**Bước 1: Cài đặt OpenVPN và Easy-RSA**

**Mục tiêu: Cài đặt phần mềm cần thiết để chạy VPN server và tạo chứng chỉ bảo mật.**

1. **Mở terminal trên Ubuntu (Ctrl+Alt+T).**

**A screenshot of a computer

AI-generated content may be incorrect.**

* **OpenVPN tạo một kênh truyền bảo mật (VPN tunnel) giữa server và client.**
* **Easy-RSA giúp xây dựng hệ thống chứng chỉ, bao gồm CA (Certificate Authority), khóa riêng, và chứng chỉ cho server/client.**cho server/client.

**Bước 2. Khởi tạo PKI và CA (build-ca)**

Mục tiêu: Tạo hệ thống chứng chỉ (CA) để xác thực server và client.

A screenshot of a computer

AI-generated content may be incorrect.

**Giải thích**:

* **PKI** quản lý khóa công khai để mã hóa và xác thực.
* **CA** giống như một "phòng công chứng" xác nhận danh tính server/client.
* **ca.crt** dùng để xác minh chứng chỉ, còn **ca.key** dùng để ký chứng chỉ mới. Mất ca.key là mất khả năng ký chứng chỉ mới!

**Bước 3: Tạo và ký chứng chỉ cho server**

Mục tiêu: Tạo khóa riêng và chứng chỉ cho VPN server, được CA xác nhận.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

**Giải thích**:

* Chứng chỉ server giúp client xác minh server là hợp lệ.
* **Common Name** (CN) định danh server, client sẽ kiểm tra CN này khi kết nối.

**Bước 4: Tạo khóa DH và TLS Auth**

Mục tiêu: Tăng cường bảo mật với khóa Diffie-Hellman (DH) và TLS Auth.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

**Giải thích**:

* **DH key**: Tạo khóa phiên an toàn, đảm bảo nếu khóa bị lộ, các phiên cũ vẫn an toàn.
* **ta.key**: Thêm lớp bảo vệ cho giao thức TLS, ngăn chặn các gói tin giả mạo.

**Bước 5: Cấu hình file /etc/openvpn/server.conf**

A screenshot of a computer

AI-generated content may be incorrect.

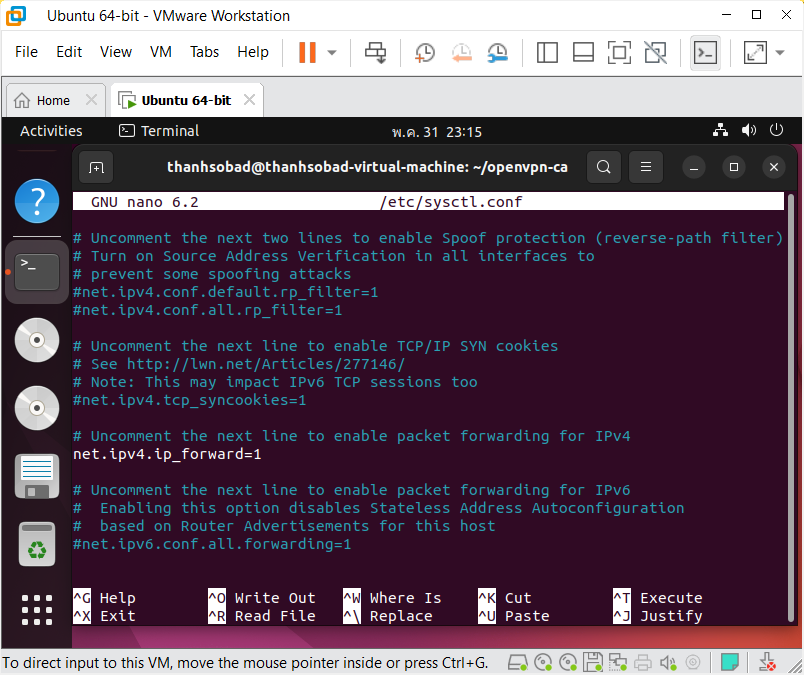
**Giải thích**:

* **port 1194, proto udp, dev tun**: Sử dụng cổng 1194, giao thức UDP, và thiết bị tun cho VPN.
* **ca, cert, key, dh**: Trỏ đến các file chứng chỉ và khóa.
* **server 10.8.0.0 255.255.255.0**: Gán dải IP 10.8.0.0/24 cho client.
* **push "redirect-gateway"**: Định tuyến toàn bộ lưu lượng client qua VPN.
* **DNS**: Cung cấp DNS công khai (1.1.1.1, 8.8.8.8) cho client.
* **cipher, auth, tls**: Đảm bảo mã hóa mạnh (AES-256, SHA256, TLS 1.2+).
* **log**: Ghi log để debug nếu cần.

