

Guía práctica: Arquitectura de red segmentada en AWS con VPC, NAT Gateway y Bastion Host

Autor: Gustavo Auger Gac

Fecha: 24 Julio 2025

Introducción

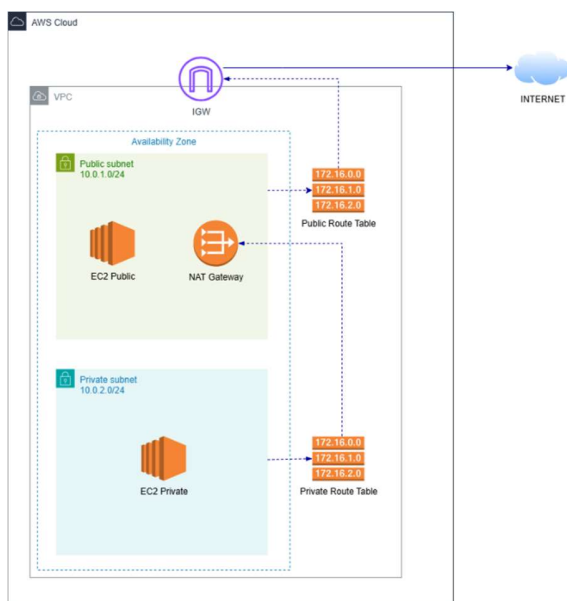
Este documento explica paso a paso cómo crear una red segmentada en AWS utilizando una VPC, subredes públicas y privadas, un NAT Gateway, un Internet Gateway, grupos de seguridad, y una instancia bastion para acceder de forma segura a instancias privadas. Toda la configuración se realizó dentro de la capa gratuita de AWS, incluyendo validaciones mediante conexiones SSH y pruebas de conectividad con curl.

¿Qué verás en esta guía?

- Crear una VPC con subred pública y privada
- Crear y asociar gateways y configurar rutas para control de tráfico.
- Usar un bastion host (instancia pública) como punto de salto hacia una instancia privada.
- Configurar reglas con Security Groups para un entorno seguro.
- Validar la arquitectura con comandos como ssh y curl.

Diagrama de la arquitectura

Este diagrama representa la arquitectura implementada en AWS, con separación de subredes, ruteo, gateways y puntos de acceso:



Paso 1: Crear una VPC.

Se crea una VPC con el rango CIDR 10.0.0.0/16:

Crear VPC [Información](#)

Una VPC es una parte aislada de la nube de AWS que contiene objetos de AWS, como instancias de Amazon EC2.

Configuración de la VPC

Recursos que se van a crear [Información](#)
Crea únicamente el recurso de VPC o la VPC y otros recursos de red.

☒ Solo la VPC ☐ VPC y más

Etiqueta de nombre - opcional
Crea una etiqueta con una clave de "Nombre" y el valor que usted especifique.

vpc-M4-L5

Bloque de CIDR IPv4 [Información](#)
☒ Entrada manual de CIDR IPv4
☐ Bloque de CIDR IPv4 asignado por IPAM

CIDR IPv4
10.0.0.0/16
El tamaño del bloque CIDR debe estar entre /16 y /28.

Bloque de CIDR IPv6 [Información](#)
☒ Sin bloque de CIDR IPv6
☐ Bloque de CIDR IPv6 asignado por IPAM
☐ Bloque de CIDR IPv6 proporcionado por Amazon
☐ CIDR IPv6 de mi propiedad

Tenencia [Información](#)
Predeterminado

Etiquetas
Una etiqueta es una marca que se asigna a un recurso de AWS. Cada etiqueta consta de una clave y un valor opcional. Puede utilizar las etiquetas para buscar y filtrar sus recursos o hacer un seguimiento de los costos de AWS.

Clave **Valor - opcional**

Puede agregar 49 etiquetas más

Paso 2: Crear subred pública y privada.

Se crean dos subredes (una pública y una privada) dentro de la VPC:

Configuración de la subred
Especifique los bloques de CIDR y la zona de disponibilidad de la subred.

