

## S7: Laboratorio: Creación de una VPC y lanzamiento de un servidor web

En este laboratorio usted:

- Crear una Virtual Private Cloud (VPC)
- Crear subredes
- Configurar un grupo de seguridad
- Lanzar una instancia de Amazon Elastic Compute Cloud (Amazon EC2) en la VPC

### Tarea 1: crear una VPC

En esta tarea, utilizará el asistente de la VPC para crear una VPC, una puerta de enlace de Internet y dos subredes en una única zona de disponibilidad. Una puerta de enlace de Internet es un componente de la VPC que permite la comunicación entre las instancias de la VPC e Internet.

Después de crear una VPC, puede agregar subredes. Cada subred reside por completo en una zona de disponibilidad y no puede abarcar otras zonas. Si el tráfico de una subred se dirige a una puerta de enlace de Internet, la subred recibe el nombre de subred pública. Si una subred no dispone de una ruta a la puerta de enlace de Internet, la subred recibe el nombre de subred privada.

El asistente también creará una puerta de enlace de NAT, que se utiliza para brindar conectividad a Internet a instancias EC2 en las subredes privadas.

1. En la Consola de administración de AWS, en la barra de búsqueda, ingrese y seleccione la VPC para ir al VPC Dashboard (Panel de la VPC).
2. Elija Create VPC (Crear VPC) y configure las siguientes opciones:
  - Resources to create (Recursos a crear): elija VPC and more (VPC y más)
  - En Name tag auto-generation (Generación automática de etiqueta de nombre): desmarque Auto-generate (Auto generar)
  - IPv4 CIDR: ingrese 10.0.0.0/16
  - IPv6 CIDR block (Bloque de CIDR IPv6) seleccione No IPv6 CIDR block (sin bloque de CIDR IPv6).
  - Tenancy (Tenencia): seleccione Default (Predeterminado).
  - Number of availability Zones (AZs) (Número de zonas de disponibilidad): 1
  - Number of public subnets (Número de subredes públicas): 1
  - Number of private subnets (Número de subredes privadas): 1
  - Expand Customize subnets CIDR blocks (Personalizar bloques de CIDR de las subredes)
  - Public subnet CIDR block in region (Bloque de CIDR de la subred pública): 10.0.0.0/24
  - Private subnet CIDR block in region (Bloque de CIDR de la subred privada): 10.0.1.0/24
  - NAT gateways (Puertas de enlace NAT): seleccione In 1 AZ (En 1 zona de disponibilidad)
  - VPC endpoints (Puntos de enlace de la VPC): elija None (Ninguno).

## Configuración de la VPC

### Recursos que se van a crear [Información](#)

Cree únicamente el recurso de VPC o la VPC y otros recursos de red.

☐ Solo la VPC

☒ VPC y más

### Generación automática de etiquetas de nombre [Información](#)

Ingrese un valor para la etiqueta Nombre. Este valor se utilizará para generar automáticamente etiquetas Nombre para todos los recursos de la VPC.

☐ Generar automáticamente

### Bloque de CIDR IPv4 [Información](#)

Determine la IP inicial y el tamaño de la VPC mediante la notación CIDR.

10.0.0.0/16

65.536 IPs

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 proporcionado por Amazon

### Tenencia [Información](#)

Predeterminado

### Número de zonas de disponibilidad (AZ) [Información](#)

Elija la cantidad de zonas de disponibilidad en las que desea aprovisionar subredes. Le recomendamos que tenga al menos dos para incrementar la disponibilidad.

1

2

3

► Personalizar las zonas de disponibilidad

### Cantidad de subredes públicas [Información](#)

La cantidad de subredes públicas que se van a agregar a la VPC. Utilice subredes públicas para las aplicaciones web que deban ser accesibles públicamente a

### Cantidad de subredes públicas [Información](#)

La cantidad de subredes públicas que se van a agregar a la VPC. Utilice subredes públicas para las aplicaciones web que deban ser accesibles públicamente a través de Internet.

