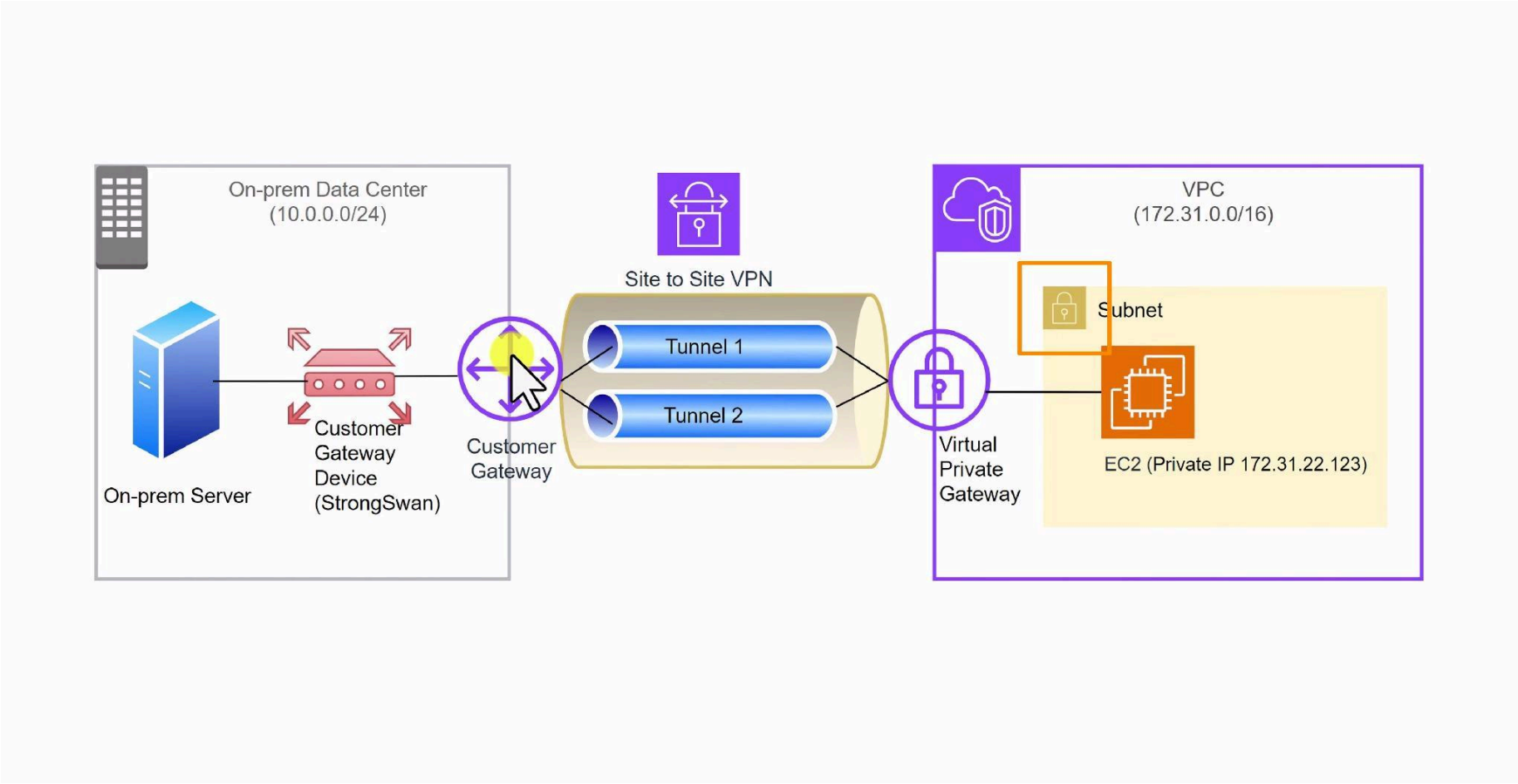
Hướng Dẫn: AWS Site-to-Site VPN - Kết nối On-Premise với Amazon VPC

Bước 1

Mô hình: Bên trái là On-premise Data Center (gồm Raspberry Pi làm Customer Gateway cài StrongSwan VPN, và 1 server). Bên phải là AWS VPC với EC2 instance. Mục tiêu: thiết lập Site-to-Site VPN kết nối 2 bên qua IPSec tunnel.

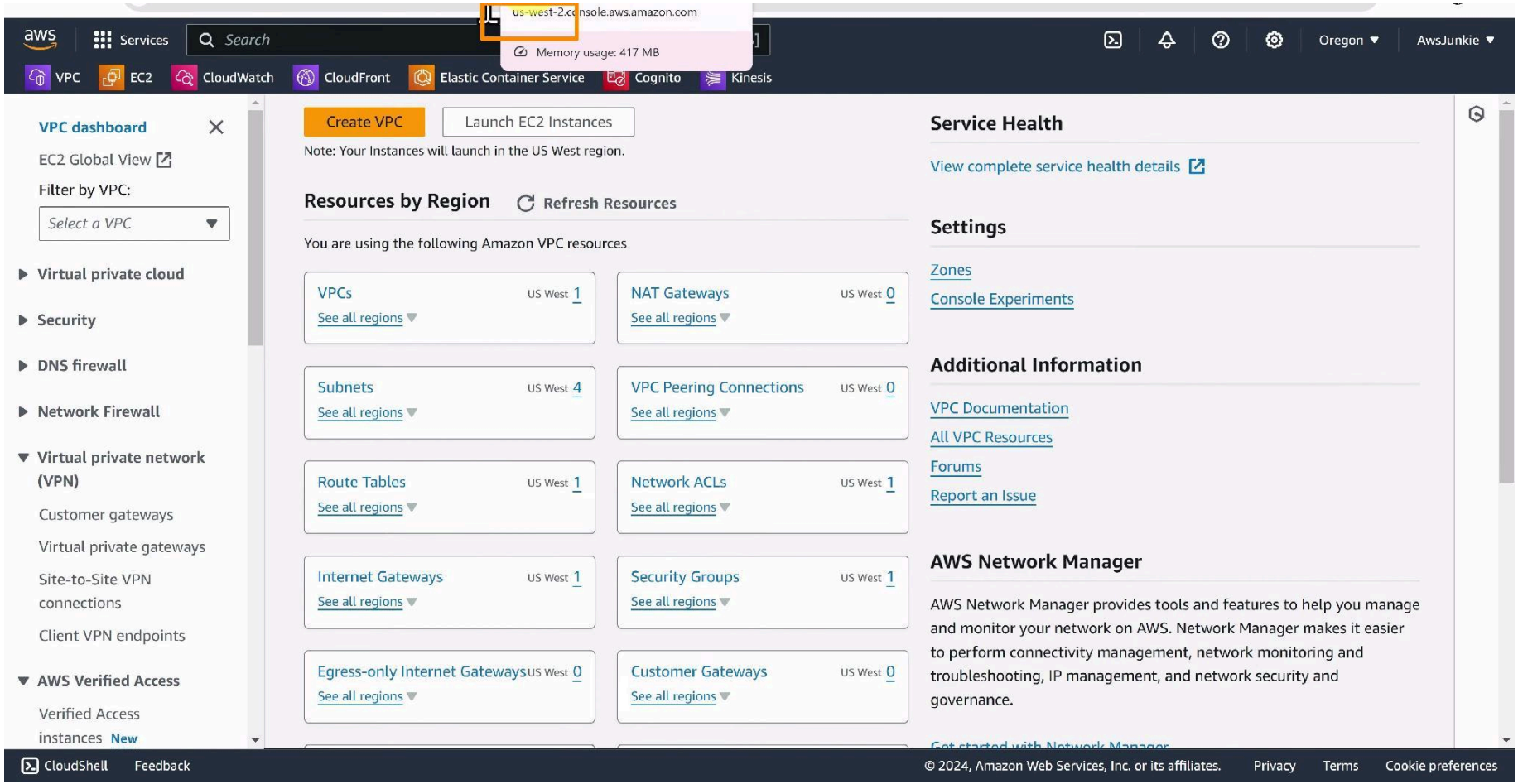
Bước 2

Trên AWS cần tạo: Customer Gateway (đại diện thiết bị on-prem), Virtual Private Gateway (điểm vào/ra VPN traffic cho VPC), và VPN Connection. Cấu hình 2 tunnel (Tunnel 1 & Tunnel 2) để đảm bảo redundancy và high availability.



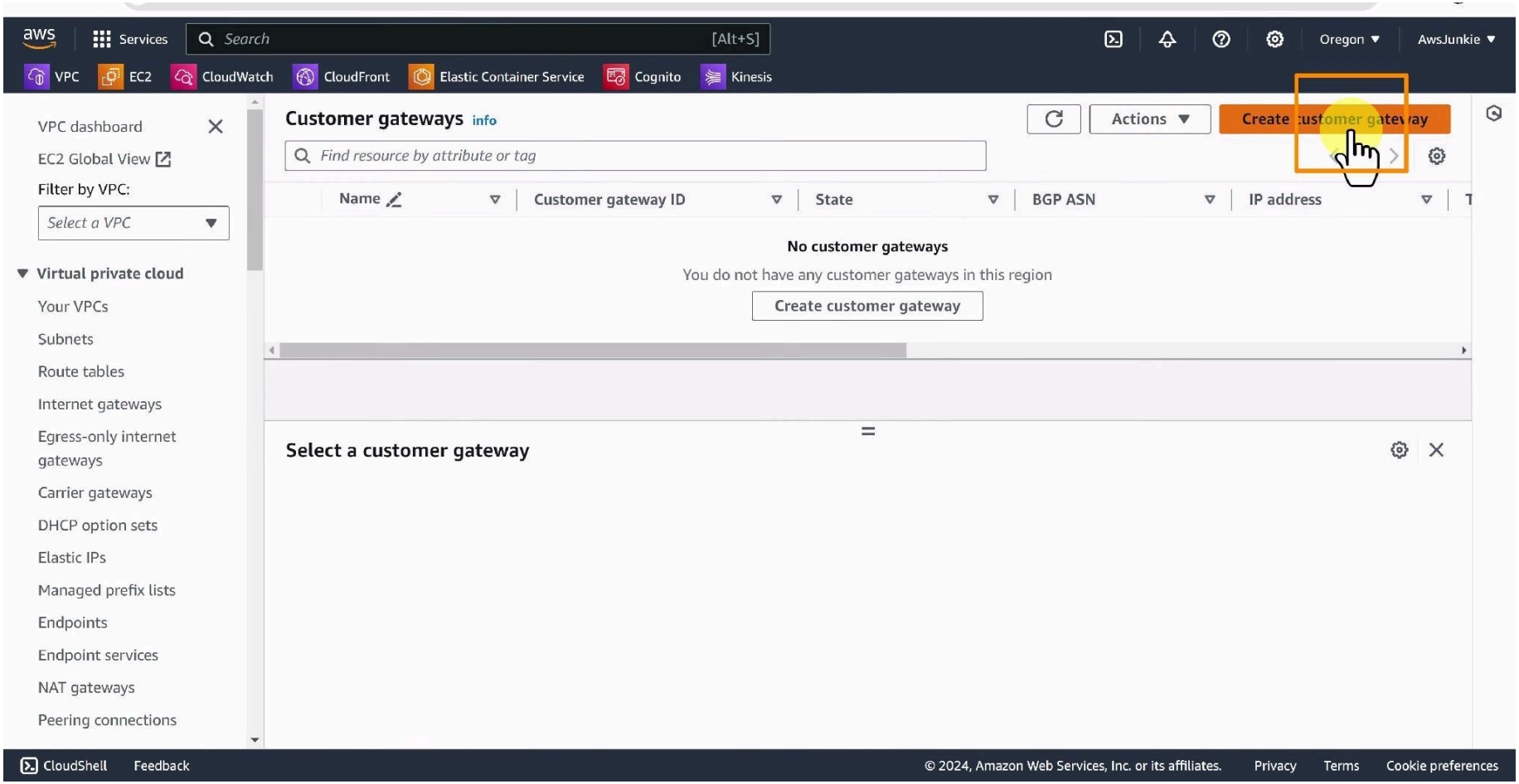
Bước 3

Đăng nhập AWS Console, mở VPC Dashboard. Trong menu bên trái phần Virtual Private Network, tìm các mục: Customer Gateways, Virtual Private Gateways, Site-to-Site VPN Connections.



