

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**  
**KHOA AN TOÀN THÔNG TIN**



**Kỹ thuật giấu tin**

**BÀI BÁO BÀI TẬP LỚN**

Đề tài: Giấu tin trong tiêu đề gói tin qua mô hình mạng WAN

Giảng viên: Đỗ Xuân Chợ

Lớp: 03

Nhóm: 07

Thành viên:

Nguyễn Quốc Khánh	B20DCAT103
-------------------	------------

Nguyễn Quý Dũng	B20DCAT031
-----------------	------------

Chu Quang Long	B20DCAT111
----------------	------------

Phạm Thanh Tùng	B20DCAT171
-----------------	------------

*Hà Nội, tháng 5 năm 2024*

## Mục Lục

Danh Mục Hình Ảnh .....	3
Lời nói đầu.....	4
I. Giới thiệu.....	5
II. Tổng quan.....	5
2.1. Giấu tin mạng.....	5
2.2. Mạng diện rộng (WAN).....	6
2.3. Transmission Control Protocol (TCP).....	8
2.4. Kiểm trúc của TCP MSS options .....	10
III. Cấu hình mô hình WAN .....	11
IV. Công cụ và công nghệ sử dụng.....	15
4.1. OpenVPN.....	15
4.2. Scapy .....	15
4.3. Wireshark .....	16
4.4. Ngôn ngữ Python .....	16
V. Nghiên cứu thực nghiệm .....	17
5.1. Máy gửi .....	17
5.1.1. Chuẩn bị dữ liệu bí mật: .....	17
5.1.2. Tạo gói tin:.....	17
5.1.3. Gửi gói tin:.....	17
5.2. Máy nhận .....	17
5.2.1. Đọc gói tin.....	18
5.2.2. Đọc trường options .....	18
5.2.3. Hiển thị thông điệp .....	18
VI. Kết quả thực nghiệm.....	19
VII. Kết luận.....	20
7.1. Ưu điểm: .....	20
7.2. Nhược điểm: .....	20
VIII. Tài liệu tham khảo.....	21

## **Danh Mục Hình Ảnh**

Hình 1. Sơ đồ mô hình WAN. ....	8
Hình 2. Kiến trúc tiêu đề gói tin IPv4.....	8
Hình 3. Kiến trúc của trường options. ....	10
Hình 4. Mô hình mạng ảo WAN. ....	11
Hình 5: Tạo máy Server trên AWS.....	12
Hình 6: Cấu hình Routing cho máy chủ. ....	12
Hình 7: Cấu hình VPN Gateway cho user. ....	12
Hình 8: User tải file cấu hình về từ giao diện người dung. ....	13
Hình 9: Cấu hình file cài đặt trên máy client.....	13
Hình 10: Cấu hình ip_forward trên máy client.....	14
Hình 11: Admin nhận diện được người dùng truy cập.....	14
Hình 12. Giao diện của wireshark. ....	16
Hình 13. Giao diện gửi gói tin. ....	17
Hình 14. Giao diện wireshark bắt gói tin.....	18
Hình 15. Thông điệp được trích ra.....	19

## **Lời nói đầu**

Trong lĩnh vực an ninh mạng, Steganography - nghệ thuật giấu tin - đóng một vai trò quan trọng trong việc bảo vệ dữ liệu và truyền tải thông tin một cách an toàn. Một trong những lĩnh vực mới nổi trong Steganography là Network Steganography, nơi mà thông tin được giấu trong gói tin mạng mà không gây nghi ngờ.

Đề tài này tập trung vào việc áp dụng kỹ thuật Steganography vào môi trường mạng WAN (Wide Area Network) sử dụng các công cụ và kỹ thuật hiện đại. Tìm hiểu cách sử dụng các tính năng và tùy chọn của gói tin mạng để giấu thông tin và truyền tải nó một cách an toàn qua mạng.

Thông qua việc nghiên cứu và thực nghiệm, khám phá cách thức giấu tin trong các gói tin mạng TCP/IP, cũng như phân tích và giải mã thông tin được giấu từ các gói tin đã nhận. Giúp hiểu rõ hơn về cách hoạt động của Steganography trong môi trường mạng WAN và áp dụng nó vào thực tiễn để bảo vệ thông tin một cách hiệu quả.

## **I. Giới thiệu**

Trong thời đại mạng liên kết ngày nay, bảo mật thông tin đóng vai trò quan trọng và cần thiết. Steganography là một kỹ thuật giấu dữ liệu bí mật bên trong một tấm bìa. Các phương tiện vật chứa phổ biến bao gồm hình ảnh, video, âm thanh, tài liệu và giao thức mạng. Steganography mạng là một phương pháp sử dụng các giao thức mạng thông dụng (bao gồm cả trường tiêu đề và trường tải trọng) để ẩn đi một tin nhắn bí mật.

Bộ giao thức TCP/IP luôn là mục tiêu tiềm năng cho kỹ thuật giấu tin mạng từ khi ra đời. Nó cung cấp nhiều khả năng tạo ra các kênh ẩn dùng để truyền thông một cách bí mật. Trong đề tài này, khám phá cách giấu tin bằng cách sử dụng trường MSS (Maximum Segment Size) trong tùy chọn của gói tin và truyền chúng qua hệ thống Wide Area Network (WAN).

Kỹ thuật này triển khai việc ẩn thông điệp dựa trên việc sử dụng tùy chọn Maximum Segment Size, một trường thường được sử dụng để xác định lượng dữ liệu lớn nhất trong tiêu đề TCP chỉ định, điều này làm cho việc phát hiện khả năng liên lạc bí mật trở nên khó khăn hơn.

## **II. Tổng quan**

### **2.1. Giấu tin mạng**

Giấu tin mạng là một lĩnh vực quan trọng trong bảo mật mạng, nơi mà các phương pháp giấu tin và ẩn dữ liệu được áp dụng để bảo vệ thông tin truyền qua mạng một cách an toàn. Kỹ thuật giấu tin trong mạng có mục tiêu là ẩn dữ liệu trong các giao thức mạng, bao gồm cả trường tiêu đề và tải trọng của gói tin mạng.