0

1

### Cantidad de subredes privadas [Información](#)

La cantidad de subredes privadas que se van a agregar a la VPC. Utilice subredes privadas para proteger los recursos del backend que no necesitan acceso público.

0

1

2

### ▼ Personalizar bloques de CIDR de subredes

Bloque de CIDR de la subred pública en us-west-2a

10.0.0.0/24

256 IPs

Bloque de CIDR de la subred privada en us-west-2a

10.0.1.0/24

256 IPs

### Gateways NAT (\$) [Información](#)

Elija el número de zonas de disponibilidad (AZ) en las que crear gateway NAT. Tenga en cuenta que hay un cargo por cada puertan de enlace NAT.

Ninguna

En 1 AZ

1 por zona de disponibilidad

### Puntos de enlace de la VPC [Información](#)

Los puntos de enlace pueden ayudar a reducir los cargos de gateway NAT y mejorar la seguridad gracias a la posibilidad de acceder a S3 directamente desde la VPC. De forma predeterminada, se utiliza una política de acceso completo. Puede personalizar esta política en cualquier momento.

Ninguna

Gateway de S3

### Opciones de DNS [Información](#)

☒ Habilitar nombres de host DNS

☒ Habilitar la resolución de DNS

### ► Etiquetas adicionales

3. En el panel de vista previa, asigne los siguientes nombres a los recursos: VPC: Lab VPC

- Subredes (2)
- Primera casilla, subred pública uno sin etiqueta de nombre: Public Subnet 1
- Segunda casilla, subred privada uno sin etiqueta de nombre: Private Subnet 1
- Tablas de enrutamiento (2)
- Primera casilla, tabla de enrutamiento pública sin etiqueta de nombre: Public Route Table
- Segunda casilla, tabla de enrutamiento privada sin etiqueta de nombre: Private Route Table





4. Elija Create VPC (Crear VPC).

## Flujo de trabajo de creación de VPC

~ Verificar la creación de una VPC: [vpc-0618072080076fe0b](#) 

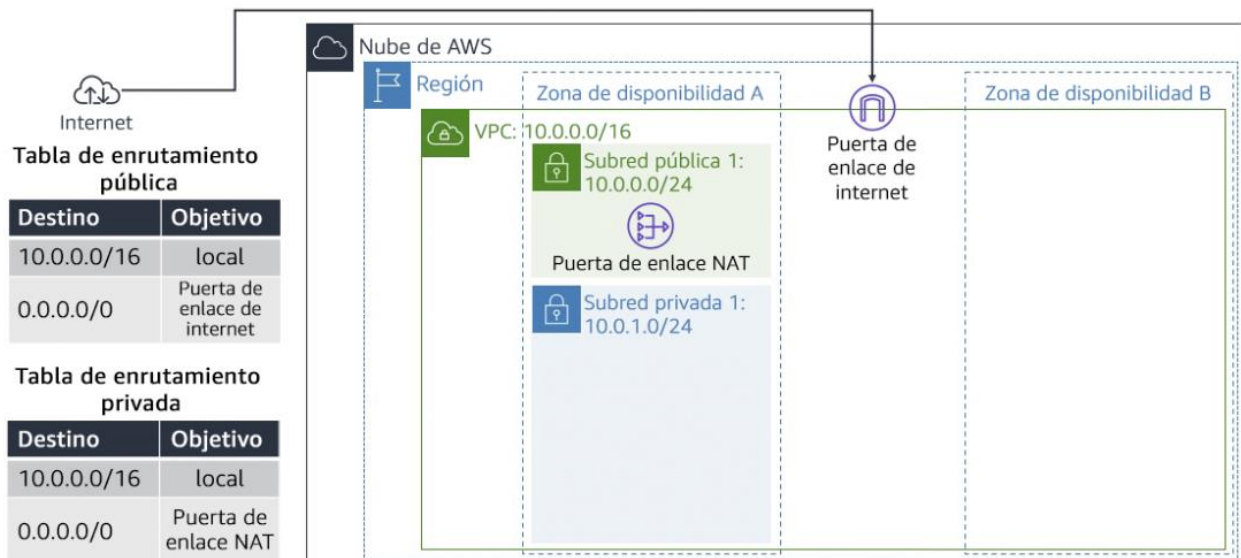
17%

### ▼ Detalles

- ✓ Crear VPC: [vpc-0618072080076fe0b](#) 
- ✓ Habilitar nombres de host DNS
- ✓ Habilitar la resolución de DNS
- ⏸ Verificar la creación de una VPC: [vpc-0618072080076fe0b](#) 
- 🕒 Crear subred
- 🕒 Crear subred
- 🕒 Crear una gateway de Internet
- 🕒 Adjuntar gateway de Internet a la VPC
- 🕒 Crear tabla de enrutamiento
- 🕒 Crear ruta
- 🕒 Asociar tabla de enrutamiento
- 🕒 Asignar IP elástica
- 🕒 Crear gateway NAT
- 🕒 Espere a que se activen las gateways NAT
- 🕒 Crear tabla de enrutamiento
- 🕒 Crear ruta
- 🕒 Asociar tabla de enrutamiento
- 🕒 Verificando la creación de la tabla de enrutamiento

5. Seleccione View VPC (Ver VPC).

Los detalles de *Lab-vpc* se muestran según la configuración.



La subred pública tiene un enrutamiento entre dominios sin clase (CIDR) de 10.0.0.0/24, lo que significa que contiene todas las direcciones IP que comienzan con 10.0.0.x.

La subred privada tiene un CIDR de 10.0.1.0/24, lo que significa que contiene todas las direcciones IP que comienzan con 10.0.1.x.

## Tarea 2: Crear subredes adicionales

En esta tarea, creará dos subredes adicionales en una segunda zona de disponibilidad. Esto resulta útil para crear recursos en varias zonas de disponibilidad a fin de proporcionar alta disponibilidad.

6. En el panel de navegación izquierdo, haga clic en **Subnets** (Subredes).
7. Para configurar la segunda subred pública, elija **Create subnet** (Crear subred) y configure las siguientes opciones:
  - **VPC ID** (ID de la VPC): en la lista desplegable, elija **Lab VPC** (VPC de laboratorio).
  - **Subnet name** (Nombre de subred): ingrese **Public Subnet 2**
  - **Availability Zone** (Zona de disponibilidad): en la lista desplegable, elija la segunda zona de disponibilidad.
  - **IPv4 CIDR block** (Bloque de CIDR IPv4): ingrese **10.0.2.0/24**
8. Elija **Create subnet** (Crear subred).

### 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.  
  
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.

**IPv4 VPC CIDR block** [Información](#)  
Choose the IPv4 VPC CIDR block to create a subnet in.

**IPv4 subnet CIDR block**  
 256 IPs  

< > ^ v

**▼ Etiquetas: opcional**

**Clave**

**Valor - opcional**

Quitar

Agregar nueva etiqueta

Puede agregar 49 más etiquetas.

Quitar

Agregar nueva subred

Cancelar **Crear subred**

La subred tendrá todas las direcciones IP que comiencen con **10.0.2.x**.

9. Para configurar la segunda subred privada, seleccione **Create subnet** (Crear subred) y configure las siguientes opciones:

- **VPC ID** (ID de la VPC): en la lista desplegable, elija **Lab VPC** (VPC de laboratorio).
- **Subnet name** (Nombre de subred): ingrese **Private Subnet 2**
- **Availability Zone** (Zona de disponibilidad): en la lista desplegable, elija la segunda zona de disponibilidad.
- **IPv4 CIDR block** (Bloque de CIDR IPv4): ingrese **10.0.3.0/24**

### 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.

Private Subnet 2

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. Oeste (Oregón) / us-west-2b

**IPv4 VPC CIDR block** [Información](#)  
Choose the IPv4 VPC CIDR block to create a subnet in.

10.0.0.0/16

**IPv4 subnet CIDR block**

10.0.3.0/24 256 IPs

< > ^ v

▼ **Etiquetas: opcional**

Clave	Valor - opcional
<div>Q Name X</div>	<div>Q Private Subnet 2 X</div>

Quitar

Agregar nueva etiqueta

Puede agregar 49 más etiquetas.

Quitar

Agregar nueva subred

Cancelar

Crear subred

10. Elija **Create subnet** (Crear subred).

La subred tendrá todas las direcciones IP que comiencen con **10.0.3.x**.

### Tarea 3: asociar las subredes y agregar rutas

11. En el panel de navegación izquierdo, elija **Route Tables** (Tablas de enrutamiento).
12. Seleccione **Public Route Table** (Tabla de enrutamiento pública)
13. En el panel inferior, haga clic en la pestaña **Subnet associations** (Asociaciones de subredes).
14. En **Subnets without explicit associations** (Subredes sin asociaciones explícitas), elija **Edit subnet associations** (Editar asociaciones de subredes).
15. Marque la casilla de **Public Subnet 2** (Subred pública 2).
16. Elija **Save associations** (Guardar asociaciones).

## Editar asociaciones de subredes

Cambiar las subredes que están asociadas a esta tabla de enrutamiento.

### Subredes disponibles (1/4)

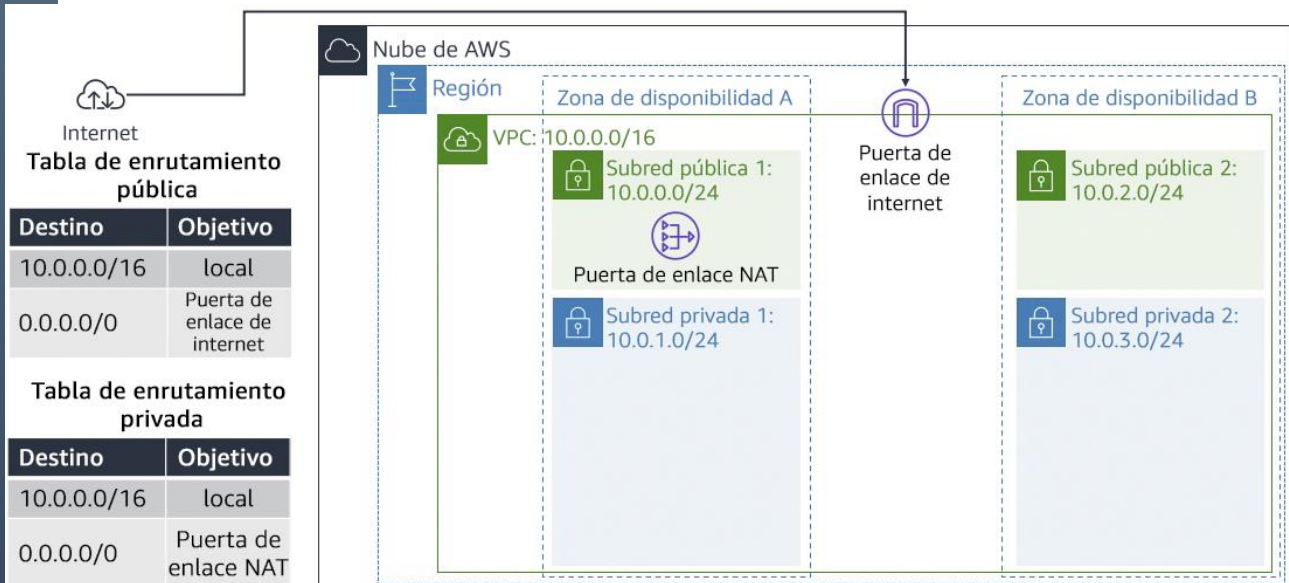
🔍 Filtrar asociaciones de subredes

<input type="checkbox"/>	Nombre	ID de subred	CIDR IPv4
<input type="checkbox"/>	Public Subnet 1	<a href="#">subnet-06b3f01351012dcf6</a>	10.0.0.0/24
<input type="checkbox"/>	Private Subnet 2	<a href="#">subnet-0b1eb7b34713eb669</a>	10.0.3.0/24
<input type="checkbox"/>	Private Subnet 1	<a href="#">subnet-0b9267788446f0a62</a>	10.0.1.0/24
<input checked="" type="checkbox"/>	Public Subnet 2	<a href="#">subnet-0bc5ddc0b79d1ca9f</a>	10.0.2.0/24

Ahora configurará la tabla de enrutamiento que utilizan las subredes privadas.

17. Seleccione **Private route table** (Tabla de enrutamiento privada).
18. En el panel inferior, haga clic en la pestaña **Subnet associations** (Asociaciones de subredes).
19. En **Subnets without explicit associations** (Subredes sin asociaciones explícitas), elija **Edit subnet associations** (Editar asociaciones de subredes).
20. Marque la casilla de **Private Subnet 2** (Subred privada 2).
21. Elija **Save associations** (Guardar asociaciones).

Ahora la VPC tiene subredes públicas y privadas configuradas en dos zonas de disponibilidad:



# Editar asociaciones de subredes

Cambiar las subredes que están asociadas a esta tabla de enrutamiento.

Subredes disponibles (1/4)

Filtrar asociaciones de subredes

<div><div></div></div>	Nombre	ID de subred	CIDR IPv4
<input type="checkbox"/>	Public Subnet 1	<a href="#">subnet-06b3f01351012dcf6</a>	10.0.0.0/24
<input checked="" type="checkbox"/>	Private Subnet 2	<a href="#">subnet-0b1eb7b34713eb669</a>	10.0.3.0/24
<input type="checkbox"/>	Private Subnet 1	<a href="#">subnet-0b9267788446f0a62</a>	10.0.1.0/24
<input type="checkbox"/>	Public Subnet 2	<a href="#">subnet-0bc5ddc0b79d1ca9f</a>	10.0.2.0/24

## Tarea 4: crear un grupo de seguridad de VPC

En esta tarea, creará un grupo de seguridad de la VPC, que actúa como un firewall virtual para la instancia. Cuando se lanza una instancia, se asocian a ella uno o varios grupos de seguridad. Puede agregar reglas a cada grupo de seguridad que permitan el tráfico hacia las instancias asociadas o desde ellas.

22. En el panel de navegación izquierdo, elija **Security Groups** (Grupos de seguridad).

23. Elija **Create security group** (Crear grupo de seguridad).

24. Configure el grupo de seguridad con las siguientes opciones:

- **Security group name** (Nombre del grupo de seguridad) ingrese **Web Security Group**
- **Description** (Descripción): ingrese **Enable HTTP access**
- **VPC:** elija **Lab VPC** (VPC de laboratorio).

25. En **Inbound rules** (Reglas de entrada), seleccione **Add rule** (Agregar regla).

26. Configure las siguientes opciones:

- **Type** (Tipo): elija **HTTP**.
- **Source** (Fuente): seleccione **Anywhere IPv4** (IPv4 en cualquier lugar).
- **Description** (Descripción): ingrese **Permit web requests**

27. Elija **Create security group** (Crear grupo de seguridad).

En la siguiente tarea, utilizará este grupo de seguridad cuando lance una instancia de EC2.

**Detalles básicos**

Nombre del grupo de seguridad [Información](#)

Web Security Group

El nombre no se puede editar después de su creación.

Descripción [Información](#)

Enable HTTP access

VPC [Información](#)

vpc-0618072080076fe0b (Lab VPC)

**Reglas de entrada** [Información](#)

Este grupo de seguridad no tiene reglas de entrada.

Agregar regla

**Reglas de salida** [Información](#)

Tipo <a href="#">Información</a>	Protocolo <a href="#">Información</a>	Intervalo de puertos <a href="#">Informición</a>	Destino <a href="#">Información</a>
HTTP	TCP	80	Anywhere-IPv4

0.0.0.0/0

Agregar regla



## Tarea 5: lanzar una instancia de servidor web

En esta tarea, lanzará una instancia de EC2 en la VPC nueva. Configuraré la instancia para que actúe como un servidor web.

28. En la Consola de administración de AWS, en la barra de **búsqueda**, ingrese y seleccione la **EC2** para ir a la **Consola de administración de EC2**.
29. En el panel de navegación izquierdo, seleccione **Instances** (Instancias).
30. Elija **Launch Instances** (Iniciar instancias) y configure las siguientes opciones:

- En la sección **Name and tags** (Nombre y etiquetas), **Name** (Nombre): **Web Server 1**
- En la sección **Application and OS Images (Amazon machine Image)** (Imágenes de la aplicación y el sistema operativo [Imagen de máquina de Amazon]), configure las siguientes opciones:
- **Quick Start**: seleccione **Amazon Linux**.
- **Imagen de máquina de Amazon (AMI)**: en el menú desplegable, seleccione **Amazon Linux 2023 AMI**.
- En la sección **Instance type** (Tipo de instancia), elija **t3.micro**.
- En la sección **Key pair (login)** (Par de claves [inicio de sesión]), seleccione **AWS Labs KeyPair- <random string - stack id>**.

31. En la sección **Network Settings** (Configuración de red), seleccione **Edit** (Editar) y configure las siguientes opciones:

- **VPC - required** (VPC: obligatoria): elija **Lab VPC** (VPC de laboratorio).
- **Subnet** (Subred): elija **Public Subnet 2** (Subred pública 2).
- **Auto-assign public IP** (Asignar automáticamente IP pública): elija **Enable** (Habilitar).
- En **Firewall (security groups)** (Firewall [grupos de seguridad]): elija **Select existing security group** (Seleccionar grupo de seguridad existente).
  - Seleccione **Web Security Group** (Grupo de seguridad web).

32. Expanda **Advanced details** (Detalles avanzados).

33. En **User data** (Datos de usuario), copie y pegue el siguiente código.

```
#!/bin/bash
```

```
#Install Apache Web Server and PHP
```

```
dnf install-y httpd mariadb105-server php
```

```
#Download Lab files
```

```
wget https://us-east-1-tcprod.s3.amazonaws.com/courses/CUR-TF-100-RSNETK/v3.0.0.prod-ea58589a/267-lab-NF-build-vpc-web-server/scripts/lab-app.zip
```

```
unzip lab-app.zip-d /var/www/html/
```

```
#Turn on web server
```

```
systemctl enable httpd
```

```
systemctl start httpd
```

34. Seleccione **Launch Instance** (Iniciar instancia).
35. Para ver las instancias lanzadas, elija **View all instances** (Ver todas las instancias).
36. Espere a que **Web Server 1** (Servidor web 1) muestre el mensaje **2/2 checks passed** (2/2 comprobaciones aprobadas) en la columna **Status Checks** (Comprobaciones de estado).
37. Esto puede tardar unos minutos. Para actualizar la página, elija actualizar en la parte superior de la página.

