AWS Static Website Deployment Guide (Detailed)

1. Create Security Group
• Find Security Group in EC2 Sidebar
• Add inbound rules: HTTP, HTTPS (Anywhere IPv4), SSH (My IP)
• Outbound rules: All Traffic → Anywhere IPv4
• Click Create Security Group

2. Launch EC2 Instance
• EC2 → Launch Instance
• Choose OS: Windows (.NET), macOS (Cloud/Robo), Linux (General)
• Popular Linux: Ubuntu, Amazon Linux, Debian etc.
• Create Key Pair (.ppk format)
• Attach Security Group

3. Connect Using PuTTY
• Hostname = Your Public IP
• Load .ppk key: SSH → Auth → Credentials
• Save session and Open

4. Install Nginx
sudo apt update
sudo apt install nginx

5. Upload Files with FileZilla
• Add .ppk to SFTP settings
• Connect using host, username, port 22
• Go to /var/www/html
• sudo chown ubuntu /var/www/html
• Upload your website files

6. Setup Route53
• Create hosted zone using domain
• A Record → Public IP
• CNAME → www → root domain

7. Domain Provider DNS
• Edit Type A → Add server IP

8. Free SSL (Certbot)
sudo apt install certbot python3-certbot-nginx
sudo certbot --nginx -d example.com -d www.example.com
sudo certbot renew --dry-run

Flowchart (Text Diagram)
Start → Create Security Group → Launch EC2 Instance → Connect via PuTTY → Install Nginx → Upload Website → Setup DNS → SSL Setup → Website Live

Quick Revision Notes

1. Create SG → Allow HTTP/HTTPS + SSH
2. Launch EC2 → Linux + Key Pair (.ppk)
3. Connect PuTTY → Load key → Login
4. Install Nginx → apt update + apt install nginx
5. File Upload → /var/www/html → chown → upload
6. DNS: A Record = IP, CNAME = www
7. SSL → certbot --nginx

Short Flowchart:
Security Group → EC2 → PuTTY → Nginx → Upload → DNS → SSL → Done