COLOMBIA POTENCIA DE LA VIDA

TIC

LECCIÓN 3: CONFIGURACIÓN DE SUBREDES PÚBLICAS Y PRIVADAS Y PROTOCOLOS DE INTERNET

TALENTO TECH | AZ PROYECTOS EDUCATIVOS | UTP Universidad Tecnológica de Pereira

EN ESTA, SE DESCRIBE CÓMO CONFIGURAR SUBREDES PÚBLICAS Y PRIVADAS Y PROTOCOLOS DE INTERNET.

PUERTA DE ENLACE DE INTERNET

- Proporciona un Objetivo en las tablas de enrutamiento de la VPC para el tráfico direccionable en Internet

- Realiza la traducción de direcciones de red (NAT) de las instancias a las que les han asignado direcciones IPv4 públicas

- Es compatible con el tráfico IPv4 e IPv6

- No supone ningún cargo adicional en su cuenta

UNA PUERTA DE ENLACE DE INTERNET TIENE DOS PROPÓSITOS:

- Proporciona un objetivo en las tablas de enrutamiento de la VPC para el tráfico direccionable en Internet
- Realiza la traducción de direcciones de red (NAT) de las instancias a las que se les han asignado direcciones IPv4 públicas

Una puerta de enlace de internet admite tráfico IPv4 e IPv6, y no provoca riesgos de disponibilidad ni limitaciones de ancho de banda en el tráfico de su red. Tener una puerta de enlace de internet en su cuenta no supone ningún gasto adicional.

COLOMBIA POTENCIA DE LA VIDA

TIC

PARA HABILITAR EL ACCESO DESDE O HACIA INTERNET PARA LAS INSTANCIAS DE UNA SUBRED EN UNA VPC, DEBE HACER LO SIGUIENTE:

1. **Crear una puerta de enlace de internet y adjuntarla a su VPC.**
2. **Agregar una ruta a la tabla de enrutamiento de la subred que dirija el tráfico de Internet a la puerta de enlace de internet.**
3. **Confirmar que cada instancia en su subred tiene una dirección IP única global (dirección IPv4 pública, dirección IP elástica o dirección IPv6).**
4. **Confirmar que las reglas ACL y de grupo de seguridad de su red permiten que el tráfico relevante fluya hacia y desde su última instancia.**

Para más información, consulte Conexión a Internet mediante una puerta de enlace de Internet en la Guía del usuario de Amazon VPC en https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Internet_Gateway.html

PUERTA DE ENLACE NAT

- Admite instancias en una subred privada para conectarse a internet o a otros servicios de AWS.

- Impide que la Internet inicie una conexión con esas instancias

- Requiere que Se especifique 10 siguiente en el momento la creación:

-Subred pública en la debe residir la puerta de enlace de NAT
- Una dirección IP elástica para asociar con la puerta de enlace NAT

- Tras su creación es necesario actualizar la tabla de enrutamiento de una o varias subredes privadas para dirigir el tráfico de Internet a la puerta de enlace NAT.

Una puerta de enlace de traducción de direcciones de red (NAT) permite a las instancias de una subred privada conectarse a Internet o a otros servicios de AWS. Una puerta de enlace NAT también impide que Internet inicie una conexión con esas instancias.

Para crear una puerta de enlace NAT, debe especificar la subred pública en la que se debe ubicar la puerta de enlace NAT. También debe especificar una dirección IP elástica para asociar a la puerta de enlace NAT. Después de crear una puerta de enlace NAT, debe actualizar la tabla de enrutamiento que está asociada a una o más de las subredes privadas para dirigir el tráfico de Internet a la puerta de enlace NAT. De esa manera, las instancias de sus subredes privadas se pueden comunicar con Internet.

También puede utilizar una instancia NAT en una subred pública de su VPC en lugar de una puerta de enlace NAT. Sin embargo, una puerta de enlace NAT es un servicio NAT administrado que ofrece mayor disponibilidad, mayor ancho de banda y menos esfuerzo administrativo. Para los casos prácticos habituales, AWS recomienda utilizar una puerta de enlace NAT en lugar de una instancia de NAT.

