

Laboratorio de desafíos: Creación de un entorno de red de VPC para the Café

En este Laboratorio vamos a crear un entorno de redes en AWS e implementar capas de seguridad para proteger los recursos.

Una solicitud empresarial para la cafetería: crear una red de VPC que permita al personal de la cafetería administrar de forma remota y segura el servidor de aplicaciones web (Desafío n.º 1)

Tarea 1: creación de una subred pública

Abrimos la consola VPC y accedemos a la sección de subredes donde crearemos una con la VPC que nos ha creado el laboratorio.

La subred debe tener las siguientes especificaciones:

VPC

ID de la VPC
Cree subredes en esta VPC.

vpc-0bbe8a11f2cf833ec (Lab VPC) ▼

Subred 1 de 1

Nombre de la subred
Cree una etiqueta con una clave de "Nombre" y el valor que especifique.

Public Subnet

El nombre puede tener un máximo de 256 caracteres.

Zona de disponibilidad [Información](#)
Elija la zona en la que residirá la subred o deje que Amazon elija una por usted.

EE.UU. Este (Norte de Virginia) / us-east-1a ▼

Bloque de CIDR de VPC IPv4 [Información](#)
Elija el bloque de CIDR de la VPC IPv4 en el que crear una subred.

10.0.0.0/16 ▼

Bloque de CIDR de la subred IPv4

10.0.0.0/24 256 IPs

< > ^ v

Una vez creada, debemos crear una puerta de enlace de internet y adjuntarla a nuestra VPC:

Se ha creado la siguiente gateway de Internet: igw-0007abafe44f74b60 - mi-gateway-de-internet. Ahora puede asociar a una VPC para permitir que la VPC se comuniquen con Internet.

Asociar a una VPC

VPC > Gateways de Internet > igw-0007abafe44f74b60

igw-0007abafe44f74b60 / mi-gateway-de-internet

Acciones

Detalles

Información

ID de gateway de Internet

igw-0007abafe44f74b60

Estado

Detached

ID de la VPC

-

Propietario

0854

Conectar a la VPC

Desconectar de la VPC

Administrar etiquetas

Eliminar

Conectar a la VPC (igw-0007abafe44f74b60)

Info

VPC

Conecte una gateway de Internet a la VPC para habilitar la comunicación con Internet. Especifique la VPC a la que desea conectar.

VPC disponibles

Conecte la gateway de Internet a esta VPC.

Q vpc-0bbe8a11f2cf833ec

X

Por último vamos a editar nuestra tabla de enrutamiento y añadirle la ruta 0.0.0.0. :

rtb-0999830c28a789bb9

Detalles

Rutas

Asociaciones de subredes

Asociaciones de borde

Propagación de rutas

Etiquetas

Rutas (1)

Ambos

Editar rutas

Q Filtrar rutas

< 1 >

Destino

Destino

Estado

Propagada

10.0.0.0/16

local

Activo

No

Esta es la tabla asociada a nuestra VPC

Destino

Destino

Estado

10.0.0.0/16

local

Activo

Q 0.0.0.0/0

X

Q local

X

Puerta de enlace de Internet

igw-0007abafe44f74b60

-

Agregar ruta

Agregamos esa ruta y le ponemos la puerta de enlace de internet que acabamos de crear. Una vez creada la asociamos a la subred pública.