Subred 1 de 1

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

subnet-privada-M4-L5
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.

Estados Unidos (Norte de Virginia) / us-east-1a

Bloque de CIDR de VPC IPv4 [Información](#)
Elija el bloque CIDR IPv4 de la VPC para la subred. El CIDR IPv4 de la subred debe estar dentro de este bloque.

10.0.0.0/16

Bloque de CIDR de la subred IPv4
10.0.0.0/24 256 IPs

Etiquetas: opcional

Clave **Valor - opcional**

Puede agregar 49 más etiquetas.

Ambas subredes ya creadas:

<input type="checkbox"/>	subnet-publica-M4-L5	subnet-0f12259855a358dfa	Available	vpc-01e0cb68a2d291271 vpc-...	Desactivado	10.0.1.0/24	-	-	251
<input type="checkbox"/>	subnet-privada-M4-L5	subnet-5a86fb7bd2c3044487	Available	vpc-01e0cb68a2d291271 vpc-...	Desactivado	10.0.2.0/24	-	-	251

Paso 3: Crear y asociar el Internet Gateway.

Primero se crea el Internet Gateway:

Crear gateway de Internet Información

Una gateway de Internet es un router virtual que conecta una VPC a Internet. Para crear una nueva gateway de Internet, especifique el nombre de la gateway a continuación.

Configuración de gateway de Internet

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

gateway-M4-L5

Etiquetas: opcional
Una etiqueta es una marca que se asigna a un recurso de AWS. Cada etiqueta consta de una clave y un valor opcional. Puede utilizar las etiquetas para buscar y filtrar sus recursos o hacer un seguimiento de los costos de AWS.

Clave
Q, Name X

Valor - opcional
Q, gateway-M4-L5 X **Quitar**

Agregar nueva etiqueta
Puede agregar 49 más etiquetas.

Cancelar **Crear gateway de Internet**

Luego se asocia a la VPC creada anteriormente:

Conectar a la VPC (igw-0a679f12dac5b1228) Información

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

VPC disponibles
Conecte la gateway de Internet a esta VPC.

Q, Seleccionar una VPC

vpc-01e0cb68a2d291271 - vpc-M4-L5

Comando de la interfaz de línea de comandos de AWS

Cancelar **Conectar gateway de Internet**

Paso 4: Crear las tablas de ruteo y asociarlas

Se crean dos tablas de ruteo, una para la subred pública y otra para la privada:

Crear tabla de enrutamiento Información

Una tabla de enrutamiento especifica cómo se envían los paquetes entre las subredes de la VPC, Internet y la conexión de la VPN.

Configuración de la tabla de enrutamiento

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

route-publica-M4-L5

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

vpc-01e0cb68a2d291271 (vpc-M4-L5)

Etiquetas
Una etiqueta es una marca que se asigna a un recurso de AWS. Cada etiqueta consta de una clave y un valor opcional. Puede utilizar las etiquetas para buscar y filtrar sus recursos o hacer un seguimiento de los costos de AWS.

Clave
Q, Name X

Valor - opcional
Q, route-publica-M4-L5 X **Quitar**

Agregar nueva etiqueta
Puede agregar 49 más etiquetas.

Cancelar **Crear tabla de enrutamiento**

Configuración de la tabla de enrutamiento

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

route-privada-M4-L5

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

vpc-01e0cb68a2d291271 (vpc-M4-L5)

Etiquetas
Una etiqueta es una marca que se asigna a un recurso de AWS. Cada etiqueta consta de una clave y un valor opcional. Puede utilizar las etiquetas para buscar y filtrar sus recursos o hacer un seguimiento de los costos de AWS.

Clave
Q, Name X

Valor - opcional
Q, route-privada-M4-L5 X Quitar

Agregar nueva etiqueta
Puede agregar 49 más etiquetas.