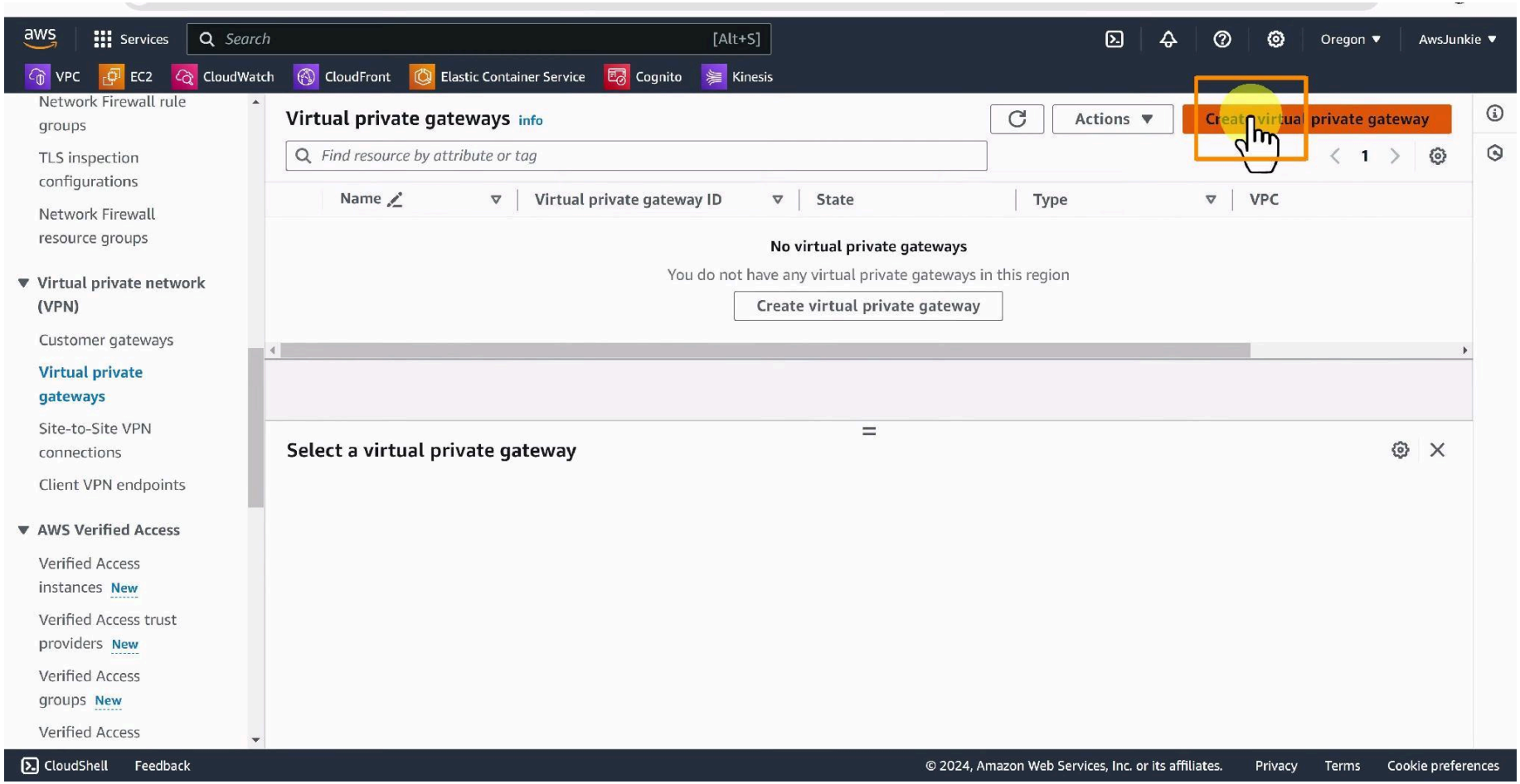
Bước 4

Tạo Customer Gateway: Click 'Customer Gateways' → 'Create Customer Gateway'. Đặt tên (ví dụ: CGW-1). Nhập Public IP address của thiết bị Customer Gateway (IP public của router/firewall on-prem). Click Create.



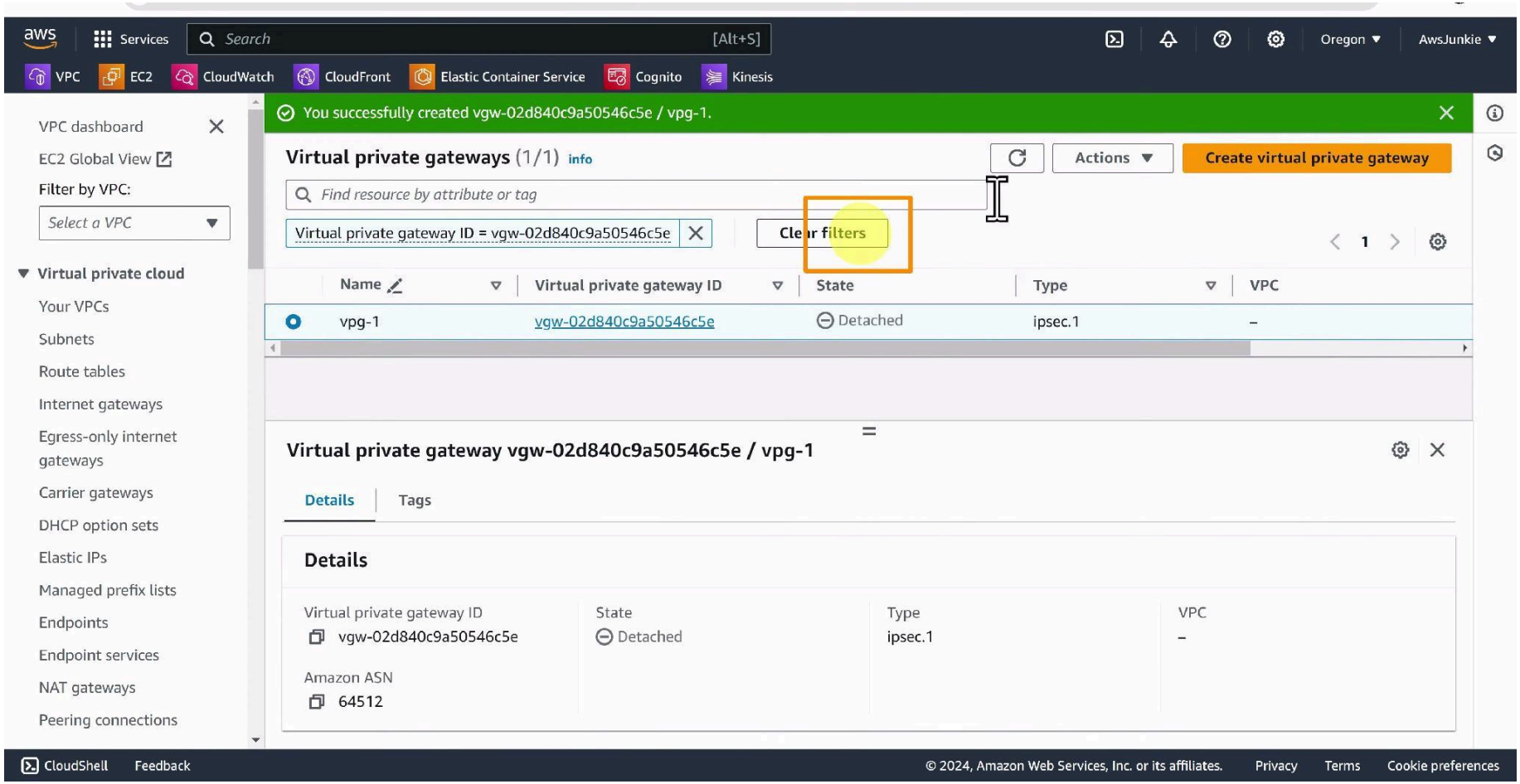
Bước 5

Tạo Virtual Private Gateway: Click 'Virtual Private Gateways' → 'Create Virtual Private Gateway'. Đặt tên (VPG-1). Để ASN mặc định (Amazon default ASN). Click Create.



