

# SECURE VPN DEPLOYMENT ON AWS USING EC2 & OPENVPN

Proof-of-Concept Documentation (DO NOT use as-is in production)

**Collaborators:** Nicolas Portilla Gomez | Joshua Shapiro | Andrew Enright

**Version:** 1.0 | **Date:** 07 06 2025

## TABLE OF CONTENTS

- 1. INTRODUCTION ..... 2
- 2. Architecture overview ..... 2
- 3. prerequisites ..... 2
- 4. implementation steps ..... 2
  - 4.1 Launch EC2 Instance..... 2
  - 4.2 Configure Security Groups ..... 3
  - 4.3 Install & Configure OpenVPN ..... 4
  - 4.4 Transfer Client Configuration File ..... 4
  - 4.5 Connect to VPN ..... 5
- 5. cost & security considerations ..... 5
- 6. outcome & verification ..... 5
- 7. future enhancements..... 6
- 8. appendix..... 6
  - Appendix A – OpenVPN Connection Status ..... 6
  - Appendix B – Public IP Verification After VPN Connection ..... 6

# 1. INTRODUCTION

This documentation outlines the process of deploying a secure VPN server on AWS EC2 using OpenVPN. Readers will learn how to provision an EC2 instance, configure OpenVPN, and securely connect client devices to route traffic through AWS.

## 2. ARCHITECTURE OVERVIEW

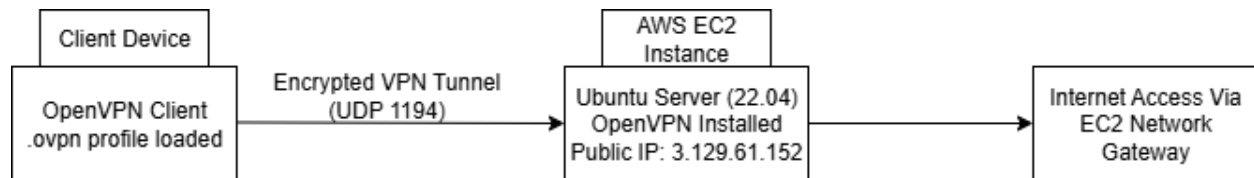


Figure 1: Project Network Diagram

## 3. PREREQUISITES

Item	Notes
AWS Account (Free Tier)	IAM user with EC2 & Security Group Permissions
OpenVPN Client	Installed locally (Windows, macOS, or Linux)
SSH Client	PuTTY or OpenSSH for EC2 access
.ovpn profile	Generated after server setup

## 4. IMPLEMENTATION STEPS

### 4.1 Launch EC2 Instance

1. Navigate to EC2 -> Launch Instance.

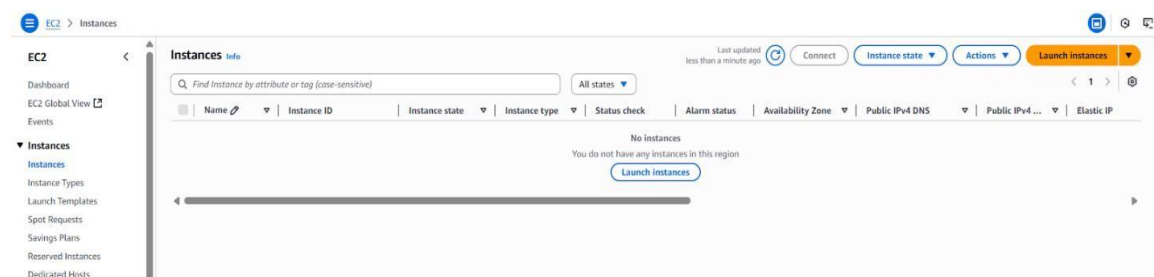


Figure 2: AWS EC2 Instance Dashboard

2. AMI: Ubuntu Server 22.04 LTS

Name and tags

Info

Name

OpenVPN-Server

Add additional tags

▼ Application and OS Images (Amazon Machine Image)

Info

An AMI contains the operating system, application server, and applications for your instance. If you don't see a suitable AMI below, use the search field or choose

Browse more AMIs.

Q Search our full catalog including 1000s of application and OS images

Recents

Quick Start

Amazon Linux

aws

macOS

Mac

Ubuntu

ubuntu

Windows

Microsoft

Red Hat

Red Hat

SUSE Linux

SUSE

Debian

debian

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Ubuntu Server 22.04 LTS (HVM), SSD Volume Type

ami-0b05d988257befb8b6 (64-bit (x86)) / ami-0c96d7d095577f8de (64-bit (Arm))

Virtualization: hvm    ENA enabled: true    Root device type: ebs

Free tier eligible

Figure 3: AMI Selection

- Instance type: t2.micro (Free Tier)
- Configure key pair for SSH access.