Para más información, consulte los siguientes temas en la Guía del usuario de Amazon VPC:
Puertas de enlace NAT en https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html
Instancias de NAT en https://docs.aws.amazon.com/vpc/latest/userguide/VPC_NAT_Instance.html
Compare puertas de enlace NAT e instancias de NAT en https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-comparison.html

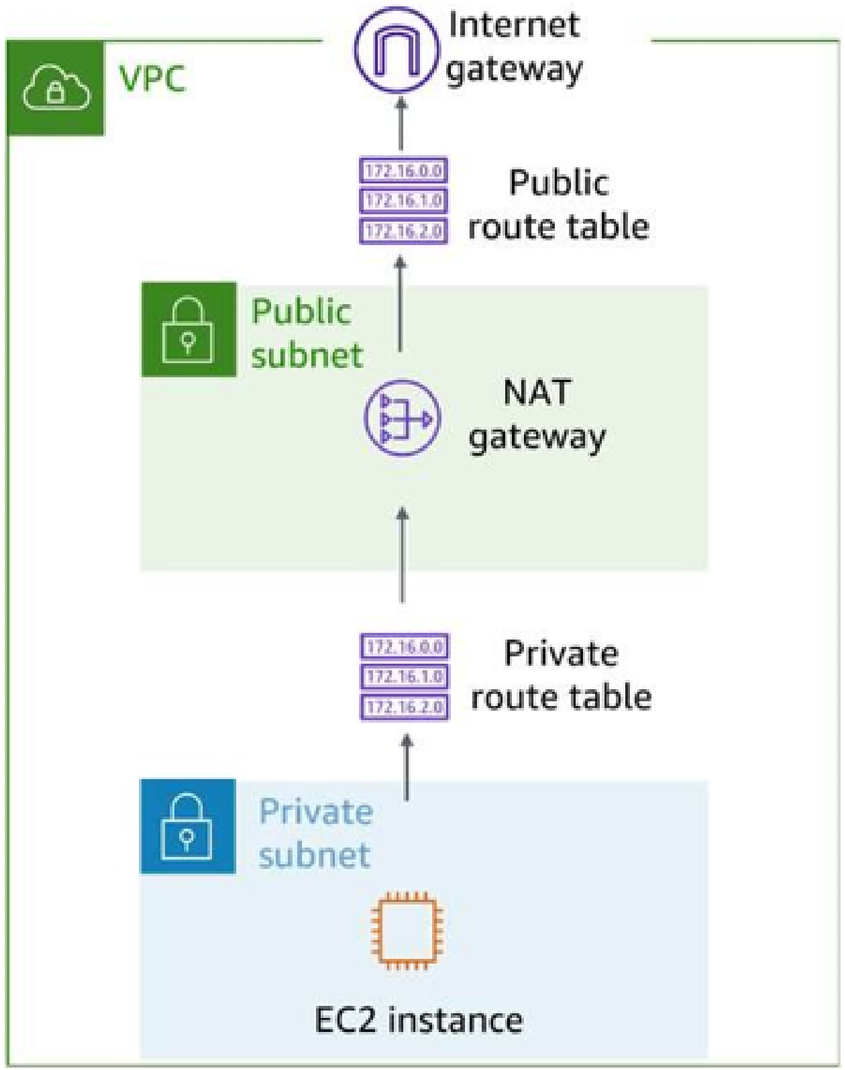
SUBRED PRIVADA

• Todas Las subredes constan de un rango contiguo de direcciones IP.

• No se puede acceder a las interfaces adjuntas a instancias en subredes privadas desde fuera de la VPC principal.

• Las subredes privadas para instancias de base datos a la que no necesario acceder a través de la Internet pública.

El diagrama de una VPC con una subred pública y otra privada. Una instancia de EC2 en la subred privada dirige el tráfico a una tabla de enrutamiento privada y, a continuación, a una puerta de enlace NAT en la subred pública. A partir de ahí, el tráfico se encamina a una tabla de enrutamiento pública y luego a una puerta de enlace de internet.


VPC
Internet gateway
172.16.0.0
172.16.1.0
172.16.2.0
Public route table
Public subnet
NAT gateway
172.16.0.0
172.16.1.0
172.16.2.0
Private route table
Private subnet
EC2 instance

- Todas las subredes constan de un rango contiguo de direcciones IP. Estas direcciones no deben solaparse con otras subredes de su VPC.