Cancelar Crear tabla de enrutamiento

Se asocian las subredes a sus tablas de ruteo respectivas:



En la tabla pública, se agrega una ruta para permitir salida a internet a través del Internet Gateway:

Tablas de enrutamiento (1/6) Información

Buscar tablas de enrutamiento por atributo o etiqueta

✓	Name	ID de tabla de enrutam...	Asociaciones de subre...	Asociaciones de...	Principal	VPC	ID de propietario
✓	route-publica-M4-L5	rtb-00ced28b9218ccbe	subnet-0f12259835c838...	-	Sí	vpc-01e0cb68a2d291271 vpc-M4-L5	638178518198
	route-privada-M4-L5	rtb-0be0f5ab4cf1869b83	subnet-0a8bfb7bd290d4...	-	No	vpc-01e0cb68a2d291271 vpc-M4-L5	638178518198
	mi-vpc-rds-rtb-private1-us-east-1a	rtb-0509c6c802da2168	subnet-0c7bf75df301be2...	-	No	vpc-0d20a30d668c06fde mi-vpc-rds-vpc	638178518198
	mi-vpc-rds-rtb-public	rtb-099dc199dedd1cf76	subnet-0e23dfe76d81d...	-	No	vpc-0d20a30d668c06fde mi-vpc-rds-vpc	638178518198
	-	rtb-0baf1a02717abf814	-	-	Sí	vpc-07b49d02c1b3e0d7	638178518198
	-	rtb-0a61d758924a90a0e	-	-	Sí	vpc-0d20a30d668c06fde mi-vpc-rds-vpc	638178518198

rtb-00ced28b9218ccbe / route-publica-M4-L5

Detalles **Rutas** Asociaciones de subredes Asociaciones de borde Propagación de rutas Etiquetas

Rutas (1)

Destino: 10.0.0.0/16 Objetivo: local Estado: Activo Propagada: No

Ambos Editar rutas

Se configura para que todo el tráfico (0.0.0.0/0) se enrute por el Internet Gateway:

Editar rutas

Destino: 10.0.0.0/16

Destino: local Estado: Activo Propagada: No

Q, 0.0.0.0/0 X

Puerta de enlace de Internet

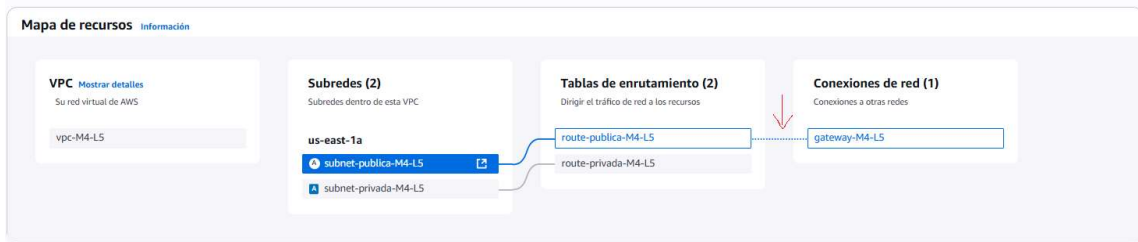
Utilizar: "igw-0a679f12dac5b1228"

igw-0a679f12dac5b1228 (gateway-M4-L5)

Agregar ruta

Cancelar Vista previa Guardar cambios

Resultado final:



Paso 5: Crear el NAT Gateway y asociarlo

El NAT Gateway permite que las instancias en la subred privada accedan a internet sin estar expuestas directamente.

Se crea en la subred pública:

Crear gateway NAT Información

Servicio administrado de traducción de direcciones de red (NAT) de alta disponibilidad que las instancias de subredes privadas pueden utilizar para conectarse a servicios de otras VPC, redes locales o Internet.

Configuración de gateway NAT

Nombre - opcional
Cree una etiqueta con una clave de "Nombre" y el valor que especifique.
NAT-M4-L5
El nombre puede tener un máximo de 256 caracteres.