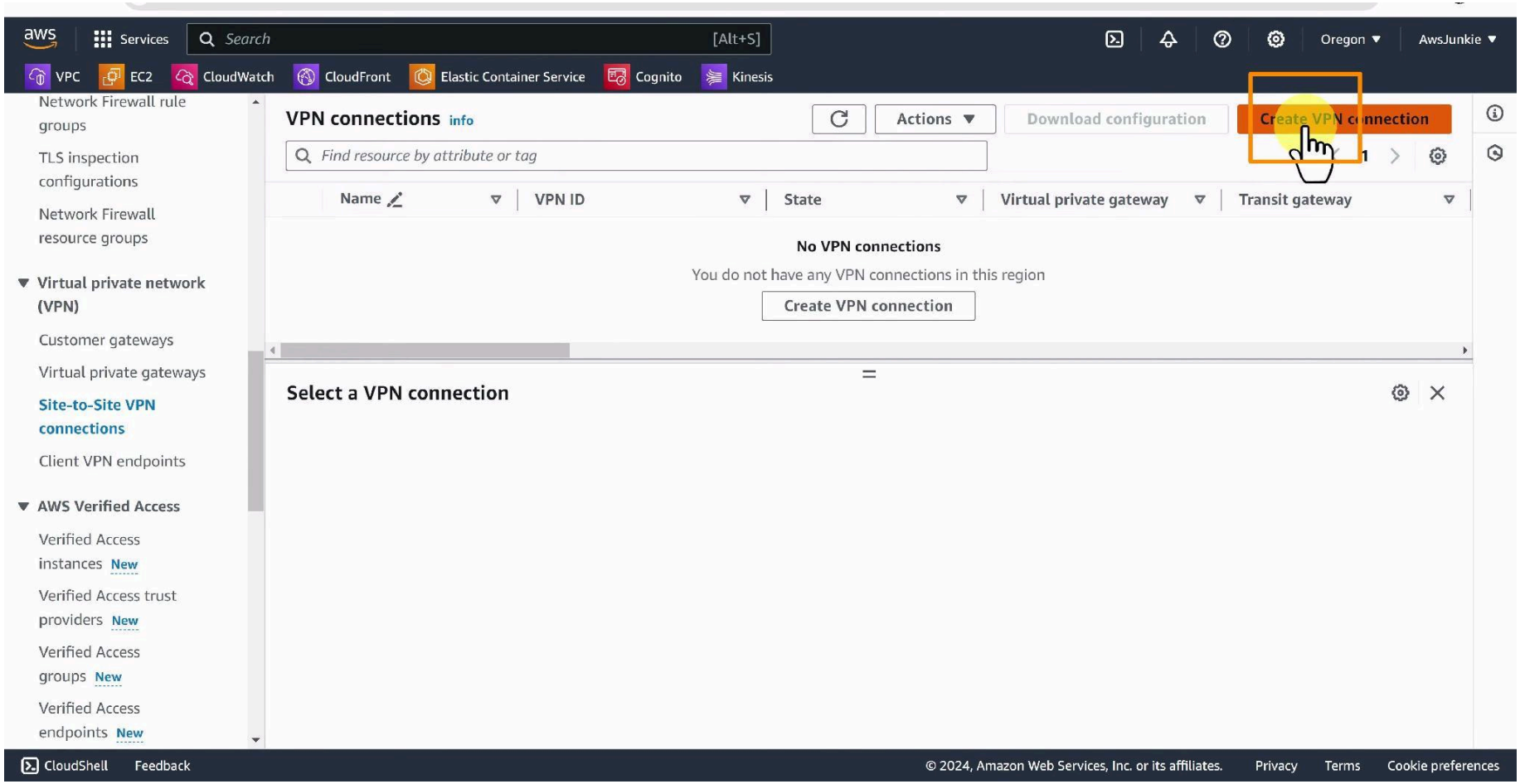
Bước 6

Attach Virtual Private Gateway vào VPC: Chọn VPG vừa tạo (đang ở trạng thái Detached) → Actions → Attach to VPC → Chọn VPC cần kết nối → Click Attach. Đợi trạng thái chuyển sang Attached.



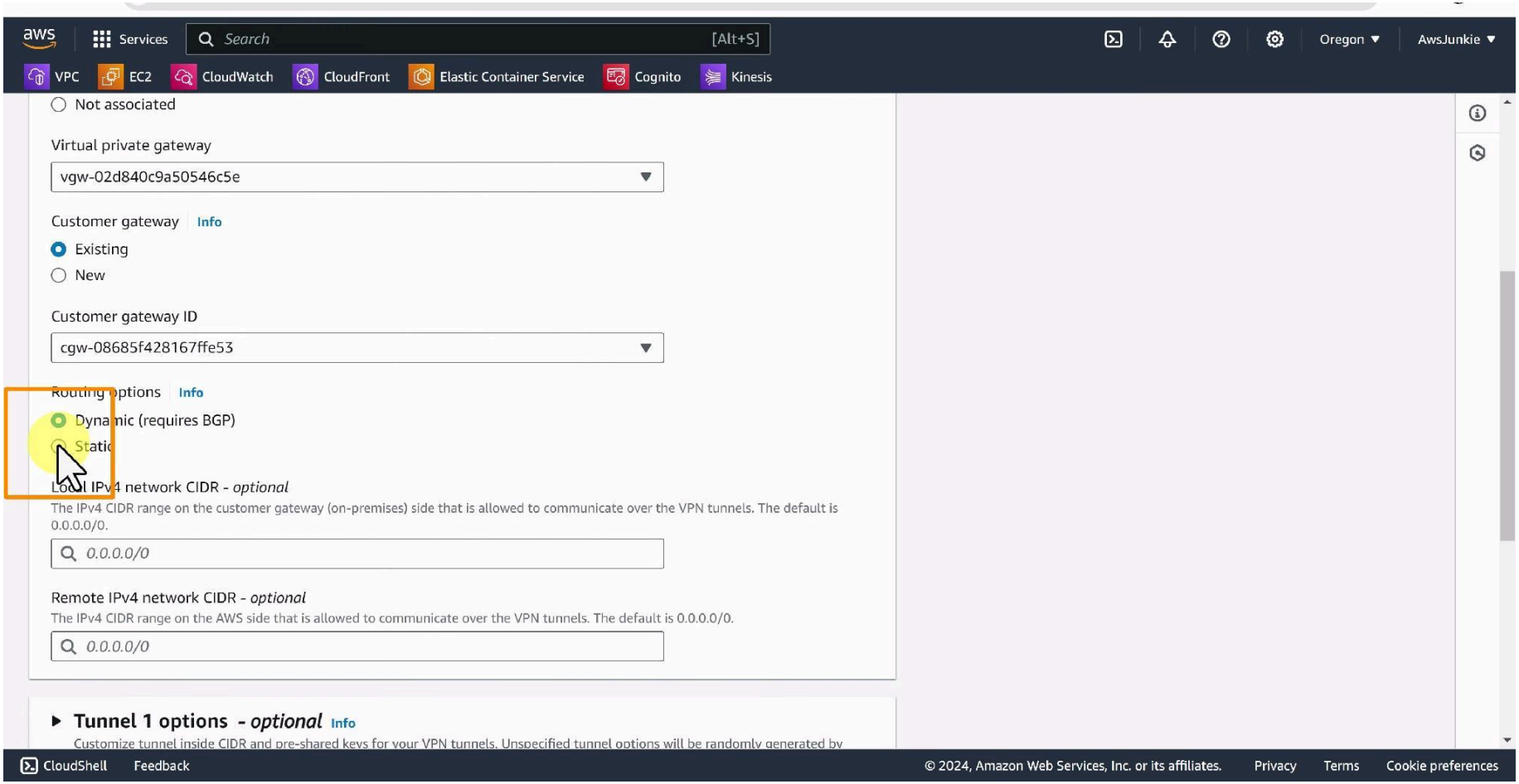
Bước 7

Tạo VPN Connection: Click 'Site-to-Site VPN Connections' → 'Create VPN Connection'. Đặt tên (VPN-1). Target Gateway: chọn Virtual Private Gateway vừa tạo. Customer Gateway: chọn Existing → chọn CGW đã tạo.



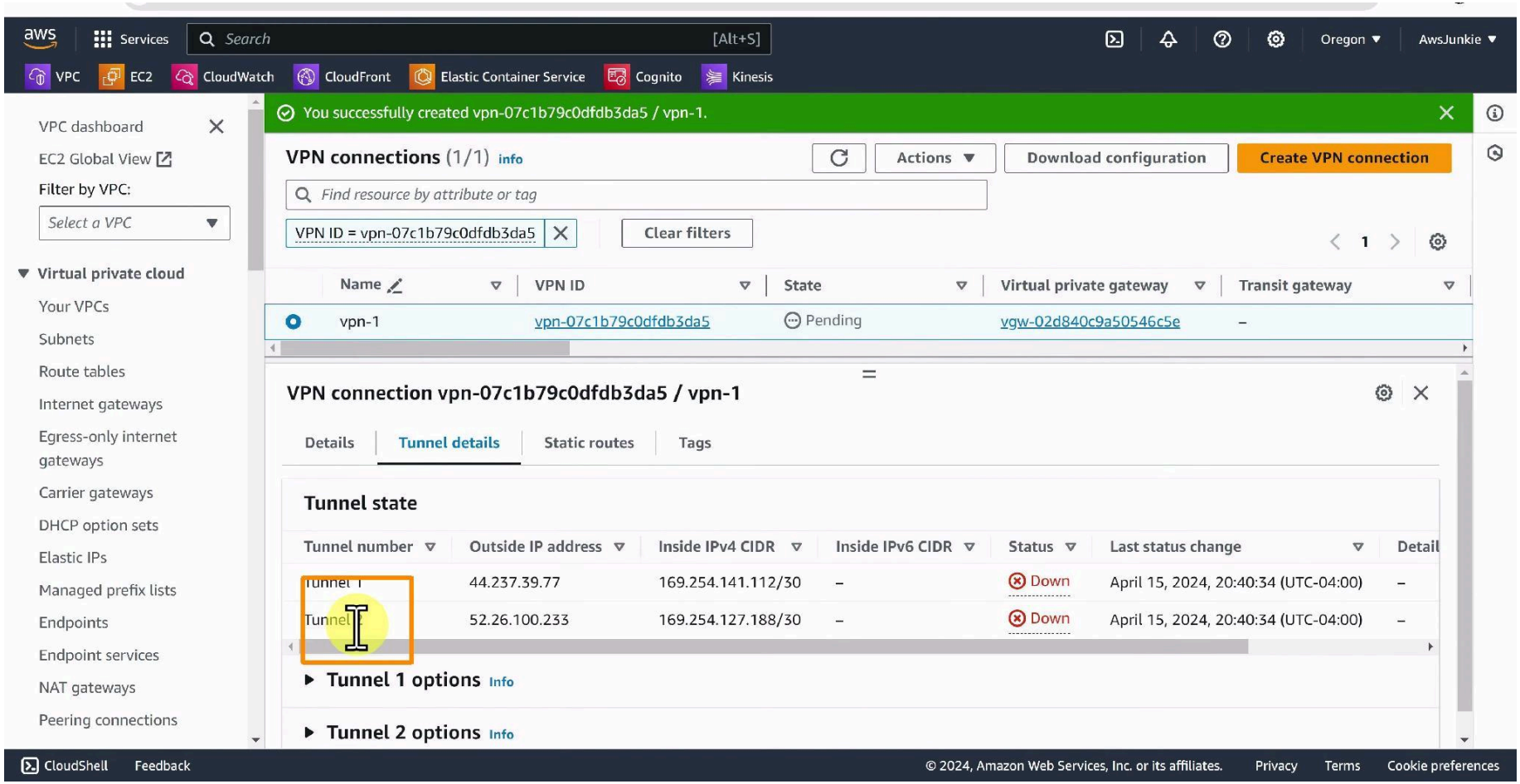
Bước 8

Cấu hình Routing: Vì không có BGP, chọn 'Static'. Nhập Static IP Prefix = CIDR range của mạng on-prem (ví dụ: 10.1.0.0/24). Click 'Create VPN Connection'.