Tarea 2: creación de un host bastión

Ahora crearemos un host de bastión en la subred pública que acabamos de hacer. Abrimos la consola EC2 y creamos una instancia con las siguientes especificaciones:

Nombre y etiquetas

Información

Nombre

Bastion Host

Amazon Linux

aws

macOS

Mac

Ubuntu

ubuntu

Windows

Microsoft

Red Hat

Red Hat

SUSE L

SUSE

Buscar más AMI

Inclusión de AMI de AWS, Marketplace y la comunidad

Imágenes de máquina de Amazon (AMI)

Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type

Apto para la capa gratuita

ami-0d94353f7bad10668 (64 bits (x86)) / ami-06f4469ebae67ec26 (64 bits (Arm))

Virtualización: hvm

Activado para ENA: true

Tipo de dispositivo raíz: ebs

Descripción

Nombre del par de claves - obligatorio

vockey

Crear un nuevo par de claves

▼ Configuraciones de red

Información

VPC : obligatorio

Información

vpc-0bbe8a11f2cf833ec (Lab VPC)

10.0.0.0/16

Subred

Información

subnet-0775caa6ea840cfcc

Public Subnet

VPC: vpc-0bbe8a11f2cf833ec

Propietario: 085461668525

Zona de disponibilidad: us-east-1a

Direcciones IP disponibles: 251

CIDR: 10.0.0.0/24

Crear nueva subred

Asignar automáticamente la IP pública

Información

Desactivar

Firewall (grupos de seguridad)

Información

Reglas de grupos de seguridad de entrada

▼

Regla del grupo de seguridad 1 (TCP, 22, 87.222.76.47/32)

Eliminar

Tipo	Información	Protocolo	Información	Intervalo de puertos	Información
ssh		TCP		22	
Tipo de origen	Información	Nombre	Información	Descripción - opcional	Información
Mi IP		<div>Q Add CIDR, prefix list or security</div> <div>87.222.76.47/32 X</div>		por ejemplo, SSH para Admin Desk	

El resto lo dejamos por defecto.

Básicamente hemos creado una instancia con máquina principal Linux, que usa las claves de sesión Vodkey(por defecto), lo hemos metido en la Red Privada Virtual que venía creada por defecto, le hemos especificado que esté en la subred Pública y creado un grupo de seguridad que permita conexiones SSH desde mi IP.

Tarea 3: asignación de una dirección IP elástica al host bastión

Una IP elástica es, básicamente, una IP estática que se puede asociar a una instancia EC2, y eso es lo que vamos a hacer ahora mismo, en la consola de EC2 nos vamos al panel izquierdo y buscamos IP elásticas:

- ▼ Red y seguridad
- Security Groups
 - Direcciones IP elásticas
 - Grupos de ubicación
 - Pares de claves
 - Interfaces de red

Aquí le damos a asignar la dirección IP elástica, y elegimos el grupo de borde de red, en este caso solo tenemos la zona en la que estamos trabajando:

Grupo de borde de red

Información

Q us-east-1 X

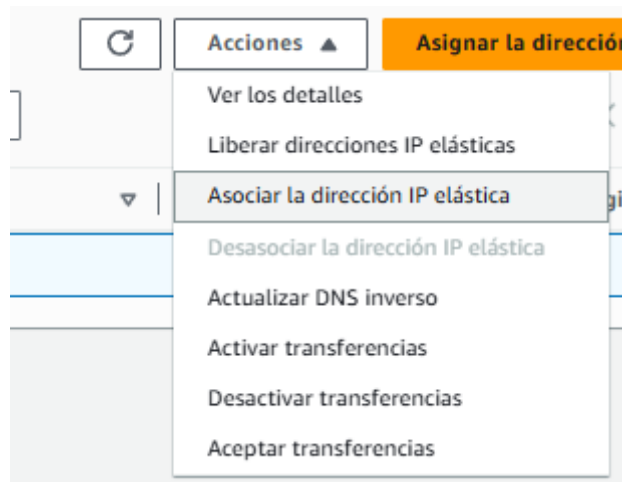
us-east-1 (us-east-1a, us-east-1b, us-east-1c, us-east-1d, us-east-1e, us-east-1f)

☒ Grupo de direcciones IPv4 de Amazon

Le damos abajo a asignar y ya la tenemos creada, ahora solo queda asignarla a nuestra instancia:

Name	Dirección IPv4 asign...	Tipo	ID de asignación	Registro DNS inverso
-	52.23.29.56	IP pública	eipalloc-03ac3587e4207cfde	-

Seleccionamos la IP elástica, pulsamos acciones y le damos a asociar la dirección IP:



Elegimos nuestra instancia y dejamos la IP privada que nos diga la página:

Instancia

Dirección IP privada
La dirección IP privada a la que desea asociar la dirección IP elástica.

