

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

The screenshot shows the uCertify AWS lab environment. At the top, there's a browser-like header with tabs, a search bar, and various icons. Below it, the uCertify navigation bar displays 'UNIVERSITY OF MARYLAND GLOBAL CAMPUS' and 'COURSE - CompTIA Network+ (N10-009)'. The main content area is the AWS Console Home, showing the 'Recently visited' section with links to Billing and Cost Management, EC2, VPC, Amazon SageMaker AI, Simple Queue Service, AWS Glue, and IAM. To the right, there's a sidebar titled 'Activity' and 'Evidence'. The 'Activity' tab is active, displaying a note about AWS updates and a 'Watch me first to get started' video thumbnail. The 'Evidence' tab is also present. At the bottom, there's a task bar with a progress bar, a 'SUBMIT' button, and a 'CLOSE' button. The status bar at the very bottom shows the time as 18:24 and the date as 12/1/2025.

Tool and Service Used

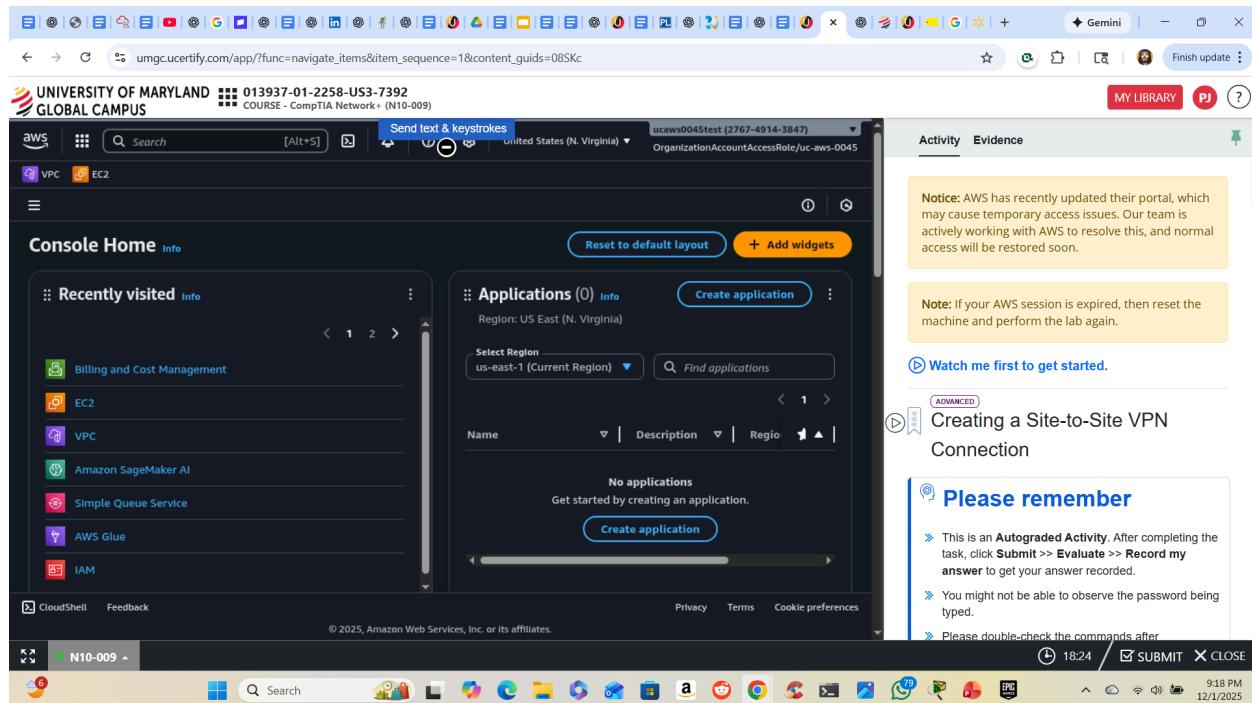
- **AWS Console:** Management interface for creating network resources
- **Amazon VPC:** Provides isolated networking infrastructure in AWS
- **Virtual Private Gateway (VGW):** AWS-side VPN endpoint
- **Customer Gateway (CGW):** Represents the on-premises router
- **Site-to-Site VPN service:** Establishes 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.



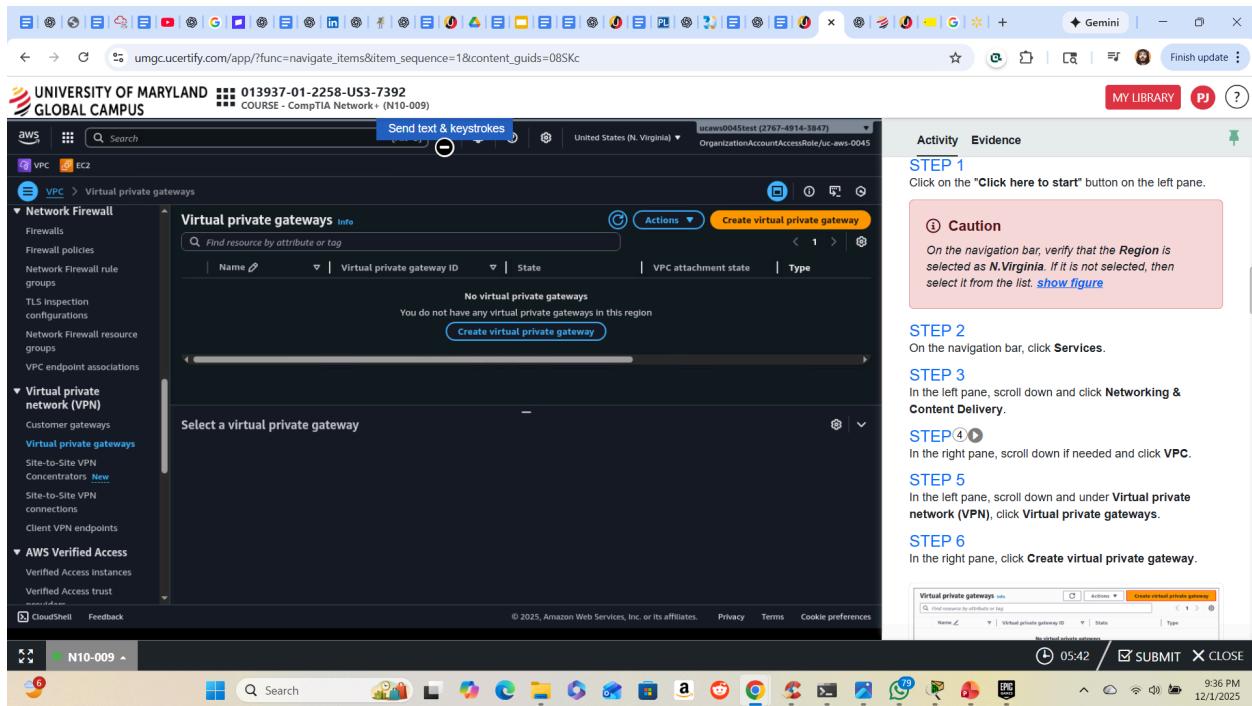
Step 2:

Create a Virtual Private Gateway (VGW)

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

Input:

- **Name tag:** uc certify - VPG
- **Type:** ipsec . 1 (Default)



The screenshot shows the AWS VPC service interface. In the top navigation bar, the URL is umgc.uncertify.com/app/?func=navigate_items&item_sequence=1&content_guids=08SKc. The top right corner has a 'MY LIBRARY' button and a 'Finish update' link. The main content area displays a table titled 'Virtual private gateways (1)'. The table has columns: Name, Virtual private gateway ID, State, VPC attachment state, Type, and VPC. One row is present, showing 'ucertify-VPG' with ID 'vgw-020daa173576f7a9f', State 'Pending', Attachment state 'Detached', Type 'Ipsec.1', and VPC '-'. A green success message at the top says 'You successfully created vgw-020daa173576f7a9f / ucertify-VPG.' Below the table, there's a note 'Select a virtual private gateway'. On the right side of the screen, there's a sidebar titled 'Activity' and 'Evidence' with a search bar for 'Name' and a 'Create virtual private gateway' button.

Figure B: The Details section

STEP ⑧
In the right pane, you will observe the newly created virtual private gateway with the name **ucertify-VPG**.



Figure C: The newly created virtual private gateway

Note

Creating a virtual private gateway is necessary for creating a VPN connection in AWS as it acts as the gateway on the AWS side of the VPN connection and facilitates communication between your VPC and networks connected to the VPN.

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

The screenshot shows the 'Create VPN connection' page in the AWS VPC console. The 'Details' section is highlighted, showing the following configuration:

- Name tag - optional:** vpn-01
- Target gateway type:** Virtual private gateway (selected)
- Virtual private gateway:** Select a virtual private gateway (dropdown menu)
- Customer gateway:** Existing (radio button selected)
- Customer gateway ID:** Select a customer gateway (dropdown menu)

A callout box labeled 'Figure E: The Details section' points to the 'Name tag - optional' field. Another callout box labeled 'Figure D: The Site-to-Site VPN connections' points to the 'Target gateway type' dropdown.

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**

The screenshot shows the AWS VPC console interface. On the left, there's a sidebar with icons for VPC, EC2, and other services. The main area has a breadcrumb trail: AWS > VPC > VPN connections > Create VPN connection. A search bar at the top says "Send text & keystrokes". The "Tunnel 2 options - optional" section is expanded, showing the "Inside IPv4 CIDR for tunnel 2" field containing "169.254.8.0/30" and the "Pre-shared key for tunnel 2" field containing "uc_123456". Below these, there are sections for "Advanced options for tunnel 2" (with "Use default options" selected) and "VPN logging". On the right, there's a "STEP 6" section with instructions to scroll down and expand Tunnel 2 options, and a "STEP 7" section with instructions to keep all remaining details as default, scroll down, and click the "Create VPN connection" button. A preview window on the right shows the newly created VPN connection named "ucify-VPN" in the "VPN connections" list. The bottom of the screen shows the Windows taskbar with various pinned icons.

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 / uc certify-VPN"

The screenshot shows the AWS VPC console with the URL umgc.uctcertify.com/app/?func=navigate_items&item_sequence=1&content_guids=08SKc. The left sidebar shows 'Network Firewall', 'Virtual private network (VPN)', and 'AWS Verified Access'. The main pane displays a table titled 'VPN connections (1) Info' with one row: Name: uc certify-VPN, VPN ID: vpn-05a0ef42209cd9a88, State: Pending, Virtual private gateway: vgw-020daa173576f7a9f, and Transit gateway: -.

STEP 6
Scroll down, expand **Tunnel 2 options**, and type the following details:
a. Inside IPv4 CIDR for tunnel 2: **169.254.8.0/30** ⓘ
b. Pre-shared key for tunnel 2: **uc_123456** ⓘ

STEP 7
Keep all the remaining details as default, scroll down, and then click the **Create VPN connection** button.

In the right pane, you will observe the VPN connection with the name **uc certify-VPN**.

Figure G: The newly created VPN connection

Lab Summary
Now, you are equipped with the knowledge and skills to create a VPN.
Submit your task, and after that, you can perform some additional tasks/activities given below:

06:42 / SUBMIT X CLOSE
10:15 PM 12/1/2025

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.