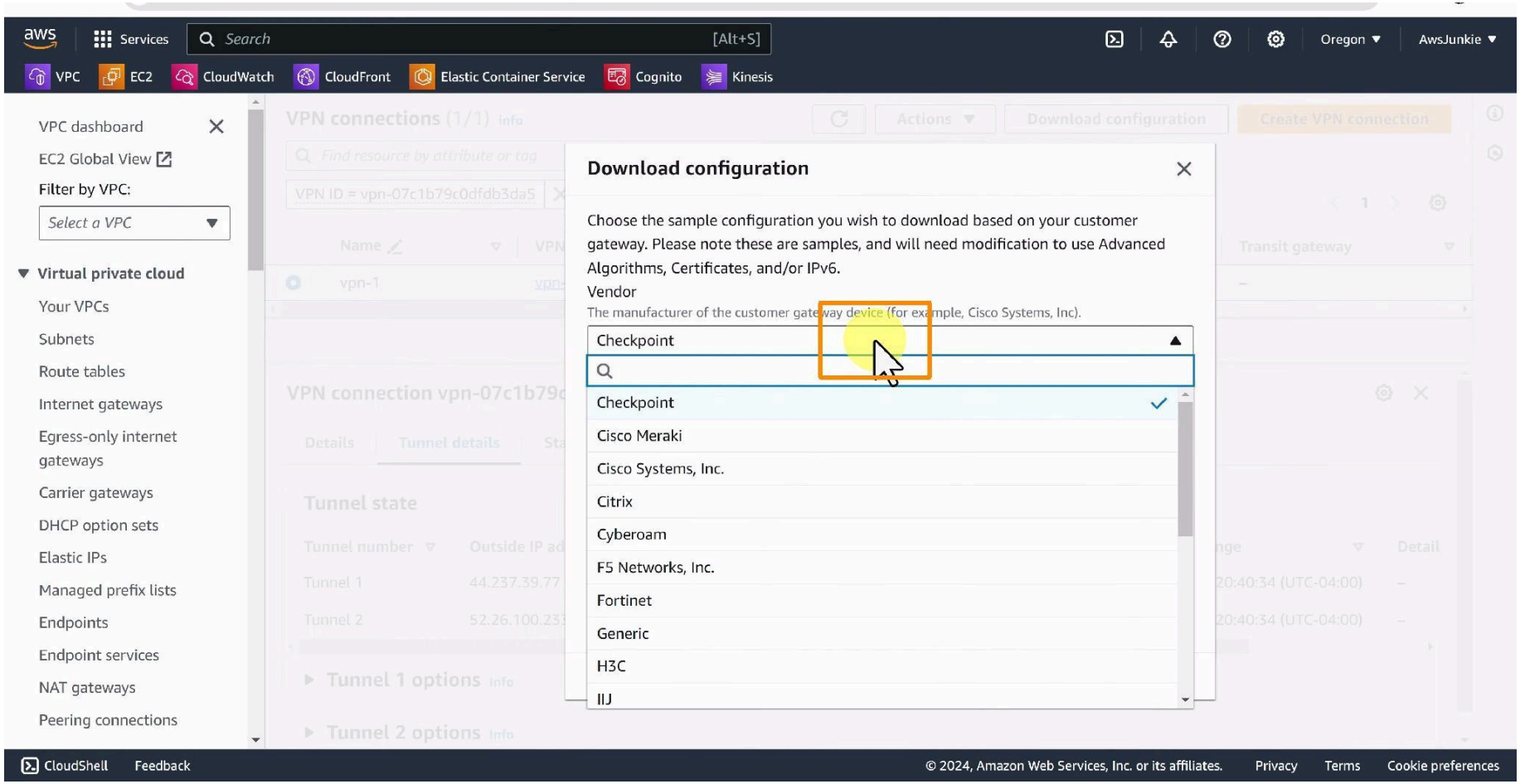
Bước 9

Kiểm tra VPN Connection: Click vào tab Tunnel Details. Thấy 2 tunnel đã được tạo nhưng trạng thái đang Down (vì chưa cấu hình phía on-prem).



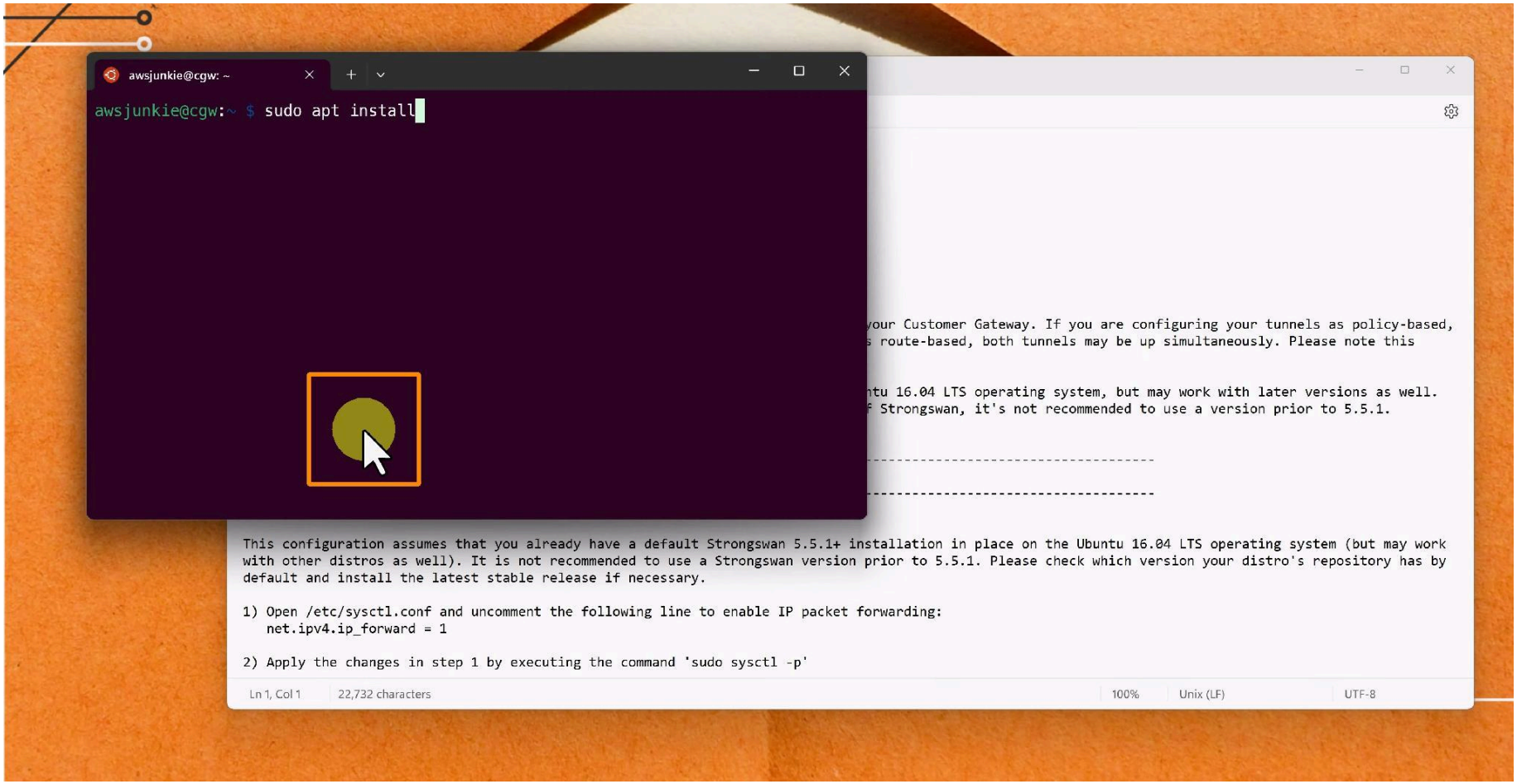
Bước 10

Download Configuration: Click 'Download Configuration'. Chọn Vendor = StrongSwan (hoặc vendor phù hợp với thiết bị của bạn). File này chứa toàn bộ thông tin cần cấu hình trên Customer Gateway device.



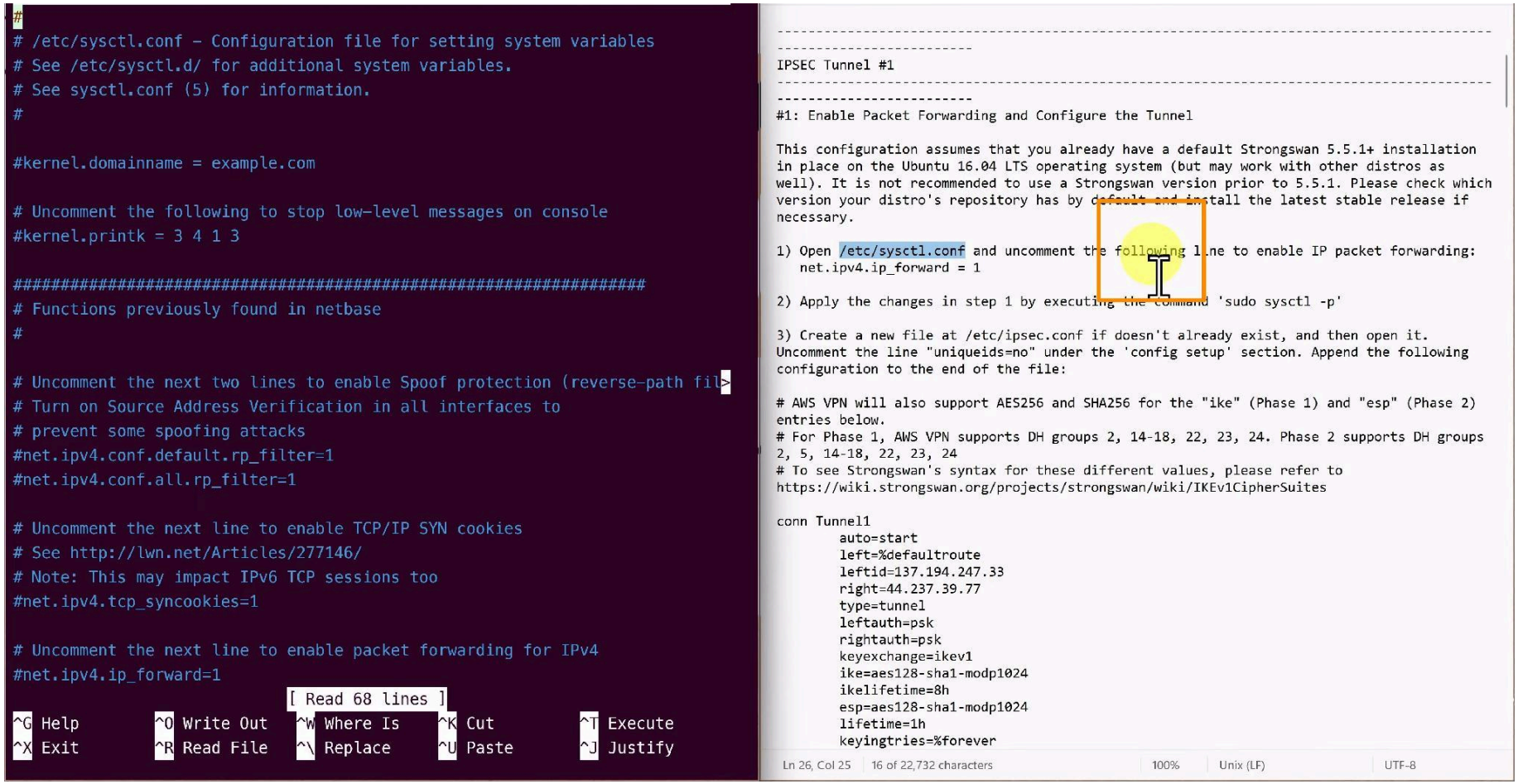
Bước 11

SSH vào Customer Gateway device (Raspberry Pi). Cài đặt StrongSwan: chạy lệnh 'sudo apt install strongswan'.