- Las interfaces adjuntas a instancias de EC2 en subredes privadas no son accesibles desde fuera de la VPC principal. Sin embargo, mediante el uso de una puerta de enlace NAT administrada por AWS, las instancias de EC2 pueden realizar solicitudes salientes, como por ejemplo para la aplicación de parches, y la respuesta del recurso externo se permitirá de nuevo.

- Las subredes privadas suelen utilizarse para alojar instancias de base de datos (DB) a las que no es necesario acceder a través de la Internet pública.

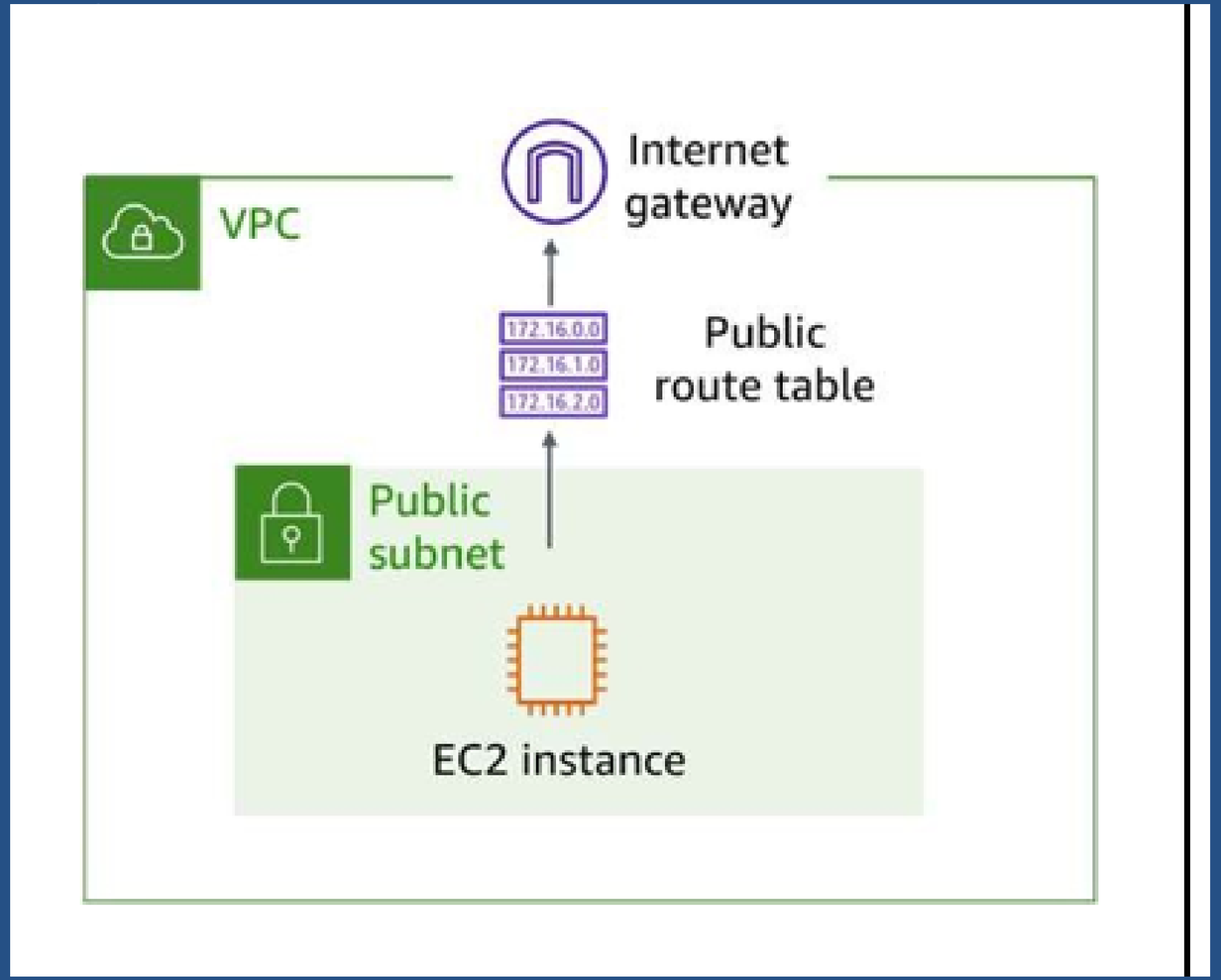
- Una puerta de enlace NAT debe tener asignada una dirección IP elástica.