Subred
Seleccione una subred en la que va a crear la gateway NAT.
subnet-Of12259835c838dfa (subnet-publica-M4-L5)

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-0b43a22089a5d6872 [Asignar IP elástica](#)

► **Configuraciones adicionales** Información

Etiquetas
Una etiqueta es una marca que se asigna a un recurso de AWS. Cada etiqueta consta de una clave y un valor opcional. Puede utilizar las etiquetas para buscar y filtrar sus recursos o hacer un seguimiento de los costos de AWS.

Clave **Valor - opcional** [Quitar](#)

[Agregar nueva etiqueta](#)
Puede agregar 49 más etiquetas.

[Cancelar](#) [Crear gateway NAT](#)

Luego se asocia a la tabla de ruteo privada:

Editar rutas

Destino	Destino	Estado	Propagada
10.0.0.0/16	local	Activo	No
<input type="text" value="0.0.0.0/0"/>	<input type="text" value="Puerta de enlace NAT"/>	-	No

[Agregar ruta](#)

[Quitar](#)

Utilizar: "nat-07c2164a7b31ff6f7"

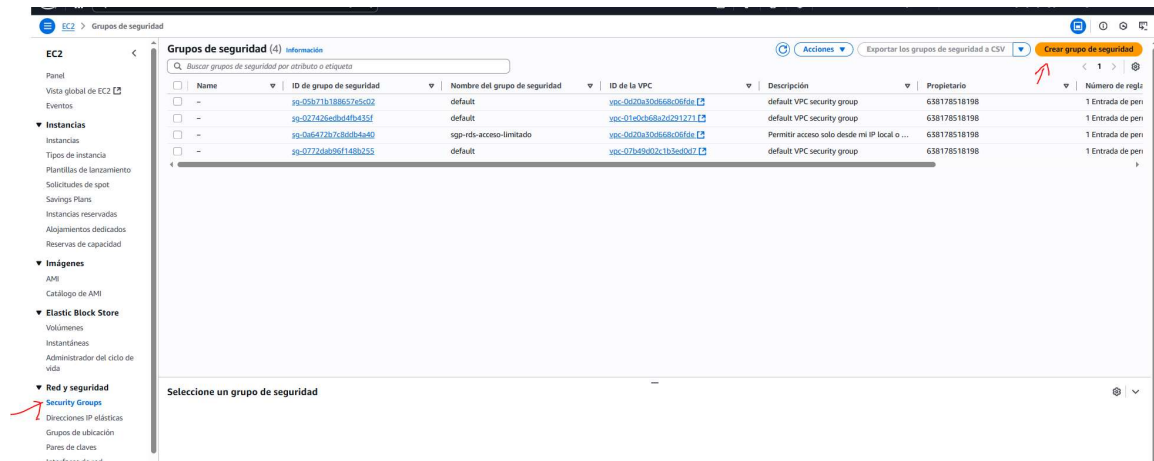
[Cancelar](#) [Vista previa](#) [Guardar cambios](#)

Resultado final:



Paso 6: Configurar los grupos de seguridad

Creación del Security Group:



Reglas de entrada configuradas:

Detalles básicos
Nombre del grupo de seguridad información
SG-M4-L5
El nombre no se puede editar después de su creación.
Descripción información
Permite HTTP, HTTPS desde todos y SSH desde mi IP
VPC información
vpc-01e0cb68a2d291271 (vpc-M4-L5)

Reglas de entrada información

Tipo	Protocolo	Intervalo de puertos	Origen	Descripción: opcional	
HTTP	TCP	80	Anywh... 0.0.0.0/0	Acceso web	Eliminar
HTTPS	TCP	443	Anywh... 0.0.0.0/0	Acceso seguro	Eliminar
SSH	TCP	22	Mi IP 0.0.0.0/0	Admin vía SSH	Eliminar

Agregar regla

Las reglas cuyo origen es 0.0.0.0/0 o ::/0 permiten a todas las direcciones IP acceder a la instancia. Recomendamos configurar reglas de grupo de seguridad para permitir el acceso únicamente desde direcciones IP conocidas.