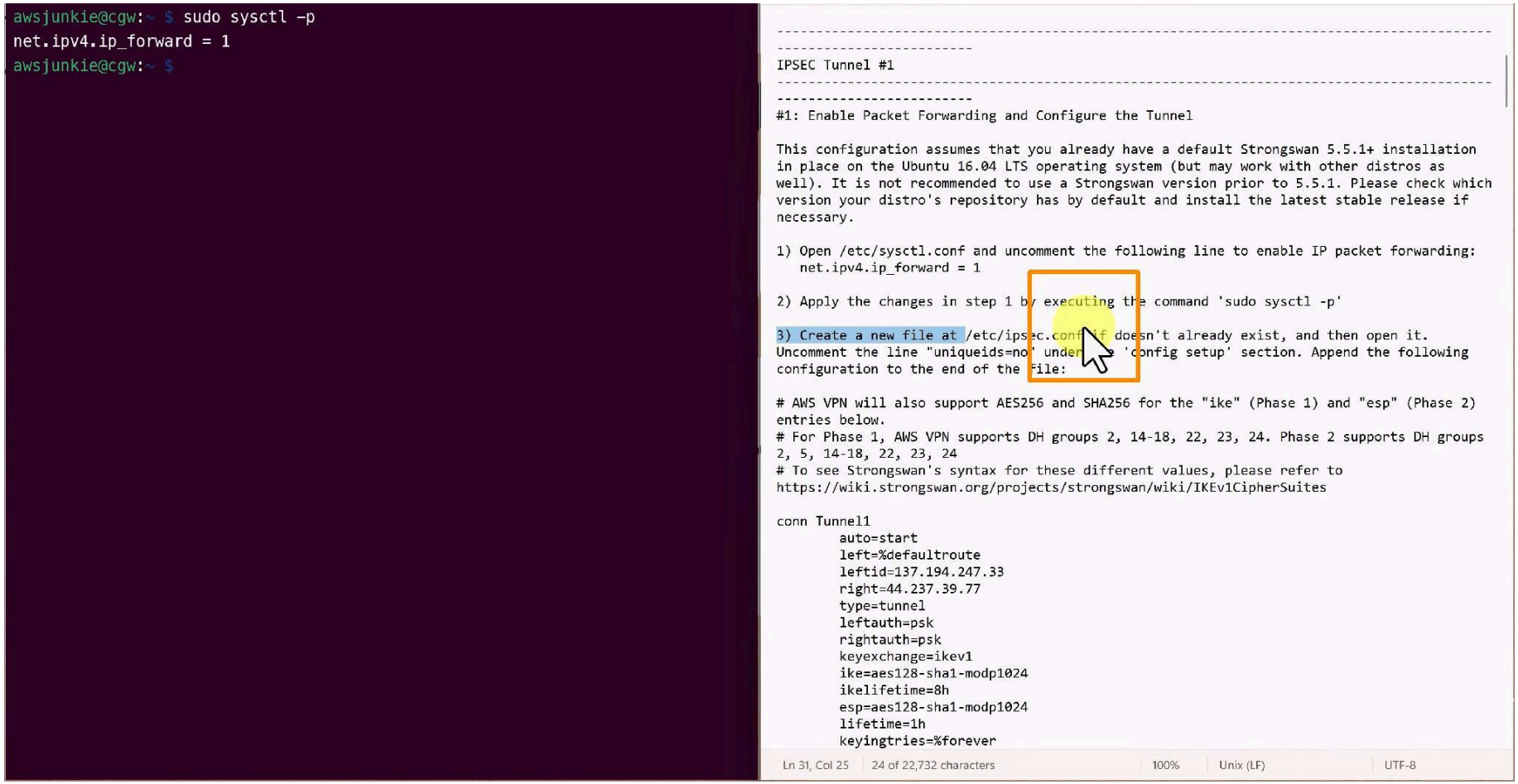
Bước 12

Bật IP Forwarding: Mở file /etc/sysctl.conf, uncomment dòng 'net.ipv4.ip_forward=1'. Lưu file. Apply bằng lệnh 'sudo sysctl -p'.



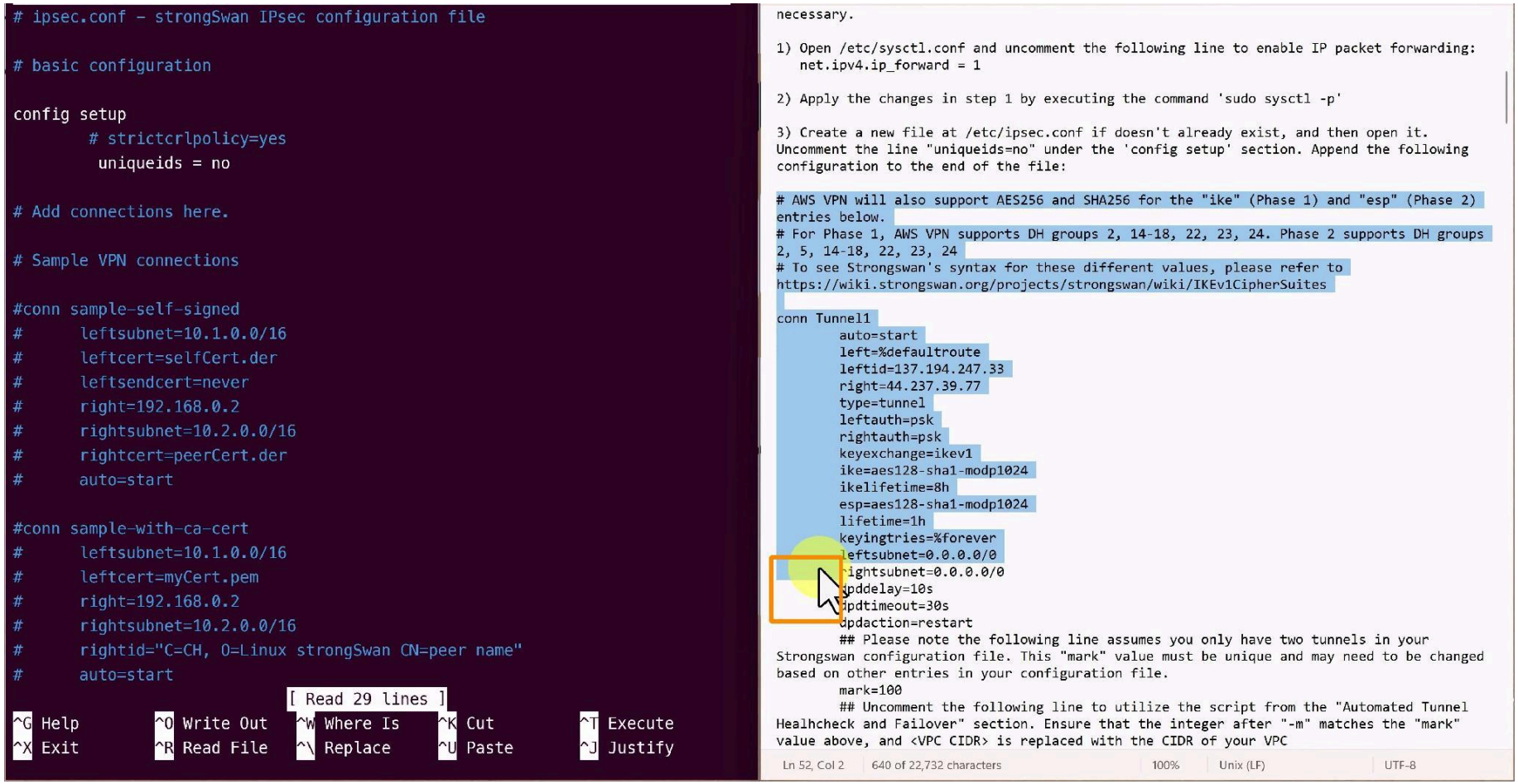
Bước 13

Cấu hình IPSec: Mở file /etc/ipsec.conf (tạo mới nếu chưa có). Uncomment dòng 'uniqueids = no'.