Kỹ thuật giấu tin mạng có thể triển khai thông qua việc tạo ra các kênh bí mật để liên lạc giữa người gửi và người nhận thông tin bí mật. Các kênh bí mật này có thể được phân loại thành các loại sau:

- Kênh ẩn dữ liệu dựa trên lưu trữ: Dữ liệu bí mật được ẩn trong phần lưu trữ của các đơn vị dữ liệu giao thức (Field Data Unit - PDU). Điều này có thể thực hiện thông qua việc sử dụng các trường dự phòng trong tiêu đề hoặc một phần nhỏ của tải trọng của PDU.
- Kênh bí mật dựa trên thời gian: Các kênh bí mật này được tạo ra dựa trên số thứ tự, thời gian hoặc độ trễ trong PDU.
- Kênh bí mật kết hợp: Sự kết hợp giữa các kênh lưu trữ và thời gian được sử dụng để tạo ra các kênh bí mật, hỗ trợ việc truyền thông bí mật một cách hiệu quả.

Hiệu quả của kỹ thuật giấu tin mạng có thể được đánh giá thông qua các đặc điểm sau:

- Dung Lượng: Đây là lượng thông tin bí mật mà PDU có thể chứa.
- Tính Mạnh Mẽ: Đánh giá sự phù hợp của kỹ thuật với các điều kiện không có lỗi, trong đó thông tin bí mật phải có khả năng chống lại sự thay đổi hoặc lỗi.
- Không Thể Nhận Thấy: Đánh dấu tính không thể phát hiện của một tin nhắn bí mật.

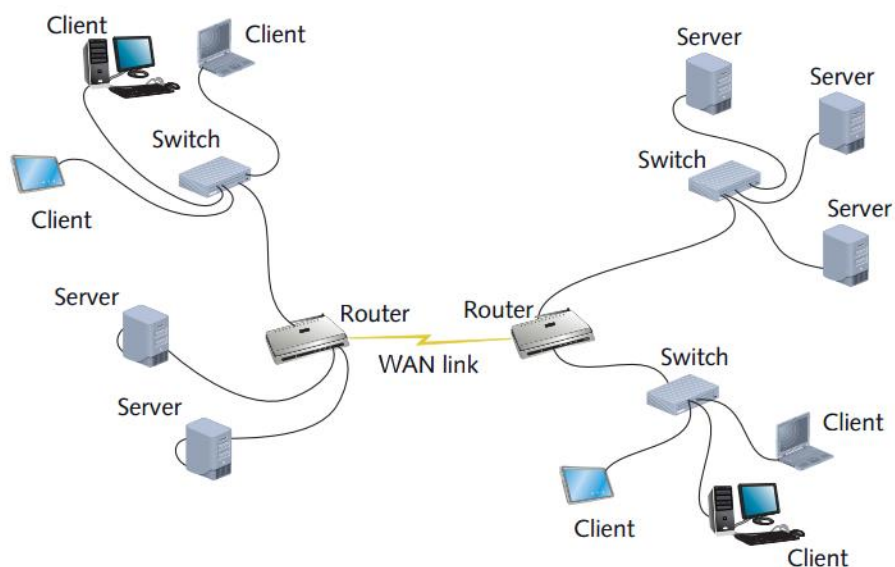
## **2.2. Mạng diện rộng (WAN)**

Mạng diện rộng (WAN) là một hệ thống mạng kết nối các mạng cục bộ (LAN) và các thiết bị mạng khác nhau trên một khu vực lớn, thậm chí trên các khu vực địa lý khác nhau. Các mạng WAN thường được sử dụng để kết nối các vị trí địa lý xa nhau, như các văn phòng chi nhánh của một công ty hoặc các tổ chức trên toàn thế giới.

Mô hình WAN là một hệ thống phức tạp và đa dạng, bao gồm nhiều thành phần khác nhau được tích hợp để tạo ra một mạng mạnh mẽ và linh hoạt. Sự kết hợp của các thành phần này cùng nhau tạo ra một hạ tầng mạng toàn diện, giúp cho việc truyền tải thông tin một cách hiệu quả và bảo mật trên các khu vực địa lý khác nhau trên thế giới.

Một mô hình WAN bao gồm các thành phần sau:

- **Nút Kết Nối (Router):** Là các thiết bị mạng chịu trách nhiệm định tuyến và chuyển tiếp dữ liệu giữa các mạng LAN và giữa các mạng WAN.
- **Trung Tâm Dữ Liệu (Data Center):** Đây là các trung tâm dữ liệu hoặc trung tâm máy chủ lớn được sử dụng để lưu trữ và quản lý dữ liệu của các tổ chức.
- **Liên Kết Truyền Thông:** Các kết nối truyền thông được sử dụng để kết nối các vị trí khác nhau trên mạng WAN. Các loại kết nối có thể bao gồm cáp quang, cáp đồng, mạng di động, và kết nối vệ tinh.
- **Bộ Điều Khiển Truy Cập (Access Control Devices):** Là các thiết bị như bộ định tuyến, bộ chuyển mạch, hoặc bộ định tuyến tự động được sử dụng để quản lý và kiểm soát việc truy cập vào mạng WAN.
- **Bộ Trung Chuyển (Switches):** Được sử dụng để kết nối các thiết bị mạng trong cùng một mạng LAN và điều khiển việc chuyển tiếp dữ liệu giữa chúng.
- **Dịch Vụ Mạng (Network Services):** Là các dịch vụ như mạng riêng ảo (VPN), bảo mật mạng, quản lý mạng và các dịch vụ khác được cung cấp trên mạng WAN để đảm bảo tính bảo mật và hiệu suất của mạng.



Hình 1. Sơ đồ mô hình WAN.

