AWS Site-to-Site VPN

By Don Chen

# Description

We set up some services in AWS in a private subnet. We would like our on-premises users to be able to securely and seamlessly access the AWS services by setting up a site-to-site VPN.

# Prerequisites

* Logins for AWS.
* Logins for edge router.

# Step by Step Instructions

## AWS Configurations

1. Login to AWS.
2. Search for VPC and then click on VPC.

A screenshot of a computer

AI-generated content may be incorrect.

1. In the left tab, scroll down until you see “Customer gateways”. Click on it.

A screenshot of a computer

AI-generated content may be incorrect.

1. Click on “Create customer gateway”.
2. Enter the info as shown below, then click “Create customer gateway”.

A screenshot of a computer

AI-generated content may be incorrect.

1. Click on “Virtual private gateways” on the left tab. Click on “Create virtual private gateway”.
2. Type “VPG\_HQ” for the name. Click on “Create virtual private gateway”.
3. Select the virtual private gateway you just created. Click on actions. Click on “Attach to VPC”. Select the VPC that has our AWS services. Click “attach to VPC”.
4. Click on “[Site-to-Site VPN connections](https://us-east-2.console.aws.amazon.com/vpcconsole/home?region=us-east-2#VpnConnections:)” in the left tab. Click on “Create VPN connection”.
5. For the name, use “VPN\_HQ”. Select the virtual private gateway we just created. Select the customer gateway we just created. For routing options, select static. Add the Static IP prefixes, local IPv4, and Remote IPv4 addresses as shown below. Click on “create vpn connection”.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

1. Select the VPN you just created. Click on “Download configuration”.
2. Enter in the information as shown below. Then click download. This file will be used to configure the edge router. We will call this the Edge Router Configuration File.

A screenshot of a computer

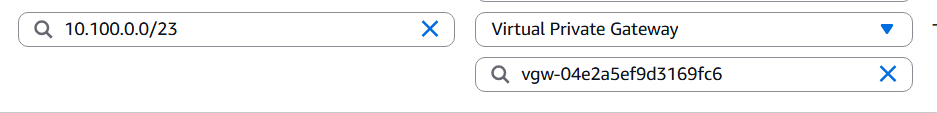
AI-generated content may be incorrect.

1. Click on “Route tables” on the left tab. Select the route table associated with the subnet 10.0.1.0/24. Click on “Routes” at the bottom, then click on “Edit routes”. It will look like the picture below.

A screenshot of a computer

AI-generated content may be incorrect.

1. Click on “Add route”. For the destination, use “10.100.0.0/23”, for the target, select “Virtual Private Gateway”, and select the virtual private gateway we created earlier. Then save.



## Edge Router Configurations

1. Remote into the edge router. Login to privileged exec mode.
2. Copy and paste in the command below:

copy running-config flash:/before\_AWS\_tunnel.cfg

1. Enter configuration mode. Paste in everything from the Edge Router Configuration File that was downloaded from AWS.
2. Copy and paste in the command below:

ip route 10.0.1.0 255.255.255.0 Tunnel1 track 100

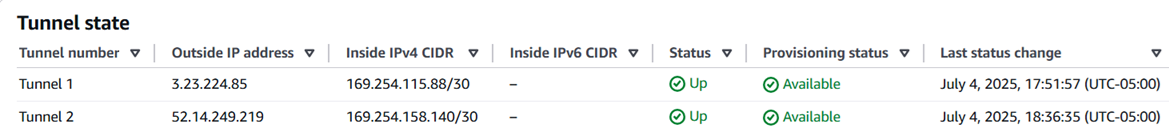
ip route 10.0.1.0 255.255.255.0 Tunnel2 track 200

End

Write mem

# Verification

1. Login to AWS. Go to the VPC dashboard. Click on “Site-to-Site VPN connections”. Select the VPN tunnel we created. Click on “Tunnel details” at the bottom. Verify that both tunnels are up.



1. Remote into the edge router. Attempt to ping any instances in the private subnet of AWS. If it succeeds, then everything works.

# Roll Back Plan

## AWS

1. Login to AWS.
2. Go to the VPC dashboard.
3. Click on “Site-to-Site VPN connections” on the left tab. Delete the VPN connection we made earlier by selecting it and clicking on “Actions”.
4. Click on “Virtual Private Gateways” on the left tab. Detach the virtual private gateway, then delete it.
5. Click on “[Customer gateways](https://us-east-2.console.aws.amazon.com/vpcconsole/home?region=us-east-2#CustomerGateways:)” on the left tab. Delete the customer gateway.
6. Click on “Route tables” on the left tab. Select the route table associated with the 10.0.1.0/24 subnet. Click on “Routes” at the bottom. Click “Edit routes”. Remove the route with the destination of 10.100.0.0/23.

## Edge Router

1. Remote into the edge router and login to privileged exec mode.
2. Copy and paste the command below:

copy flash:/before\_AWS\_tunnel.cfg running-config

1. Press enter.
2. Copy and paste the command below:

Write mem