Nueva asociación

Si ahora nos vamos a nuestras instancias, vemos que la instancia tiene la misma IP pública que la elástica y la privada que tenía por defecto(dada por la propia subred):

▼ Resumen de instancia	Información	
ID de la instancia i-010c7176ceb819958 (Bastion Host)	Dirección IPv4 pública 52.23.29.56 dirección abierta	Direcciones IPv4 privadas 10.0.0.30
Dirección IPv6 -	Estado de la instancia ✓ En ejecución	DNS de IPv4 pública ec2-52-23-29-56.compute-1.amazonaws.com dirección abierta

Tarea 4: prueba de la conexión con el host bastión

Vamos a probar la conexión a nuestro bastión que acabamos de crear utilizando la herramienta PuTTY, para ello necesitaremos las claves de acceso.pem de la par de claves Vodkey que podremos encontrar en los detalles del Laboratorio.

Configurar PuTTY es muy sencillo, solo tendremos que poner los siguientes datos:

La IP pública del host(IP elástica):

Specify the destination you want to connect to

Host Name (or IP address)	Port
52.23.29.56	22

Connection type:

☒ SSH ☐ Serial ☐ Other: Telnet

Y en esta ruta, poner el archivo de claves:

Category:

- Behaviour
- Translation
- + Selection
- Colours
- Connection
 - Data
 - Proxy
 - SSH
 - Kex
 - Host keys
 - Cipher
 - Auth
 - Credentials
 - Public-key authentication
 - Private key file for authentication:
C:\Users\nicor\Downloads\labsuser.ppk
 - Certificate to use with the private key (optional):
 - Plugin to provide authentication responses
 - GSSAPI
 - TTY

Connection/SSH/Auth/Credentials

Le damos a conectar y listo:

```
 login as: ec2-user  
 Authenticating with public key "imported-openssh-key"  
#  
~\_####_ Amazon Linux 2  
~~\_#####\  
~~\_###| AL2 End of Life is 2025-06-30.  
~~\_#/_____  
~~ V~' '->  
~~~~  
~~~~_. / A newer version of Amazon Linux is available!  
~~~~_/ /  
~~~~/_m/' _____ Amazon Linux 2023, GA and supported until 2028-03-15.  
https://aws.amazon.com/linux/amazon-linux-2023/  
[ec2-user@ip-10-0-0-30 ~]$
```

Nos pedirá un usuario que también podemos poner uno por defecto en PuTTY

Tarea 5: creación de una subred privada

No todos los servicios pueden estar en subredes públicas debido a la poca seguridad de estas, servicios como bases de datos es mejor que se encuentren a salvo dentro de las subredes privadas.

Vamos a crear una nueva igual que la tarea 1 pero vamos a hacerla privada.

Nombre de la subred
Cree una etiqueta con una clave de "Nombre" y el valor que especifique.

Private Subnet

El nombre puede tener un máximo de 256 caracteres.

Zona de disponibilidad [Información](#)
Elija la zona en la que residirá la subred o deje que Amazon elija una por usted.

EE.UU. Este (Norte de Virginia) / us-east-1a ▼

Bloque de CIDR de VPC IPv4 [Información](#)
Elija el bloque de CIDR de la VPC IPv4 en el que crear una subred.

10.0.0.0/16 ▼

Bloque de CIDR de la subred IPv4

10.0.1.0/24 256 IPs

Ponemos esta configuración y le damos a crear subred.

Tarea 6: creación de una puerta de enlace de NAT

Vamos a crear una puerta de enlace para que los elementos de la subred privada puedan conectarse a internet.