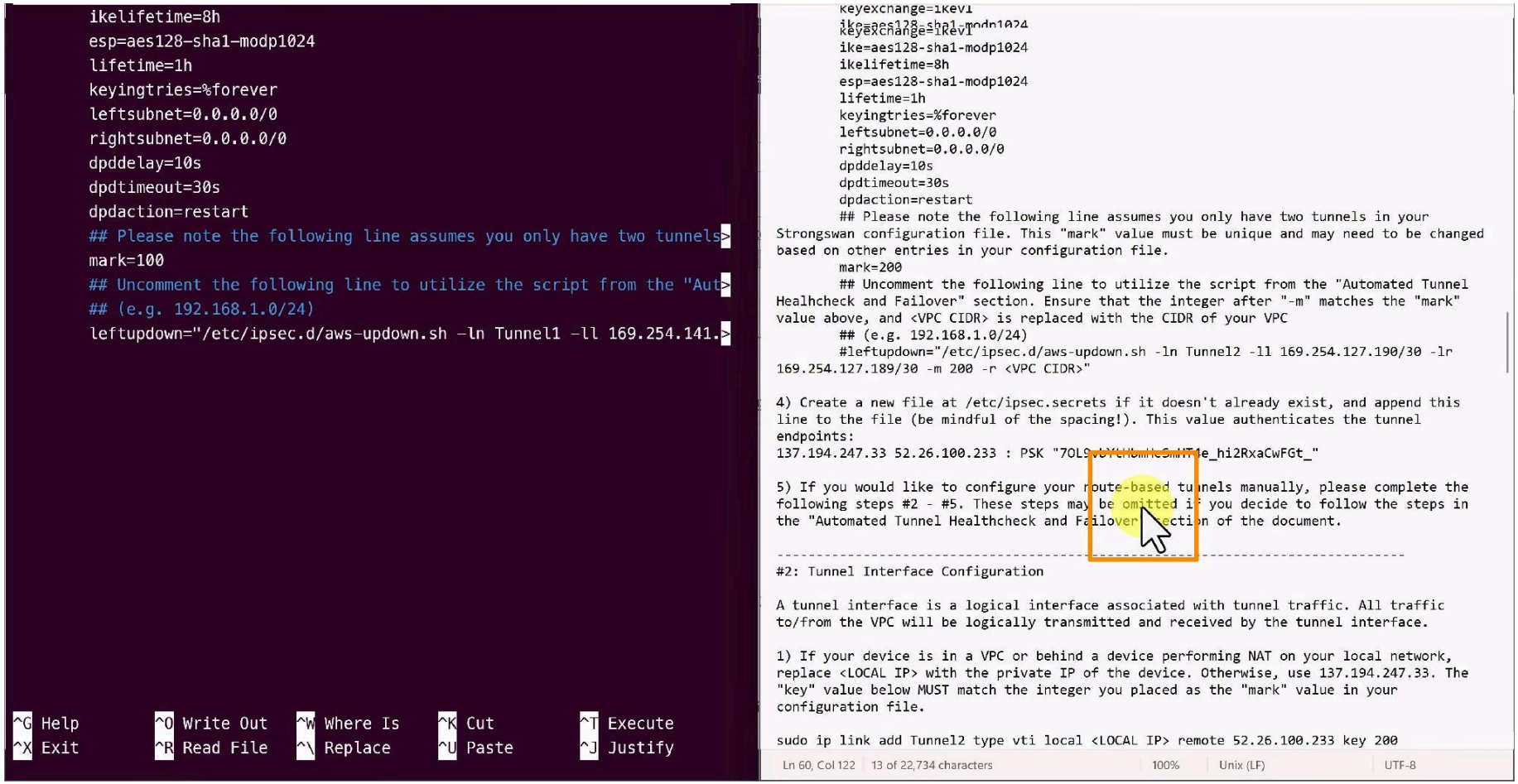
Bước 14

Copy cấu hình Tunnel 1 từ file configuration đã tải: Uncomment dòng 'leftupdown', thay CIDR range VPC side vào đúng vị trí. Copy toàn bộ section 'conn Tunnel1' và paste vào cuối file ipsec.conf.



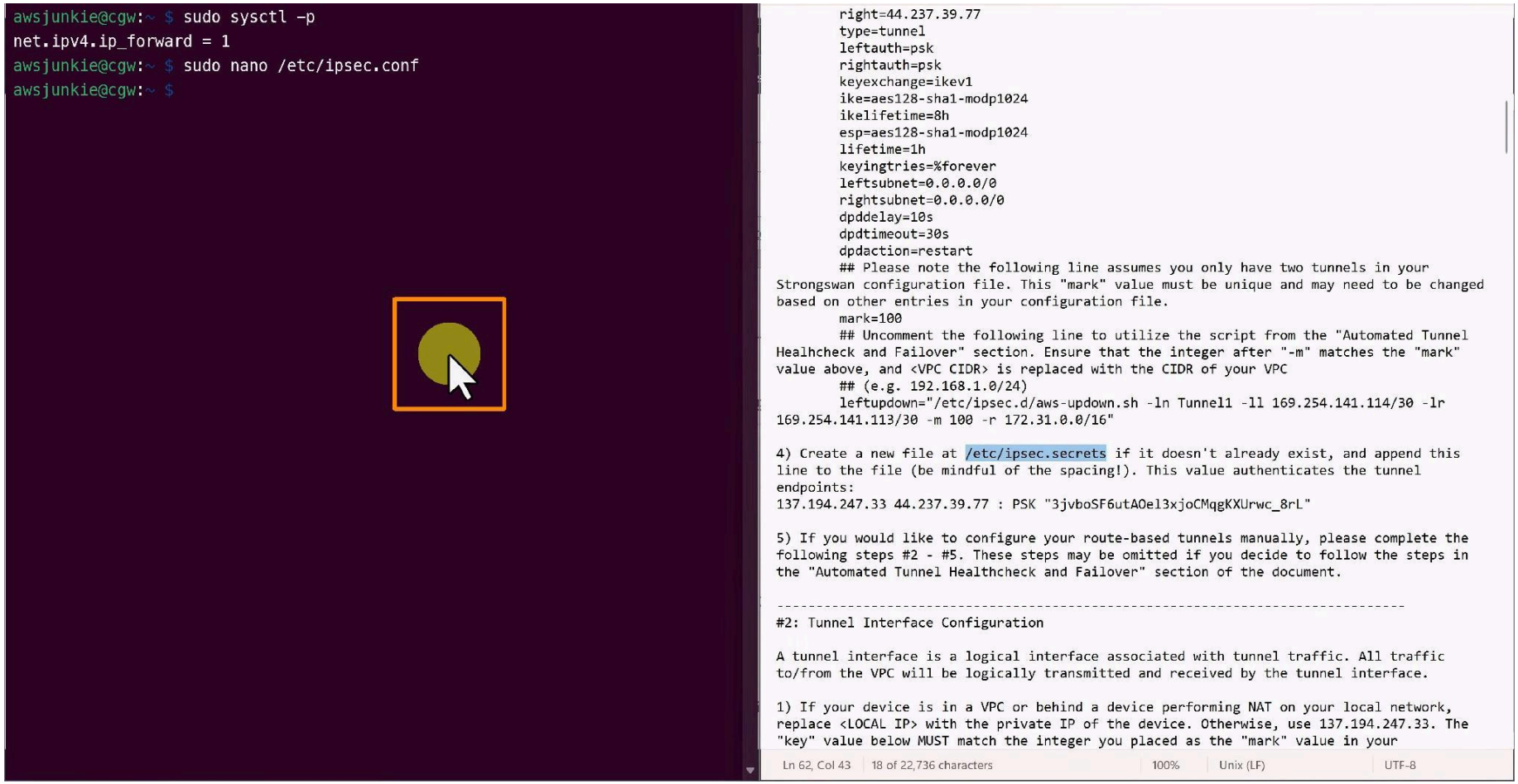
Bước 15

Copy cấu hình Tunnel 2: Làm tương tự - uncomment 'leftupdown', thay CIDR range, copy toàn bộ section 'conn Tunnel2' và paste vào cuối file ipsec.conf. Lưu file.



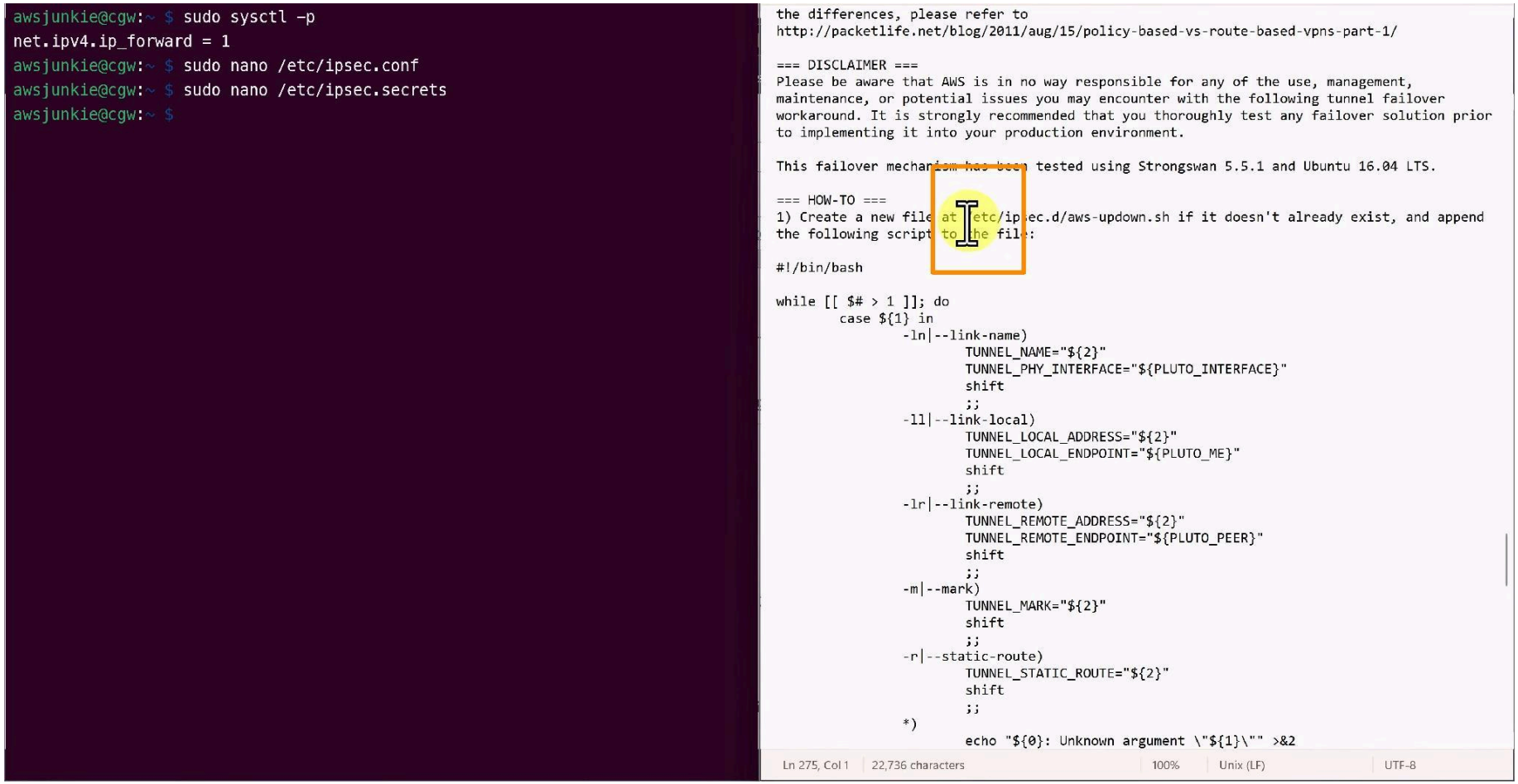
Bước 16

Cấu hình Shared Secrets: Mở file /etc/ipsec.secrets (tạo mới nếu chưa có). Copy Pre-Shared Key của Tunnel 1 và Tunnel 2 từ file configuration, paste vào file ipsec.secrets. Lưu file.