SUBRED PÚBLICA

• Cuando el tráfico externo necesita llegar a una interfaz, como una instancia de Amazon Elastic Compute Cloud (Amazon EC2), la interfaz requiere lo siguiente:

• Se debe asignar una dirección IP pública a una instancia de EC2.
• La tabla de enrutamiento de la subred debe incluir una entrada para la interfaz.

• Con estos dos factores, la subred se considera pública.


Internet gateway
VPC
172.16.0.0
172.16.1.0
172.16.2.0
Public route table
Public subnet
EC2 instance

El diagrama de una VPC con una subred pública. El tráfico de una instancia de EC2 en la subred va a una tabla de enrutamiento pública y luego a una puerta de enlace de internet.

Cuando el tráfico externo necesita llegar a una interfaz, como una instancia de EC2, la interfaz requiere lo siguiente:

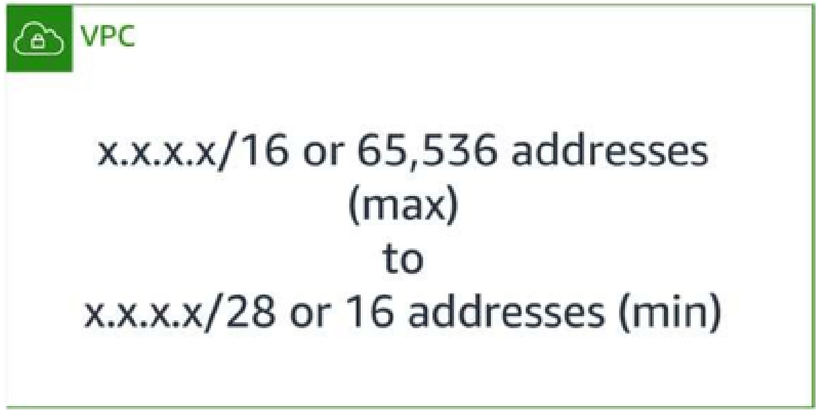
Se debe asignar una dirección IP pública a una instancia de EC2.
La tabla de enrutamiento de la subred debe incluir una entrada para la interfaz.

Con estos dos factores, la subred se considera pública.

A menudo, las empresas colocan servidores web dentro de una subred pública, sin embargo, AWS recomienda utilizar un equilibrador de carga en la subred pública y hacer que el equilibrador de carga retransmita el tráfico a los servidores web alojados en subredes privadas.

DIRECCIONAMIENTO IP

- Cuando se crea una VPC, se asigna un rango CIDR (un rango de direcciones privadas).
- No puede cambiar el rango en una VPC o subred, pero puede agregar más rangos CIDR a su VPC.
- El mayor tamaño de bloque de CIDR es /16, y el menor es /28.
- Los rangos de CIDR de las subredes no deben solaparse.



Las direcciones IP habilitan los recursos de su VPC para comunicarse entre sí y con los recursos de Internet. Al crear una VPC, se le asigna un rango de Classless Inter-Domain Routing (CIDR), que es un rango de direcciones privadas.
El bloque de CIDR puede ser tan grande como /16 (que son 216 o 65.536 direcciones) o tan pequeño como /28 (que son 24 o 16 direcciones).

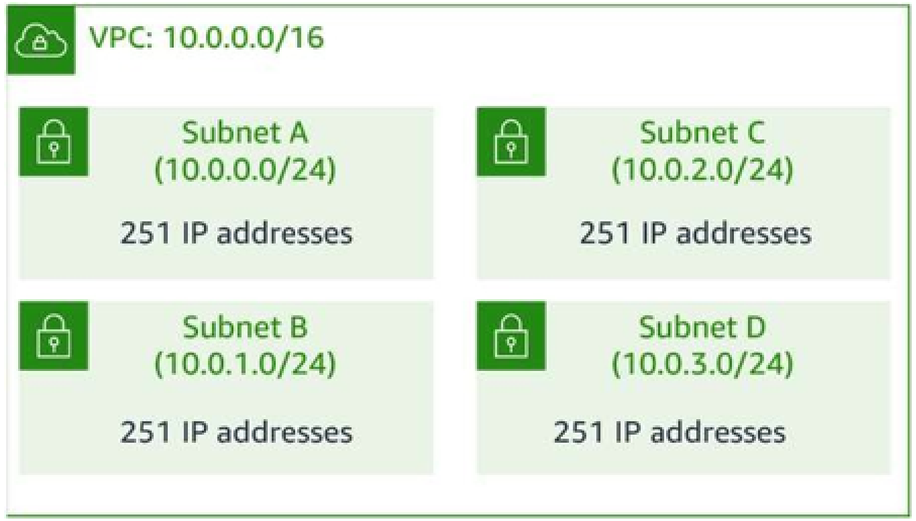
El bloque de CIDR de una subred puede ser el mismo que el bloque de la VPC en la que se encuentra la subred. Esto significa que la VPC y la subred tienen el mismo tamaño; la VPC tiene una única subred.

El bloque de CIDR de una subred puede ser un subconjunto del bloque de CIDR para la VPC. Esta estructura admite la definición de múltiples subredes. Si crea más de una subred en una VPC, los rangos de CIDR de las subredes no deben solaparse. No puede tener direcciones IP duplicadas en la misma VPC.

Para más información, consulte Dimensionamiento de VPC en la Guía del usuario de Amazon VPC en https://docs.aws.amazon.com/vpc/latest/userguide/configure-your-vpc.html#vpc-sizing.

DIRECCIONES IP RESERVADAS

Ejemplo: una VPC con un bloque de CIDR IPv4 de 10.0.0.0/16 tiene 65.536 direcciones IP en total. La VPC tiene cuatro subredes, todas con bloques de CIDR /24. Aunque cada subred tiene 256 direcciones IP, solo 251 direcciones IP están disponibles para su uso en cada una.



Direcciones IP para el bloque de CIDR 10.0.0.0/24	Reservado para
10.0.0.0	Direcciones de red
10.0.0.1	Comunicaciones internas
10.0.0.2	Resolución del sistema de nombres de dominio (DNS)
10.0.0.3	Uso futuro
10.0.0.255	Dirección de difusión de red

Al crear una subred, esta necesita su propio bloque de CIDR. Para cada bloque de CIDR que especifique, AWS reserva cinco direcciones IP dentro de ese bloque, y usted no puede utilizar estas cinco direcciones. AWS reserva estas direcciones IP para los siguientes fines:

Direcciones de red
Enrutador local de la VPC (comunicaciones internas)
Resolución del sistema de nombres de dominio (DNS)
Uso futuro
Dirección de difusión de red

Por ejemplo, supongamos que se crea una subred con un bloque de CIDR IPv4 de 10.0.0.0/24, que tiene 256 direcciones IP en total. La subred tiene 256 direcciones IP, pero solo 251 están disponibles porque cinco (5) están reservadas para AWS.

DIRECCIÓN IP PÚBLICA

• Una dirección IP pública es una dirección IP que se utiliza para acceder a Internet.

• Se puede asignar automáticamente una dirección IP pública si se modifican las propiedades de auto asignación de direcciones IP públicas de la subred.

• Las direcciones IP públicas son dinámicas. Si detiene o inicia su instancia, se le asignará una nueva IP pública. Para proyectos de producción, utilice una dirección IP elástica en lugar de una IP pública asignada, que se disociará si detiene la instancia.

Cuando se crea una VPC, cada instancia de esa VPC obtiene automáticamente una dirección IP privada. También se puede solicitar que se asigne una dirección IP pública cuando crea la instancia al modificar las propiedades de asignación automática de dirección IP pública de la subred. Una dirección IP pública se utiliza para acceder a Internet.

Las direcciones IP públicas son dinámicas. Si se detiene o se inicia su instancia, se le asignará una nueva IP pública. Para proyectos de producción, se utiliza una dirección IP elástica en lugar de una IP pública asignada, que se disocia si detiene la instancia.

Para más información, consulte Direcciones IPv4 públicas en la Guía del usuario de Amazon VPC en https://docs.aws.amazon.com/vpc/latest/userguide/how-it-works.html#vpc-public-ipv4-addresses.

LA DIRECCIÓN IP ELÁSTICA

- Está asociada a una cuenta de AWS
- Es estática y no cambia con el tiempo
- Procede del conjunto de direcciones IPv4 de Amazon
- Si desasigna una dirección IP elástica, se le cobrará hasta que la elimine por completo.

Las direcciones IP elásticas se asignan a su cuenta y siguen siendo las mismas. Utilice una dirección IP elástica cuando trabaje en un proyecto a largo plazo y la configuración de direcciones IP pueda llevarle mucho tiempo.

