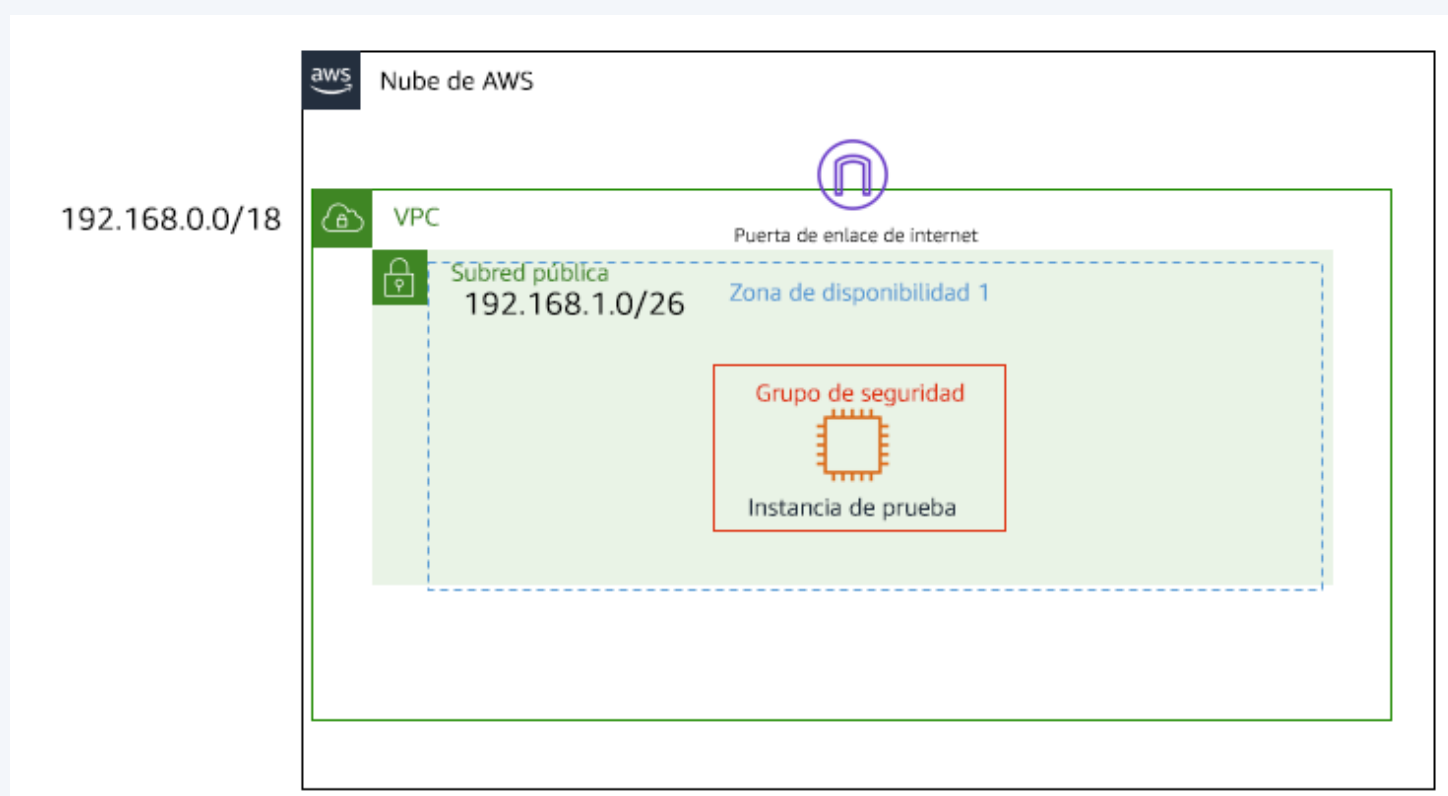


19°

Lab - AWS re/Start

Creación de recursos de redes dentro de una VPC



Tarea 01



Resolviendo el Ticket de Brock

¡Hola, equipo de soporte en la nube!