Le damos a crear gateway NAT y ponemos lo siguiente:

Configuración de gateway NAT

Nombre - opcional
Cree una etiqueta con una clave de "Nombre" y el valor que especifique.

Lab NAT Gateway

El nombre puede tener un máximo de 256 caracteres.

Subred
Seleccione una subred en la que va a crear la gateway NAT.

subnet-0775caa6ea840cfcc (Public Subnet) ▼

Tipo de conectividad
Seleccione un tipo de conectividad para la gateway NAT.

☒ Pública
☐ Privada

ID de asignación de IP elástica [Información](#)
Asigne una dirección IP elástica a la gateway NAT.

eipalloc-07986efc149b37f5a ▼

Asignar IP elástica

► Configuraciones adicionales [Información](#)

Ahora necesitaremos crear una nueva tabla de rutas, la crearemos con las siguientes especificaciones:

Nombre - opcional
Cree una etiqueta con una clave de "Nombre" y el valor que especifique.

Private Route Table

VPC
La VPC que se debe usar para esta tabla de enrutamiento.

vpc-0bbe8a11f2cf833ec (Lab VPC)

Destino

10.0.0.0/16

Q 0.0.0.0/0 X

Destino

local

Q local X

Puerta de enlace NAT

Q nat-0652866d844f1919d X

Es

✓

-

Y por ultimo adjuntamos la subred privada a la nueva tabla de enrutamiento.

Buscar asociación de subredes

<

1

>

Nombre	ID de subred	CIDR IPv4	CIDR IPv6
Private Subnet	subnet-099bee867100c034f	10.0.1.0/24	-

Tarea 7: creación de una instancia de Amazon EC2 en la subred privada

Vamos a crear una nueva instancia con las siguientes especificaciones:

Nombre y etiquetas Información

Nombre

Private Instance

Amazon Linux

aws

macOS

Mac

Ubuntu

ubuntu

Windows

Microsoft

Red Hat

Red Hat

SUSE L

SUSE

Buscar más AMI

Inclusión de AMI de AWS, Marketplace y la comunidad

Imágenes de máquina de Amazon (AMI)

Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type
ami-0d94353f7bad10668 (64 bits (x86)) / ami-06f4469ebae67ec26 (64 bits (Arm))
Virtualización: hvm Activado para ENA: true Tipo de dispositivo raíz: ebs

Apto para la capa gratuita

Descripción

Tipo de instancia

t2.micro

Apto para la capa gratuita

Familia: t2 1 vCPU 1 GiB Memoria Generación actual: true

Bajo demanda Windows base precios: 0.0162 USD por hora

Bajo demanda SUSE base precios: 0.0116 USD por hora

Bajo demanda RHEL base precios: 0.0716 USD por hora

Bajo demanda Linux base precios: 0.0116 USD por hora

Se aplican costos adicionales a las AMI con software preinstalado

Crear par de claves

Nombre del par de claves

Con los pares de claves es posible conectar:

vockey2

El nombre puede incluir hasta 255 caracter

Tipo de par de claves

☒ RSA

Par de claves pública y privada cifra mediante RSA

Formato de archivo de clave privada

☐ .pem

Para usar con OpenSSH

☒ .ppk

Para usar con PuTTY

VPC : obligatorio | [Información](#)

vpc-0bbe8a11f2cf833ec (Lab VPC)
10.0.0.0/16

Subred | [Información](#)

subnet-099bee867100c034f Private Subnet
VPC: vpc-0bbe8a11f2cf833ec Propietario: 085461668525
Zona de disponibilidad: us-east-1a Direcciones IP disponibles: 251 CIDR: 10.0.1.0/24

Asignar automáticamente la IP pública | [Información](#)

Desactivar

Firewall (grupos de seguridad) | [Información](#)

Un grupo de seguridad es un conjunto de reglas de firewall que controlan el tráfico de la instancia. Agrega tráfico específico llegue a la instancia.

