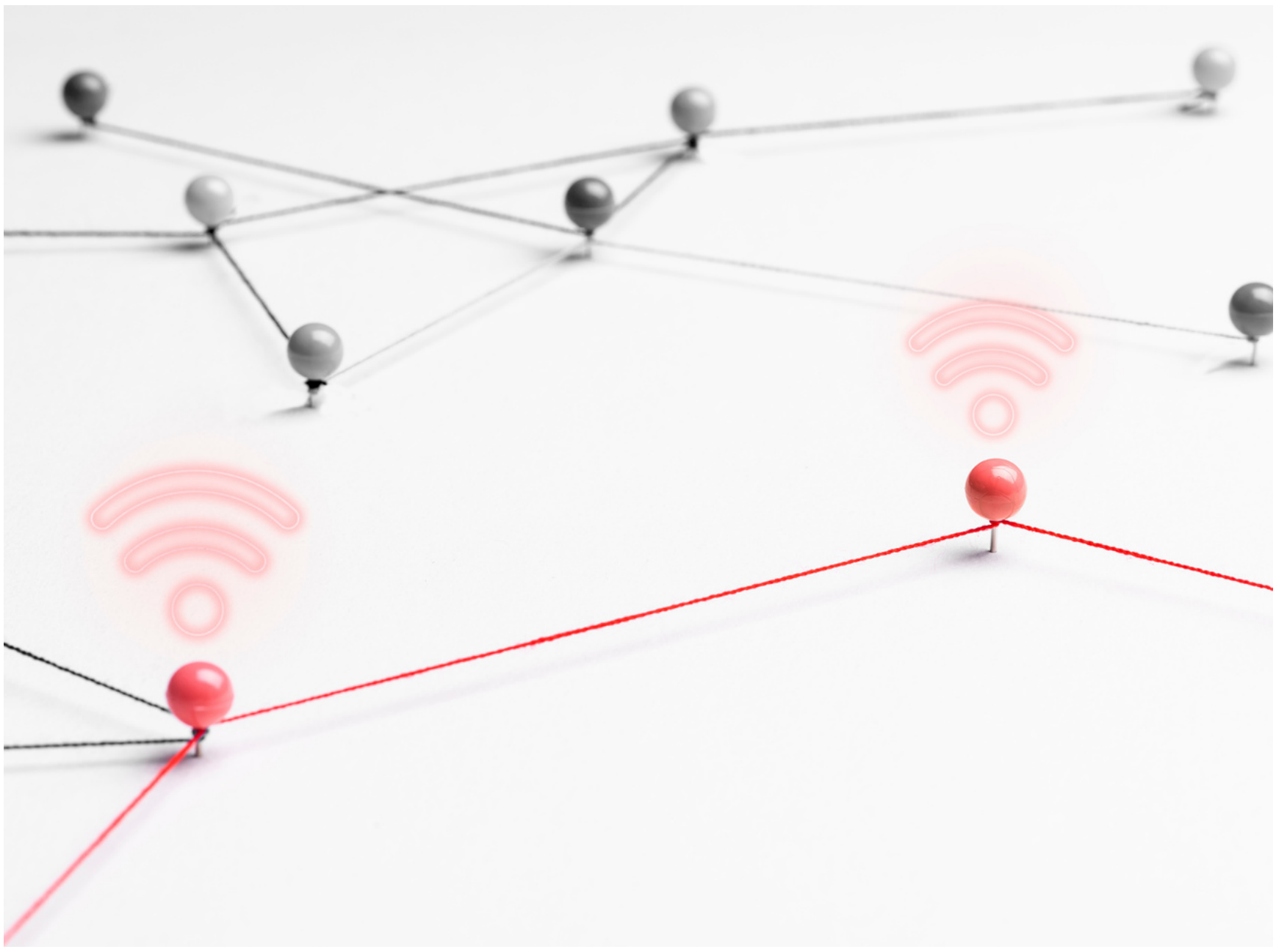
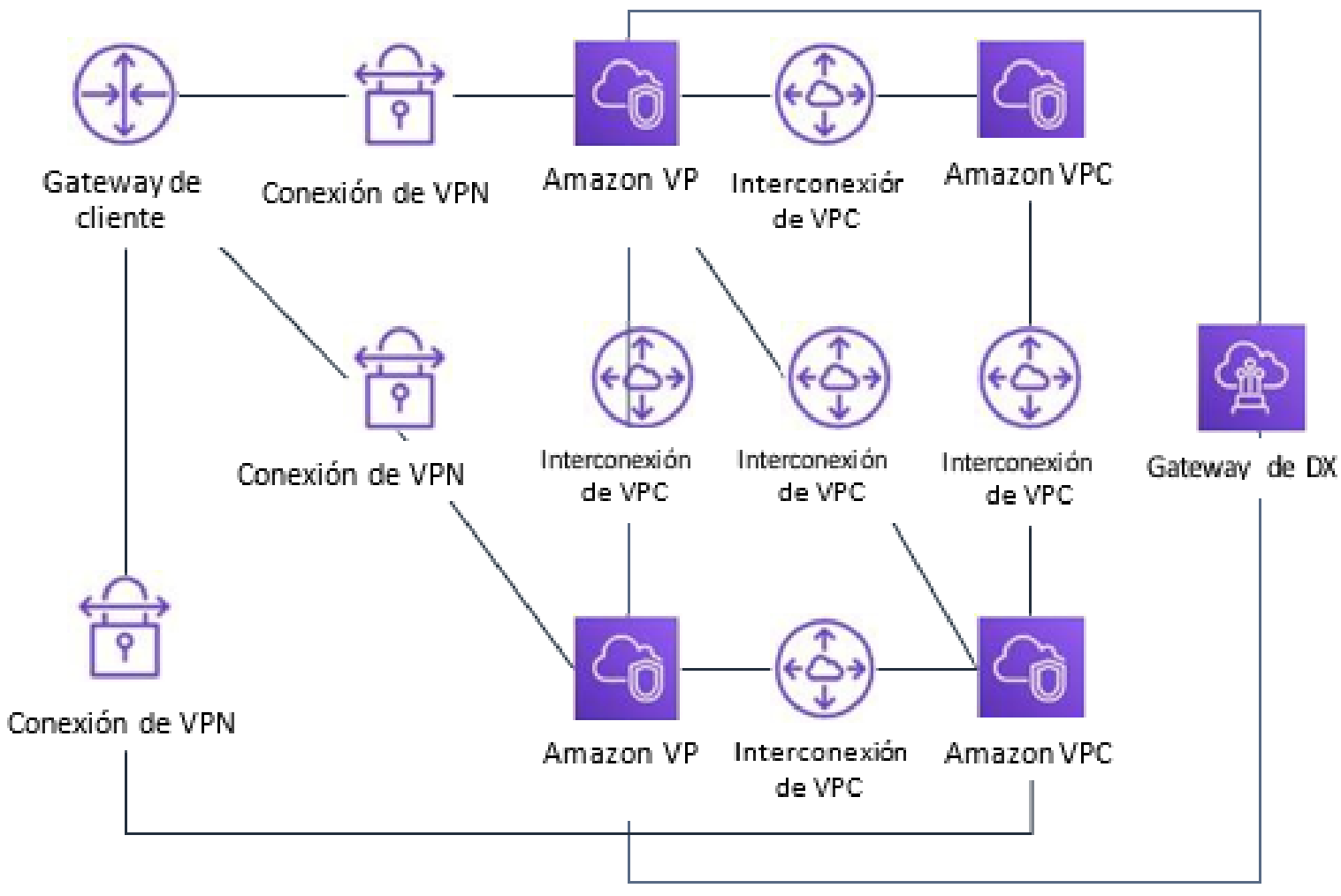
LECCIÓN 5: ESCALADO DE LA RED DE VPC CON AWS TRANSIT GATEWAY Y CONEXIÓN DE LA VPC A LOS SERVICIOS DE AWS COMPATIBLES.