**Bước 6: Bật IP Forwarding và cấu hình Firewall**

Mục tiêu: Cho phép server chuyển tiếp lưu lượng từ client ra Internet và mở cổng cần thiết.

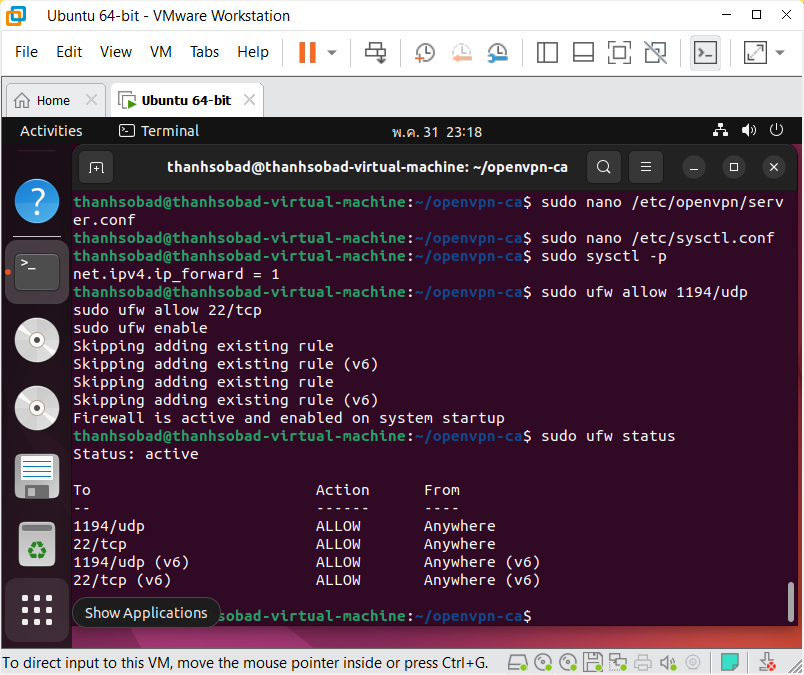
**Bật IP Forwarding**



A screenshot of a computer

AI-generated content may be incorrect.

**Cấu hình Firewall (UFW)**

****

**Giải thích:**

* IP Forwarding: Cho phép server chuyển tiếp dữ liệu từ client ra Internet, hoạt động như một router.
* UFW: Mở cổng 1194 (UDP) cho OpenVPN và 22 (TCP) cho SSH.

**Bước 7: Khởi động và kích hoạt dịch vụ OpenVPN**

Mục tiêu: Chạy OpenVPN server và đảm bảo nó hoạt động.

**A screenshot of a computer

AI-generated content may be incorrect.**

**Giải thích**:

* Dịch vụ openvpn@server sử dụng file server.conf để chạy.
* File ta.key cần được bảo vệ vì nó xác thực gói tin giữa client và server.

**Bước 8: Tạo yêu cầu và ký chứng chỉ cho client**

Mục tiêu: Tạo chứng chỉ cho client để kết nối an toàn với server.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

**Bước 9: Tạo file cấu hình client (client1.ovpn)**

Mục tiêu: Tạo file cấu hình để client Windows kết nối với server.

A screenshot of a computer

AI-generated content may be incorrect.

**Giải thích**:

* File client1.ovpn chứa thông tin để client kết nối: IP/port server, giao thức, và đường dẫn đến các file chứng chỉ/khóa.
* **remote**: Chỉ định IP và cổng của server (1194).
* **ca, cert, key, tls-auth**: Liên kết với các file chứng chỉ và khóa.

**Bước 10: Chuyển file sang Windows**

Mục tiêu: Chuẩn bị các file cần thiết để client Windows kết nối.