Una dirección IP elástica es una dirección IP pública y estática diseñada para el cómputo en la nube dinámico. Se puede asociar una dirección IP elástica con cualquier instancia o interfaz de red para cualquier VPC en su cuenta.

Con una dirección IP elástica, puede enmascarar los errores de una instancia o del software volviendo a mapear rápidamente la dirección a otra instancia de la cuenta. Si lo prefiere, puede especificar la dirección IP elástica en un registro DNS para el dominio, de modo que el dominio apunte a la instancia. Si su instancia no tiene una dirección IPv4 pública, puede asociar una dirección IP elástica a la instancia para permitir la comunicación con Internet. Por ejemplo, esto permite que se conecte a la instancia desde su equipo local.

Una dirección IP elástica es estática y no cambia con el tiempo. Procede del conjunto de direcciones IPv4 de Amazon o de un conjunto de direcciones IP personalizadas que haya aportado a su cuenta de AWS. Si desasigna una dirección IP elástica, se le cobrará hasta que la elimine por completo. Es posible que se apliquen costos adicionales cuando utilice direcciones IP elásticas, por lo que es importante liberarlas cuando ya no las necesite.

Las direcciones IP elásticas se asignan a su cuenta y siguen siendo las mismas. Utilice una dirección IP elástica cuando trabaje en un proyecto a largo plazo y la configuración de direcciones IP puede llevarle mucho tiempo.

Para más información, consulte Associate Elastic IP Addresses with Resources in Your VPC (Asociar direcciones IP elásticas con recursos en su VPC) en la Guía del usuario de Amazon VPC en https://docs.aws.amazon.com/vpc/latest/userguide/vpc-eips.html

INTERFAZ DE RED ELÁSTICA

• Una interfaz de red elástica es una interfaz de red virtual. Puede hacer lo siguiente:

• Adjuntarla a una instancia.
• Desconectarla de la instancia y conectarla a otra instancia para redirigir el tráfico de red.

• Sus atributos siguen cuando se reasigna a una nueva instancia.

• Cada instancia de su VPC tiene una interfaz de red predeterminada, a la que se puede asignar una dirección IPv4 privada del rango de su VPC.

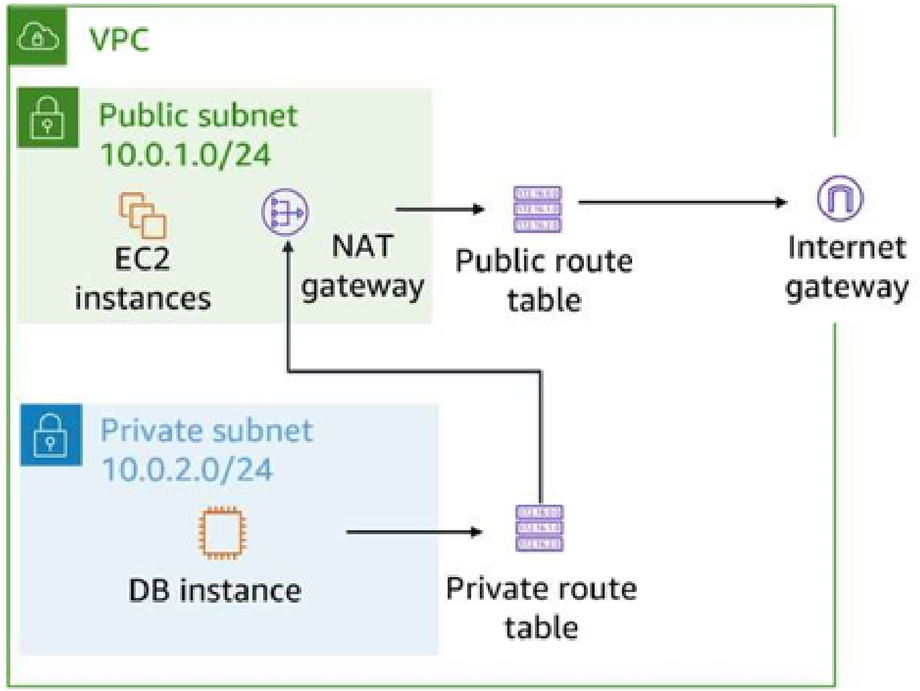
Una interfaz de red elástica es una interfaz de red virtual que se puede conectar o desconectar de una instancia en una VPC. Los atributos de una interfaz de red la siguen cuando se vuelve a conectar a otra instancia. Al mover una interfaz de red de una instancia a otra, el tráfico de red se redirige a la nueva instancia.