☒ Crear grupo de seguridad

☐ Seleccionar un grupo de seguridad existente

Nombre del grupo de seguridad - obligatorio

Private Instance GS

Este grupo de seguridad se aplicará a todas las interfaces de red. El nombre de seguridad debe comenzar con sg-

Reglas de grupos de seguridad de entrada

▼ Regla del grupo de seguridad 1 (TCP, 22, sg-0605bc23f1c6cb32f)

Eliminar

Tipo | [Información](#)

ssh

Protocolo | [Información](#)

TCP

Intervalo de puertos | [Información](#)

22

Tipo de origen | [Información](#)

Personalizada

Origen | [Información](#)

Q Add CIDR, prefix list or security

sg-0605bc23f1c6cb32f X

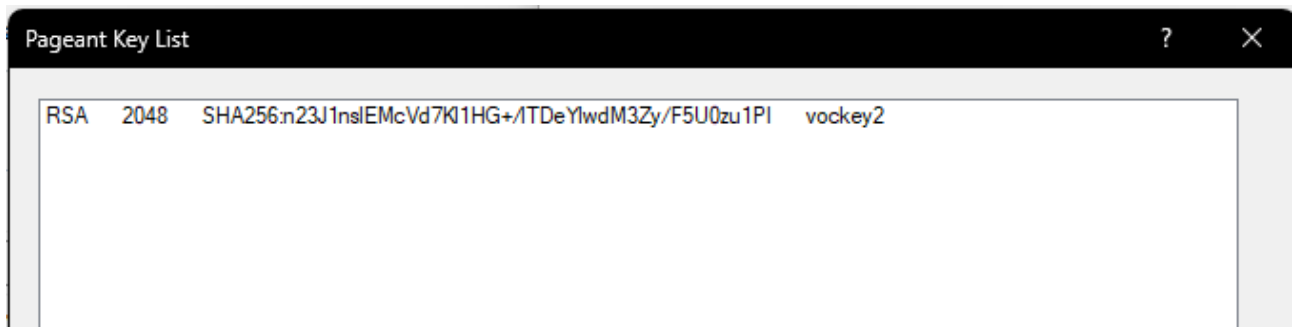
Descripción - opcional | [Información](#)

por ejemplo, SSH para Admin Des

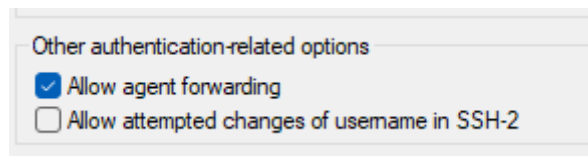
El resto lo dejamos por defecto y le damos a lanzar.

Tarea 8: configuración del cliente SSH para acceso directo de SSH

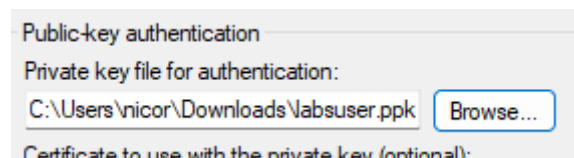
Para esta tarea necesitaremos instalar Pageant y dejarlo abierto en segundo plano. Lo abrimos desde la flechita de Windows y le damos a añadir clave(Add Key) y seleccionamos la clave que nos descargamos antes vodkey2.ppk.



Agregamos también la clave anterior labuser.ppk y cerramos Pageant. Ahora abrimos PuTTY y nos vamos a **Connection > (Conexión) SSH > Auth (Autenticación)**:



Ponemos esto así, en credenciales, ponemos la clave labuser.ppk:



Debemos poner la IP de la instancia a la que nos queremos conectar(Bastion Host) y conectarnos con PuTTY.