### 2.3. Transmission Control Protocol (TCP)

Giao thức Kiểm soát Truyền tin (TCP) là một trong những giao thức quan trọng nhất trong lớp vận chuyển của mô hình OSI. Tiêu đề gói TCP bao gồm các trường sau:

+	Bít 0 - 3	4 - 9	10 - 15	16 - 31
0	Source Port			Destination Port
32	Sequence Number			
64	Acknowledgement Number			
96	Data Offset	Reserved	Flags	Window
128	Checksum			Urgent Pointer
160	Options (optional)			
160/192+	Data			

Hình 2. Kiến trúc tiêu đề gói tin IPv4.



**Cổng nguồn (Source Port):** Xác định cổng nguồn của gói tin, nơi mà dịch vụ gửi gói tin được mở trên máy gửi.

**Cổng đích (Destination Port):** Xác định cổng đích của gói tin, nơi mà dịch vụ nhận gói tin được mở trên máy nhận.

**Số thứ tự (Sequence Number):** Xác định số thứ tự của dữ liệu trong gói tin, giúp quản lý thứ tự và phục hồi gói tin nếu cần thiết.

**Số xác nhận (Acknowledgment Number):** Được sử dụng trong quá trình xác nhận gói tin, xác định số lượng byte dữ liệu đã nhận được một cách chính xác.

**Độ dài Tiêu đề (Header Length):** Trường này xác định độ dài của tiêu đề TCP, được biểu diễn bằng số từ 32-bit. Giá trị tối đa của trường này là 15, do kích thước của trường độ dài tiêu đề là 4-bit.

**Cờ (Flags):** Bao gồm các cờ như SYN, ACK, RST, và FIN để xác định trạng thái và mục đích của gói tin trong quá trình thiết lập và đóng kết nối.

**Cửa sổ (Window):** Xác định kích thước của cửa sổ trượt, được sử dụng để kiểm soát lưu lượng dữ liệu trên đường truyền.

**Kiểm tra Tổng (Checksum):** Một giá trị dài 16 bit được sử dụng để kiểm tra tính toàn vẹn của tiêu đề và dữ liệu TCP.

**Điều tra Ưu tiên (Urgent Pointer):** Được sử dụng khi cần xử lý dữ liệu ưu tiên, xác định vị trí của dữ liệu cấp bách trong gói tin.

**Tùy chọn (Options):** Là trường tùy chọn và có thể chứa các tùy chọn như cửa sổ có thể mở rộng, dấu thời gian, và tùy chọn mở rộng TCP khác.

.

## 2.4. Kiến trúc của TCP MSS options

Kiến trúc của TCP MSS (Maximum Segment Size) options liên quan đến việc quản lý kích thước tối đa của một đoạn dữ liệu mà một giao thức vận chuyển có thể chấp nhận trong một gói tin TCP. Trường này thường được sử dụng trong các giao thức vận chuyển như TCP để xác định kích thước tối đa của các đoạn dữ liệu trong một phiên truyền dữ liệu.

Option Type (2 bytes)	Option Length (2 bytes)	Maximum Segment Size (variable)
--------------------------	----------------------------	------------------------------------

Hình 3. Kiến trúc của trường options.

Dưới đây là một mô tả về kiến trúc của TCP MSS options:

**MSS Value (Giá trị MSS):** Trường này chứa giá trị của kích thước tối đa của một đoạn dữ liệu mà một máy chủ có thể gửi. Giá trị này được trao đổi giữa các máy chủ trong quá trình thiết lập kết nối TCP, thông qua các tùy chọn TCP MSS trong gói tin SYN.

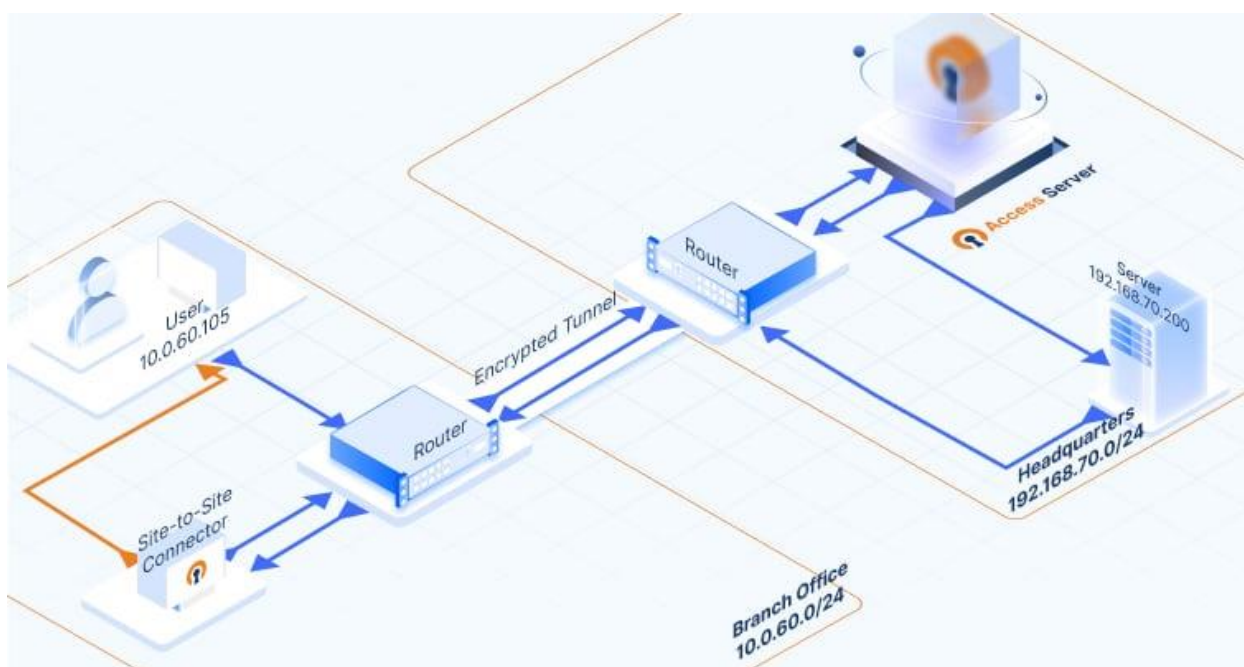
**Length (Độ dài):** Trường này xác định độ dài của tùy chọn MSS, thường là 4 byte.