Cada instancia de una VPC tiene una interfaz de red predeterminada (la interfaz de red principal) a la que se puede asignar una dirección IPv4 privada del rango de su VPC. No se puede separar una interfaz de red principal de una instancia. Puede crear y adjuntar una interfaz de red adicional a cualquier instancia de su VPC. El número de interfaces de red que se pueden conectar varía según el tipo de instancia.

En determinadas circunstancias, puede tener dos interfaces de red en una instancia de EC2, lo que es ideal para análisis forenses. Asocie la interfaz de red a una instancia forense y comience a rastrear el ataque.

TABLAS DE ENRUTAMIENTO Y RUTAS

- Una tabla de enrutamiento contiene un conjunto de reglas (o rutas) que puede configurar para dirigir el tráfico de red de su subred.
- Cada ruta especifica un destino y un objetivo.
- De forma predeterminada, cada tabla de enrutamiento contiene una ruta local para la comunicación dentro de la VPC.
- Cada subred debe tener su propia tabla de enrutamiento.



El diagrama de una VPC con tablas de enrutamiento públicas y privadas. La subred pública contiene una instancia de EC2 y una puerta de enlace NAT. La puerta de enlace NAT dirige el tráfico a una tabla de enrutamiento pública y, a continuación, a una puerta de enlace de internet. La subred privada contiene una instancia de EC2 cuyo tráfico se dirige a una tabla de enrutamiento privada. Desde allí, el tráfico se dirige a la puerta de enlace NAT de la subred pública.

Una tabla de enrutamiento contiene una serie de reglas (llamadas rutas) que determinan hacia dónde se dirige el tráfico de red de su subred. Cada ruta especifica un destino y un objetivo. El destino es el bloque de CIDR de destino, a donde desea que vaya el tráfico de su subred. El objetivo es el objetivo a través del cual se envía el tráfico de destino. Una tabla de enrutamiento es una simple tabla de búsqueda que mantiene un registro de las rutas, como un mapa, y las utiliza para determinar por dónde reenviar el tráfico.

De forma predeterminada, cada tabla de enrutamiento que crea contiene una ruta local para la comunicación dentro de la VPC. No puede eliminar la entrada de ruta local, que se utiliza para las comunicaciones internas. Pero puede personalizar una tabla de enrutamiento agregando rutas.

Cada subred debe tener su propia tabla de enrutamiento o utilizar la tabla de enrutamiento principal de la VPC matriz (que controla el enrutamiento para todas las subredes que no están explícitamente asociadas a ninguna otra tabla de enrutamiento).

La tabla de enrutamiento principal es la tabla de enrutamiento que se asigna automáticamente a su VPC. La tabla de enrutamiento principal controla el enrutamiento de todas las subredes que no estén asociadas de forma explícita a ninguna otra tabla de enrutamiento. Una subred puede asociarse solamente a una tabla de enrutamiento por vez, pero pueden asociarse varias subredes a la misma tabla de enrutamiento.

Consulte Configurar tablas de enrutamiento en la Guía del usuario de Amazon VPC en https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Route_Tables.html

COLOMBIA POTENCIA DE LA VIDA

TIC

ESTAS SON ALGUNAS CONCLUSIONES CLAVE DE ESTA LECCIÓN 3 DEL MÓDULO 2:

LAS SUBREDES PÚBLICAS SE UTILIZAN CUANDO EL TRÁFICO EXTERNO NECESITA LLEGAR A UNA INTERFAZ, COMO UNA INSTANCIA DE EC2.

LAS SUBREDES PRIVADAS SUELEN UTILIZARSE PARA ALOJAR INSTANCIAS DE BASE DE DATOS A LAS QUE NO ES NECESARIO ACCEDER A TRAVÉS DE LA INTERNET PÚBLICA.

LAS TABLAS DE ENRUTAMIENTO DETERMINAN DÓNDE DEBE DIRIGIRSE EL TRÁFICO EN SU VPC.

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

UTP Universidad Tecnológica de Pereira