Futuralis

Futuralis SoftEther VPN (Remote Access)

Complete Setup

&

Client Guide

Aravind Pamula | Sales | apamula@futuralis.com

Table of Contents

1 Introduction

Futuralis SoftEther VPN AMI lets you deploy a secure remote access VPN on AWS in just minutes. This guide covers everything from launching your VPN server, securing it, and connecting with Windows/Mac clients.

2 Subscribe and Launch Your VPN AMI

2.1 Subscribe to the AMI

- Visit the Futuralis SoftEther VPN AMI on AWS Marketplace.
- Click **Continue to Subscribe** to start your subscription.
- Review the pricing and terms, then select **Continue to Configuration** to proceed with your deployment.

2.2 Launch a New EC2 Instance

- Choose your preferred AWS region.
- Under "Fulfillment Option," select the latest version, and click **Continue to Launch**.
- Choose **Launch through EC2.**

2.3 EC2 Instance Configuration

- Instance Type
  - Recommended Minimum: t3.medium (2 vCPU, 4 GB RAM)
  - For higher performance or more users, select a larger instance type (e.g., t3.large, m6a.large, or higher).
- EBS Root Volume
  - 20 GB gp3 (General Purpose SSD)
- Subnet & VPC
  - Select a **public subnet** in your VPC to ensure the VPN server is accessible from the internet.

- Public IP
    - Assign a public IP at launch
- IAM Role (Advanced)
    - Attach an SSM-enabled IAM role (instance profile) if you wish to use AWS Systems Manager for advanced administration.
- Key Pair
    - Select an existing SSH key pair, or create a new one, to enable SSH access to the EC2 instance.
- Security Group
    - Define required **inbound rules** for VPN and management ports.
        - TCP 22: SSH (admin only, restrict to your IP)
        - TCP 443: VPN SSL/Management UI (open as needed)
        - UDP 500, 4500, 1701: L2TP/IPsec (for mobile clients)
        - TCP 5555: Web admin (optional, restrict to admin IP)
        - TCP 992: Legacy VPN client
    - Ensure **outbound rules** permit internet access.
        - Allow all outbound traffic (default AWS SG config), unless you have stricter requirements.
- Elastic IP (Recommended)
    - After instance launch, allocate and associate an **Elastic IP** using the EC2 Console.
    - An Elastic IP ensures your VPN server's public IP remains constant, even after reboots or stops.

3 Connect to Your EC2 Server

3.1 SSH to Your Server

- Open a terminal and run:
  - ssh ec2-user@<your-elastic-ip>

    (Use the SSH key you chose at launch)
- Windows **users**: You can use PuTTY to connect (enter Elastic IP, username ec2-user, and your private key).
- AWS **Console**: Go to your EC2 instance, click **Connect**, and follow the options for **EC2 Instance Connect** or **Session Manager** if enabled.

3.2 Set the VPN Admin Password

- Run:
  - sudo /usr/local/scripts/set-vpn-admin.sh
- Follow the prompt to set a strong admin password.

3.3 Create Your First VPN User

- Run:
  - sudo /usr/local/scripts/add-vpn-user.sh
- Enter the VPN username and password as prompted.

3.4 Set the IPSec Pre-shared Key (PSK)

- Run:
    - sudo /usr/local/scripts/set-vpn-psk.sh
- Choose a PSK (recommended: max 9 characters for compatibility).

4 Download and Configure Your VPN Client

4.1 Windows Setup

- Download the **SoftEther VPN Client** and **Server Manager** from SoftEther Download Page.

- For setup steps and screenshots, see: **Windows VPN Setup Guide**

4.2 Mac Setup

- Use the built-in **L2TP over IPsec** client (System Settings → Network → Add VPN).

- For a detailed walkthrough, see: **Mac VPN Setup Guide**

5 Advanced VPN Server Management

5.1 List All VPN Users

```
sudo /usr/local/vpnserver/vpncmd localhost /SERVER /HUB:VPNVirtualHub /CMD UserList
```

5.2 Delete a VPN User

```
sudo /usr/local/vpnserver/vpncmd localhost /SERVER /HUB:VPNVirtualHub /CMD UserDelete <username>
```

5.3 Lock/Unlock a VPN User

```
sudo /usr/local/vpnserver/vpncmd localhost /SERVER /HUB:VPNVirtualHub /CMD UserLock <username>
```

```
sudo /usr/local/vpnserver/vpncmd localhost /SERVER /HUB:VPNVirtualHub /CMD UserUnlock <username>
```

6 Security & Best Practices

- **Restrict SSH & Web admin ports to your IP** for maximum safety.
- Change admin/user passwords regularly.
- If exposing the VPN UI (443/5555), consider limiting by IP or using MFA.
- Do not share admin or user credentials.
- Remove or rotate unused users promptly.
- Always assign an Elastic IP for stable client access.

7 Support & Further Help

Need help automating deployments, integrating with SSO, or troubleshooting your VPN? **Futuralis is here to help – just one click away!**

- Email: support@futuralis.com
- Contact: futuralis.com/contact-us

Our experts can assist with advanced automation, custom VPN solutions, and secure enterprise deployments.