COURSEWARE

EC2 VPC Internet Gateways

Contents

- [Overview](#)
- [Allowing Your EC2 Instances Internet Access](#)
- [Creating an Internet Gateway](#)
    - [Basic Usage](#)
- [Attaching an Internet Gateway to a VPC](#)
    - [Basic Usage](#)
- [View Existing Internet Gateways](#)
- [Detaching Internet Gateways](#)
- [Deleting Internet Gateways](#)
- [Tutorial](#)
- [Exercises](#)

Overview

An internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between instances in your VPC and the internet.
It therefore imposes no availability risks or bandwidth constraints on your network traffic.

An internet gateway serves two purposes: to provide a target in your VPC route tables for internet-routable traffic, and to perform network address translation (NAT) for instances that have been assigned public IPv4 addresses.

An internet gateway supports IPv4 and IPv6 traffic.

Allowing Your EC2 Instances Internet Access

To enable access to or from the internet for instances in a VPC subnet, you must do the following:

- Attach an internet gateway to your VPC.
- Ensure that your subnet's route table points to the internet gateway.
- Ensure that instances in your subnet have a globally unique IP address (public IPv4 address, Elastic IP address, or IPv6 address).
- Ensure that your network access control and security group rules allow the relevant traffic to flow to and from your instance.

To use an internet gateway, your subnet's route table must contain a route that directs internet-bound traffic to the internet gateway.
You can scope the route to all destinations not explicitly known to the route table (0.0.0.0/0 for IPv4 or ::/0 for IPv6), or you can scope the route to a narrower range of IP addresses; for example, the public IPv4 addresses of your company's public endpoints outside of AWS, or the Elastic IP addresses of other Amazon EC2 instances outside your VPC.
If your subnet is associated with a route table that has a route to an internet gateway, it's known as a public subnet.

To enable communication over the internet for IPv4, your instance must have a public IPv4 address or an Elastic IP address that's associated with a private IPv4 address on your instance.
Your instance is only aware of the private (internal) IP address space defined within the VPC and subnet.
The internet gateway logically provides the one-to-one NAT on behalf of your instance, so that when traffic leaves your VPC subnet and goes to the internet,

the reply address field is set to the public IPv4 address or Elastic IP address of your instance, and not its private IP address.

Conversely, traffic that's destined for the public IPv4 address or Elastic IP address of your instance has its destination address translated into the instance's private IPv4 address before the traffic is delivered to the VPC.

Creating an Internet Gateway

Basic Usage

Creating an Internet Gateway is very simple, as no parameters are required:

```
aws ec2 create-internet-gateway
```

Attaching an Internet Gateway to a VPC

Basic Usage

You must have an existing VPC to attach the internet gateway to.

To attach an Internet Gateway to a VPC, you must provide the IDs for both the VPC and the Internet Gateway:

```
# aws ec2 attach-internet-gateway --internet-gateway-id [INTERNET_GATEWAY_ID] --
vpc-id [VPC_ID]
aws ec2 attach-internet-gateway --internet-gateway-id igw-0a831f55f06387254 --
vpc-id vpc-05207b1e60ee695c5
```

View Existing Internet Gateways

We can use the `describe-internet-gateways` command to see the existing Internet Gateways.

This will also give us useful information, such as their IDs and the VPCs that they are attached to:

```
aws ec2 describe-internet-gateways
```

Detaching Internet Gateways

Before you can delete an Internet Gateway, it must be detached. If you don't do this, you will get an error stating that the IG has dependencies that can't be deleted.

Detaching an Internet Gateway can be done by providing the Internet Gateway ID and the ID of the VPC that it is attached to:

```
# aws ec2 detach-internet-gateway --internet-gateway-id [INTERNET_GATEWAY_ID] --
vpc-id [VPC_ID]
aws ec2 detach-internet-gateway --internet-gateway-id igw-0a831f55f06387254 --
vpc-id vpc-05207b1e60ee695c5
```

Deleting Internet Gateways

An Internet Gateway can be deleted by providing the ID of the Internet Gateway:

```
# aws ec2 delete-internet-gateway --internet-gateway-id [INTERNET_GATEWAY_ID]
aws ec2 delete-internet-gateway --internet-gateway-id igw-0a831f55f06387254
```

Tutorial

Try to complete the following tasks:

- Create a VPC
- Create an Internet Gateway
- Attach the new Internet Gateway to the VPC that you created

- View information about the Internet Gateway, does it say that it is attached to a VPC?
- Detach the Internet Gateway
- Delete the VPC and Internet Gateway that you created

Exercises

There are no exercises for this module.