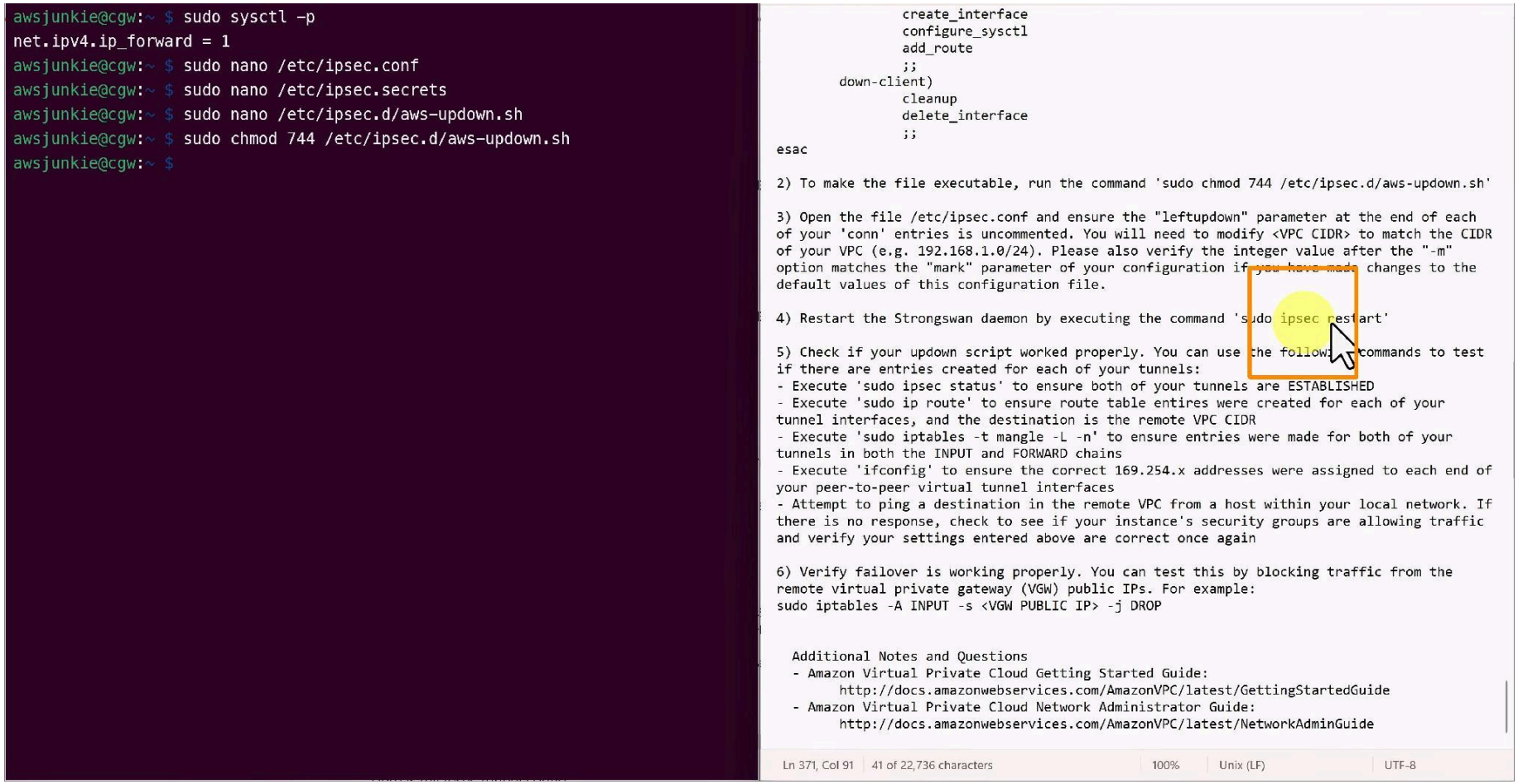
Bước 17

Tạo script Up/Down: Tạo file /etc/ipsec.d/aws-updown.sh. Copy toàn bộ script từ section 'Automated Tunnel Healthcheck and Failover' trong file config. Thêm dòng 'src [local IP]' vào cuối lệnh 'ip route add'. Lưu file và chmod +x để cấp quyền thực thi.



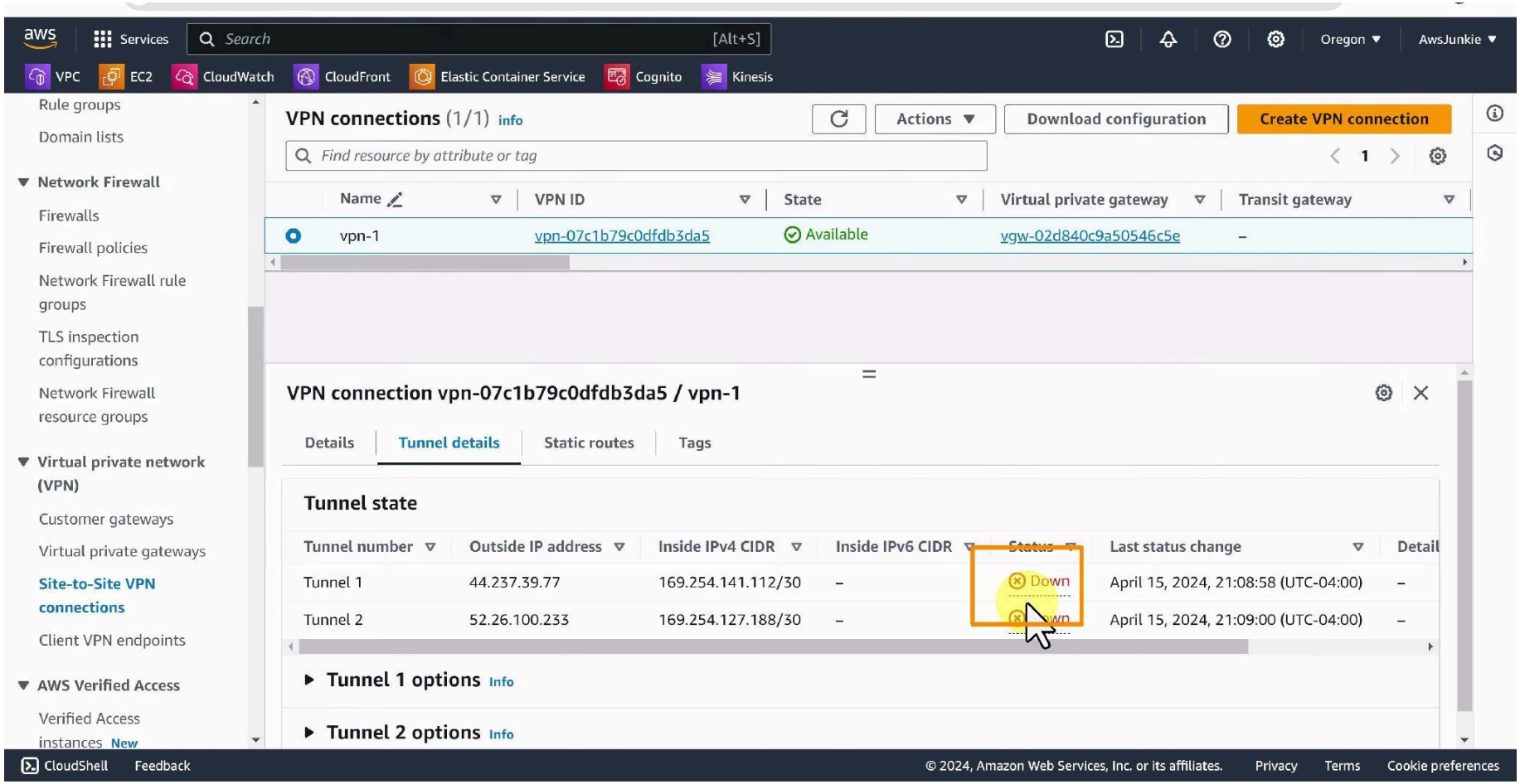
Bước 18

Khởi động lại StrongSwan: Chạy 'sudo ipsec restart'. Kiểm tra trạng thái: 'sudo ipsec status'. Kết quả hiển thị Tunnel 1 và Tunnel 2 đều ESTABLISHED.



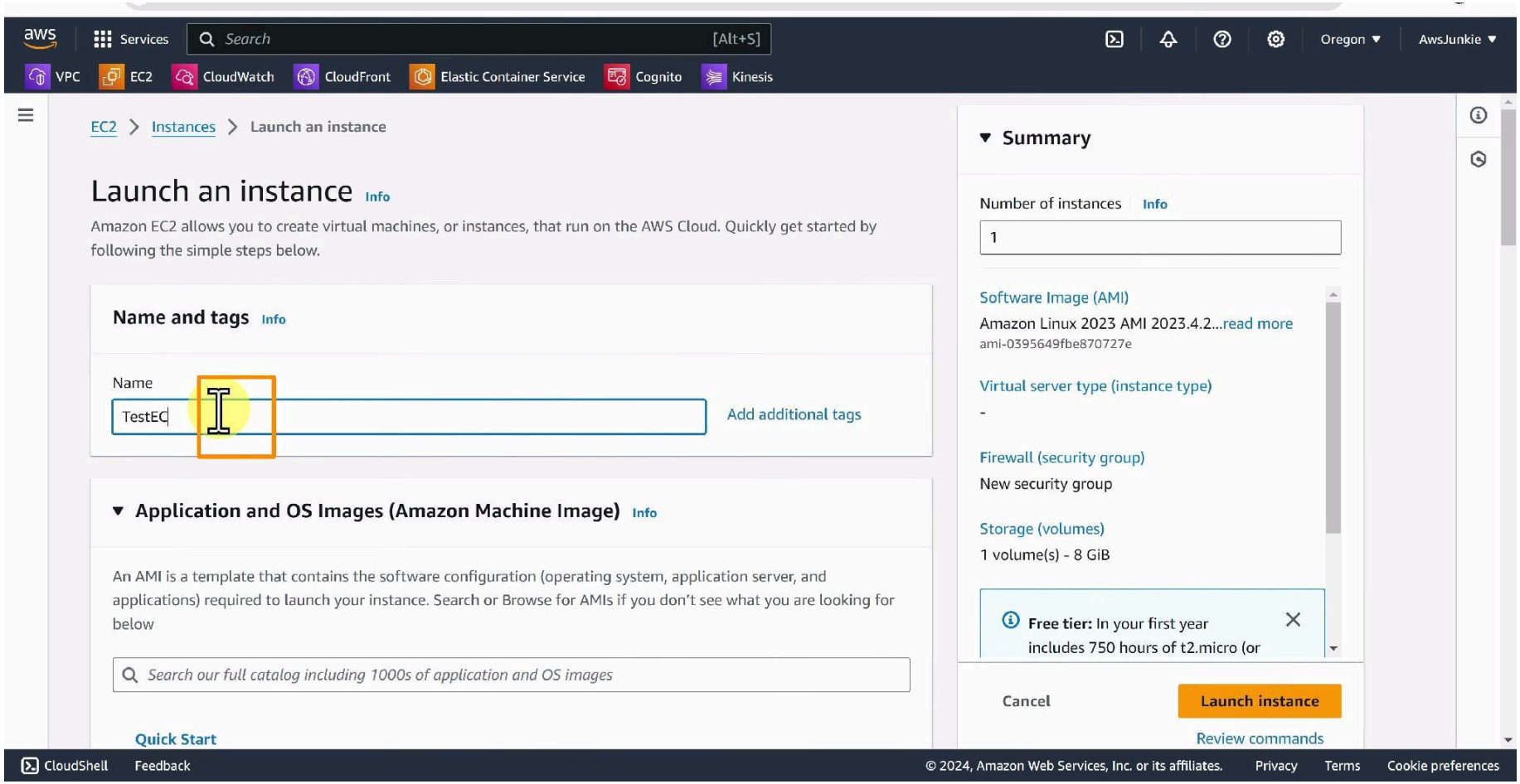
Bước 19

Xác nhận trên AWS Console: Quay lại VPN Connection → Click Refresh → Chọn VPN → Tab Tunnel Details: cả 2 tunnel đều hiện trạng thái UP.