Reglas de salida información

Tipo	Protocolo	Intervalo de puertos	Destino	Descripción: opcional	
Todo el tráfico	Todo	Todo	Persona... 0.0.0.0/0		Eliminar

Agregar regla

Resultado final del grupo de seguridad:

El grupo de seguridad (sg-07c17f2679a6d4116 | SG-M4-L5) se ha creado correctamente

Detalles

sg-07c17f2679a6d4116 - SG-M4-L5

Acciones

Detalles

Nombre del grupo de seguridad
SG-M4-L5

Propietario
638178518198

ID del grupo de seguridad
sg-07c17f2679a6d4116

Número de reglas de entrada
3 Entradas de permisos

Descripción
Permite HTTP, HTTPS desde todos y SSH desde mi IP

Número de reglas de salida
1 Entrada de permiso

ID de la VPC
vpc-07b49d02c1b3ed0d7

Reglas de entrada

Reglas de salida

Compartiendo : *novedad*

Asociaciones de VPC : *novedad*

Etiquetas

Reglas de entrada (3)

Buscar

Administrar etiquetas

Editar reglas de entrada

	Name	ID de la regla del gr...	Versión de IP	Tipo	Protocolo	Intervalo de puertos	Origen	Descripción
<input type="checkbox"/>	-	sg-077753318b59d25	IPv4	SSH	TCP	22		Admin via SSH
<input type="checkbox"/>	-	sg-01785fcc6f37e3f9	IPv4	HTTP	TCP	80	0.0.0.0/0	Acceso web
<input type="checkbox"/>	-	sg-0188c48a7daa558c1	IPv4	HTTPS	TCP	443	0.0.0.0/0	Acceso seguro

Paso 7: Lanzar las instancias EC2

Instancia EC2 pública:

Nombre y etiquetas

Información

Nombre

EC2-PUBLICA

Agregar etiquetas adicionales

▼ Imágenes de aplicaciones y sistemas operativos (Imagen de máquina de Amazon)

Información

An AMI contains the operating system, application server, and applications for your instance. If you don't see a suitable AMI below, use the search field or choose Browse more AMIs.

Q Busque en nuestro catálogo completo que incluye miles de imágenes de sistemas operativos y aplicaciones

Inicio rápido

Amazon Linux

macOS

Ubuntu

Windows

Red Hat

SUSE Linux

Debian

Buscar más AMI

Inclusión de AMI de AWS, Marketplace y la comunidad

Imágenes de máquina de Amazon (AMI)

AMI de Amazon Linux 2023 kernel-6.1

Apto para la capa gratuita

ami-08a6efd148b1f7504 (64 bits (x86), uefi-preferred) / ami-0aaf509a1ebd95e61 (64 bits (Arm), uefi)

Virtualización: hvm Activado para ENA: true Tipo de dispositivo raíz: ebs

Descripción

Amazon Linux 2023 (kernel-6.1) es un sistema operativo moderno y de uso general basado en Linux que incluye 5 años de soporte a largo plazo. Está optimizado para AWS y diseñado para proporcionar un entorno de ejecución seguro, estable y de alto desempeño para desarrollar y ejecutar sus aplicaciones en la nube.

Amazon Linux 2023 AMI 2023.8.20250721.2 x86_64 HVM kernel-6.1

Arquitectura

64 bits (x86)

Modo de arranque

uefi-preferred

ID de AMI

ami-08a6efd148b1f7504

Fecha de publicación

2025-07-19

Nombre de usuario

ec2-user

Proveedor verificado

Para efectos de prueba se utilizan configuraciones de la capa gratuita. En el caso de la instancia pública, **la asignación de IP pública debe estar habilitada** (en la imagen aparece desactivada, pero debe corregirse). Se utiliza un par de claves .pem ya generado o uno nuevo.

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

Puede utilizar un par de claves para conectarse de forma segura a la instancia. Asegúrese de que tiene acceso al par de claves seleccionado antes de lanzar la instancia.

