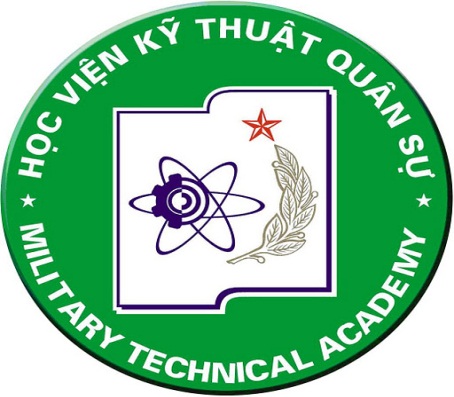
****

**BÁO CÁO**

**HỌC PHẦN**

**XÂY DỰNG, QUẢN TRỊ VÀ BẢO TRÌ HỆ THỐNG**

**Đề Tài**

**Xây dựng hệ thống tường lửa sử dụng UFW trong phòng thủ mạng**

* **Giáo viên hướng dẫn:** Tạ Minh Thanh
* **Lớp:** CNM14
* **Sinh viên thực hiện:** Hoàng Hùng Lâm - 15150138

MỤC LỤC

[MỤC LỤC 2](#_Toc529716482)

[Lời Mở Đầu 3](#_Toc529716483)

[Chương I: Xây dựng một firewall server sử dụng ufw trong phòng thủ mạng trên hệ điều hành Ubuntu](#_Toc529716484) 3

Bước 1[) Sử dụng IPv6 với UFW (Tùy chọn)](#_Toc529716505) 3

Bước 2[) Thiết lập chính sách mặc định](#_Toc529716505) 4

Bước 3[) Cho phép kết nối SSH](#_Toc529716505) 5

Bước 4[) Bật UFW](#_Toc529716505) 5

Bước 5[) Cho phép các kết nối khác](#_Toc529716505) 6

Bước 6[) Từ chối kết nối](#_Toc529716505) 7

Bước 7[) Xóa quy tắc](#_Toc529716505) 7

Bước 8[) Kiểm tra trạng thái và quy tắc UFW](#_Toc529716505) 9

Bước 9[) Vô hiệu hóa hoặc đặt lại UFW](#_Toc529716505) 10

Bước 10[) Cấu hình thiết lập màn hình cho UFW (dùng GUFW)](#_Toc529716505) 10

[Chương II: Xây dựng các kịch bản để phòng chống các truy xuất trái phép vào trong dịch vụ được triển khai trên server.](#_Toc529716485) 11

[Chương III: Xây dựng các kịch bản giám sát cho phòng thủ mạng và từ đó đưa ra cách phòng chống đồng thời lọc các gói tin đáng ngờ trong giao tiếp mạng 13](#_Toc529716504)

# 

# LỜI MỞ ĐẦU

UFW, hoặc Uncomplicated Firewall, là một giao diện iptables được hướng tới việc đơn giản hóa quá trình cấu hình tường lửa. Trong khi iptables là một công cụ vững chắc và linh hoạt, người mới bắt đầu có thể khó học cách sử dụng nó để cấu hình tường lửa đúng cách. Nếu bạn muốn bắt đầu bảo vệ mạng của mình và bạn không chắc chắn nên sử dụng công cụ nào, UFW có thể là lựa chọn phù hợp với bạn.

# Chương I: Xây dựng một firewall server sử dụng ufw trong phòng thủ mạng trên hệ điều hành Ubuntu

UFW được cài đặt mặc định trên Ubuntu. Nếu nó đã được gỡ cài đặt vì một số lý do, bạn có thể cài đặt nó