Hace unos días, me puse en contacto con ustedes para solicitar ayuda a fin de **configurar mi VPC**. Pensé que sabía adjuntar todos los recursos para establecer una **conexión a Internet**, pero ni siquiera puedo hacer ping por fuera de la VPC. ¡Todo lo que necesito es hacer ping! ¿Me pueden ayudar a configurar mi VPC donde tenga conectividad de red y pueda hacer ping? A continuación, se encuentra la arquitectura.

¡Gracias!

Brock, propietario de la empresa emergente

Nota, es conveniente recordar que para que los servicios dentro de una **subred pública tengan conexión a internet** es necesario una **puerta de enlace de internet (IGW)**. Y si quiero que un servicio dentro de una subred privada tenga conexión a internet, debemos usar una puerta de enlace NAT (el cual estará dentro de la subred pública).

Tarea 01



OJO:

- Los **grupos de seguridad** funcionan al **nivel de la instancia y tienen estado (stateful)**, lo que significa que **bloquean todo de forma predeterminada**.
- Las **NACL** funcionan al **nivel de la subred y no tienen estado**, lo que significa que **no bloquean nada de forma predeterminada**.
- una **tabla de enrutamiento** contiene las reglas o **rutas** que determinan **a dónde se dirigirá el tráfico** de red que se encuentra **en la subred y la VPC**

Empezamos por la creación de la VPC:

Create VPC [Info](#)

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as subnets, route tables, and security groups.

VPC settings

Resources to create [Info](#)
Create only the VPC resource or the VPC and other networking resources.

☐ VPC only ☒ VPC and more

Name tag auto-generation [Info](#)
Enter a value for the Name tag. This value will be used to auto-generate Name tags for all resources in the VPC.

☒ Auto-generate
Test VPC

IPv4 CIDR block [Info](#)
Determine the starting IP and the size of your VPC using CIDR notation.

192.168.0.0/18 16,384 IPs

CIDR block size must be between /16 and /28.

IPv6 CIDR block [Info](#)
☒ No IPv6 CIDR block
☐ Amazon-provided IPv6 CIDR block

Tenancy [Info](#)
Default

Tarea 01



Luego procedemos a **crear la subred** pública con el bloque CIDR de direcciones IP públicas requerido:

Create subnet [Info](#)

VPC

VPC ID

Create subnets in this VPC.

vpc-06d9cf01a6049e932 (Test VPC-vpc) ▼

Associated VPC CIDRs

IPv4 CIDRs

192.168.0.0/18

Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name

Create a tag with a key of 'Name' and a value that you specify.

Public Subnet

The name can be up to 256 characters long.

Availability Zone [Info](#)

Choose the zone in which your subnet will reside, or let Amazon choose one for you.

No preference ▼

IPv4 VPC CIDR block [Info](#)

Choose the IPv4 VPC CIDR block to create a subnet in.

192.168.0.0/18 ▼

IPv4 subnet CIDR block

192.168.1.0/28 16 IPs

< > ^ ▼

< SWIPE ≡

Tarea 01



Ahora, procedemos a crear la *tabla de enrutamiento*, que nos indicará **las direcciones IP y target** dentro de la VPC y subreds (dónde se dirige el tráfico), **define si una subred es pública o privada**.

OJO:

- Se debe asociar una tabla de enrutamiento a cada subred. Y se van asignando las rutas según se van creando los servicios en la VPC

[VPC](#) > [Route tables](#) > Create route table

Create route table [Info](#)

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Route table settings

Name - *optional*
Create a tag with a key of 'Name' and a value that you specify.

VPC
The VPC to use for this route table.

Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - <i>optional</i>	
<input type="text" value="Name"/>	<input type="text" value="Public route table"/>	<input type="button" value="Remove"/>

You can add 49 more tags.

[VPC](#) > [Internet gateways](#) > Create internet gateway

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.

[VPC](#) > [Internet gateways](#) > **Attach to VPC (igw-0cb49e72e9cb8173f)**

VPC

Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.