Nombre del par de claves - *obligatorio*

FINAL [Crear un nuevo par de claves](#)

▼ Configuraciones de red [Información](#)

VPC: *obligatorio* [Información](#)

vpc-01e0cb68a2d291271 (vpc-M4-L5) [10.0.0.0/16](#) [Crear un nuevo VPC](#)

Subred [Información](#)

subnet-0f12259835c838dfa subnet-publica-M4-L5 [Crear nueva subred](#)

VPC: vpc-01e0cb68a2d291271 Propietario: 638178518198 Zona de disponibilidad: us-east-1a
Tipo de zona: Zona de disponibilidad Direcciones IP disponibles: 250 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. Agregue reglas para permitir que un tráfico específico llegue a la instancia.

☐ Crear grupo de seguridad ☒ Seleccionar un grupo de seguridad existente

Grupos de seguridad comunes [Información](#)

Seleccionar grupos de seguridad

SG-M4-L5 sg-07c17f2679a6d4116 [Compare reglas de grupo de seguridad](#)

VPC: vpc-07b49d02c1b3ed0d7

Los grupos de seguridad que agrega o elimine aquí se agregarán a todas las interfaces de red o se eliminarán de ellas.

► Configuración de red avanzada

Luego, se repite el proceso para lanzar una instancia EC2, pero esta vez seleccionando la subred privada.

Paso 8: Probar la conectividad

Se establece la conexión SSH a la instancia pública usando Git Bash:

```
ssh -i FINAL.pem ec2-user@13.220.202.106
```

- FINAL.pem: clave privada generada y descargada previamente
- ec2-user: usuario por defecto en Amazon Linux
- 13.220.202.106: IP pública de la EC2 pública

Resultado:

```
gauche@DESKTOP-RKHA003 MINGW64 /c/users/gauge/Downloads  
$ chmod 400 FINAL.pem  
  
gauche@DESKTOP-RKHA003 MINGW64 /c/users/gauge/Downloads  
$ ssh -i FINAL.pem ec2-user@13.220.202.106  
The authenticity of host '13.220.202.106 (13.220.202.106)' can't be established.  
ED25519 key fingerprint is SHA256:ARCGwzadm5v8CL3jZRduilCVlmh9cxD3xcO1EfilJTE.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])?  
  
gauche@DESKTOP-RKHA003 MINGW64 /c/users/gauge/Downloads  
$ ssh -i FINAL.pem ec2-user@13.220.202.106  
The authenticity of host '13.220.202.106 (13.220.202.106)' can't be established.  
ED25519 key fingerprint is SHA256:ARCGwzadm5v8CL3jZRduilCVlmh9cxD3xcO1EfilJTE.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '13.220.202.106' (ED25519) to the list of known hosts  
  
~  
_#####_ Amazon Linux 2023 ✓✓  
~~ \#####\|  
~~ \|###|\n\n ~ \|#/\n ~ V- '-> https://aws.amazon.com/linux/amazon-linux-2023  
~~~~~  
~~~~~  
~/m/' _/_/_/  
[ec2-user@ip-10-0-1-221 ~]$
```

☒ EC2-PUBLICA

f-t3c83bbbf707d9997

☒ En ejecución

t3.micro

☐ Inicializando

Ver alarmas +

us-east-1a

-

13.220.202.106

-

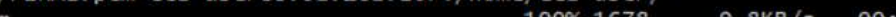
Conexión a la instancia privada desde la pública

Para acceder a la instancia privada:

1. Nos conectamos primero a la EC2 pública.
2. Copiamos el archivo .pem a esa instancia:

```
scp -i FINAL.pem FINAL.pem ec2-user@<IP PUBLICA>
```

Resultado:



A terminal window titled 'MINGW64:/c:/Users/gauge' shows the execution of an SCP command. The command is: `$ scp -i C:/Users/gauge/Downloads/descargas/FINAL.pem C:/Users/gauge/Downloads/descargas/FINAL.pem ec2-user@3.92.182.207:/home/ec2-user/FINAL.pem`. The output shows the file was successfully transferred: `100% 1678 9.8KB/s 00:00`.