Tarea 9: prueba de la conexión SSH desde el host bastión

Vamos a conectarnos a la instancia privada a través de ssh, para ello debemos poner el siguiente comando:

```
ssh ec2-user@<private-ip-address-of-instance-in-private-subnet>
```

```

Last login: Mon May 27 21:49:10 2024 from 47.76.222.87.dynamic.jazztel.es

#
~\_##### Amazon Linux 2
~~\_#####\
~~\_####| AL2 End of Life is 2025-06-30.
~~\_#/
~~ V~' '->
~~~
~~~ /
~~~.-./
~~~ /- /
~~~ /m/'

A newer version of Amazon Linux is available!

Amazon Linux 2023, GA and supported until 2028-03-15.
https://aws.amazon.com/linux/amazon-linux-2023/

[ec2-user@ip-10-0-0-30 ~]$ ssh ec2-user@10.0.1.176
The authenticity of host '10.0.1.176 (10.0.1.176)' can't be established.
ECDSA key fingerprint is SHA256:p9tsOJSUs5SwwfgK9S788/b9o/Hrwi8v4m2sZMYHkcc.
ECDSA key fingerprint is MD5:8a:af:f1:l8:5d:70:28:9f:77:44:d4:l2:bf:cf:65:aa.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.1.176' (ECDSA) to the list of known hosts.

#
~\_##### Amazon Linux 2
~~\_#####\
~~\_####| AL2 End of Life is 2025-06-30.
~~\_#/
~~ V~' '->
~~~
~~~ /
~~~.-./
~~~ /- /
~~~ /m/'

A newer version of Amazon Linux is available!

Amazon Linux 2023, GA and supported until 2028-03-15.
https://aws.amazon.com/linux/amazon-linux-2023/

[ec2-user@ip-10-0-1-176 ~]$

```

Estando conectados a la instancia privada vamos a intentar hacer un ping a google:

```
[ec2-user@ip-10-0-1-176 ~]$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=107 time=1.94 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=107 time=1.39 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=107 time=1.49 ms
^C
```

Vemos que tiene internet. Si nos fijamos, la instancia privada no tiene IP pública:

▼ Resumen de instancia Información	
ID de la instancia	Dirección IPv4 pública
 i-088dc1f561378c7e4 (Private Instance)	–
Dirección IPv6	Estado de la instancia
–	 En ejecución

Nuevo requisito empresarial: Mejora de la capa de seguridad para recursos privados (Desafío n.º 2)

Tarea 10: creación de una ACL de red

Las ACL de red proporcionan una capa adicional de protección. Vamos a crear una ACL de red personalizada para controlar el tráfico hacia y desde la *Private Subnet*.

Nos vamos a la consola VPC y miramos la ACL predeterminada:

Reglas de entrada (2)							Editar reglas de entrada
Filter inbound rules							< 1 > ⚙
Número de regla	Tipo	Protocolo	Rango de puertos	Origen	Permitir/denegar		
100	Todo el tráfico	Todo	Todo	0.0.0.0/0	Allow		
*	Todo el tráfico	Todo	Todo	0.0.0.0/0	Deny		

Reglas de salida (2)							Editar reglas de salida
Filter outbound rules							< 1 > ⚙
Número de regla	Tipo	Protocolo	Rango de puertos	Destino	Permitir/denegar		
100	Todo el tráfico	Todo	Todo	0.0.0.0/0	Allow		
*	Todo el tráfico	Todo	Todo	0.0.0.0/0	Deny		

Vemos que la configuración por defecto deniega todo el tráfico. Vamos a crear una personalizada con las siguientes especificaciones:

Configuración de ACL de red

Nombre - *opcional*

Crea una etiqueta con una clave de "Nombre" y el valor que usted especifique.

Lab Network ACL

VPC

La VPC que se debe usar para esta ACL de red.

vpc-0bbe8a11f2cf833ec (Lab VPC)

Creo que no lo he entendido muy bien, ya permite el tráfico por defecto...

