi truy cập vào trang web với một trình duyệt cơ bản thì có hiển thị một cảnh báo rằng nó không thể được xác thực, nên rất khó cho người dùng có thể hiển thị màn hình kế tiếp. Do đó, phải sử dụng SSL server certificate được xác thực bởi một bên thứ ba đáng tin cậy.

- Khi đó thì FTP sẽ trở thành **FTPS (File Transfer Protocol Secure)**.

+ FTPS cho phép mã hóa cả hai kênh điều khiển và dữ liệu, sau đó xác thực kết nối thông qua cả bộ thông tin gồm ID người dùng và mật khẩu, certificate hoặc kết hợp cả hai.



Hình 7. Minh họa FTPS

# III. Cài đặt hệ thống FTP server

## *1. Cài đặt và cấu hình vsftpd*

* **Bước 1**: Cài đặt vsftpd, sử dụng hai câu lệnh:
* *Sudo apt update*
* *Sudo apt install vsftpd*

*Text

Description automatically generated*

Hình 8. Kiểm tra phiên bản của vsftpd

Có thể sao lưu bản bản config cũ nếu ghi đè config mới lên config cũ:

*Sudo cp /etc/vsftpd.conf /etc/vsftpd.conf.orig*

* **Bước 2**: Cấu hình UFW để mở cổng cho FTP

Mở các cổng 20(cho FTP command), cổng 21(FTP data port), 990(TLS FPT data port) và dải port 35000-40000

* *Sudo ufw allow 20:21/tcp*
* *Sudo ufw allow 990/tcp*
* *Sudo ufw allow 35000:40000/tcp*
* *Sudo ufw status*

Text

Description automatically generated

Hình 9. Kết quả sau khi cấu hình tường lửa

* **Bước 3:** Cấu hình vsftpd:

- Chỉnh sửa file cấu hình: *sudo nano /etc/vsftpd.conf*

- Để giới hạn người dung truy cập vào vsftpd, thêm dòng:

* *Anonymous\_enable = NO*
* *Local\_enable = YES*

- Cấu hình quyền ghi để cho phép upload file lên Server

* *Write\_enable = YES*

- Để giới hạn người dung chỉ có thể thao tác trên thư mục cụ thể thì thêm:

* *Chroot\_local\_user = YES*
* *Allow\_writeable\_chroot = YES*

- Cấu hình minimum port và maximum port bằng cách thêm:

* *Userlist\_enable = YES*
* *Userlist\_file = /etc/vsftpd.userlist*
* *Userlist\_deny = NO*

- Người dùng có thể truy cập các username được lưu tại /etc/vsftpd.userlist

* **Bước 4:** Cấu hình thư mục người dùng

- Để thêm người dùng vào FTP server, đầu tiên cần tạo người dùng mới:

* *Sudo adduser huytuan*

Text

Description automatically generated

Hình 10. Tạo người dùng mới

- Thêm người dùng mới tạo vào danh sách người dùng của FTP server:

* *Echo “huytuan” | sudo tee -a /etc/vsftpd.userlist*

*-* Sau khi thêm người dùng vào danh sách, tạo thư mục và cấp quyền sở hữu cho người dùng:

* *Sudo mkdir /home/huytuan/ftp/upload* (tạo thư mục theo tên người dùng)
* *Sudo chown huytuan:huytuan /home/huytuan/ftp/upload* (cấp quyền sở hữu cho người dùng huytuan và nhóm người dùng huytuan)
* *Sudo chmod 755 /home/huytuan/ftp/upload* (Cấp quyền hạn cho người dùng)

- Kiểm tra lại quyền thư mục:

* *Sudo ls -al /home/huytuan/ftp*

Text

Description automatically generated

Hình 11. Kiểm tra thư mục vừa tạo

- Tạo một file và thêm nội dung trong thư mục upload:

* *Echo “Nguyễn Huy Tuân” | sudo tee /home/huytuan/ftp/upload/test.txt*

## *2. Demo kết nối máy chủ FTP server bằng Windown client*

- Tải phần mềm FileZilla Client

Graphical user interface, text

Description automatically generated

Hình 12. Giao diện của FileZilla

- Thêm tên miền và IP của server vào file host trong đường dẫn **C:\Windows\System32\Drivers\etc\hosts**

Graphical user interface, text

Description automatically generated

Hình 13. Thêm tên miền

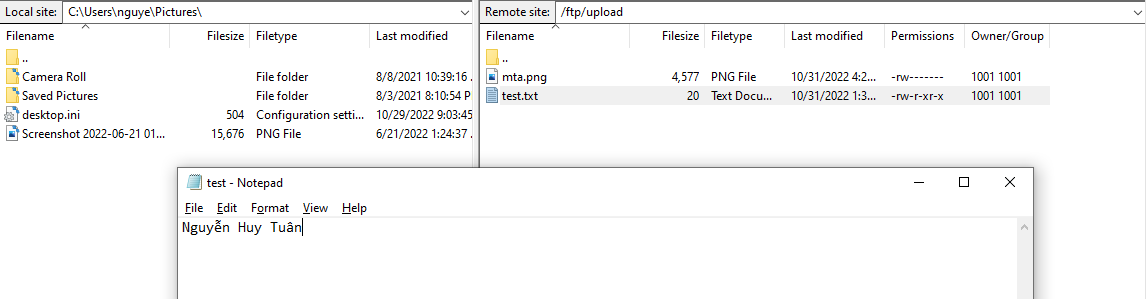
- Nhập tên miền, username, password vào phần mềm filezilla và nhấn vào connect:

Graphical user interface, text

Description automatically generated

Hình 14. Tạo kết nối tới Server

- Kết nối đến máy chủ thành công, ta tiến hành xem các file đã có trong thư mục người dùng sở hữu:



Hình 15. Kết quả khi truy cập thành công vào Server

- Ta thấy được nội dung file, ta có thể tiến hành sửa thành “**Nguyễn Huy Tuân đã sửa**”:

Graphical user interface, application, Word

Description automatically generated

Hình 16. Kết quả khi thực hiện sửa tập tin

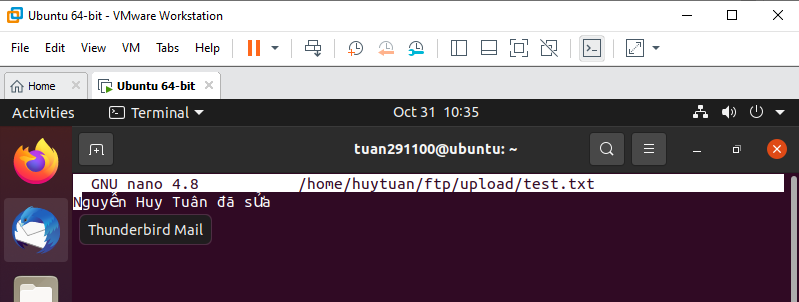
- Nhấn Yes để tiến hành gửi lại file về server:

Text

Description automatically generated

Hình 17. Gửi tập tin đã sửa về Server

- Ta thấy gửi lại file thành công, ta có thể kiểm tra lại ở bên server:

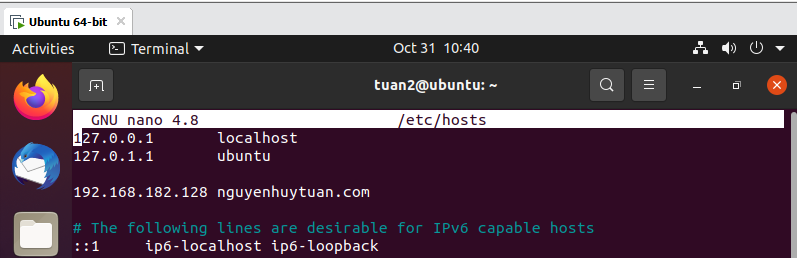


Hình 18. Kiểm tra tập tin tại Server

- Bên cạnh đó với quyền mà người dùng đã được cấp ở bên máy chủ, người dùng cũng có thể thêm và xóa file qua phần mềm FileZilla client.

## *3. Demo kết nối máy chủ FTP server bằng Ubuntu client*

- Thêm tên miền và địa chỉ IP của server vào file hosts ở bên máy khách



Hình 19. Thêm tên miền vào file hosts

- Kết nối tới máy chủ thông qua tên miền:

Text

Description automatically generated

Hình 20. Kết nối với Server bằng tên miền

- Ta sử dụng các câu lệnh của FTP để thao tác trong thư mục.

- Xem đường dẫn hiện tại trên máy chủ đang truy cập:

Text

Description automatically generated

Hình 21. Kết quả kiểm tra đường dẫn hiện đang truy cập

- Xem tên và các tệp trên máy chủ đang truy cập:

Text

Description automatically generated

Hình 22. Kết quả hiển thị danh sách các tệp

- Tải file về máy:

Text

Description automatically generated

Hình 23. Kết quả tải về tập tin

- Tải file lên máy chủ:

Text

Description automatically generated

Hình 24. Kết quả upload tệp lên Server

- Bên máy chủ ta có thể thay đổi lại quyền để hạn chế khả năng của người dùng, ta tiến hành bỏ quyền sửa file của người dùng:

Graphical user interface, text

Description automatically generated

Hình 25. Thay đổi quyền người dùng

- Lúc ngày người dùng chỉ còn quyền đọc, ta thử lại bên client:

Text

Description automatically generated

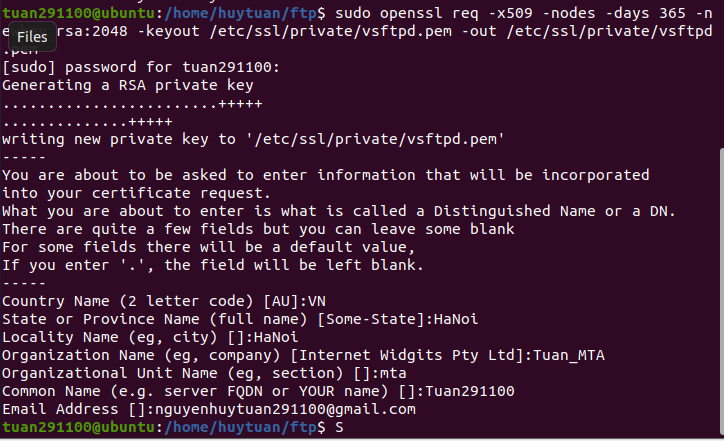
Hình 26. Kiểm tra sự thay đổi về quyền

- Lúc này người dùng đã không upload được file lên server

## *4. Mã hóa kết nối FTP với SSL/TLS*

- Để mã hóa kết nối FTP, ta cần một chứng chỉ SSL, và cấu hình vsftpd sử dụng nó, sử dụng openSSL để tạo chứng chỉ:

* *Sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/vsftpd.pem -out /etc/ssl/private/vsftpd.pem*



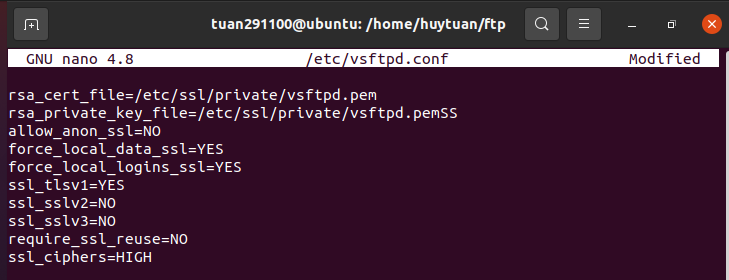
Hình 27. Tạo chứng chỉ SSL

- Sau đó cấu hình cho vsftpd:

* *Sudo nano /etc/vsftpd.conf*

- Thêm vào file config

* *rsa\_cert\_file=/etc/ssl/private/vsftpd.pem*
* *rsa\_private\_key\_file=/etc/ssl/private/vsftpd.pem*
* *ssl\_enable=YES*
* *allow\_anon\_ssl=NO*
* *force\_local\_data\_ssl=YES*
* *force\_local\_logins\_ssl=YES*
* *ssl\_tlsv1=YES*
* *ssl\_sslv2=NO*
* *ssl\_sslv3=NO*
* *require\_ssl\_reuse=NO*
* *ssl\_ciphers=HIGH*



Hình 28. Cấu hình file config

- Lưu các cấu hình và khởi động lại dịch vụ:

* *Sudo systemctl restart vsftpd*

- Kiểm tra cấu hình mã hóa FTP bằng phần mềm FileZilla Client:

Graphical user interface, text, application

Description automatically generated

Hình 29. Kết quả sau khi mã hóa kết nối

- Ta thấy khi kết nối tới FTP server thì hiện lên cảnh báo Unknow cetification ()

# TÀI LIỆU THAM KHẢO

1. Đặng Đỗ Hải*. [FTP] [Phần 1] Tìm hiểu về giao thức FTP (File Transfer Protocol)*. Đăng tải ngày 03/01/2020 tại:

<https://news.cloud365.vn/ftp-tim-hieu-ve-giao-thuc-ftp/>

1. ExaVault. *How Does an FTP Server Work?* Published on 16 July 2020 from:

<https://www.exavault.com/blog/how-does-an-ftp-server-work>

1. Tmarketing. *FTP là gì? Tổng quát về FTP từ A đến Z Chi Tiết Nhất*.

<https://tmarketing.vn/ftp-la-gi-tong-quat-ve-ftp-tu-a-den-z/>

1. PAVIETNAM. *FTP là gì? Cách sử dụng, ưu điểm và nhược điểm của FTP*. Đăng tải ngày 24/08/2021 tại:

<https://kb.pavietnam.vn/ftp-la-gi-cach-su-dung-uu-diem-va-nhuoc-diem-cua-ftp.html>

1. BizflyCLOUD. *So sánh FTP, FTPS và SFTP, ưu và nhược điểm của từng giao thức và khi nào bạn nên sử dụng cái nào?* Đăng tải ngày 22/07/2019 tại:

<https://bizflycloud.vn/tin-tuc/so-sanh-ftp-ftps-va-sftp-uu-va-nhuoc-diem-cua-tung-giao-thuc-va-khi-nao-ban-nen-su-dung-20190722163805324.htm#:~:text=%C6%AFu%20%C4%91i%E1%BB%83m%20c%E1%BB%A7a%20FTP&text=FTP%20gi%C3%BAp%20cho%20b%E1%BA%A1n%20c%C3%B3,t%E1%BB%B1%20%C4%91%E1%BB%99ng%20chuy%E1%BB%83n%20t%E1%BA%ADp%20tin>

1. TEL4VN. *Cài đặt và cấu hình vsftpd làm FTP Server trên Ubuntu 20.04*. Đăng tải ngày 18/12/2020 tại:

<https://tel4vn.edu.vn/blog/how-to-install-ftp-server-use-vsftpd-with-ssl-tls/>

1. Nguyễn Ngọc Đang (123HOST). *Hướng dẫn cài đặt máy chủ FTP với VSFTPD trên Ubuntu 20.04*. Đăng tải ngày 02/12/2021 tại:

<https://123host.vn/community/tutorial/huong-dan-cai-dat-may-chu-ftp-voi-vsftpd-tren-ubuntu-20-04.html?fbclid=IwAR3WkV3rjUzOM3lfL3r5E6jIMj6ThYpU5XsNhs95kmPI6Mu_-4zg7xGWg9s>

1. WP basics. *How to Use FileZilla (FTP Tutorial).* Đăng tải ngày 2/2/2017 tại:

<https://www.youtube.com/watch?v=adxmlHDim6c>

1. Tran Thi Tinh, VIBLO. *SSL/TLS là gì?* Đăng tải ngày 5/6/2018 tại:

<https://viblo.asia/p/ssltls-la-gi-Do754wnBlM6>