3. Luego, establecemos conexión desde la pública a la IP privada de la instancia privada, dentro de la misma VPC:

```
gauche@DESKTOP-RKHA003 MINGW64 ~/Downloads/descargas
$ ssh -i FINAL.pem ec2-user@3.92.182.207

#_
#####_      Amazon Linux 2023
#####\
\###|
\#/_
V~' ' ->      https://aws.amazon.com/linux/amazon-linux-2023

Last login: Mon Jul 28 19:13:40 2025 from 191.119.29.121
[ec2-user@ip-10-0-1-221 ~]$
```

Configuración necesaria para que funcione

Es necesario agregar una nueva regla de entrada al grupo de seguridad de la instancia privada, permitiendo conexiones SSH desde la IP privada de la instancia pública:

sgr-0188c48a7daa558c1	HTTPS	TCP	443	Persona...	0.0.0.0/0	Acceso seguro	Eliminar
-	SSH	TCP	22	Persona...	10.0.1.221/32	Acceso SSH desde instancia	Eliminar

[Agregar regla](#)

Conexión desde EC2 pública a EC2 privada:

```
Warning: Identity FILE FINAL.pem not accessible: No such file or directory.
[ec2-user@ip-10-0-1-221 ~]$ ssh -i FINAL.pem ec2-user@10.0.2.218
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.218' (ED25519) to the list of known hosts.

#_
#####_      Amazon Linux 2023
#####\
\###|
\#/_
V~' ' ->      https://aws.amazon.com/linux/amazon-linux-2023

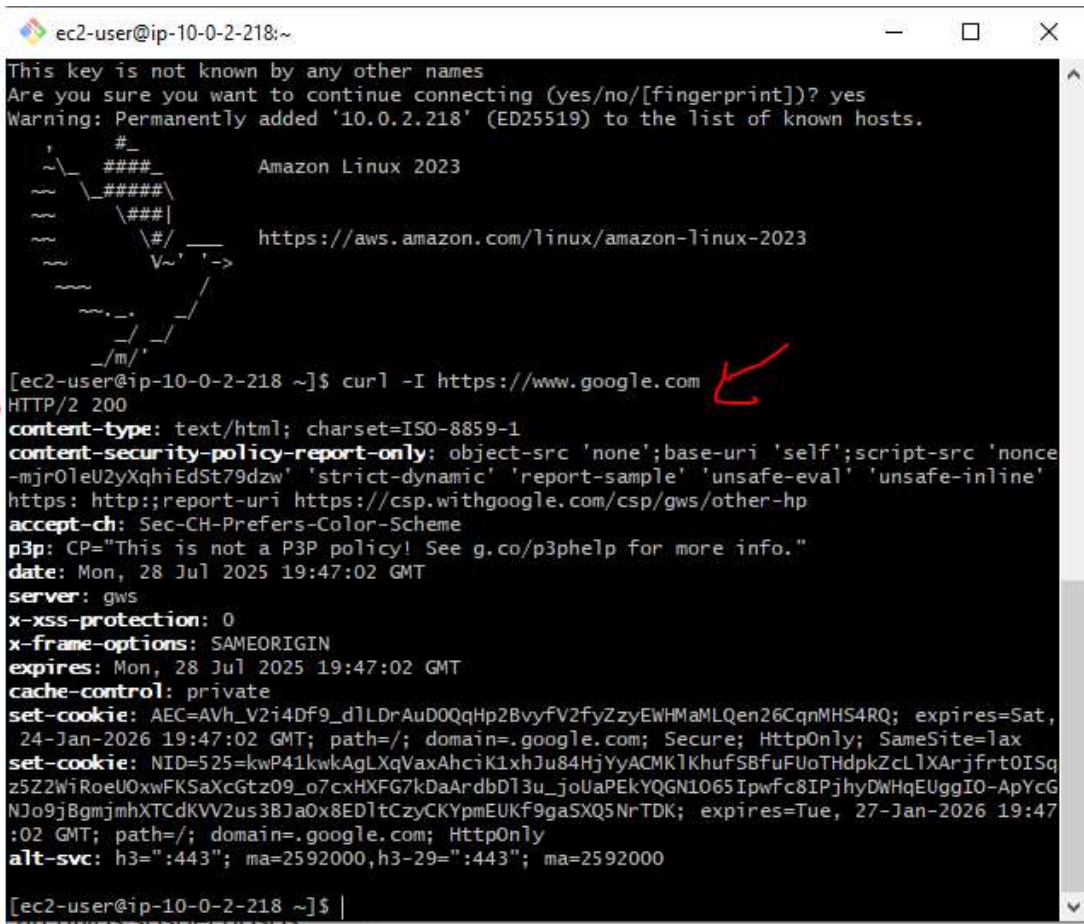
[ec2-user@ip-10-0-2-218 ~]$
```