Número de instancias [Información](#)

1

Software Image (AMI)

Amazon Linux 2023 AMI 2023.3.2...[read more](#)  
ami-0944e91aed79c721c

Virtual server type (instance type)

t3.micro

Firewall (security group)

Web Security Group

Storage (volumes)

1 volume(s) - 8 GiB

**Nivel gratuito:** El primer año incluye ×  
750 horas de uso de instancias  
t2.micro (o t3.micro en las regiones  
en las que t2.micro no esté  
disponible) en las AMI del nivel  
gratuito al mes, 30 GiB de  
almacenamiento de EBS, 2 millones  
de E/S, 1 GB de instantáneas y  
100 GB de ancho de banda a  
Internet.

```
#!/bin/bash
#Install Apache Web Server and PHP
dnf install -y httpd mariadb105-server php
#Download Lab files
wget https://us-east-1-tcprod.s3.amazonaws.com/courses/CUR-TF-100-
RSNETK/v3.0.0.prod-ea58589a/267-lab-NF-build-vpc-web-server/scripts/lab-
app.zip
unzip lab-app.zip -d /var/www/html/
#Turn on web server
systemctl enable httpd
systemctl start httpd
```

Cancelar

Lanzar instancia

[Revisar comandos](#)

Ahora se conectará al servidor web que se ejecuta en la instancia de EC2.

38. Seleccione la casilla de verificación de la instancia y elija la pestaña **Details** (Detalles).
39. Copie el valor de **Public IPv4 DNS** (DNS público de IPv4).
40. Abra una pestaña nueva del navegador web, pegue el valor de **Public DNS** (DNS público) y presione Enter.

La página debería verse de la siguiente manera:

Meta-Data	Value
InstanceId	i-05a488dac28dc5d0f
Availability Zone	us-west-2b

Current CPU Load: 0%

La siguiente es la arquitectura completa que implementó:

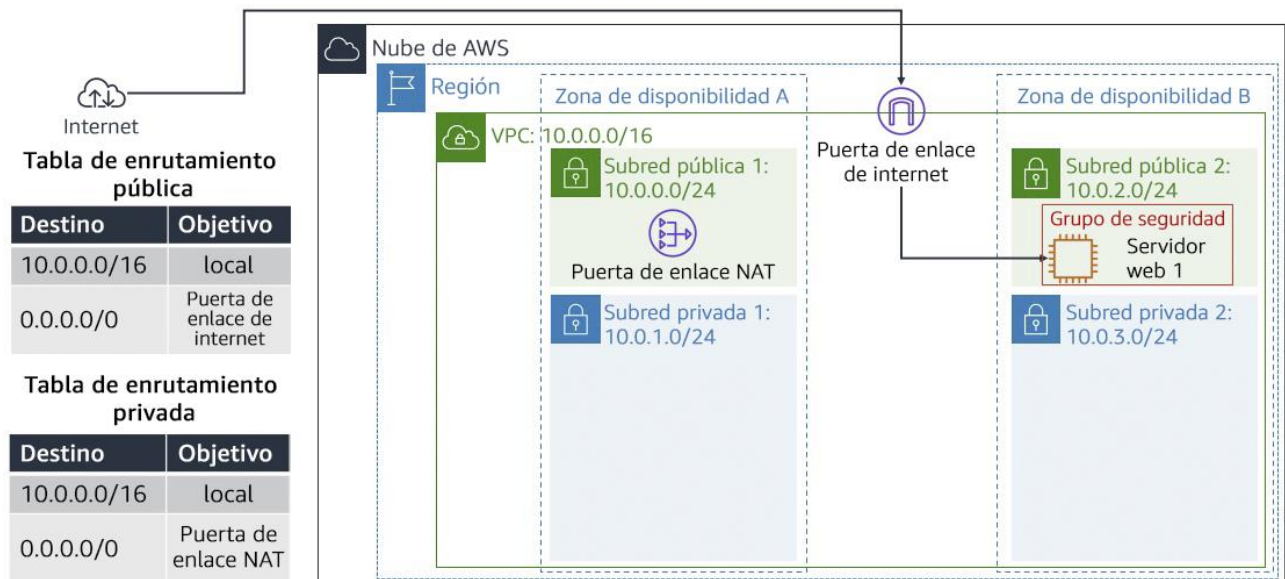


Figura: una imagen del producto final, que es la entrega de la solicitud exacta del cliente: una VPC completamente funcional con sus recursos (red y seguridad) y un servidor web.