▼ Instance type

Info | Get advice

Instance type

t2.micro

Free tier eligible

Family: t2    1 vCPU    1 GiB Memory    Current generation: true

On-Demand Ubuntu Pro base pricing: 0.0134 USD per Hour    On-Demand Linux base pricing: 0.0116 USD per Hour

On-Demand SUSE base pricing: 0.0116 USD per Hour    On-Demand Windows base pricing: 0.0162 USD per Hour

On-Demand RHEL base pricing: 0.026 USD per Hour

All generations

Compare instance types

Additional costs apply for AMIs with pre-installed software

▼ Key pair (login)

Info

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - required

OpenVPNTest2

Create new key pair

Figure 4: Instance Type & Key Pair

## 4.2 Configure Security Groups

- Allow inbound traffic:
  - UDP 1194 (OpenVPN)
  - TCP 22 (SSH)
- Restrict source IP ranges for security.

**Inbound Security Group Rules**

▼ Security group rule 1 (TCP, 22, 0.0.0.0/0) Remove

<b>Type</b> <a href="#">Info</a>	<b>Protocol</b> <a href="#">Info</a>	<b>Port range</b> <a href="#">Info</a>
ssh	TCP	22
<b>Source type</b> <a href="#">Info</a>	<b>Source</b> <a href="#">Info</a>	<b>Description - optional</b> <a href="#">Info</a>
Custom	<input type="text" value="Add CIDR, prefix list or security group"/> <input type="text" value="0.0.0.0/0"/>	e.g. SSH for admin desktop

▼ Security group rule 2 (UDP, 1194, 0.0.0.0/0) Remove

<b>Type</b> <a href="#">Info</a>	<b>Protocol</b> <a href="#">Info</a>	<b>Port range</b> <a href="#">Info</a>
Custom UDP	UDP	1194
<b>Source type</b> <a href="#">Info</a>	<b>Source</b> <a href="#">Info</a>	<b>Description - optional</b> <a href="#">Info</a>
Custom	<input type="text" value="Add CIDR, prefix list or security group"/> <input type="text" value="0.0.0.0/0"/>	e.g. SSH for admin desktop

Add security group rule

Figure 5: Security Group Rules

## 4.3 Install & Configure OpenVPN

1. Download OpenVPN install script
  - Bash `curl -O (install script)`

```
ubuntu@ip-172-31-30-161:~$ curl -O https://raw.githubusercontent.com/angristan/openvpn-install/master/openvpn-install.sh
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload   Total   Spent    Left   Speed
100 42167  100 42167    0     0  199k      0  --:--:-- --:--:-- --:--:-- 200k
```

Figure 6: Downloading OpenVPN Install Script

2. Give the script permission to run and run it
  - `Chmod +x openvpn-install.sh`
  - `Sudo ./openvpn-install.sh`

```
ubuntu@ip-172-31-30-161:~$ chmod +x openvpn-install.sh
ubuntu@ip-172-31-30-161:~$ sudo ./openvpn-install.sh
Welcome to the OpenVPN installer!
```

Figure 7: Running Installation Script

## 4.4 Transfer Client Configuration File

1. Use SCP or WinSCP to download .ovpn file from server to local machine



 OpenVPNTes2.pem	8/5/2025 4:22 PM	PEM File	2 KB
 client1.ovpn	8/5/2025 4:45 PM	OVPN Profile	0 KB