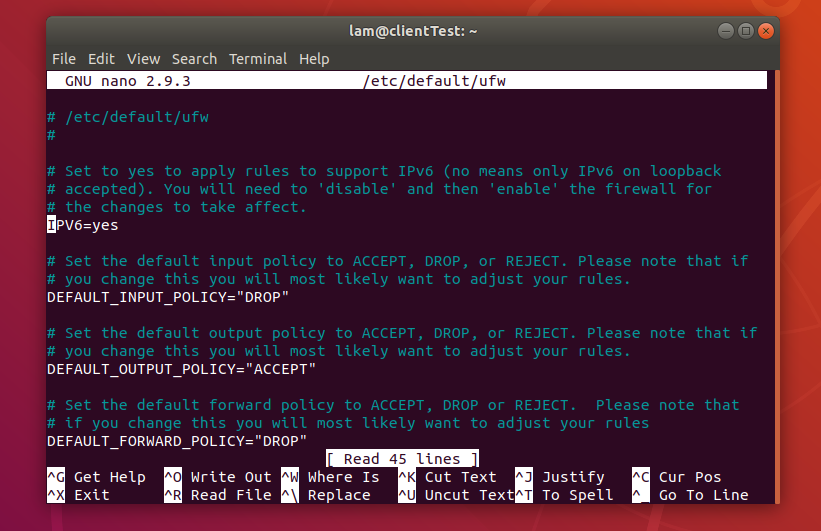
$sudo apt install ufw

## Bước 1: Sử dụng IPv6 với UFW (Tùy chọn)

Nếu máy chủ Ubuntu của bạn đã bật IPv6, hãy đảm bảo rằng UFW được cấu hình để hỗ trợ IPv6, ngoài IPv4 nó sẽ quản lý các quy tắc tường lửa cho IPv6. Để thực hiện việc này, hãy mở cấu hình UFW.

$sudo nano /etc/default/ufw

Sau đó, chắc chắn giá trị của IPV6 là **yes**



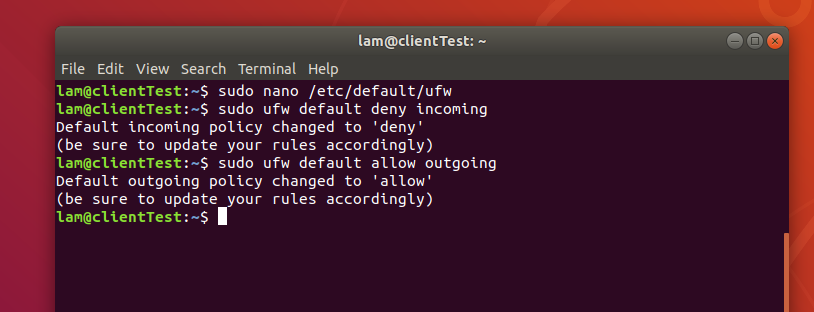
Lưu và đóng tập tin. Bây giờ, khi UFW được kích hoạt, nó sẽ được cấu hình để viết cả các quy tắc tường lửa IPv4 và IPv6.

## Bước 2: Thiết lập chính sách mặc định

Để đặt các giá trị mặc định được UFW sử dụng, hãy sử dụng các lệnh sau:

$sudo ufw default deny incoming

$sudo ufw default allow outgoing



## Bước 3: Cho phép kết nối SSH

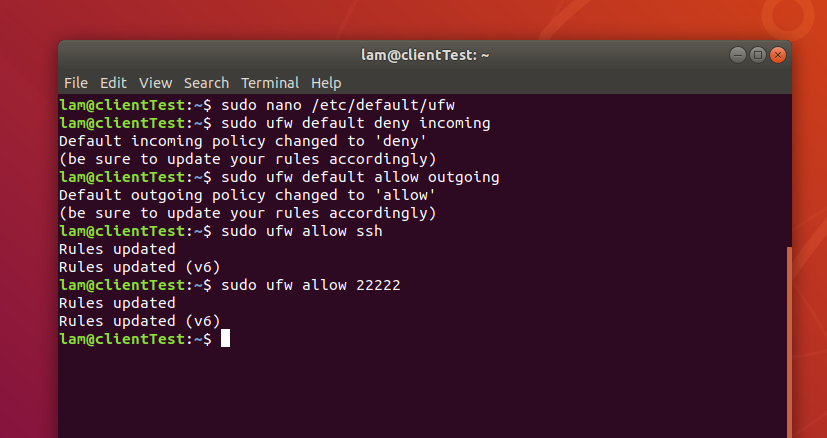
Để cấu hình máy chủ của bạn cho phép các kết nối SSH đến, bạn có thể sử dụng lệnh này:

$sudo ufw allow ssh

hoặc

$sudo ufw allow 22

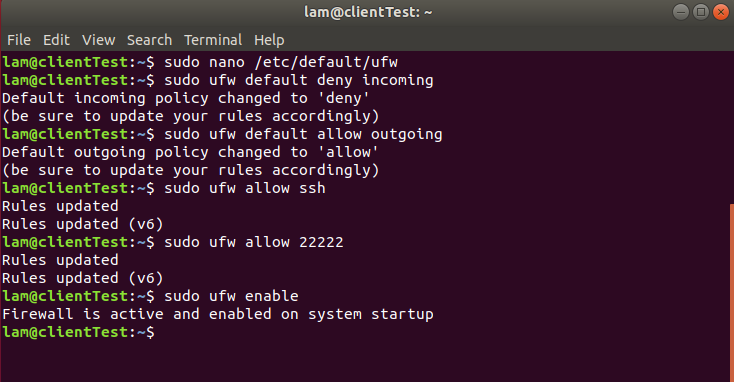
$sudo ufw allow 22222



## Bước 4: Bật UFW

Để kích hoạt UFW, sử dụng lệnh này:

$sudo ufw enable



## Bước 5: Cho phép các kết nối khác

### Phạm vi cổng cụ thể

Bạn có thể chỉ định các dải cổng với UFW. Một số ứng dụng sử dụng nhiều cổng, thay vì một cổng duy nhất.

$sudo ufw allow 8080:9000/tcp

$sudo ufw allow 8080:9000/udp

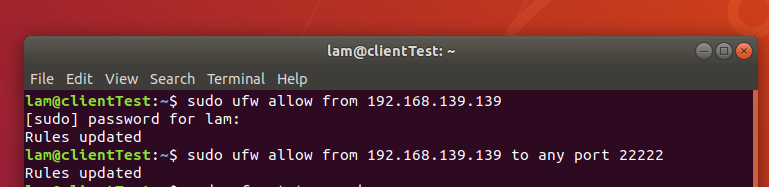
### Địa chỉ IP cụ thể

Khi làm việc với UFW, bạn cũng có thể chỉ định địa chỉ IP

$sudo ufw allow from 192.168.139.139

Bạn cũng có thể chỉ định một cổng cụ thể mà địa chỉ IP được phép kết nối bằng cách sau

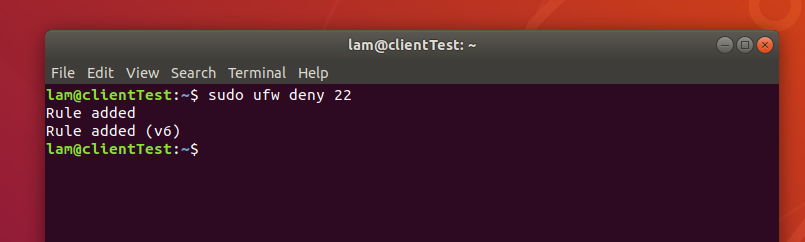
$sudo ufw allow from 192.168.139.139 to any port 22222



## Bước 6: Từ chối kết nối

Để viết các quy tắc **từ chối**, bạn có thể sử dụng các lệnh được mô tả ở trên, thay thế **allow** bằng **deny**