Prueba de salida a internet desde la instancia privada

Una vez dentro de la EC2 privada, se ejecuta el siguiente comando para verificar conectividad a internet:

`curl https://www.google.com`

Respuesta exitosa (HTTP/2 200):



```
ec2-user@ip-10-0-2-218:~
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.218' (ED25519) to the list of known hosts.

#_
~_  ####_      Amazon Linux 2023
~_  #####\
~_  \###|
~_  \#/      https://aws.amazon.com/linux/amazon-linux-2023
~_  V~'  ' ->
~_  _./
~_  _/m/'

[ec2-user@ip-10-0-2-218 ~]$ curl -I https://www.google.com
HTTP/2 200
content-type: text/html; charset=ISO-8859-1
content-security-policy-report-only: object-src 'none';base-uri 'self';script-src 'nonce
-mjr01eU2yXqhiEdSt79dzw' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline'
https: http;;report-uri https://csp.withgoogle.com/csp/gws/other-hp
accept-ch: Sec-CH-Preferences-Color-Scheme
p3p: CP="This is not a P3P policy! See g.co/p3phelp for more info."
date: Mon, 28 Jul 2025 19:47:02 GMT
server: gws
x-xss-protection: 0
x-frame-options: SAMEORIGIN
expires: Mon, 28 Jul 2025 19:47:02 GMT
cache-control: private
set-cookie: AEC=AVh_V2i4Df9_d1LDrAuD0QqHp2BvyfV2fyZzyEWHMaMLQen26CqnMHS4RQ; expires=Sat,
24-Jan-2026 19:47:02 GMT; path=/; domain=.google.com; Secure; HttpOnly; SameSite=lax
set-cookie: NID=525=kwP41kwkAgLXqVaxAhciK1xhJu84HjYyACMK1KhufSBfuFUoTHdpkZcL1XArjfrt0ISq
z5Z2WiRoeU0xwFKSaXcGtz09_o7cxHXFG7kDaArdbD13u_joUaPEkYQGN1065Ipwfc8IPjhyDWHqEUggIO-ApYcG
NJo9jBgmjmhXTCdKVV2us3BJaOx8ED1tCzyCKYpmEUKf9ga5XQ5NrTDK; expires=Tue, 27-Jan-2026 19:47
:02 GMT; path=/; domain=.google.com; HttpOnly
alt-svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

[ec2-user@ip-10-0-2-218 ~]$ |
```

Esto demuestra que:

- La instancia privada no tiene IP pública
- Accede a internet a través del NAT Gateway
- Toda la conexión es controlada:
 - SSH desde PC local → EC2 pública
 - SSH desde pública → privada
 - curl desde privada → internet

Posibles escenarios de escalabilidad y conexión híbrida

En escenarios de crecimiento, se podrían agregar nuevas subredes públicas y privadas en diferentes zonas de disponibilidad, para mejorar la tolerancia a fallos y la alta disponibilidad. También sería útil incorporar balanceadores de carga y Auto Scaling Groups para distribuir la carga y ajustar la capacidad automáticamente.

En cuanto a conectividad híbrida, se podría crear una VPN que conecte una red on-premise con esta VPC de AWS, permitiendo comunicación segura entre ambos entornos y facilitando migraciones o integraciones.