Figure 8: Generated Keys and Profiles

## 4.5 Connect to VPN

1. Import .ovpn file into OpenVPN Client.
2. Connect and verify traffic is routed through EC2 instance.

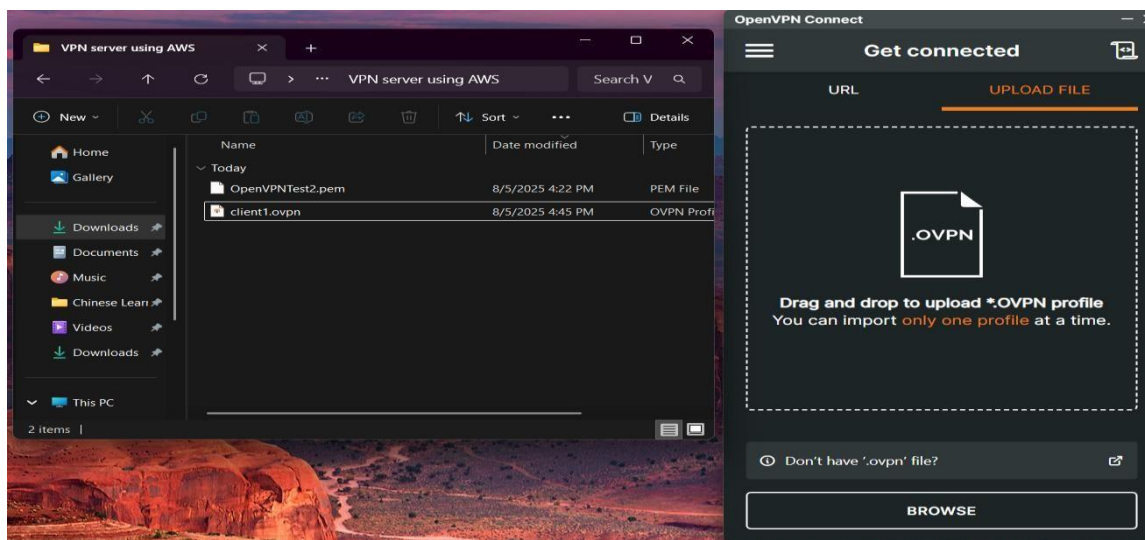


Figure 9: Importing VPN Profile

## 5. COST & SECURITY CONSIDERATIONS

Service	Free Tier?	Approx. Monthly Cost
EC2 t2.micro	Yes (750 hrs)	~0.00 (Free Tier)
Data transfer	Partial	Varies with usage

- Use IAM least privilege roles for EC2.
- Consider fail2ban or AWS WAF for SSH brute-force protection.
- Implement firewall rules to limit access.

## 6. OUTCOME & VERIFICATION

- VPN tunnel was established between client and AWS EC2. (See Appendix A)
- Verified public IP change using whatismyip.com. (See Appendix B)

## 7. FUTURE ENHANCEMENTS

- Automate setup with AWS CDK or Terraform.
- Implement MFA-based VPN authentication.
- Enable CloudWatch logs for monitoring.
- Configure certificate-based authentication.

## 8. APPENDIX

### Appendix A – OpenVPN Connection Status

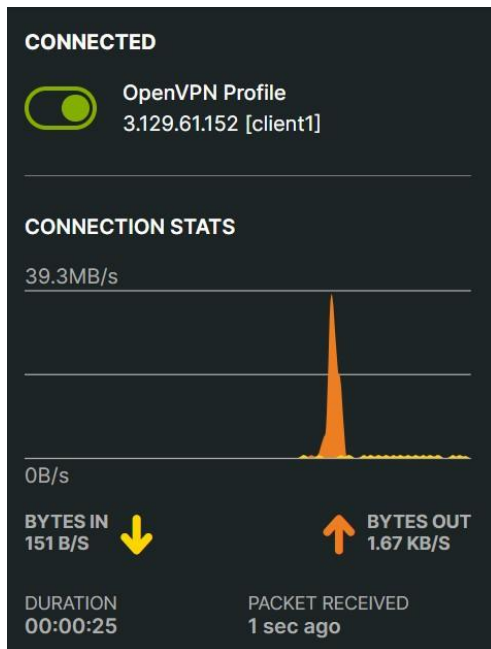


Figure 10: OpenVPN Connection Status

### Appendix B – Public IP Verification After VPN Connection

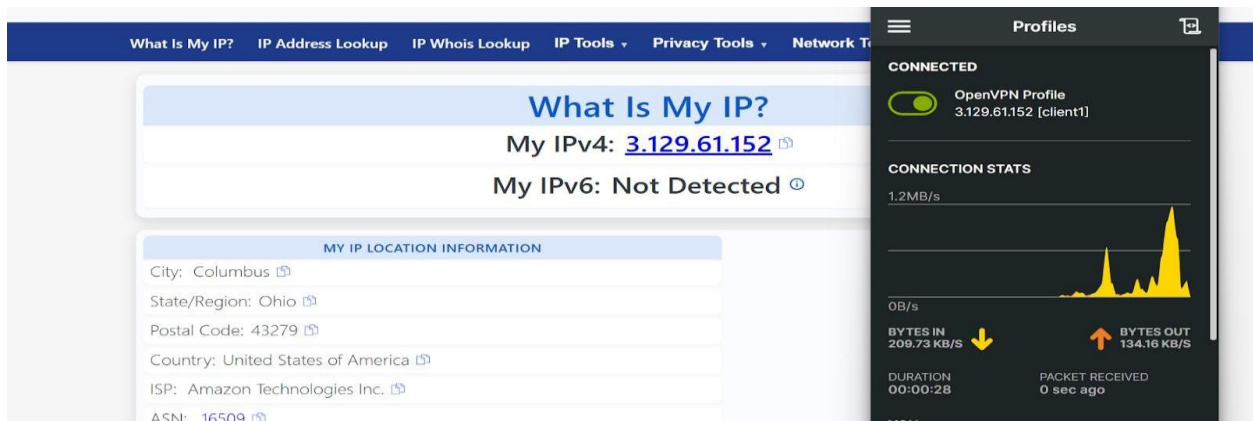


Figure 11: VPN IP Address Verification