**Kind (Loại):** Trường này xác định loại của tùy chọn, với giá trị thường là 2bytes, chỉ định tùy chọn MSS.

Tùy chọn MSS này giúp giảm nguy cơ phân mảnh dữ liệu trong các kết nối TCP bằng cách đảm bảo rằng kích thước của mỗi đoạn dữ liệu không vượt quá kích thước tối đa mà các thiết bị mạng có thể xử lý mà không cần phải phân mảnh gói tin. Điều này có thể cải thiện hiệu suất truyền dữ liệu và giảm độ trễ trong mạng.

### III. Cấu hình mô hình WAN

Trong quá trình thử nghiệm, việc tắt tường lửa đã cho phép kết nối thành công thông qua hai router khác nhau, và thông điệp đã được gửi và nhận một cách hiệu quả. Tuy nhiên, khi thực hiện thử nghiệm sử dụng hai mạng được phát từ hai thiết bị di động, việc truyền thông điệp không thành công. Do đó để có thể sử dụng bất kỳ kết nối cũng có thể gửi được thông điệp ta cần một mô hình client-server sites-to-sites VPN. Mỗi máy trong mô hình này sẽ đảm nhận một vai trò cụ thể, đòi hỏi một cấu hình chi tiết và chính xác để hỗ trợ quá trình truyền thông điệp một cách an toàn và bảo mật.

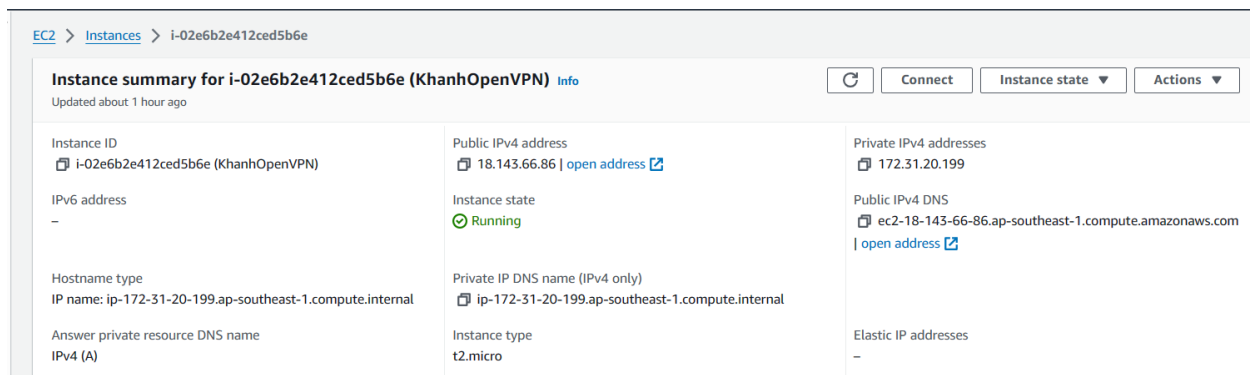


Hình 4. Mô hình mạng ảo WAN.

#### Máy chủ OpenVPN Access Server trên AWS:

Địa chỉ IP: 172.31.20.199

Máy chủ này là điểm truy cập chính cho các kết nối VPN. Sử dụng dịch vụ OpenVPN Access Server trên nền tảng AWS để cung cấp một môi trường an toàn và tin cậy cho người dùng kết nối từ xa.



Hình 5: Tạo máy Server trên AWS.

Trong giao diện admin của dịch vụ OpenVPN, cấu hình chế độ Routing trong VPN Settings để cho phép truy cập từ xa đến các dải mạng cụ thể. Dải mạng được chỉ định là 172.31.0.0/24.

Routing

Should VPN clients have access to private subnets (non-public networks on the server side)?

☐ No ☐ Yes, using NAT ☒ Yes, using Routing

Specify the private subnets to which all clients should be given access (one per line):

172.31.20.0/24

Allow access from these private subnets to all VPN client IP addresses and subnets

☒ Yes ☐ No

Should client Internet traffic be routed through the VPN?

☐ No ☒ Yes

Should clients be allowed to access network services on the VPN gateway IP address?

☐ No ☒ Yes

Hình 6: Cấu hình Routing cho máy chủ.

Tiến hành thêm người dùng trong User Management → User Permissions bật VPN Gateway và cấu hình VPN Gateway cho mỗi người dùng.

**VPN Gateway**

Configure VPN Gateway:

☐ No ☒ Yes

Allow client to act as VPN gateway for these client-side subnets:

10.30.0.0/16

**DMZ settings**

Configure DMZ IP address:

☒ No ☐ Yes

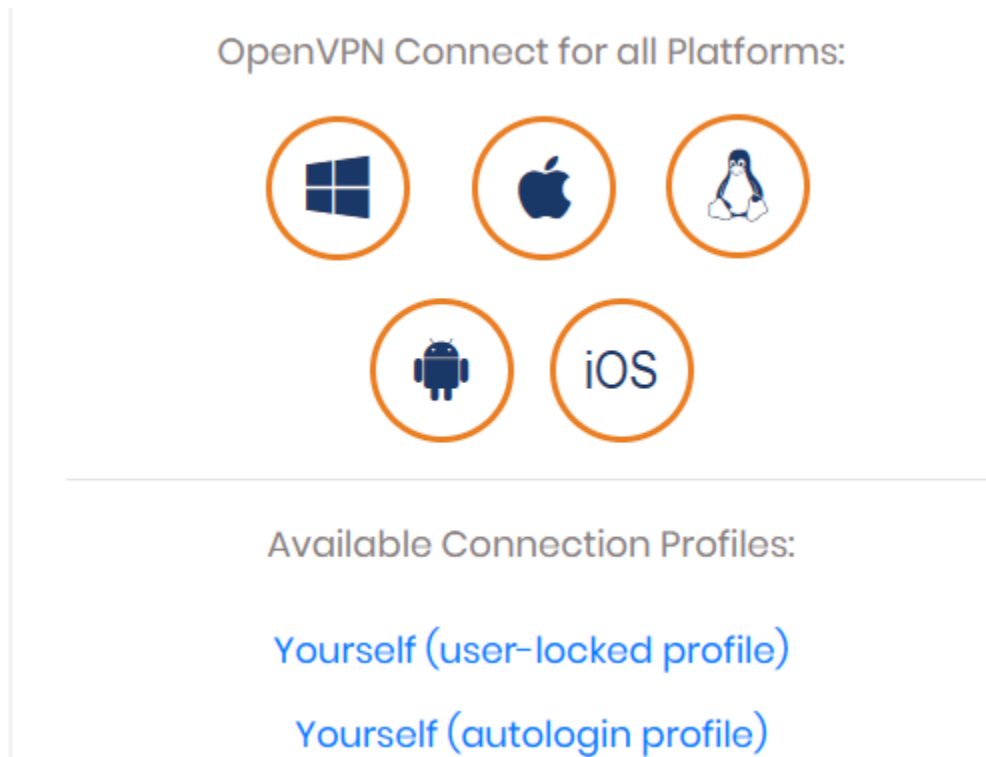
User	Default Group	Edit	VPN Gateway	DMZ	Other 1	Other 2
khanh	No Default Group		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
openvpn	No Default Group		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Hình 7: Cấu hình VPN Gateway cho user.