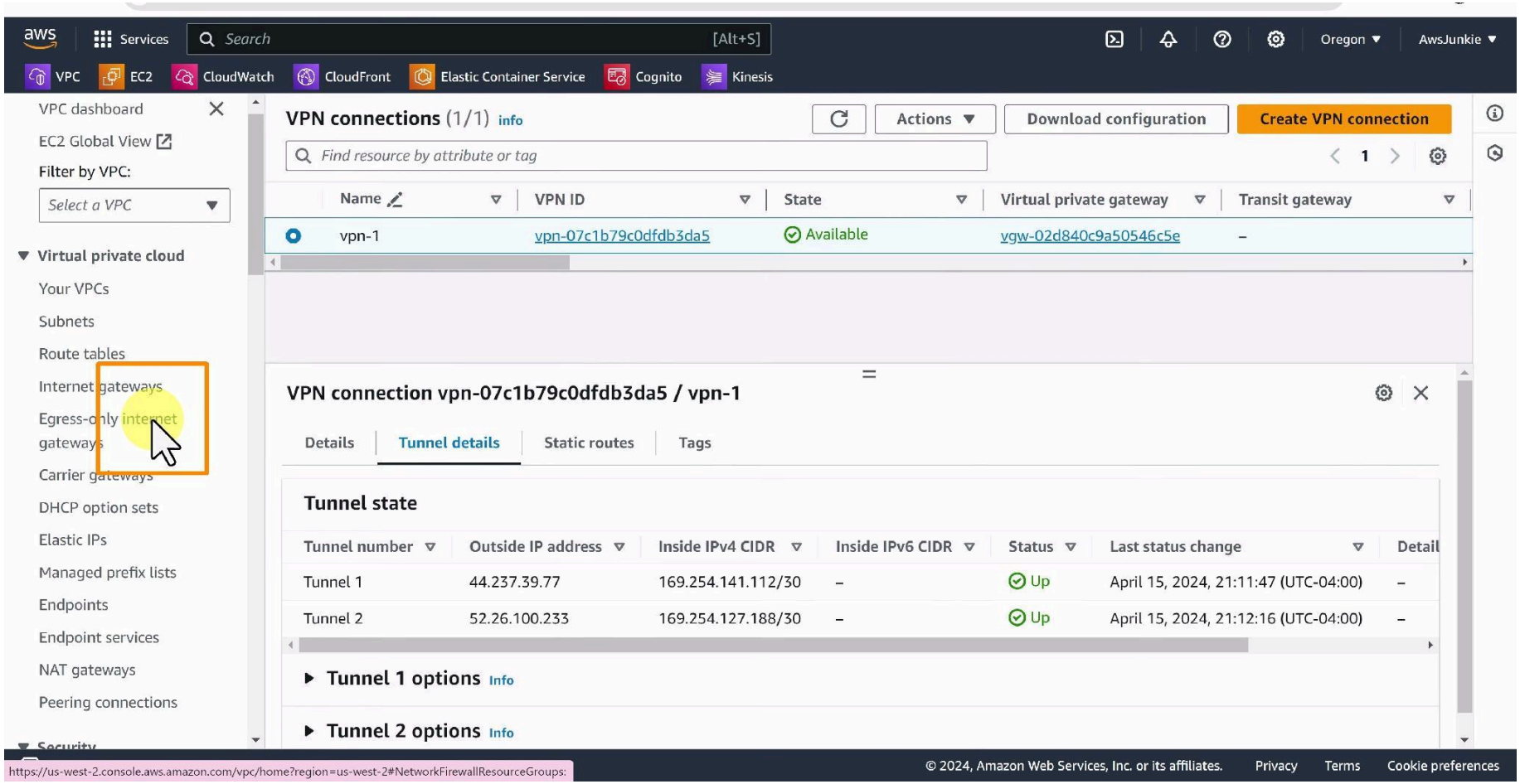
Bước 20

Tạo EC2 Instance để test: Launch Instance, đặt tên, proceed without key pair. Edit Network Settings: Disable auto-assign public IP. Security Group: Allow All ICMP từ CIDR range của on-prem data center. Click Launch.



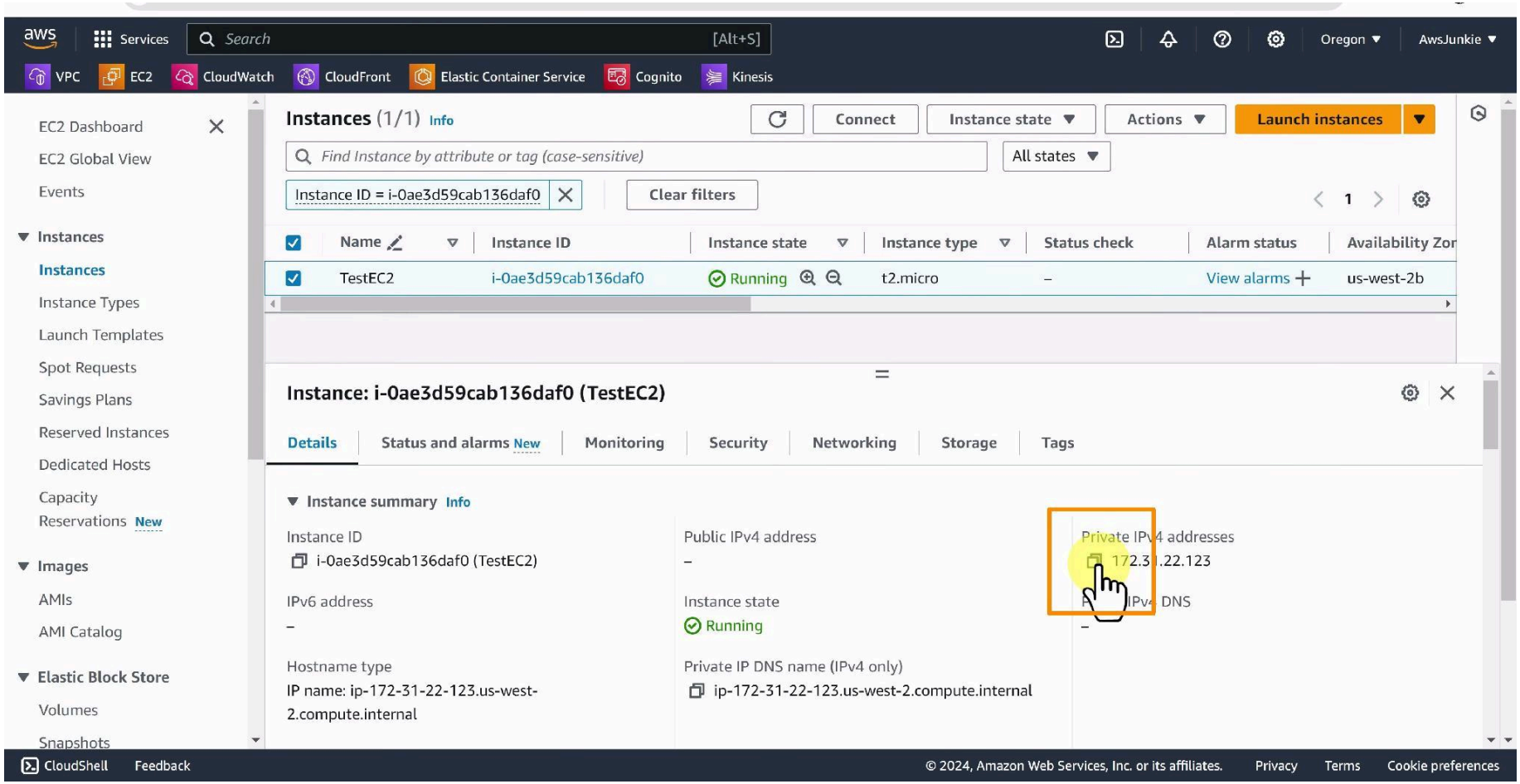
Bước 21

Cấu hình Route Table trong VPC: Vào VPC → Route Tables → Chọn route table → Tab Routes → Edit Routes → Add Route. Destination = CIDR on-prem (10.1.0.0/24), Target = Virtual Private Gateway. Save changes.



Bước 22

[KIỂM TRA] Copy Private IP của EC2 instance. Từ terminal trên Customer Gateway (on-prem), chạy lệnh 'ping [Private IP EC2]'. Kết quả: Ping thành công qua private IP → VPN Site-to-Site hoạt động!


aws
Services
Search
[Alt+S]
Oregon
AwsJunkie
VPC
EC2
CloudWatch
CloudFront
Elastic Container Service
Cognito
Kinesis
EC2 Dashboard
EC2 Global View
Events
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations New
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
Snapshots
Instances (1/1) Info
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
All states
Instance ID = i-0ae3d59cab136daf0
Clear filters
1
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zor
TestEC2
i-0ae3d59cab136daf0
Running
t2.micro
–
View alarms
us-west-2b
Instance: i-0ae3d59cab136daf0 (TestEC2)
Details
Status and alarms New
Monitoring
Security
Networking
Storage
Tags
Instance summary Info
Instance ID
i-0ae3d59cab136daf0 (TestEC2)
Public IPv4 address
–
Private IPv4 addresses
172.31.22.123
IPv6 address
–
Instance state
Running
Private IP DNS name (IPv4 only)
ip-172-31-22-123.us-west-2.compute.internal
Hostname type
IP name: ip-172-31-22-123.us-west-2.compute.internal
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences