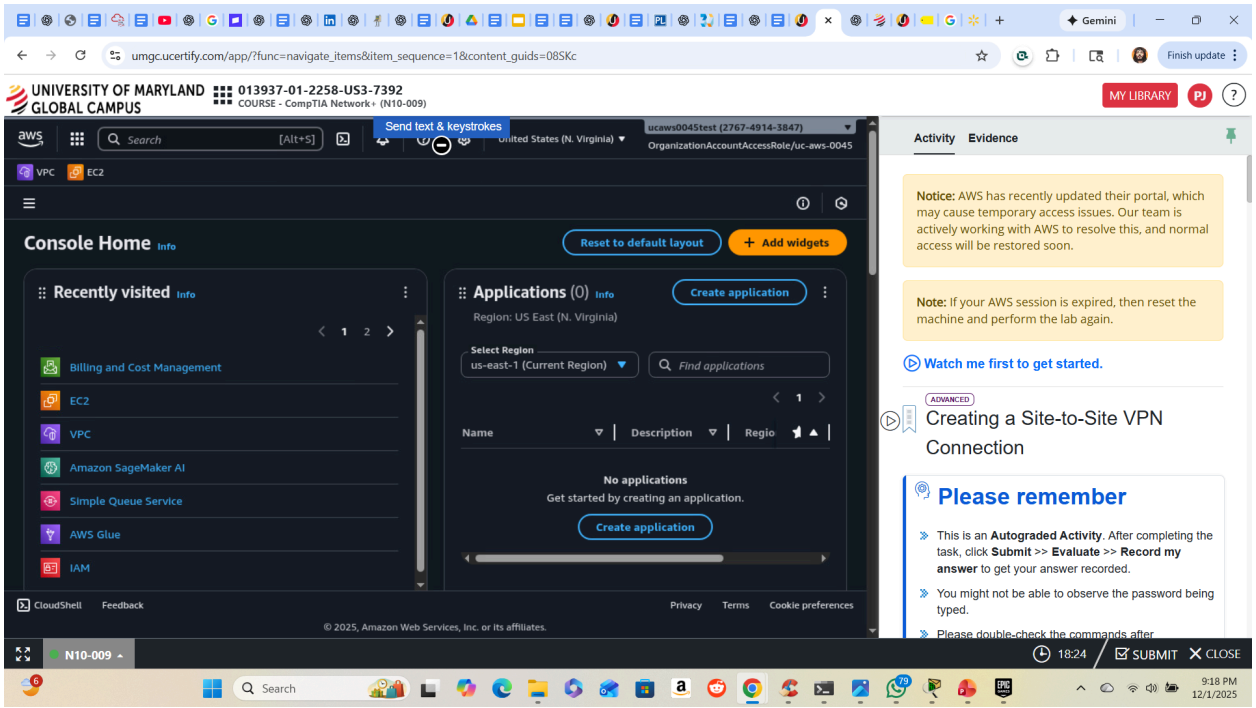
Name: Pelumi Johnson
Date: 12/2/2025
Course: CMIT 265 | Fundamentals of Networking
Platform: AWS (uCertify Lab Environment)

Project

The objective of this lab was to create a secure site to site VPN connection between an on-premises network (simulated Customer Gateway) and an AWS Virtual Private Cloud (VPC). Through this project, I learned how organizations interconnect distributed networks over the public internet using encrypted tunnels.

By the end of the lab, I was able to:

- Create a Virtual Private Gateway (VGW) for an AWS VPC
- Create a Customer Gateway (CGW) representing an on-premises router
- Configure a Site-to-Site VPN connection using IPSec tunneling
- Customize tunnel settings including Pre-Shared Keys and Inside CIDR ranges
- Verify successful deployment of the VPN connection in AWS



Tool and Service Used

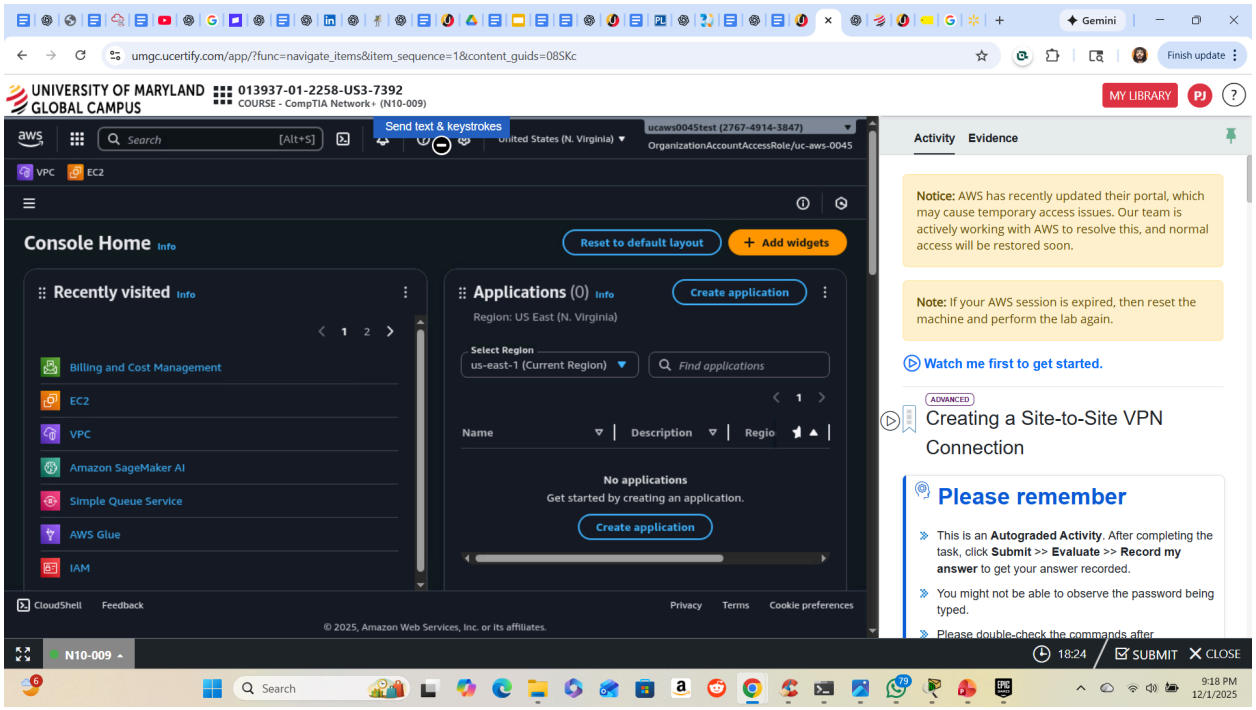
- **AWS Console:** Management interface for creating network resources
- **Amazon VPC:** Provides isolated networking infrastructure in AWS
- **Virtual Private Gateway (VGW):** AWS-side VPN endpoint
- **Customer Gateway (CGW):** Represents the on-premises router
- **Site-to-Site VPN service:** Establishes encrypted IPSec connections
- **IPSec Tunnels:** Mechanism used to create secure encrypted communications

Step by Step Project Procedure:

Step 1:

Navigate to AWS Console Home

You start on the AWS Console. Ensure your Region is set to US-East-1 (N. Virginia). This region selection matters because your VPC and VPN resources must all exist in the same region for the lab to work.



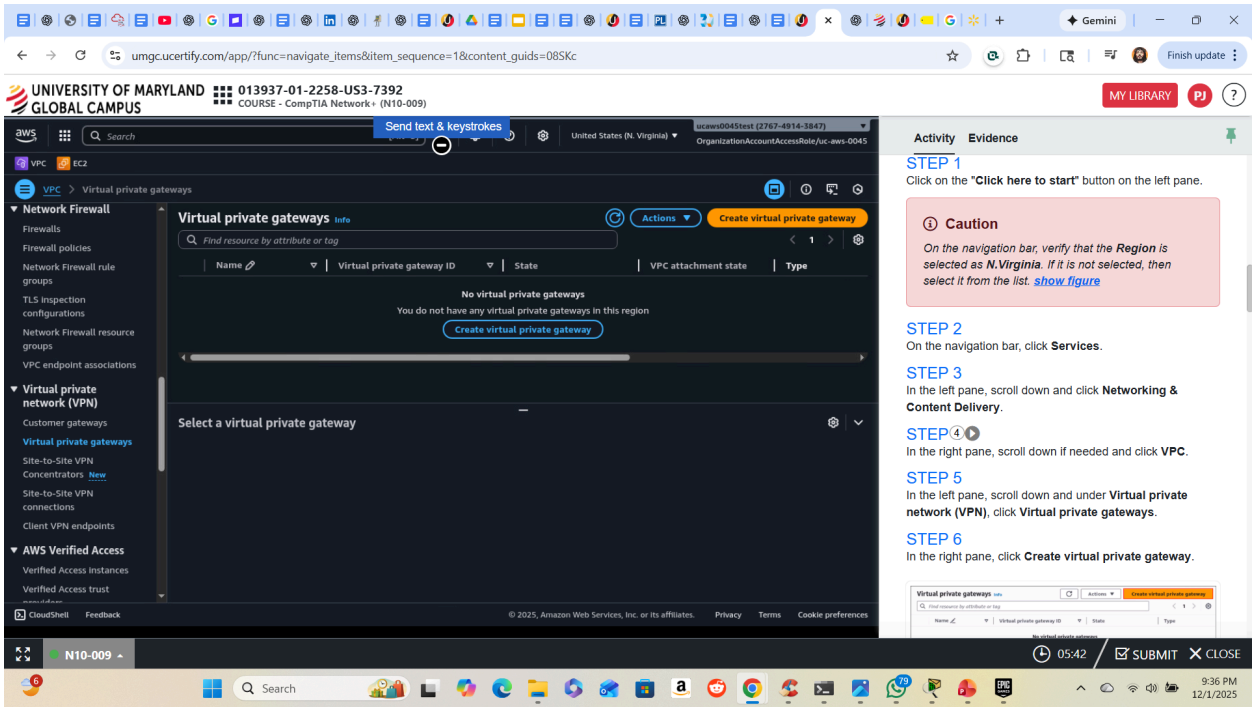
Step 2:

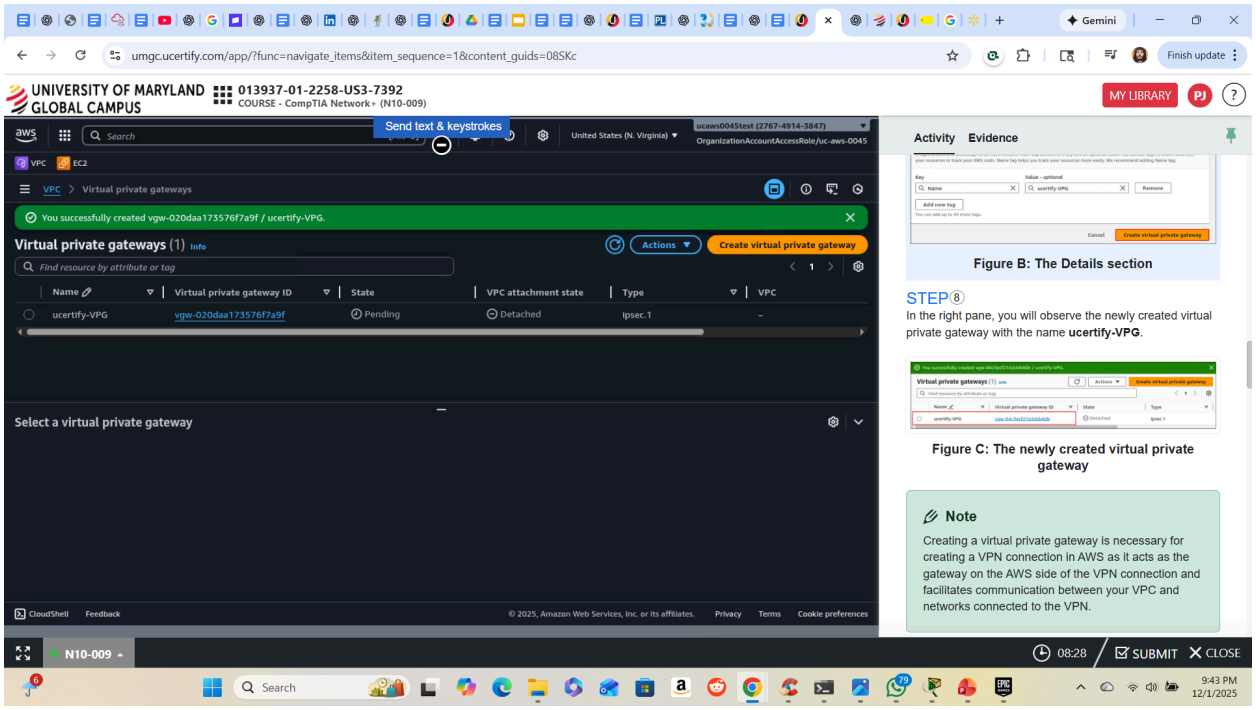
Create a Virtual Private Gateway (VGW)

Left menu → *Virtual Private Network (VPN)* → Virtual Private Gateways
Click Create Virtual Private Gateway

Input:

- **Name tag:** `ucertify-VPG`
- **Type:** `ipsec.1` (Default)





After creation, the VGW appears with:

- **State:** Pending
- **Attachment:** Detached (because not yet attached to a VPC)

What is a VGW?

A VGW is the AWS endpoint of a VPN connection.
It works like the “router” sitting on the cloud side of a site-to-site tunnel.

Step 3:

Navigate to VPC Services

Left navigation → Networking & Content Delivery → VPC

The VPC dashboard is where AWS networking components like subnets, routing tables, gateways, and firewalls live.

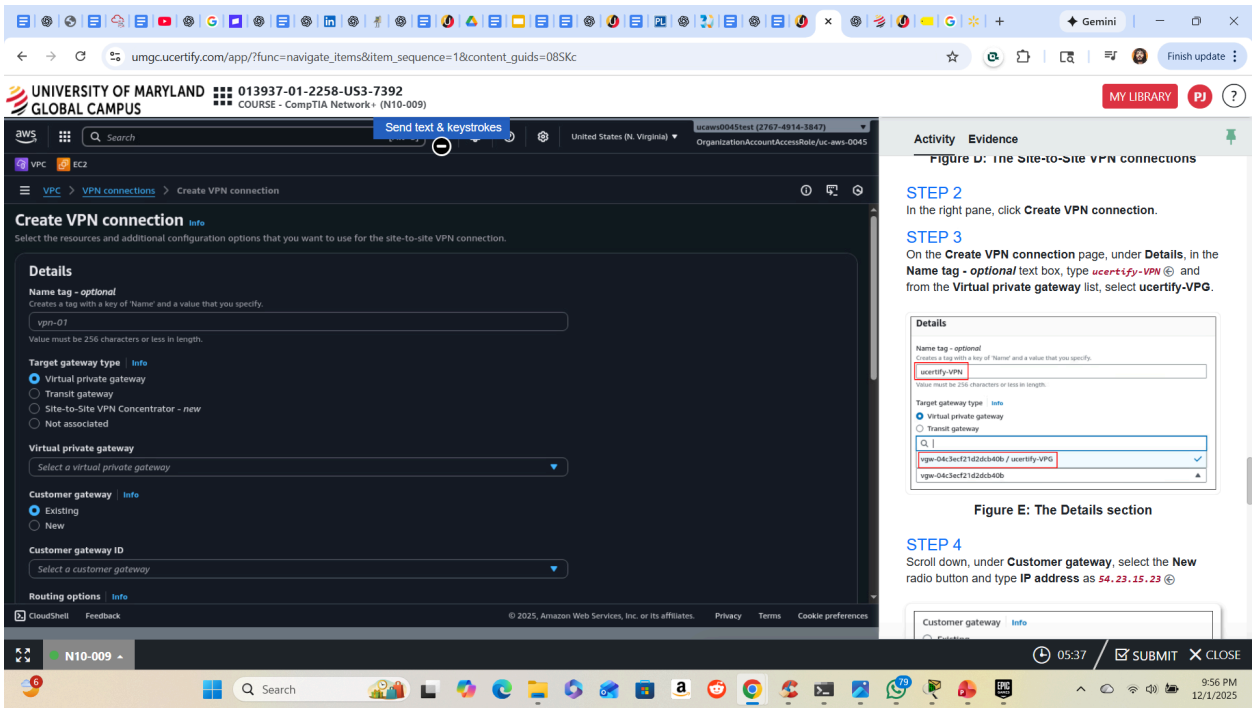
Step 4:

Create a Site-to-Site VPN Connection

Left menu → Site-to-Site VPN Connections
Click Create VPN Connection

Fill out the Details section:

- **Name tag:** `ucertify-VPN`
- **Target Gateway Type:** Virtual Private Gateway
- **Virtual Private Gateway:** select your newly created VGW (`ucertify-VPG`)
- **Customer Gateway:**
    - Select New
    - Enter provided Customer Gateway Public IP: `54.23.15.23` (given by lab)



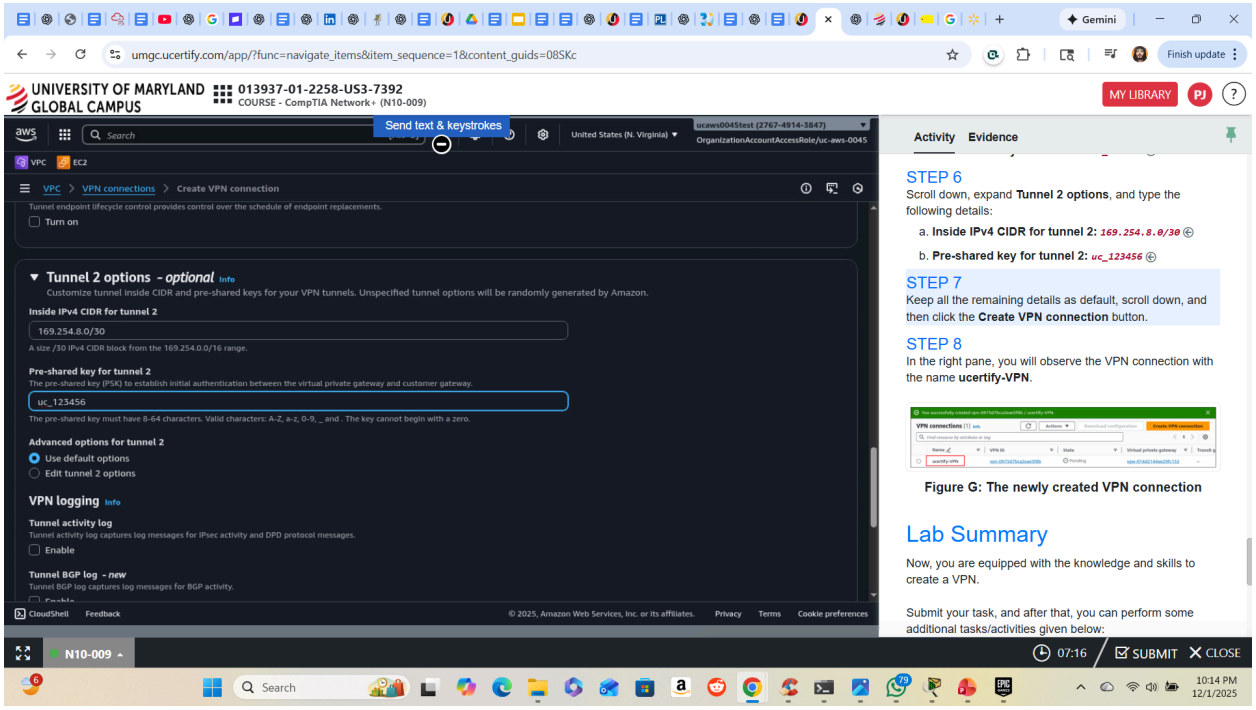
Step 5:

Configure Tunnel Options (Tunnel 2 as required)

Scroll down → Expand Tunnel 2 Options

Enter:

- **Inside IPv4 CIDR:** `169.254.8.0/30`
- **Pre-shared Key:** `uc_123456`



Explanation:

- **Inside CIDR:** small network range for the encrypted tunnel interface
- **Pre-shared key:** used to authenticate both sides of the tunnel during IPSec negotiation

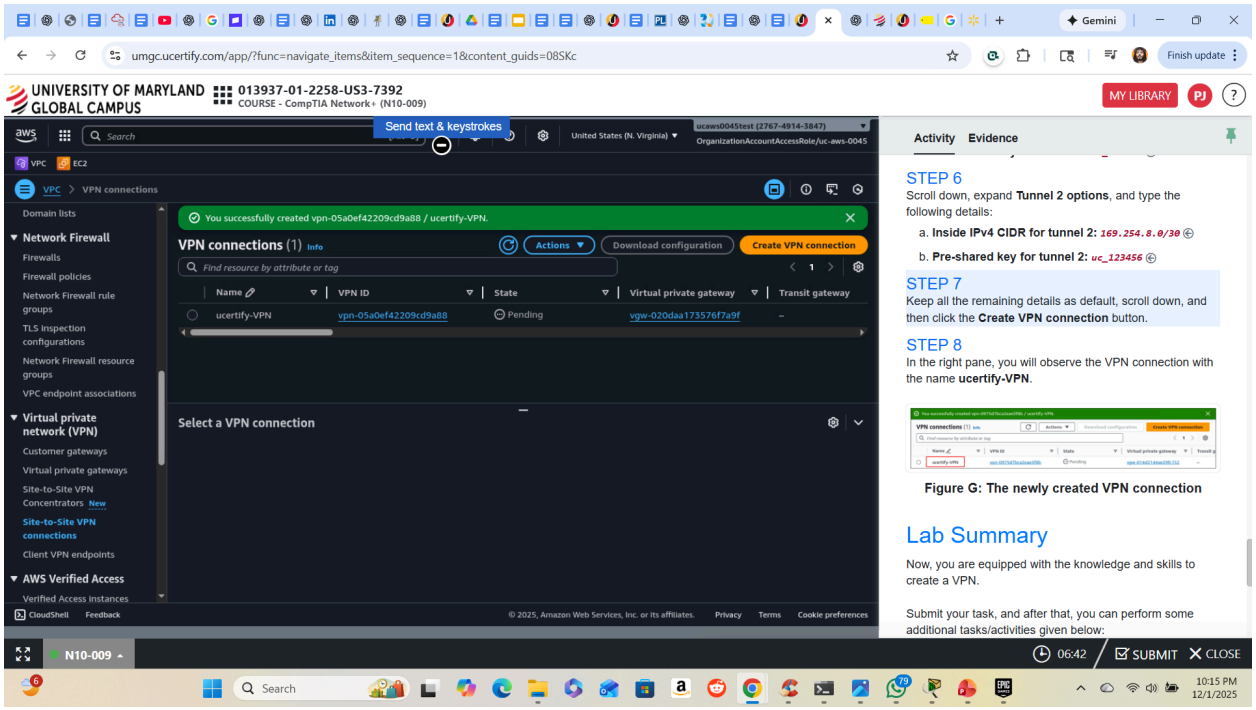
Step 6:

Create the VPN Connection

Scroll down → Click **Create VPN connection**

You will see a confirmation banner:

"You successfully created vpn-05a0ef42209cd9a88 / ucertify-VPN"



The VPN will show:

- **State:** Pending
- **Virtual Private Gateway:** Attached
- **Tunnel 1 / Tunnel 2:** Pending creation

This is expected in a sandbox environment

Key Networking Concepts Explained

- **Site-to-Site VPN:** A secure, encrypted connection between two private networks over the public internet.
- **IPSec:** The encryption protocol suite used to secure VPN tunnels.

- **Virtual Private Gateway:** The AWS endpoint of the VPN. Acts like your “cloud router.”
- **Customer Gateway:** Represents the on-premises router or firewall. Uses its own public IP to establish the encrypted tunnel.
- **Tunnel Inside CIDR:** The inner communication network used strictly by the IPSec tunnel endpoints.

Lessons Learned

- I learned how organizations securely connect remote networks and branch offices using AWS VPN technologies.

- I gained hands-on understanding of Virtual Private Gateways, Customer Gateways, and IPSec tunnel configurations.

- This lab helped me understand how cloud networking mirrors real on-prem infrastructure but with more flexibility and automation.