### Máy Ubuntu cài đặt OpenVPN client:

Địa chỉ IP: 42.118.123.150 (địa chỉ ip theo router)

Máy này được cấu hình làm OpenVPN client và kết nối đến máy chủ OpenVPN Access Server để thiết lập kết nối VPN an toàn. Được cài đặt và cấu hình OpenVPN client trên máy này và tải xuống tập tin cấu hình từ máy chủ OpenVPN Access Server.



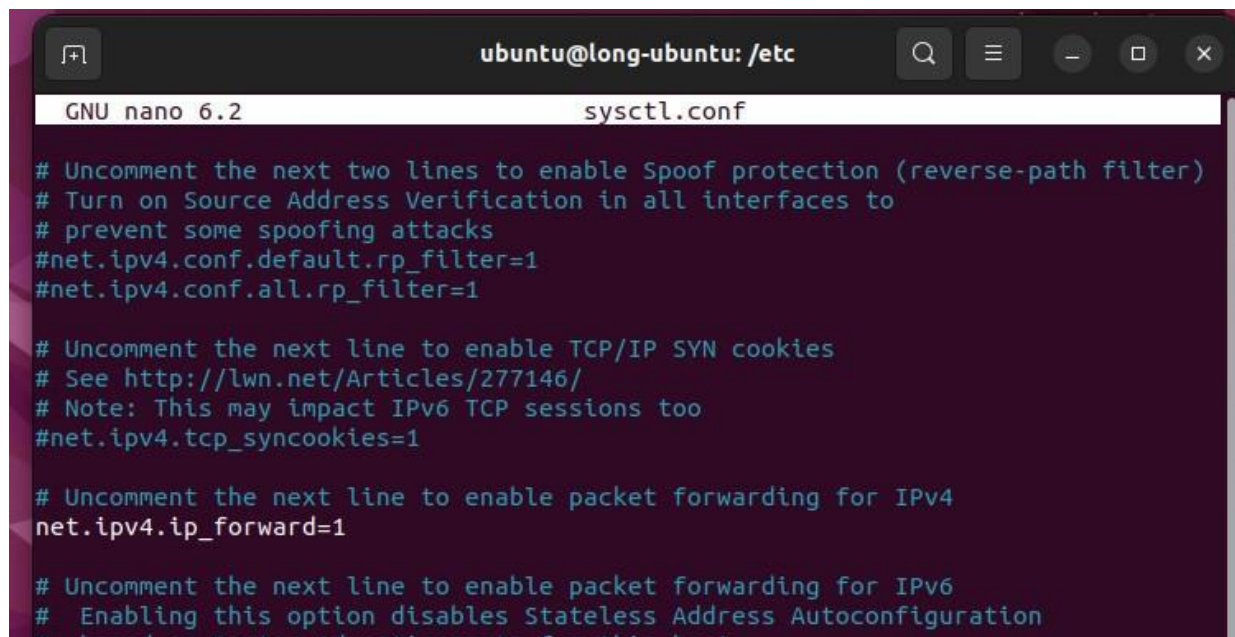
Hình 8: User tải file cấu hình về từ giao diện người dung.

Chuyển file cấu hình đã tải xuống vào thư mục /etc/openvpn để máy client nhận được ip và card mạng của vpn.

```
ubuntu@long-ubuntu:/etc$ cd openvpn/
ubuntu@long-ubuntu:/etc/openvpn$ ls
client  openvpn.conf  server  update-resolv-conf
ubuntu@long-ubuntu:/etc/openvpn$
```

Hình 9: Cấu hình file cài đặt trên máy client.

Sau đó bật tính năng `ip_forward` để có thể chuyển tiếp các gói tin trong mạng.



```
ubuntu@long-ubuntu: /etc
GNU nano 6.2 sysctl.conf

# Uncomment the next two lines to enable Spoof protection (reverse-path filter)
# Turn on Source Address Verification in all interfaces to
# prevent some spoofing attacks
#net.ipv4.conf.default.rp_filter=1
#net.ipv4.conf.all.rp_filter=1

# Uncomment the next line to enable TCP/IP SYN cookies
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1

# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1

# Uncomment the next line to enable packet forwarding for IPv6
# Enabling this option disables Stateless Address Autoconfiguration
# based on Router Advertisements for this host
```

Hình 10: Cấu hình `ip_forward` trên máy client.

Reboot máy để máy ảo nhận diện người dùng.

Search:

Common Name	Real Address	VPN Address	Bytes Sent Received	Connection Duration	Block
dung	183.80.234.148:60986	172.27.232.24	49.79KB 39.11KB	1:04:56	<input type="checkbox"/>
khanh	42.118.123.150:65053	172.27.232.26	6.91KB 7.21KB	0:23:53	<input type="checkbox"/>

Hình 11: Admin nhận diện được người dùng truy cập.

### Dải mạng VPN:

Dải mạng này được sử dụng cho các kết nối VPN giữa máy chủ OpenVPN Access Server và các máy client.

Địa chỉ IP của máy Ubuntu cài đặt OpenVPN client trong dải mạng VPN là 172.27.232.25.

Các gói tin được gửi từ máy client sẽ được định tuyến qua dải mạng VPN này để truy cập vào các tài nguyên trên máy chủ OpenVPN Access Server hoặc các dải mạng cụ thể được phép truy cập.

## **IV. Công cụ và công nghệ sử dụng**

Scapy và Wireshark là hai công cụ quan trọng trong quá trình triển khai hệ thống Steganography qua mạng WAN. Scapy cung cấp khả năng tạo và tùy chỉnh các gói tin mạng, cho phép chèn thông tin bí mật vào trường MSS của Option trong các gói tin. Đồng thời, Wireshark là công cụ phân tích gói tin mạng giúp người dùng bắt và phân tích các gói tin trên mạng, từ đó kiểm tra và đảm bảo rằng quá trình giấu tin và truyền tin diễn ra một cách an toàn và hiệu quả. Sự kết hợp giữa Scapy và Wireshark giúp cho việc triển khai và kiểm tra hệ thống Steganography qua mạng WAN trở nên thuận lợi và đáng tin cậy.

### **4.1. OpenVPN**

OpenVPN là một giải pháp mạng riêng ảo (VPN) mã nguồn mở, cung cấp khả năng kết nối an toàn và bảo mật giữa các thiết bị thông qua mạng Internet. Nó cho phép người dùng truy cập vào các tài nguyên mạng từ xa một cách an toàn, bảo vệ thông tin cá nhân khỏi các cuộc tấn công và lừa đảo. OpenVPN sử dụng mã hóa để bảo vệ dữ liệu khi truyền qua mạng và cho phép truy cập vào các tài nguyên mạng của doanh nghiệp hoặc tổ chức từ bất kỳ đâu. Cài đặt phần mềm trên máy tính và cấu hình các chứng chỉ xác nhận và tập tin cấu hình cho client và server. Có nhiều hướng dẫn chi tiết trực tuyến giúp cài đặt và cấu hình OpenVPN cho nhu cầu cụ thể của người dùng.

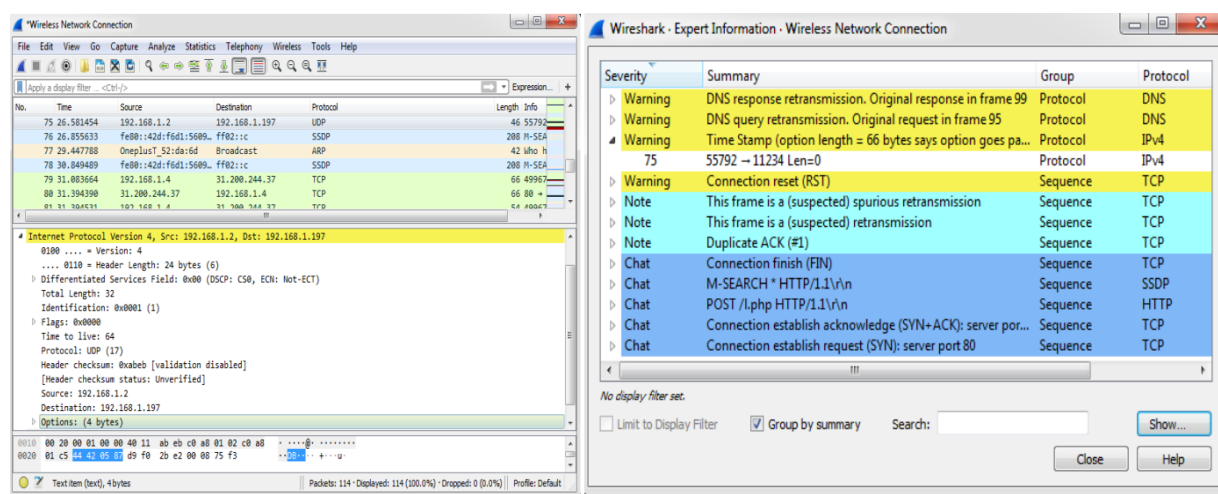
### **4.2. Scapy**

Scapy là một công cụ mạng mã nguồn mở được sử dụng để tạo và tùy chỉnh các gói tin mạng trên mạng. Trong hệ thống Steganography qua mạng, Scapy sẽ

được sử dụng để tạo và gửi các gói tin mạng đã được giấu tin. Tận dụng tính linh hoạt của Scapy để thêm thông tin bí mật vào trường MSS của Option trong các gói tin mạng.

### 4.3. Wireshark

Wireshark là một công cụ phân tích gói tin mạng mạnh mẽ, cho phép người dùng bắt và phân tích các gói tin trên mạng. Trong đề tài, Wireshark sẽ được sử dụng để bắt và phân tích các gói tin trên mạng WAN, nhằm kiểm tra xem thông tin đã được giấu tin có được truyền đi và nhận được thành công hay không. Việc sử dụng Wireshark giúp đảm bảo rằng quá trình giấu tin và truyền tin diễn ra một cách hiệu quả và không bị phát hiện.



Hình 12. Giao diện của wireshark.

### 4.4. Ngôn ngữ Python

Python là một ngôn ngữ lập trình mạnh mẽ và linh hoạt, được sử dụng rộng rãi trong lĩnh vực phát triển phần mềm và khoa học dữ liệu. Trong đề tài Python được sử dụng để viết mã để thực hiện các chức năng như gửi và bắt các gói tin mạng, cũng như thực hiện quá trình giấu tin. Sự linh hoạt của Python cho phép dễ dàng thích ứng và mở rộng chức năng của hệ thống Steganography mạng của mình theo yêu cầu cụ thể.



## V. Nghiên cứu thực nghiệm

### 5.1. Máy gửi

#### 5.1.1. Chuẩn bị dữ liệu bí mật:

Người dùng nhập tin nhắn vào chương trình. Tin nhắn sau đó được chuyển đổi thành biểu diễn nhị phân để giấu tin vào gói tin mạng.

#### 5.1.2. Tạo gói tin:

Một mảng được tạo ra và các phần tử trong mảng này được trộn lẫn, với 50% bit 0 và 50% bit 1. Điều này giúp tăng tính ngẫu nhiên của dữ liệu giấu tin.

Mỗi bit dữ liệu bí mật được giấu vào trường MSS của Option trong gói tin TCP/IP. Trường này được chọn vì trong nghiên cứu, sử dụng trường MSS trong options của gói TCP.

Một gói tin TCP/IP được tạo ra, và dữ liệu giấu tin được thêm vào trường MSS của Option trong gói tin này.

```
root@ip-172-31-20-199:~# python3 send_packet.py
Input message: Ky thuật giấu tin
Enter destination IP: 172.27.232.25
136
010010110111001001000000111010001101000011101010110000101110100001000000110011101101001011000010111010100100100000011101000110100101101110
272
WARNING: Incompatible L3 types detected using <class 'scapy.layers.inet.IP'> instead of <class 'scapy.layers.inet6.IPv46'> !
.1100
Sent 1 packets.
WARNING: Incompatible L3 types detected using <class 'scapy.layers.inet.IP'> instead of <class 'scapy.layers.inet6.IPv46'> !
.0111
Sent 1 packets.
WARNING: more Incompatible L3 types detected using <class 'scapy.layers.inet.IP'> instead of <class 'scapy.layers.inet6.IPv46'> !
.1101
Sent 1 packets.
```

Hình 13. Giao diện gửi gói tin.

#### 5.1.3. Gửi gói tin:

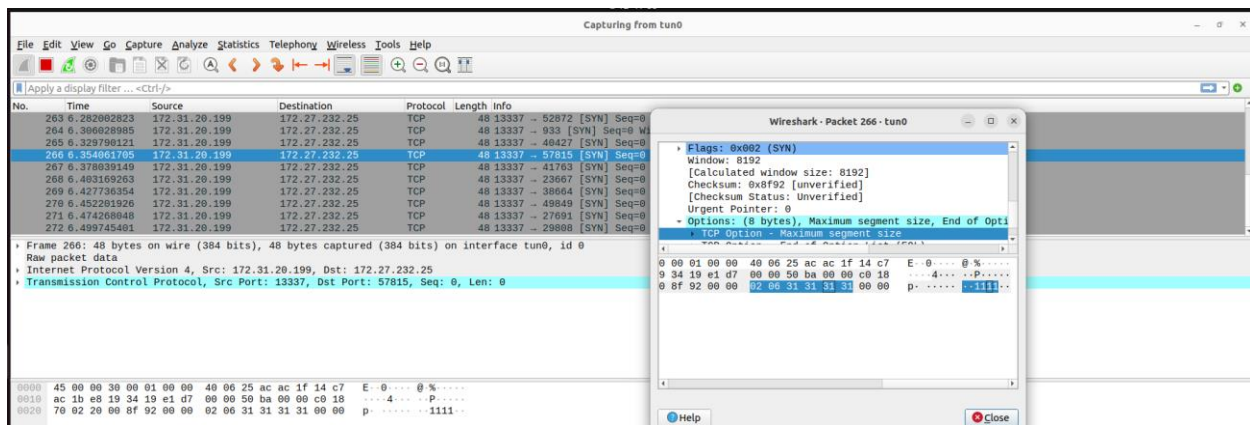
Gói tin được gửi đi tới địa chỉ IP VPN của Máy Client, đóng vai trò là máy đích trong thí nghiệm.

Gói tin được gửi đi để truyền dẫn dữ liệu giấu tin qua mạng VPN giữa máy gửi (Máy Server) và máy đích (Máy Client).

### 5.2. Máy nhận

### 5.2.1. Đọc gói tin

Các gói tin được wireshark bắt lại và được lưu dưới dạng file pcap có tên capture\_tcp\_packet.pcapng. Sử dụng thư viện Scapy để đọc các gói tin từ file pcap được lưu trữ trước đó. Mỗi gói tin được đọc được kiểm tra để xác định xem có chứa lớp IP và TCP không. Nếu có, tiếp tục xác định xem IP nguồn của gói tin có phải là IP của Máy Server không.



Hình 14. Giao diện wireshark bắt gói tin.

### 5.2.2. Đọc trường options

Lập qua từng gói tin và trích xuất trường options của gói tin TCP từ IP của Máy Server.

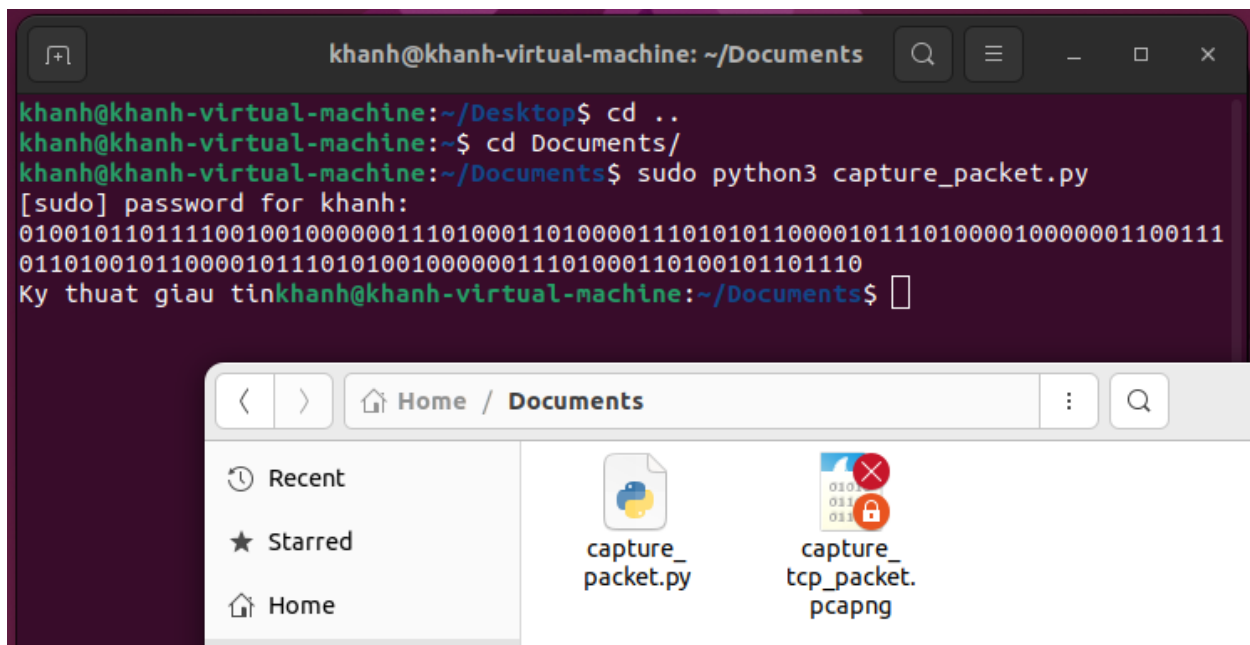
Đọc trường MSS của Option trong gói tin TCP, với giả định rằng đây là nơi dữ liệu bí mật được giấu.

Trích xuất các bit dữ liệu từ trường MSS của Option, bằng cách kiểm tra các ký tự trong chuỗi và chỉ lấy các bit sau khi kiểm tra điều kiện.

### 5.2.3. Hiển thị thông điệp

Các bit dữ liệu được chuyển đổi thành chuỗi Unicode, sau đó được ghép lại để tạo thành thông điệp ban đầu.

Thông điệp này sau đó được in ra để người dùng có thể đọc và hiểu được nội dung bí mật đã được giấu trong các gói tin mạng TCP/IP.



Hình 15. Thông điệp được trích ra.

## VI. Kết quả thực nghiệm

Kết quả thực nghiệm đã chứng minh rằng phương pháp giấu tin trong trường MSS options của gói tin IPv4 là khả thi và có thể được triển khai trên mạng WAN. Dữ liệu bí mật đã được thành công giấu trong các gói tin TCP/IP và truyền đi qua mạng WAN từ máy gửi (Máy Server) đến máy nhận (Máy Client).

Đáng chú ý, phương pháp này đã tồn tại ổn định và hiệu quả ngay cả khi di chuyển qua một mạng rộng. Việc trích xuất thông điệp từ các gói tin đã nhận cũng đã được thực hiện thành công, và thông điệp bí mật đã được hiển thị chính xác và đầy đủ.

Kết quả cụ thể của quá trình giấu tin và truyền tin được thể hiện trong chuỗi bit dữ liệu được trích xuất từ các gói tin TCP/IP. Điều này chứng minh rằng phương pháp giấu tin trong trường MSS options của gói tin IPv4 là một giải pháp hiệu quả và có thể được áp dụng trong các môi trường mạng WAN.

## **VII. Kết luận**

### **7.1. Ưu điểm:**

Tính bí mật: Phương pháp giấu tin trong gói tin mạng IPv4 giúp bảo vệ thông tin nhạy cảm một cách hiệu quả, vì dữ liệu được giấu trực tiếp trong các gói tin mạng.

Khả năng truyền tải: Dữ liệu giấu tin có thể được truyền qua mạng LAN và WAN mà không gây ra sự nghi ngờ đáng kể từ phía các thiết bị trung gian hoặc hệ thống giám sát mạng.

Dễ triển khai: Phương pháp này sử dụng các công nghệ mạng phổ biến như IPv4, TCP/IP, và không yêu cầu cấu hình phức tạp, giúp dễ dàng triển khai và sử dụng trong các môi trường thực tế.

### **7.2. Nhược điểm:**

Dung lượng giấu tin hạn chế: Vì dữ liệu bí mật được giấu trong các trường tùy chọn của gói tin mạng, nên dung lượng dữ liệu giấu tin có thể bị hạn chế, đặc biệt là trong môi trường mạng có nhiều thiết bị trung gian.

Nguy cơ bị phát hiện: Mặc dù phương pháp này có thể giúp tránh được sự phát hiện của người giám sát mạng, nhưng nó không hoàn toàn an toàn. Các kỹ thuật phát hiện giấu tin ngày càng phát triển, có thể dẫn đến việc phát hiện dữ liệu giấu tin.

Tăng overhead: Việc giấu tin trong gói tin mạng có thể tăng overhead cho mạng, đặc biệt là khi dung lượng giấu tin tăng lên, có thể ảnh hưởng đến hiệu suất và băng thông của mạng.

## VIII. Tài liệu tham khảo

- [1] Sourabh Chandra and Smita Paira, "SECURE TRANSMISSION OF DATA USING IMAGE STEGANOGRAPHY," *ICTACT Journal*, vol. 10, no. 01, pp. 2049-2053, 2019.
- [2] Punam Bedia, Arti Dua, "Network Steganography using the Overflow Field of Timestamp," *ScienceDirect*, vol. 171, no. 01, p. 1810–1818, 2020.
- [3] Józef Lubacz, Wojciech Mazurczyk, Krzysztof Szczypiorski, "Principles and Overview of Network Steganography," *IEEE Communications Magazine*, pp. 1-7, 2012.
- [4] P. Biondi, "Scapy Documentation," Scapy, 2008-2024. [Online]. Available: <https://scapy.readthedocs.io/en/latest/introduction.html>. [Accessed 2008].
- [5] I. 0x0, "Manually create and send raw TCP/IP packets," 2020. [Online]. Available: <https://inc0x0.com/tcp-ip-packets-introduction/tcp-ip-packets-3-manually-create-and-send-raw-tcp-ip-packets/>.
- [6] OpenVPN, "Site-to-site VPN routing with Access Server," OpenVPN, Inc., [Online]. Available: <https://openvpn.net/vpn-server-resources/site-to-site-routing-explained-in-detail/>. [Accessed 2024].