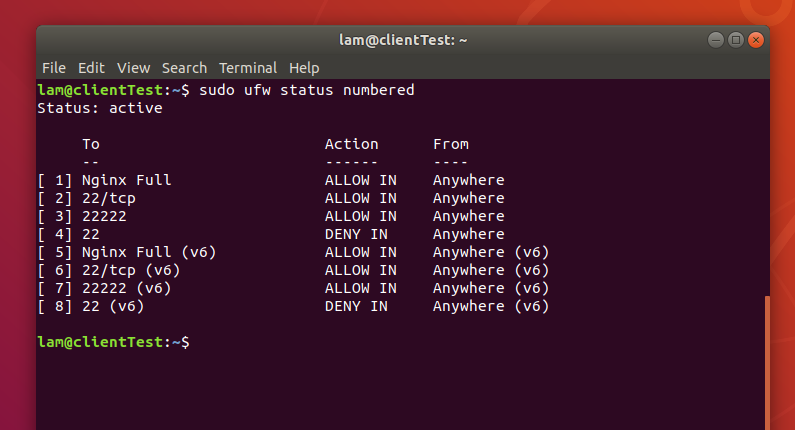
$sudo ufw deny 22



## Bước 7: Xóa quy tắc

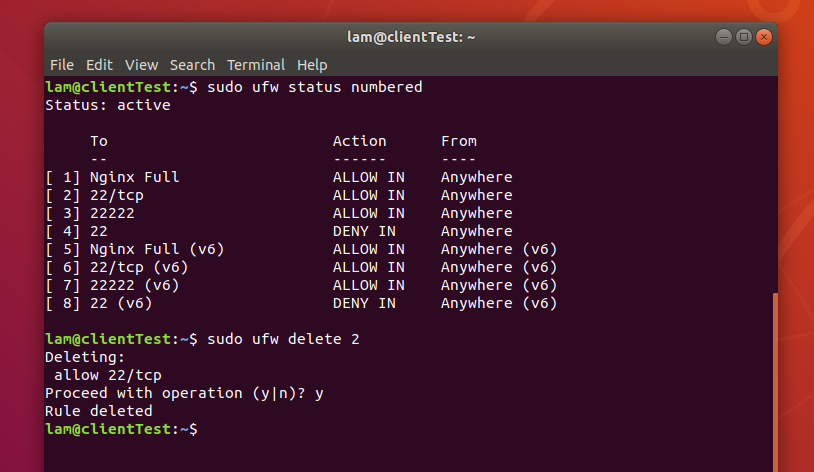
Để hiển thị các quy tắc và số bên cạnh mỗi quy tắc

$sudo ufw status numbered

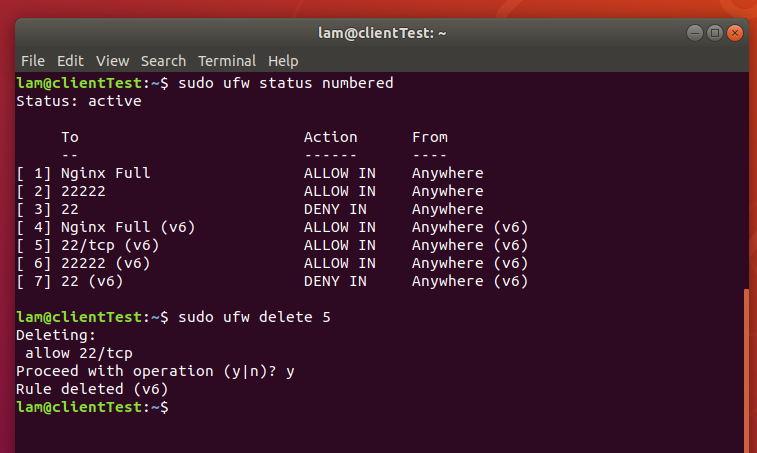


Nếu chúng ta quyết định rằng chúng ta muốn xóa quy tắc 2, cái cho phép các kết nối cổng 22/tcp (SSH), chúng ta có thể chỉ định nó trong một lệnh xóa UFW như sau:

$sudo ufw delete 2



 Lưu ý rằng nếu bạn đã bật IPv6, bạn cũng sẽ muốn xóa quy tắc IPv6 tương ứng.

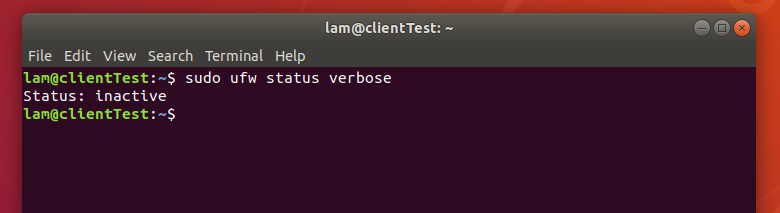


## Bước 8: Kiểm tra trạng thái và quy tắc UFW

Bất cứ lúc nào, bạn có thể kiểm tra trạng thái của UFW bằng lệnh này:

$sudo ufw status verbose

-Nếu UFW bị tắt



-Nếu UFW đang hoạt động



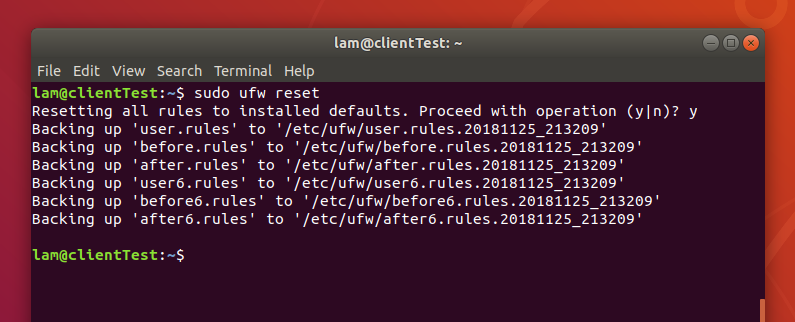
## Bước 9: Vô hiệu hóa hoặc đặt lại UFW

Nếu bạn quyết định không muốn sử dụng UFW, bạn có thể vô hiệu hóa nó bằng lệnh này:

$sudo ufw disable

Nếu bạn đã cấu hình các quy tắc UFW nhưng bạn quyết định rằng bạn muốn bắt đầu lại, bạn có thể sử dụng lệnh reset:

$sudo ufw reset



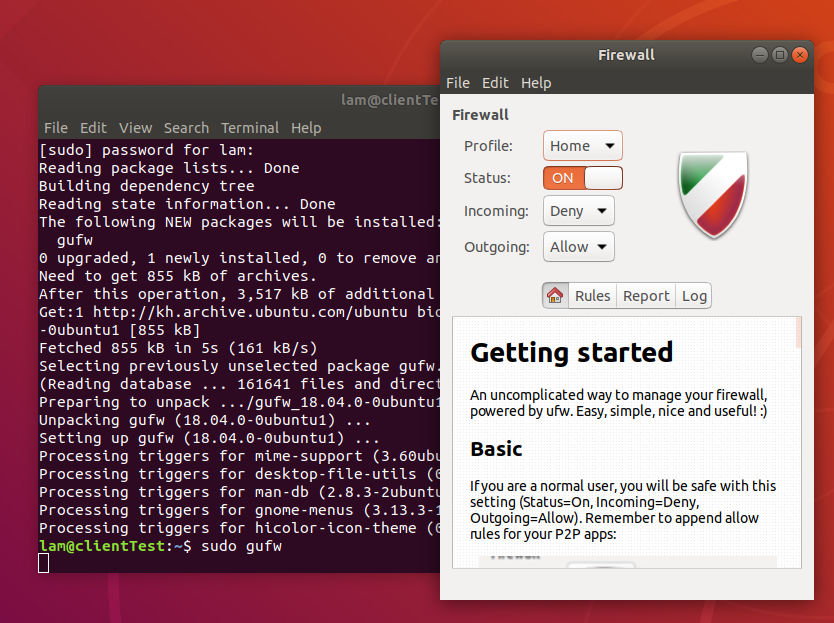
Bước 10: Cấu hình thiết lập màn hình cho UFW (dùng GUFW)

-Cài đặt GUFW

$sudo apt-get install gufw

-Để khởi động gufw dùng câu lệnh sau:

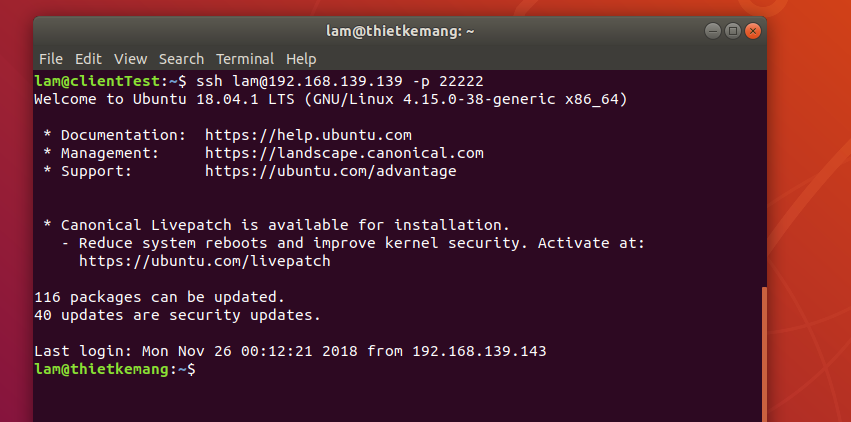
$sudo gufw



# Chương II: Xây dựng các kịch bản để phòng chống các truy xuất trái phép vào trong dịch vụ được triển khai trên server.

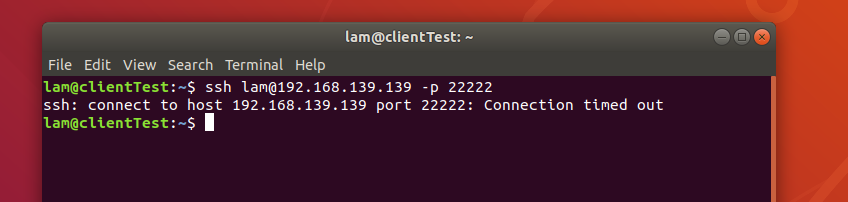
Giả sử chặn một người dùng có IP: 192.168.139.143 muốn truy cập từ xa sử dụng SSH

-Trước khi chặn



-Sau khi chặn:

$sudo ufw allow from 192.168.139.143 to any port 22222



# Chương III: Xây dựng các kịch bản giám sát cho phòng thủ mạng và từ đó đưa ra cách phòng chống đồng thời lọc các gói tin đáng ngờ trong giao tiếp mạng.

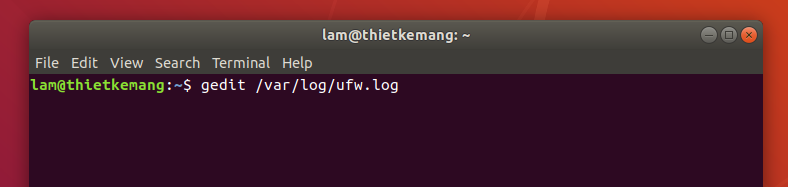
Để kiểm tra, giám sát các gói tin vào. Trong ufw, người ta sử dụng file ufw.log

Cơ chế lưu (logging) bị vô hiệu hóa mặc định, nhưng nếu muốn, người dùng vẫn có thể kích hoạt logging để lưu những thông báo của tường lửa vào nhật ký hệ thống (sys log):

$sudo ufw logging on

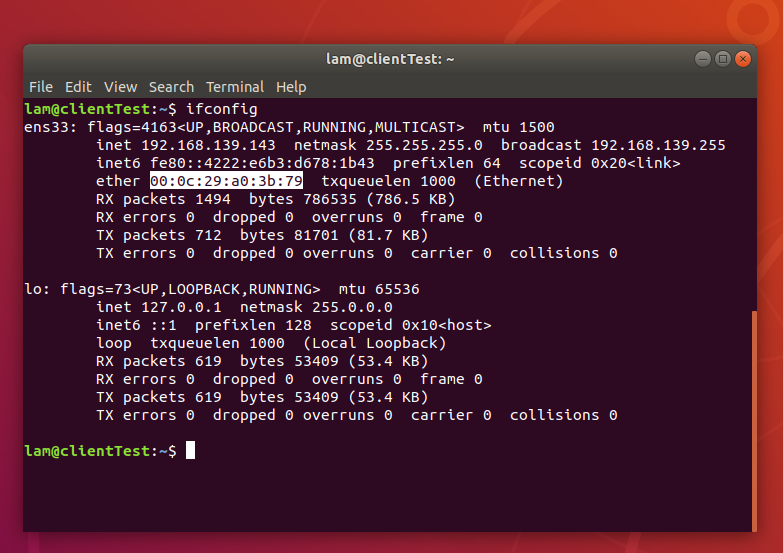
Theo mặc định file ufw.log sẽ được lưu trong thư mục /var/log. Để xem file ufw.log sử dụng lệnh

$gedit /var/log/ufw.log



-Nội dung file ufw.log





Ở đây ta có thể thấy, gói tin có địa chỉ mac 29:a0:3b:79:86 đã bị chặn lại bởi firewall