Tarea 11: prueba de la ACL de red personalizada

Vamos a crear una instancia EC2 en la subred publica con las siguientes especificaciones:

Nombre y etiquetas [Información](#)

Nombre

Amazon Linux
aws

macOS
Mac

Ubuntu
ubuntu®

Windows
Microsoft

Red Hat
Red Hat

SUSE Linux
SUSE

Imágenes de máquina de Amazon (AMI)
Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type
ami-0d94353f7bad10668 (64 bits (x86)) / ami-06f4469ebae67ec26 (64 bits (Arm))
Virtualización: hvm Activado para ENA: true Tipo de dispositivo raíz: ebs

Descripción

▼ Tipo de instancia [Información](#) | [Obtener as](#)

Tipo de instancia

Familia: t2 1 vCPU 1 GiB Memoria Generación actu
Bajo demanda Windows base precios: 0.0162 USD por hor
Bajo demanda Linux base precios: 0.0116 USD por hora

▼ Par de claves (inicio de sesión) [Información](#)

Puede utilizar un par de claves para conectarse de forma segura a la instancia. Asegúrese de seleccionar un par de claves antes de lanzar la instancia.

Nombre del par de claves - *obligatorio*

No nos vamos a conectar

Lo ponemos en la VPC nuestra y en la subred publica.

Y creamos un GS que permita ICMP desde todos lados:

Tipo [Información](#)

Protocolo [Información](#)

Intervalo de puertos [Información](#)

Tipo de origen [Información](#)

Origen [Información](#)

Descripción - opcional [Información](#)

Creamos la instancia y probamos a hacer un ping a la nueva máquina:

```
[ec2-user@ip-10-0-1-176 ~]$ ping 10.0.0.189
PING 10.0.0.189 (10.0.0.189) 56(84) bytes of data.
64 bytes from 10.0.0.189: icmp_seq=1 ttl=255 time=0.783 ms
64 bytes from 10.0.0.189: icmp_seq=2 ttl=255 time=0.536 ms
64 bytes from 10.0.0.189: icmp_seq=3 ttl=255 time=0.521 ms
```

Vamos a probar a denegar toda conexión ICMP desde la ACL a la ip de la máquina anfitriona.

Número de regla	Tipo Información	Protocolo Información	Rango de puertos Información	Origen Información	Permitir/denegar Información	
101	Todo el ICMP - IPv4	ICMP (1)	Todo	10.0.1.176/32	Denegar	Quitar
201	Todo el tráfico	Todo	Todo	0.0.0.0/0	Permitir	Quitar
*	Todo el tráfico	Todo	Todo	0.0.0.0/0	Denegar	
Agregar nueva regla Ordenar por número de regla						

Añadiendo esa regla ya no debería dejarnos hacer ping desde la máquina:

```
[ec2-user@ip-10-0-1-176 ~]$ ping 10.0.0.189
PING 10.0.0.189 (10.0.0.189) 56(84) bytes of data.
```

Vemos que ya no hace ping, es importante el orden de permitir/denegar acceso. Hasta aquí el Laboratorio, vamos con las preguntas:

¿Para qué sirve la puerta de enlace de Internet en la subred pública?

- Permite que la subred pública tenga acceso a internet

¿Qué permite a la instancia de la subred privada conectarse a Internet para poder descargar actualizaciones?

- El gateway NAT

¿Se puede acceder a la instancia en la subred privada directamente desde Internet?

- No, no tiene IP pública

¿Por qué se utilizan dos pares de claves diferentes para acceder a la instancia privada y al host bastión?

- Usar 2 pares de claves ayudan al factor riesgo de la instancia Bastion Host

¿Puede el host bastión utilizar ping y obtener una respuesta de la instancia en la subred privada?

- No, no puede

¿Qué reglas de grupo de seguridad permiten a la instancia de EC2 privada recibir el tráfico de retorno cuando hace ping a la instancia de prueba?

- Las de salida de la privada y las de entrada de test