- ▶ AWS Command Line Interface command

Cancel

Attach internet gateway

igw-0cb49e72e9cb8173f / IGW test VPC

Details

Info

Internet gateway ID

igw-0cb49e72e9cb8173f

State

Attached

VPC ID

vpc-06d9cf01a6049e932 | Test VPC-vpc

Owner

252526466788

Tags

Search tags

Key

Value

Name

IGW test VPC

[VPC](#) > [Route tables](#) > [rtb-09b4bbde3907b5ad2](#) > [Edit routes](#)

Destination	Target	Status	Propagated
192.168.0.0/18	<div>local</div> <div>Q local X</div>	Active	No
<div>Q 0.0.0.0/0 X</div> <div>Add route</div>	<div>Internet Gateway</div> <div>Q igw-0cb49e72e9cb8173f X</div>	-	No <div>Remove</div>

Cancel
Preview
Save changes

Cancel

Preview

Save changes

Tarea 01



Y ahora asociamos la tabla de enrutamiento a la subred pública que hemos creado

VPC > Route tables > rtb-09b4bbde3907b5ad2 > Edit subnet associations

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (1/1)

Q Filter subnet associations

<input checked="" type="checkbox"/>	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
<input checked="" type="checkbox"/>	Public Subnet	subnet-057d8851f560a8222	192.168.1.0/28	-	Main (rtb-094d584dcc6121961)

Selected subnets

subnet-057d8851f560a8222 / Public Subnet X

Cancel Save associations

Ahora, procedemos a crear una *lista de control de acceso de red (NACL)*, que es un firewall de la subred.
OJO: Primero se evalúa la regla con el número menor

VPC > Network ACLs > Create network ACL

Create network ACL [Info](#)

A network ACL is an optional layer of security that acts as a firewall for controlling traffic in and out of a subnet.

Network ACL settings

Name - *optional*
Creates a tag with a key of 'Name' and a value that you specify.

Public Subnet NACL

VPC
VPC to use for this network ACL.

vpc-06d9cf01a6049e932 (Test VPC-vpc)

Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - <i>optional</i>	
Q Name X	Q Public Subnet NACL X	Remove tag

Add tag

You can add 49 more tags

Cancel Create network ACL

Tarea 01



Y debemos modificar las reglas de ingreso y salida de tráfico de la subred.

En el caso de **inbound rules**, indica que hay un solo número de regla, que es 100 y que establece que **todo el tráfico**, todos los protocolos y todos los rangos de puerto desde **cualquier origen (0.0.0.0/0) pueden ingresar (entrar) a la subred**. El asterisco * **indica que se rechaza todo** lo que **no coincida con esta regla**. Similar para outbound, pero para tráfico que sale de la subred a cualquier destino (0.0.0.0/0)

Details

Inbound rules

Outbound rules

Subnet associations

Tags

Inbound rules (2)

Edit inbound rules

< 1 > ⚙

Q Filter inbound rules

Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	✔ Allow
*	All traffic	All	All	0.0.0.0/0	✘ Deny

Details

Inbound rules

Outbound rules

Subnet associations

Tags

Outbound rules (2)

Edit outbound rules

< 1 > ⚙

Q Filter outbound rules

Rule number	Type	Protocol	Port range	Destination	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	✔ Allow
*	All traffic	All	All	0.0.0.0/0	✘ Deny

Tarea 01



Ahora procedemos a crear un **grupo de seguridad**, el cual es una capa de seguridad a nivel de instancia. Pero a diferencia de la NACL, **no pueden rechazar tráfico**.

Create security group [Info](#)

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name [Info](#)

Name cannot be edited after creation.

Description [Info](#)

VPC [Info](#)

vpc-06d9cf01a6049e932 (Test VPC-vpc) ▾

Para las **reglas de entrada**, está permitiendo los tipos de tráfico **SSH, HTTP y HTTPS**, cada uno con sus propios protocolos y rango de puertos. El origen desde el que este tráfico llega a la instancia **se puede originar desde cualquier lugar**. En el caso de las **reglas de salida**, está permitiendo todo el tráfico hacia afuera de su instancia.

Inbound rules [Info](#)

Type Info	Protocol Info	Port range Info	Source Info
SSH ▾	TCP	22	Anywhe... ▾ 0.0.0.0/0 ✕
HTTP ▾	TCP	80	Anywhe... ▾ 0.0.0.0/0 ✕
HTTPS ▾	TCP	443	Anywhe... ▾ 0.0.0.0/0 ✕
Add rule			

⚠ Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP

Outbound rules [Info](#)

Type Info	Protocol Info	Port range Info	Destination Info
All traffic ▾	All	All	Anywhe... ▾ 0.0.0.0/0 ✕

Tarea 01



Ahora creamos una instancia de EC2, la cual será desplegada dentro de la subred pública creada. Luego verificaremos si todos nuestros cursos de red que hemos creado están correctamente configurados

▼ Network settings Info

VPC - required Info

vpc-06d9cf01a6049e932 (Test VPC-vpc)
192.168.0.0/18

↻

Subnet Info

subnet-057d8851f560a8222 Public Subnet

VPC: vpc-06d9cf01a6049e932 Owner: 252526466788
Availability Zone: us-west-2c IP addresses available: 11 CIDR: 192.168.1.0/28

↻ Create new subnet

Auto-assign public IP Info

Disable

▼

Firewall (security groups) Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☐ Create security group

☒ Select existing security group

Common security groups Info

Select security groups

▼

public security group sg-039b4b47dfc9cb7d6 ✕
VPC: vpc-06d9cf01a6049e932

↻ Compare security group rules

Security groups that you add or remove here will be added to or removed from all your network interfaces.

► Advanced network configuration

EC2 > Instances > i-0d18d42a7d83807bc

Instance summary for i-0d18d42a7d83807bc (Test EC2) Info

Updated less than a minute ago

↻

Connect

Instance state ▼

Actions ▼

Instance ID i-0d18d42a7d83807bc (Test EC2)	Public IPv4 address 35.91.115.247 open address	Private IPv4 addresses 192.168.1.12
IPv6 address -	Instance state Running	Public IPv4 DNS ec2-35-91-115-247.us-west-2.compute.amazonaws.com open address

SWIPE

Tarea 01



Ahora mediante la conexión por SSH, verificaremos la conectividad:

```
ec2-user@ip-192-168-1-12:~  
login as: ec2-user  
Authenticating with public key "imported-openssh-key"  
#  
~\  #####_      Amazon Linux 2023  
~~ \  #####\  
~~  \####|  
~~   \#/      https://aws.amazon.com/linux/amazon-linux-2023  
~~    V~' '->  
~~~  
~~.-.  
~~/_/  /  
_/_/m/' ->  
[ec2-user@ip-192-168-1-12 ~]$ ping google.com  
PING google.com (142.250.69.206) 56(84) bytes of data.  
64 bytes from sea30s08-in-f14.1e100.net (142.250.69.206): icmp_seq=1 ttl=117 time=9.25 ms  
64 bytes from sea30s08-in-f14.1e100.net (142.250.69.206): icmp_seq=2 ttl=117 time=10.1 ms  
64 bytes from sea30s08-in-f14.1e100.net (142.250.69.206): icmp_seq=3 ttl=117 time=9.35 ms  
64 bytes from sea30s08-in-f14.1e100.net (142.250.69.206): icmp_seq=4 ttl=117 time=9.37 ms  
64 bytes from sea30s08-in-f14.1e100.net (142.250.69.206): icmp_seq=5 ttl=117 time=9.32 ms  
^C  
--- google.com ping statistics ---  
21 packets transmitted, 21 received, 0% packet loss, time 20019ms  
rtt min/avg/max/mdev = 9.247/9.359/10.127/0.176 ms  
[ec2-user@ip-192-168-1-12 ~]$
```

Notamos que sí existe conectividad.