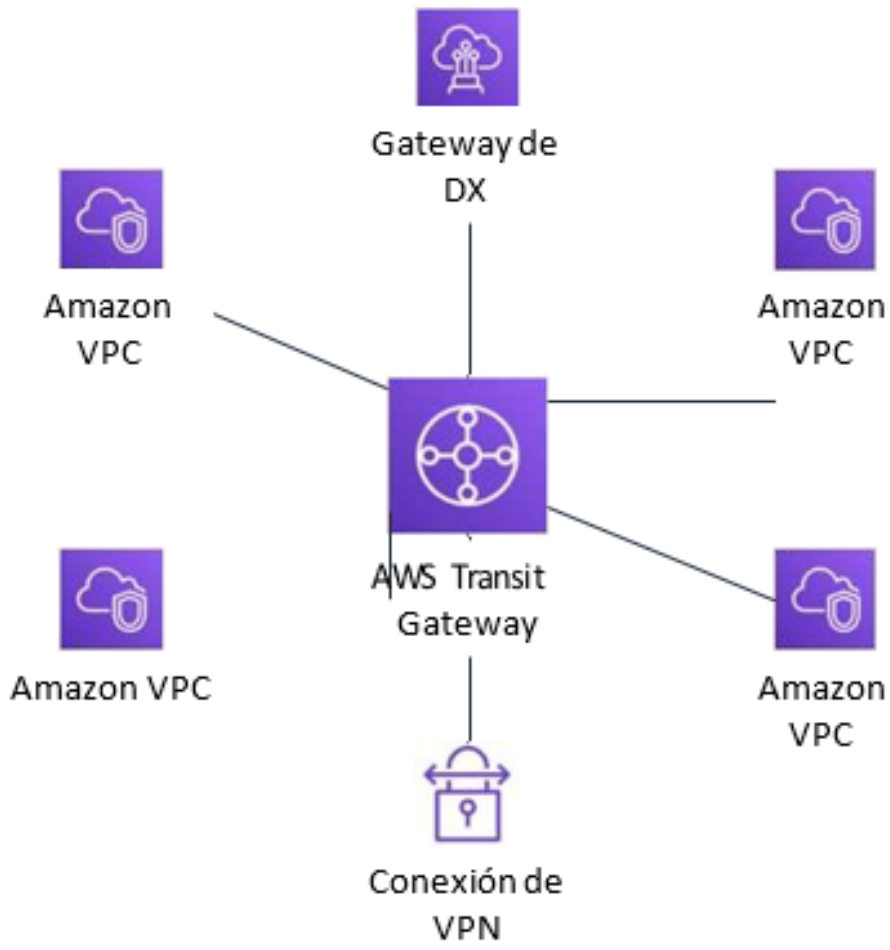


NECESIDAD DE ESCALAR REDES EN VARIAS VPC

DE ESTO:



A ESTO:



A medida que aumente el número de cargas de trabajo que se ejecutan en AWS, deberá ser capaz de ajustar la escala de sus redes en varias cuentas y VPC para seguir el ritmo de crecimiento. Puede usar la interconexión de VPC para conectar pares de VPC. Sin embargo, administrar la conectividad de un punto a otro en muchas VPC, sin la posibilidad de gestionar las políticas de conectividad de forma centralizada, puede resultar una tarea engorrosa y costosa desde un punto de vista operativo. Para la conectividad en las instalaciones, debe asociar su VPN a cada VPC. Esta solución puede requerir mucho tiempo en la etapa de creación, además de ser difícil de administrar cuando la cantidad de VPC alcance los tres dígitos.

Es importante tener en cuenta cuán grande puede llegar a ser su entorno con el paso del tiempo, qué tan bien ajustará su escala y cómo organizará las VPC. Si desea solucionar este problema, puede utilizar AWS Transit Gateway para simplificar su modelo de red.

AWS TRANSIT GATEWAY

AWS Transit Gateway es un servicio que le permite conectar las VPC y las redes en las instalaciones a una única gateway.

- **Se trata de un servicio de direccionamiento flexible, de alta disponibilidad y completamente administrado.**

- **Actúa como un concentrador para que todo el tráfico fluya entre Las redes.**

- **Conecta hasta 5000 VPC y entornos en las instalaciones con una única gateway,**

AWS Transit Gateway

AWS Transit Gateway es un servicio que le permite conectar las VPC y las redes en las instalaciones a una única gateway (llamada gateway de tránsito). Con AWS Transit Gateway, solo tiene que crear y administrar una única conexión desde la gateway central para cada VPC, centro de datos en las instalaciones u oficina remota de su red.

AWS Transit Gateway utiliza un sistema radial. Este sistema radial simplifica de forma significativa la administración y reduce los costos operativos porque cada red solo tiene que conectarse a la gateway de tránsito y no a todas las demás redes. Todas las VPC nuevas se conectan a la gateway de tránsito y luego quedan disponibles automáticamente para cualquier otra red que esté conectada a la gateway de tránsito. Esta facilidad en la conectividad simplifica el escalado de la red para acompañar su crecimiento.

Puede utilizar AWS Transit Gateway para conectar hasta 5000 VPC y redes en las instalaciones.

CONEXIÓN DE VARIAS VPC

CASO:

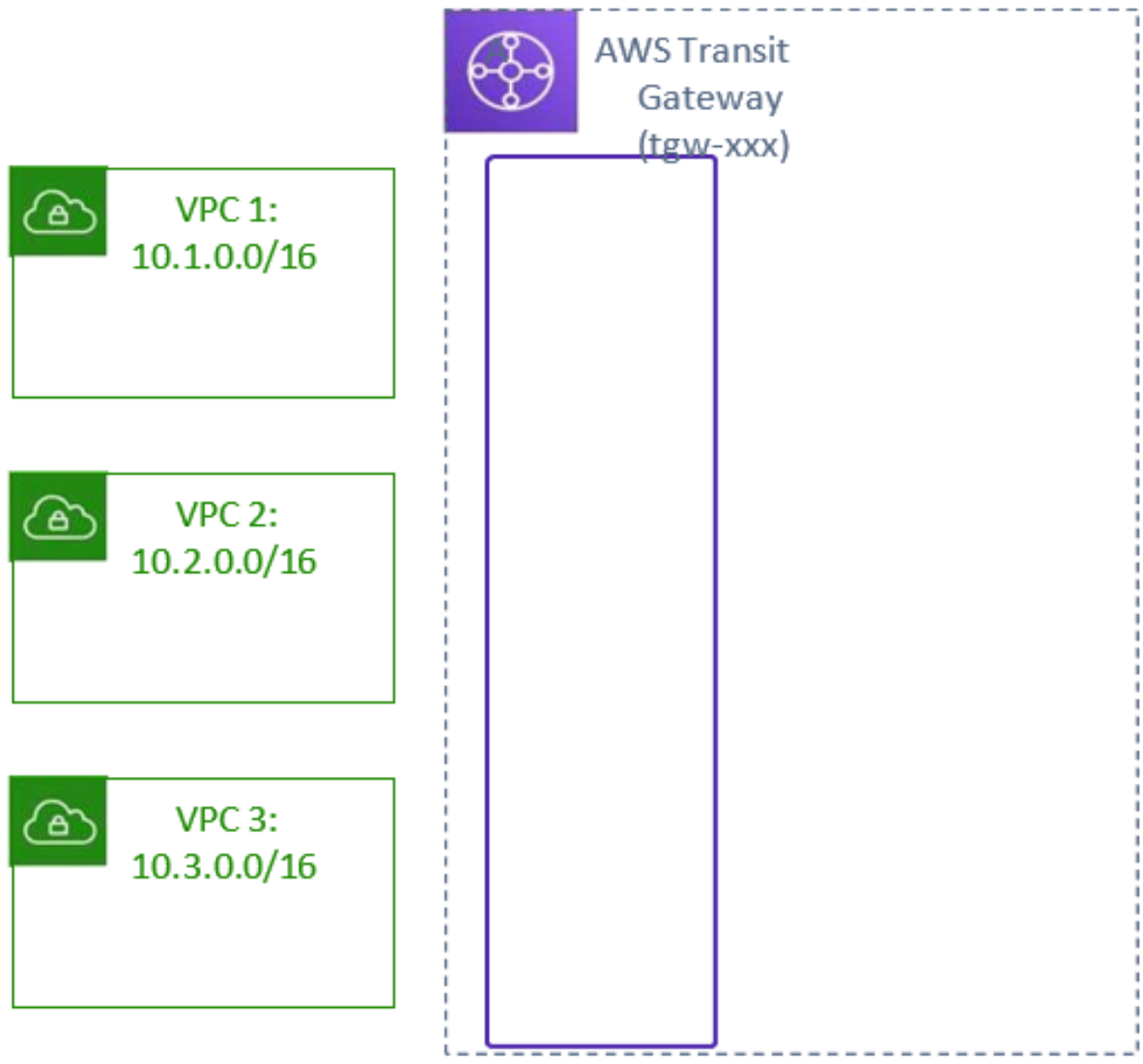
Queremos conectar tres VPC por completo

Para comprender cómo conectar varias VPC mediante AWS Transit Gateway, considere este caso. Desea conectar por completo tres VPC en su red. En este caso, aprende a implementar AWS Transit Gateway y tres VPC con espacio de dirección IP no superpuesto en una sola región. A continuación, asocia la gateway de tránsito a las VPC.

PASO 1: CREACIÓN DE LA GATEWAY DE TRÁNSITO:

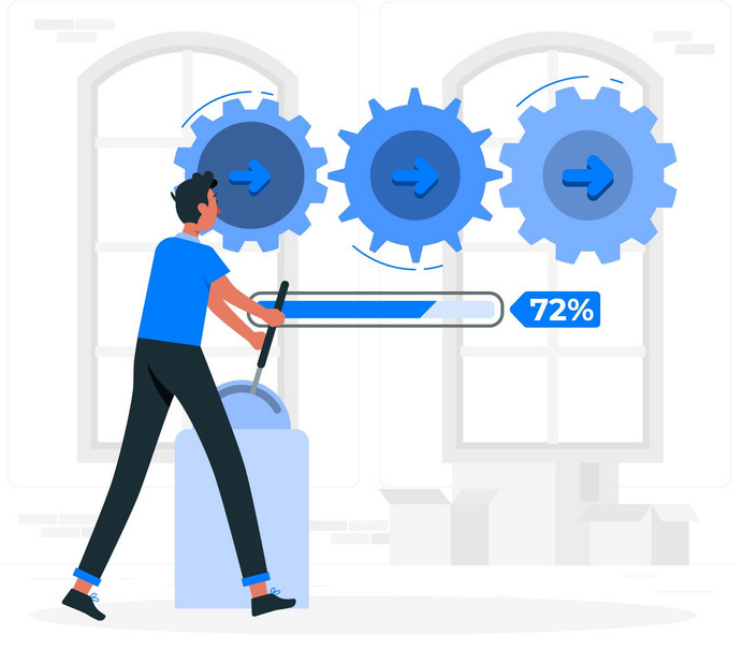
CASO:

Queremos conectar tres VPC por completo



El primer paso para conectar varias VPC consiste en crear una gateway de tránsito. Una gateway de tránsito es un concentrador de tránsito que puede utilizar para interconectar las VPC y las redes en las instalaciones. Actúa como un enrutador virtual de la región para el tráfico que fluye entre las conexiones de VPC y VPN. Una gateway de tránsito escala de forma elástica en función del volumen de tráfico de red.

Puede configurar una gateway de tránsito a través del panel de Amazon VPC. Se aplican diferentes cargos por el uso de AWS Transit Gateway, por lo que debe asegurarse de que su arquitectura y presupuesto puedan cubrir el uso de una gateway de tránsito.

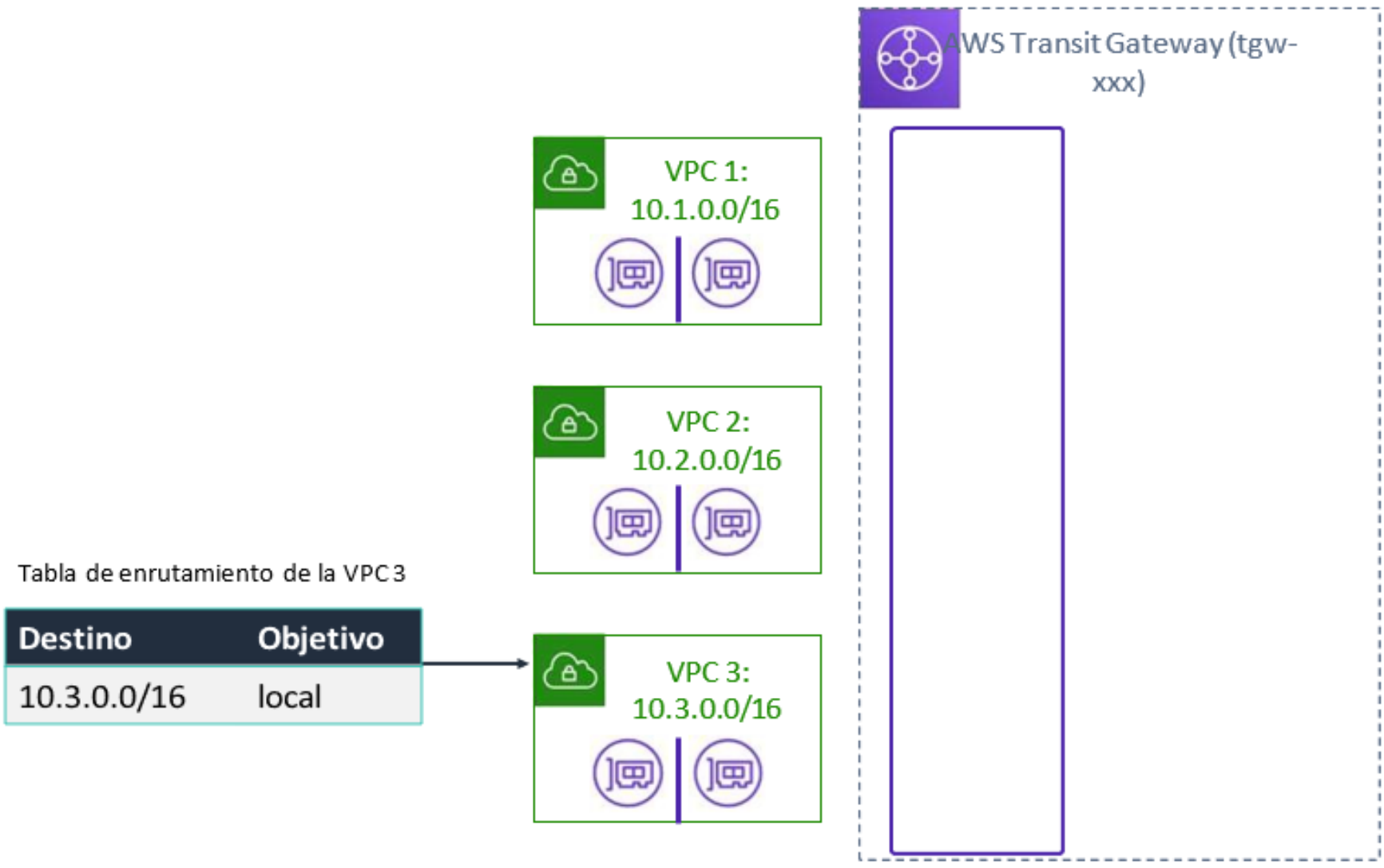


Para obtener más información, consulte ¿Qué es una gateway de tránsito?

PASO 2: IMPLEMENTACIÓN DE INTERFACES DE RED ELÁSTICAS

CASO:

Queremos conectar tres VPC por completo



AWS Transit Gateway se conecta a una VPC a través de interfaces de red elásticas (ENI), que se implementan en las subredes.

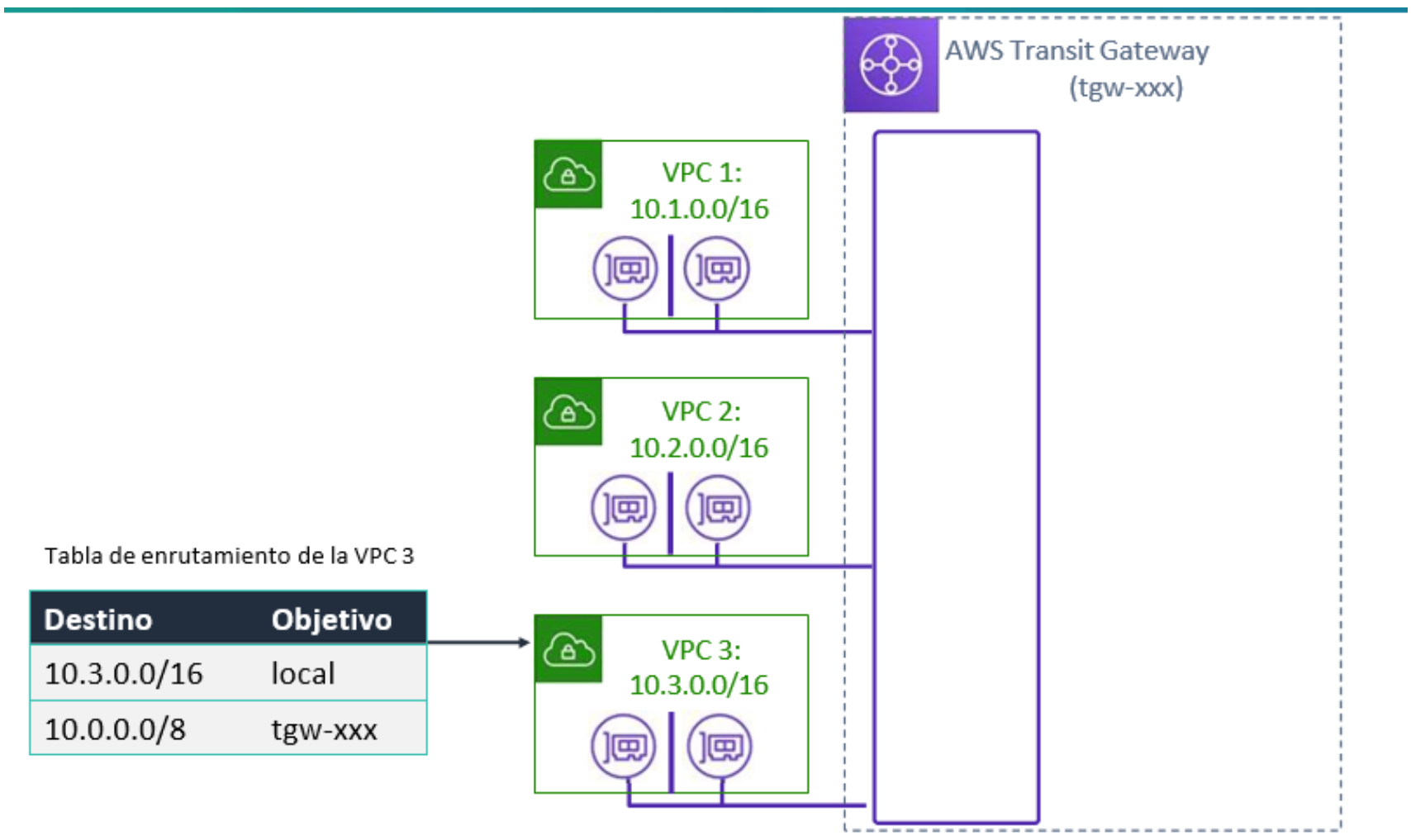
Debe asegurarse de que cada zona de disponibilidad que forma parte de la VPC tenga una ENI que conecte la VPC a la gateway de tránsito. Puede hacerlo seleccionando al menos una subred de cada zona de disponibilidad para la ENI.

Observe en este ejemplo que la tabla de enrutamiento correspondiente a la VPC 3 tiene una única ruta de destino que es local para la VPC 3 con la red 10.3.0.0/16.

PASO 3: ACTUALIZACIÓN DE LA TABLA DE ENRUTAMIENTO DE LA VPC

CASO:

Queremos conectar tres VPC por completo



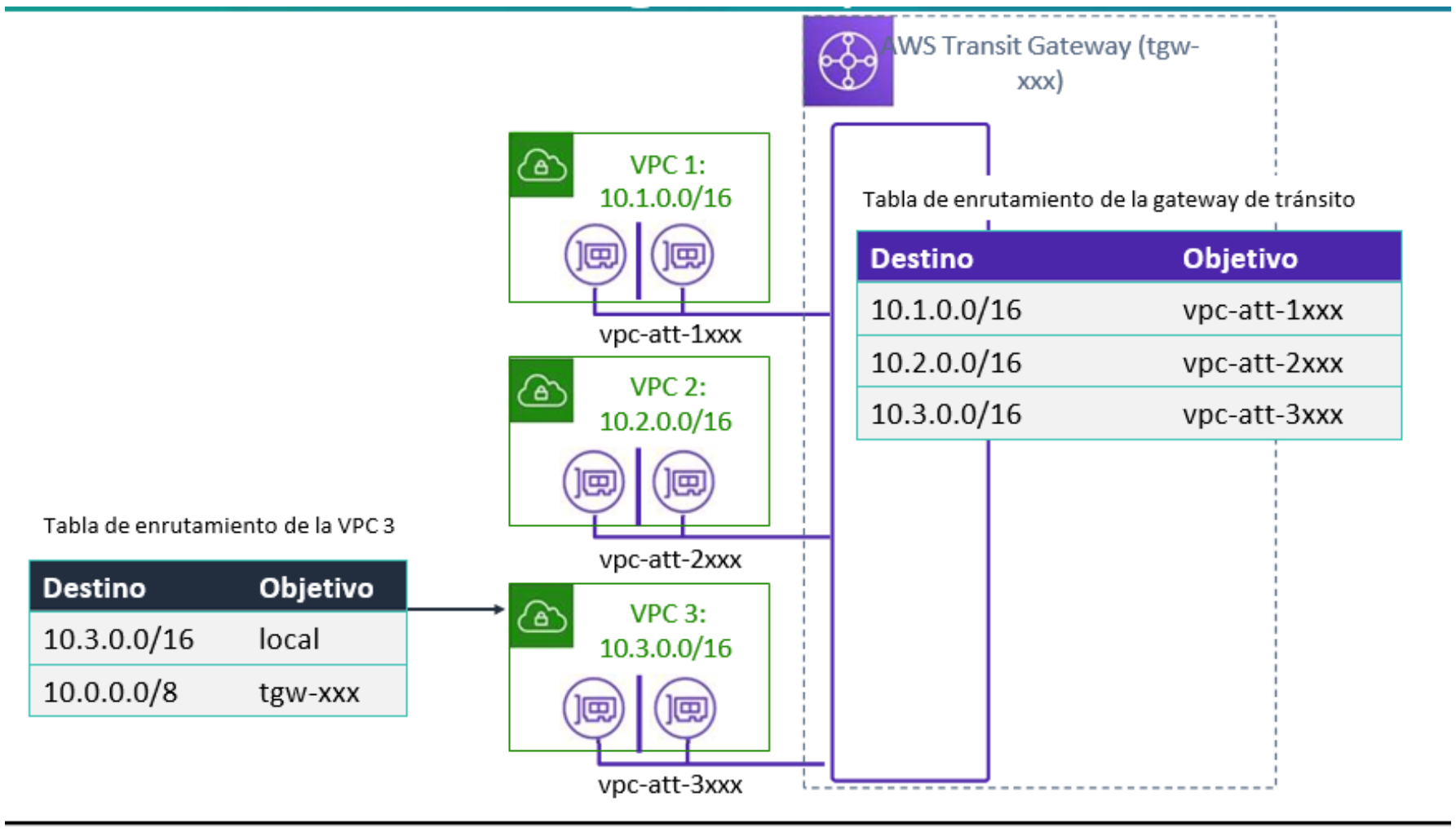
Después de asociar las ENI, el siguiente paso consiste en agregar una ruta en la tabla de enrutamiento de la VPC para enviar el tráfico que tiene como destino las otras VPC de la red a la gateway de tránsito.

En este ejemplo, la segunda línea de la tabla de enrutamiento de la VPC 3 muestra que el tráfico que tiene como destino la red 10.0.0.0/8 se envía a la gateway de tránsito. Esta ruta permite que todo el tráfico de la VPC 3 se dirija a la VPC 1 o a la VPC 2 para enviarse a la gateway de tránsito, ya que el bloque de CIDR 10.0.0.0/8 incluye los bloques de CIDR 10.X.0.0/16, que los utilizan las VPC individuales.

PASO 4: ACTUALIZACIÓN DE LA TABLA DE ENRUTAMIENTO DE LA GATEWAY DE TRÁNSITO

CASO:

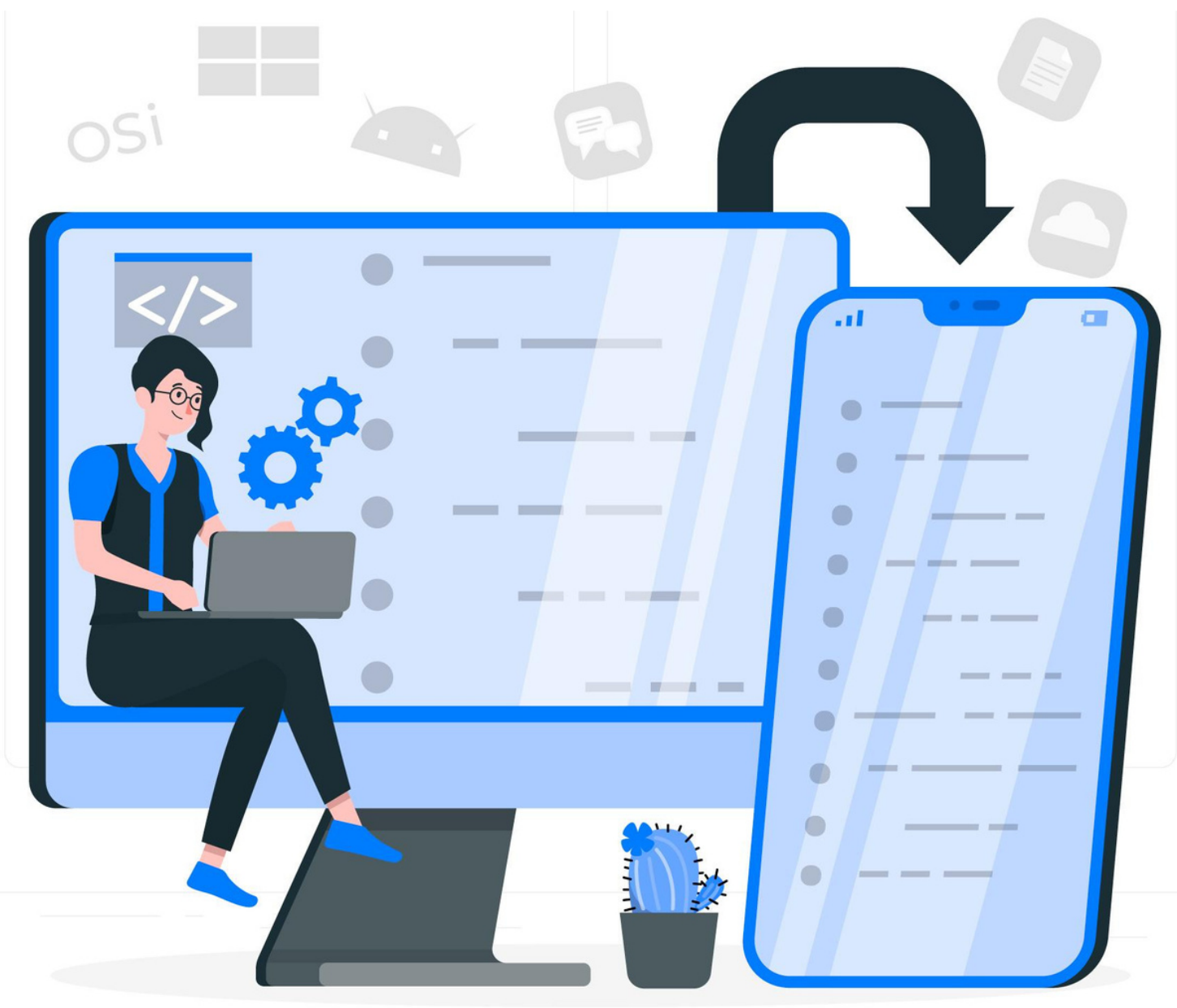
Queremos conectar tres VPC por completo



A continuación, debe configurar la tabla de enrutamiento de la gateway de tránsito para dirigir el tráfico a las VPC conectadas.

Cuando crea una gateway de tránsito, se crea una tabla de enrutamiento de la gateway de tránsito predeterminada. Cada ruta de la tabla de enrutamiento de la gateway de tránsito permite que dicha gateway envíe el tráfico que tiene como destino una de las VPC a una asociación correspondiente, que es una referencia a la ENI que está asociada a la propia VPC.

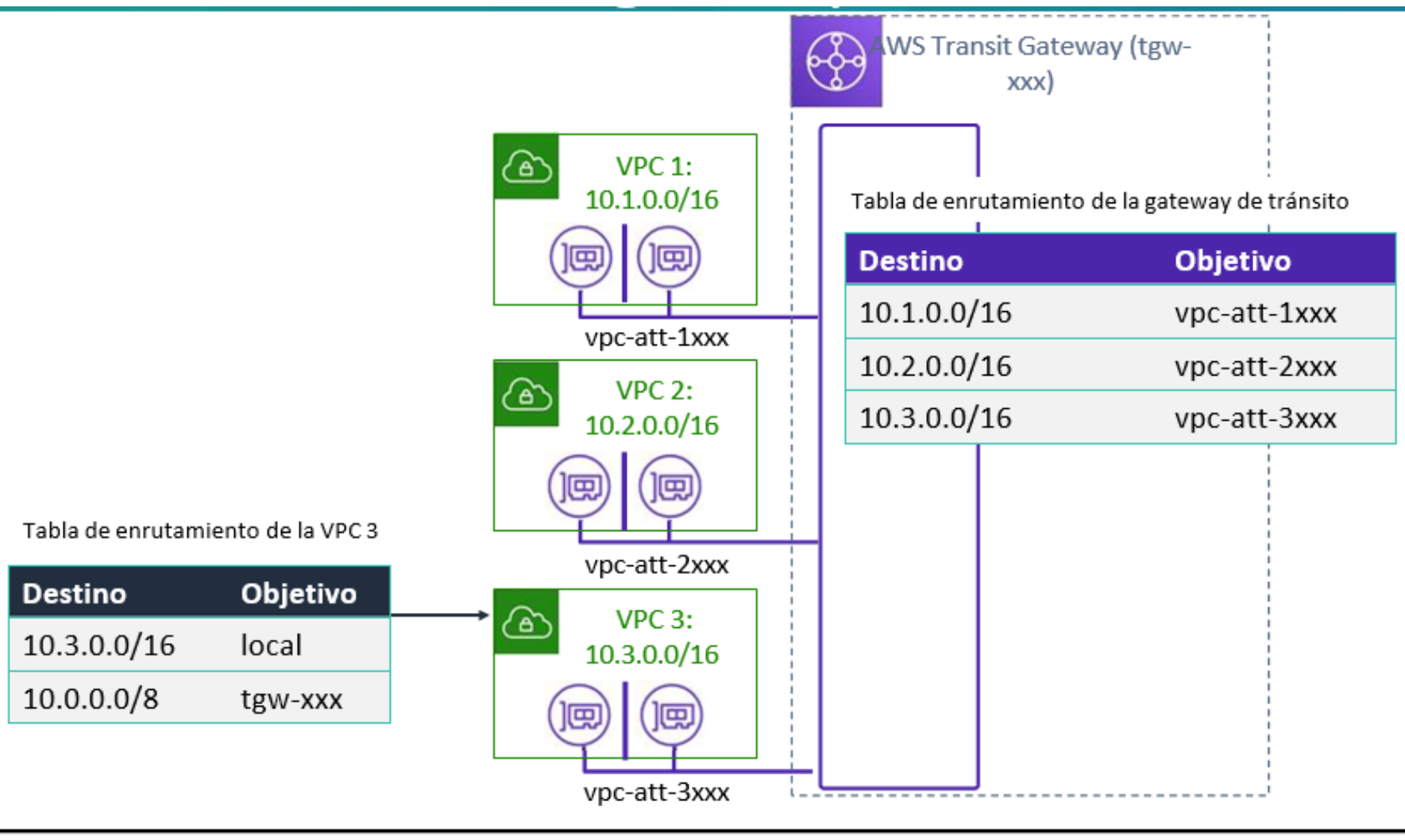
En este ejemplo, hay una ruta en la tabla de enrutamiento de la gateway de tránsito que envía todo el tráfico que tiene como destino la red 10.1.0.0/16 a vpc-att-1xxx, que es la asociación para la VPC 1. Del mismo modo, el tráfico que tenga como destino las otras redes de VPC se envía a las asociaciones correspondientes.



USO DE AWS TRANSIT GATEWAY PARA EL AISLAMIENTO DE VPC (1 DE 3)

CASO:

Queremos conectar tres VPC por completo



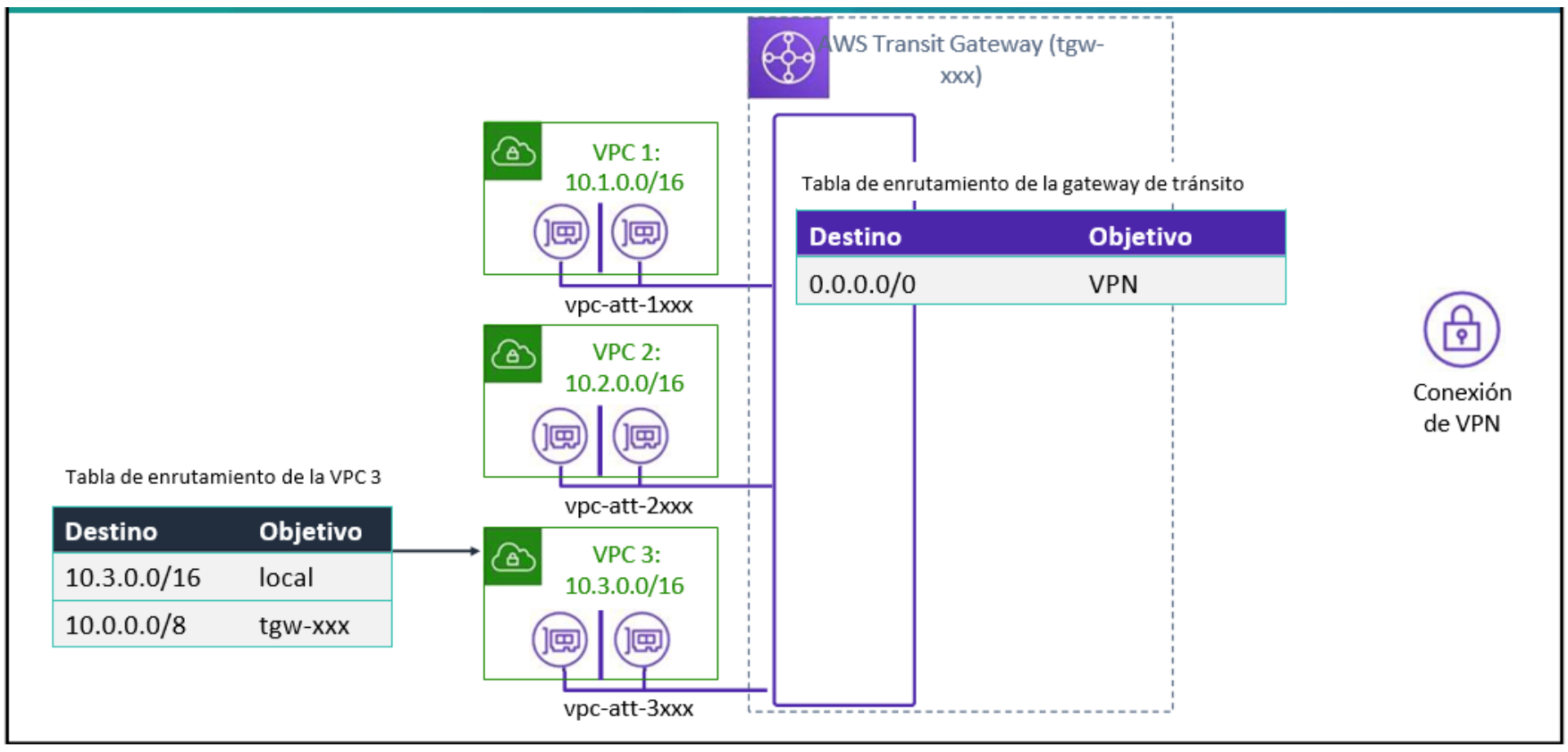
Si bien puede utilizar AWS Transit Gateway para conectar varias VPC, también puede utilizarlo para lograr aislamiento en su entorno de VPC. En este caso, desea conectar el origen de la VPN al entorno de VPC. También desea evitar que las VPC se conecten directamente entre sí, lo que dejaría que la VPN decida si el tráfico de una VPC debe enviarse a otra.

Al configurar según corresponda la tabla de enrutamiento para la gateway de tránsito, puede evitar el intercambio de información entre las VPC.

USO DE AWS TRANSIT GATEWAY PARA AISLAMIENTO DE VPC (2 DE 3)

CASO:

Ahora queremos acceso a la VPN, pero conectividad de VPC aislada.



Si desea implementar esta solución, actualice la ruta en la tabla de enrutamiento de la gateway de tránsito para enviar todo el tráfico conocido a la conexión de VPN.

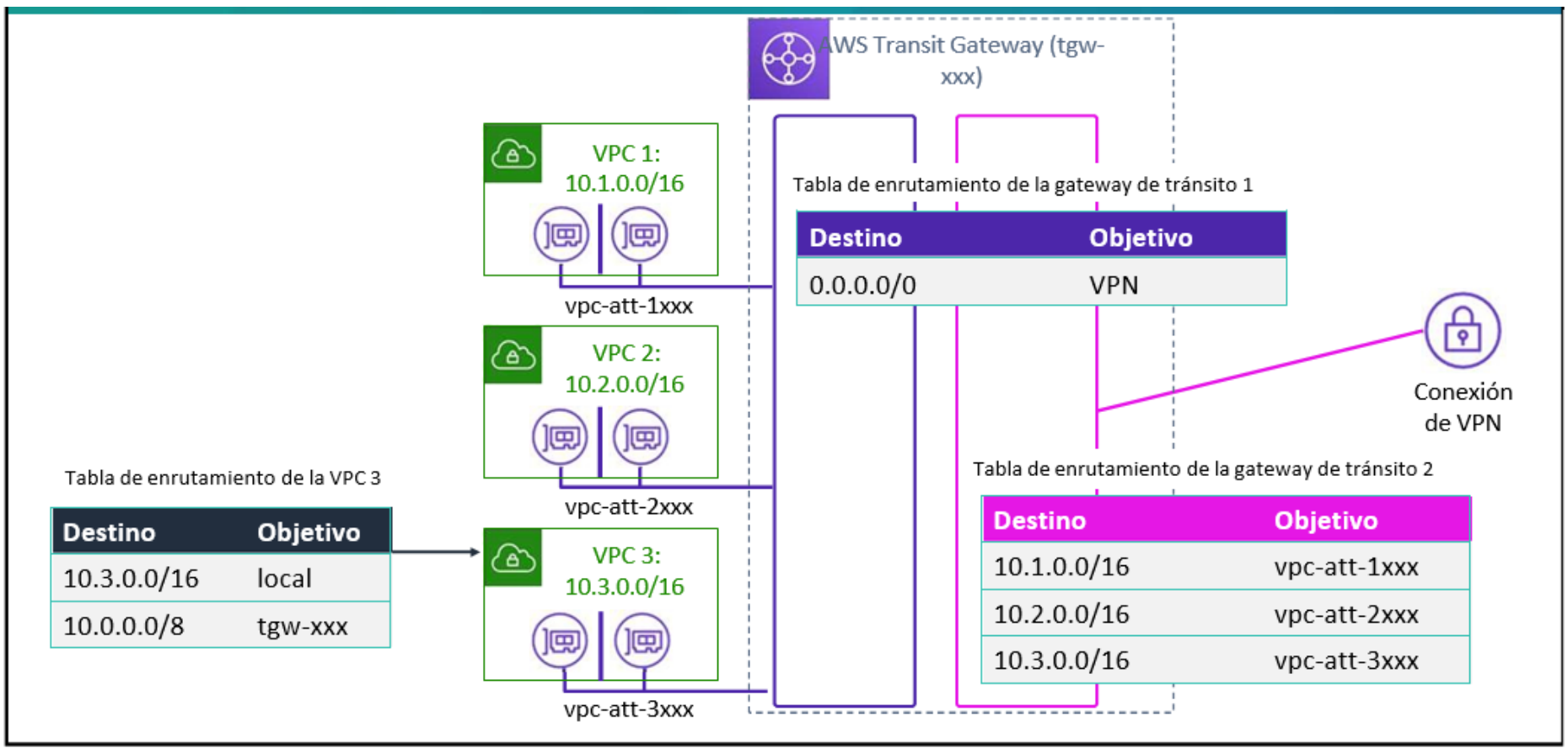
En este ejemplo, cuando el tráfico de cualquiera de las VPC de la red 10.0.0.0/8 se envía desde la VPC 3 a la gateway de tránsito, dicha gateway reenviará el tráfico a la VPN como se muestra en la diapositiva. La gateway de tránsito no enviará el tráfico a ninguna de las otras VPC porque no hay rutas que lleven a alguna de las asociaciones de la VPC.

Ahora tiene acceso de VPN aislado y seguro a su entorno de VPC sin comunicación cruzada entre las VPC.

USO DE AWS TRANSIT GATEWAY PARA AISLAMIENTO DE VPC (3 DE 3)

CASO:

Ahora queremos acceso a la VPN, pero conectividad de VPC aislada.



Puede crear varias tablas de enrutamiento de la gateway de tránsito para interacciones específicas cuyo objetivo sea dirigir el tráfico según considere conveniente.

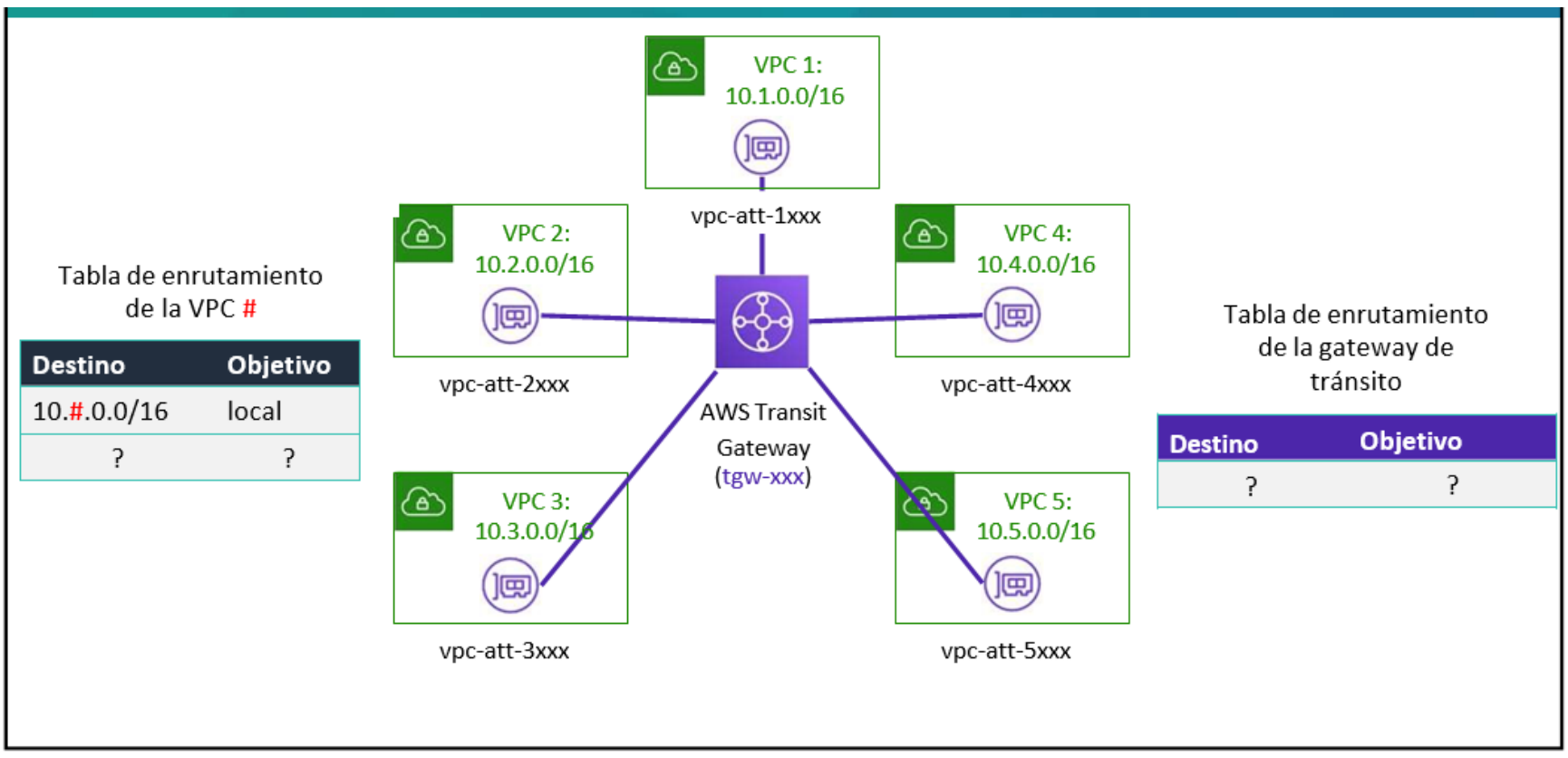
En este ejemplo, la segunda tabla de enrutamiento dirigirá el tráfico entrante de la VPN a una de las VPC correspondientes que esté asociada a la gateway de tránsito

Ahora, completará la siguiente actividad: AWS Transit Gateway: Desafío

AWS TRANSIT GATEWAY: DESAFÍO

CASO:

¿Cómo se conectan estas cinco VPC?



En esta actividad, tiene cinco VPC que desea conectar entre sí a través de AWS Transit Gateway.

Responda las siguientes preguntas:

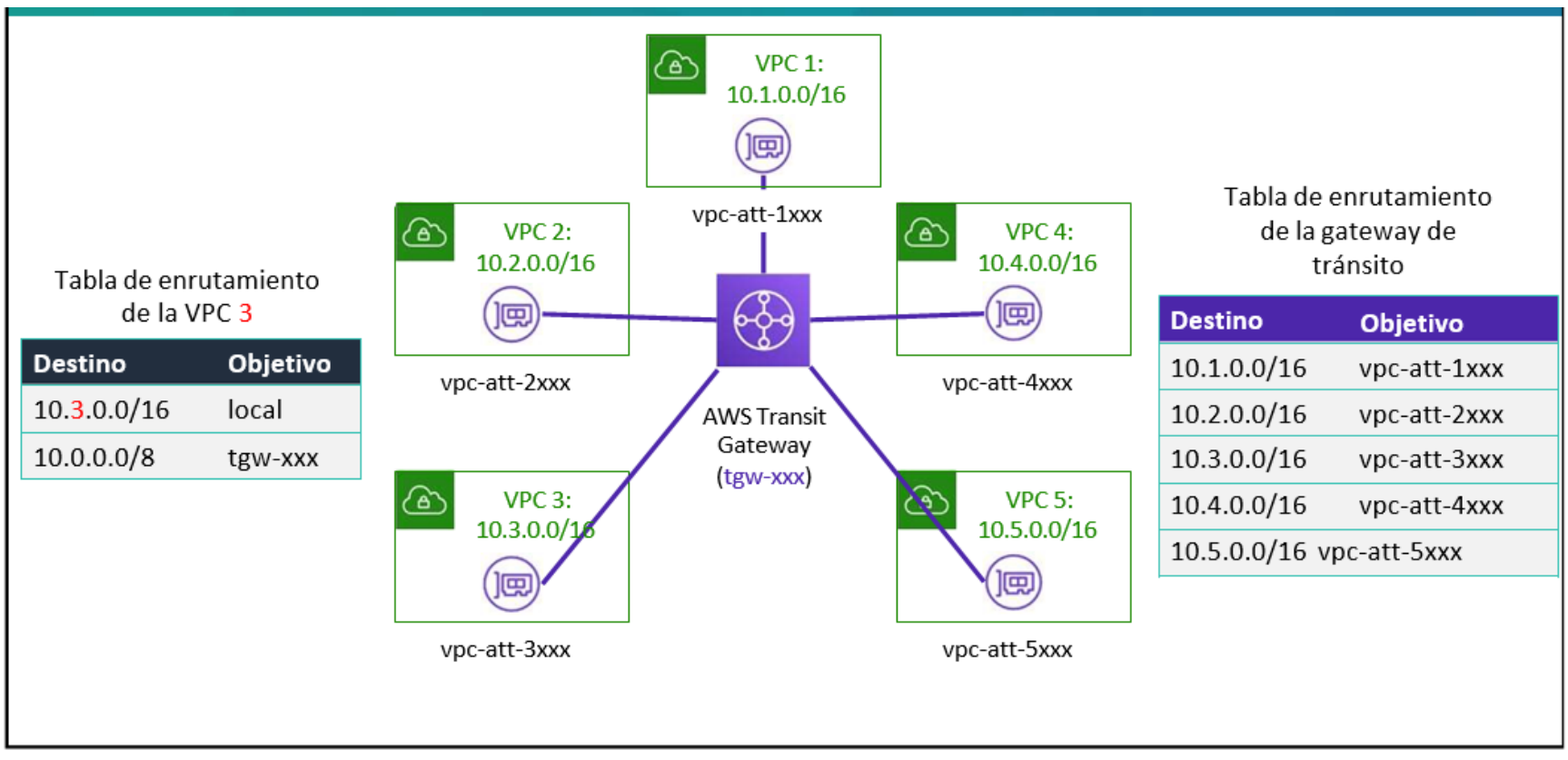
- **¿Qué rutas es necesario agregar a cada una de las tablas de enrutamiento de las VPC para habilitar la conectividad completa?**

- **¿Qué rutas es necesario agregar a la tabla de enrutamiento de la gateway de tránsito para habilitar la conectividad completa?**

ACTIVIDAD AWS TRANSIT GATEWAY: SOLUCIÓN

CASO:

¿Cómo se conectan estas cinco VPC?



¿Qué rutas debe agregar a cada tabla de enrutamiento de las VPC para habilitar la conectividad completa?

Observe la solución provista para la tabla de enrutamiento de la VPC 3. Las otras tablas de enrutamiento de las VPC se actualizan de una forma similar.

¿Qué rutas debe agregar a la tabla de enrutamiento de la gateway de tránsito para habilitar la conectividad completa?

Se debe agregar una ruta por cada asociación de VPC con el objetivo de dirigir el tráfico a cada VPC.

ESTOS SON ALGUNOS DE LOS APRENDIZAJES CLAVE DE ESTA PARTE DE LA LECCIÓN 5 DE LA UNIDAD 2:

AWS Transit Gateway le permite conectar las VPC y las redes en las instalaciones a una única gateway (llamada gateway de tránsito).

AWS Transit Gateway utiliza un sistema radial para simplificar la administración de las VPC y reducir los costos operativos.

PUNTOS DE ENLACE DE LA VPC

Le permiten conectar de forma privada la VPC con los servicios AWS compatibes y los servicios de punto de enlace de la VPC que funcionan con tecnología de AWS Privatelink.

Habilitan el tráfico entre la VPC y el otro servicio sin salir de la red de Amazon.

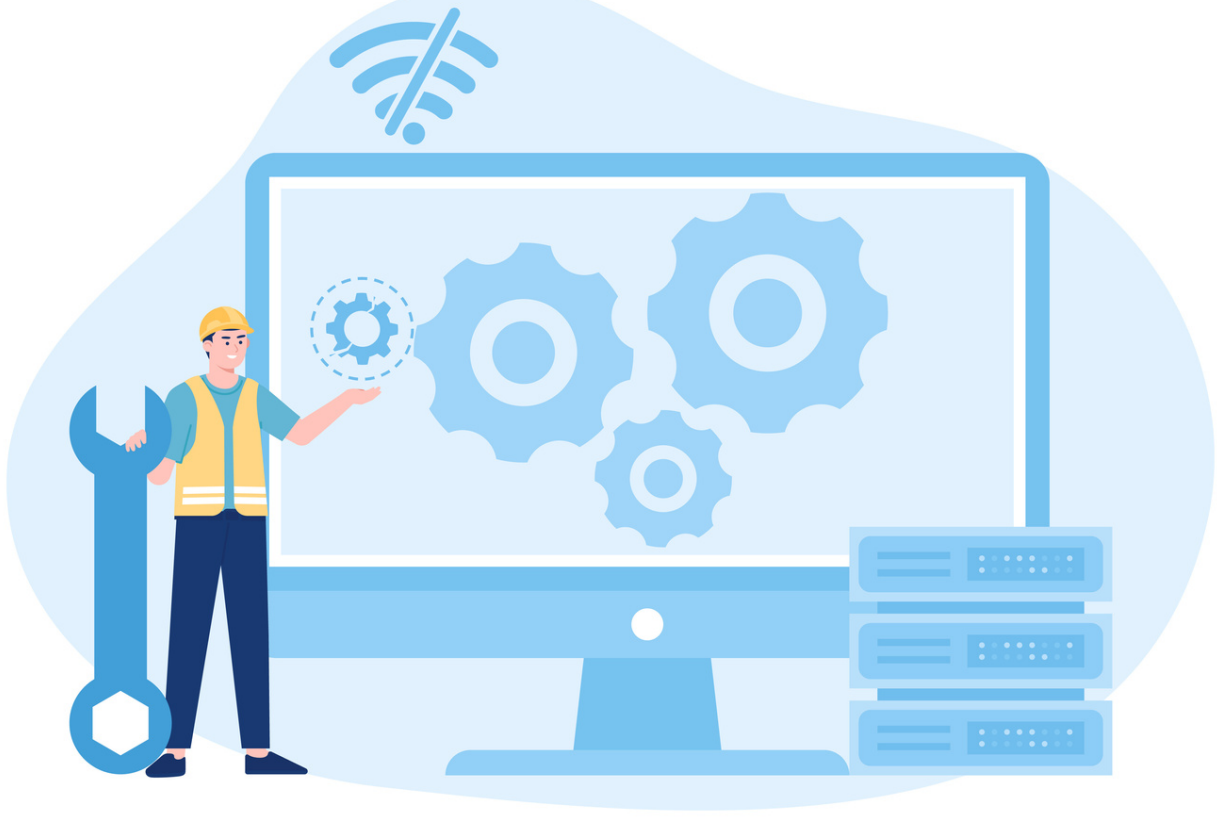
No necesitan una gateway de internet, una VPN, dispositivos de conversión de direcciones de red (NAT) ni proxies de firewall.

• Escalan de forma horizontal, son redundantes y cuentan con alta disponibilidad.

Un punto de enlace de la VPC le permite conectar de forma privada su VPC con los servicios de AWS compatibles y los servicios de punto de enlace de la VPC que funcionan con tecnología de AWS PrivateLink. Entre los servicios de punto de enlace de la VPC que funcionan con tecnología de AWS PrivateLink, podemos encontrar algunos servicios de AWS, servicios alojados por otros clientes de AWS y por socios de AWS Partner Network (APN) en sus propias VPC (denominados servicios de punto de enlace) y servicios de socios compatibles de AWS Marketplace.

Los puntos enlace de la VPC no requieren una gateway de Internet, un dispositivo NAT, una conexión de VPN ni una conexión de DX. Las instancias de la VPC no requieren direcciones IP públicas para comunicarse con los recursos en el servicio. El tráfico entre la VPC y el otro servicio no sale de la red de Amazon.

Los puntos de enlace son dispositivos virtuales. Son componentes de VPC que escalan de forma horizontal, son redundantes y cuentan con alta disponibilidad. Los puntos de enlace permiten la comunicación entre instancias de su VPC y servicios sin imponer riesgos de disponibilidad ni restricciones de ancho de banda en el tráfico de red



DOS TIPOS DE PUNTO DE ENLACE DE LA VPC:

- Punto de enlace de interfaz:
  es una interfaz de red elástica con una dirección IP privada que actúa como punto de entrada para el tráfico que tiene como destino un servicio compatible.
- Con tecnología de AWS PrivateLink
- Ejemplos:
  - Amazon CloudWatch
  - API de Amazon EC2
  - Elastic Load Balancing

- Punto de enlace de gateway:
  es una gateway que especifica como objetivo de una ruta de la tabla de enrutamiento para el tráfico que tiene como destino un servicio de AWS compatible.
- Servicios de AWS compatibles:
  - Amazon S3
  - Amazon DynamoDB

UN PUNTO DE ENLACE DE INTERFAZ

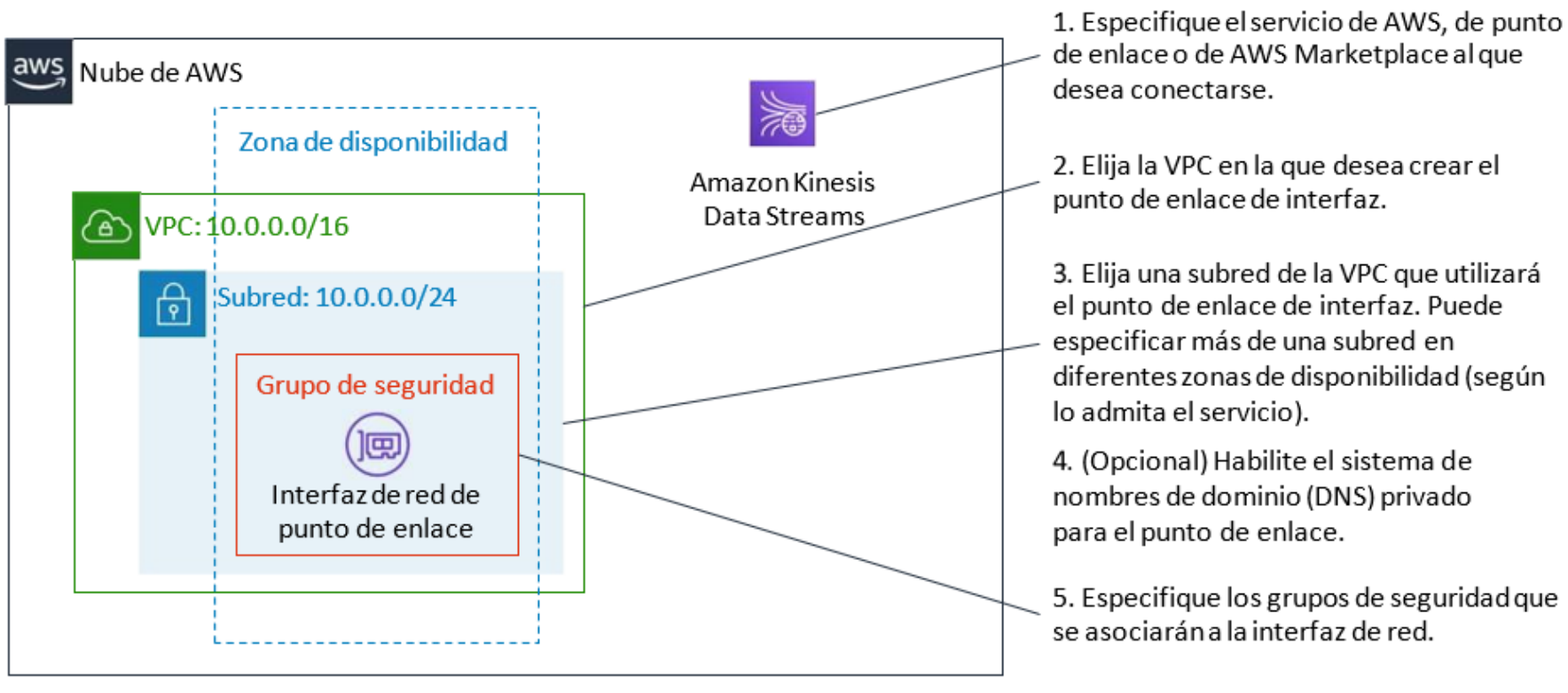
Es una interfaz de red elástica con una dirección IP privada. Esta dirección IP sirve como punto de entrada para el tráfico que tiene como destino un servicio compatible. Los puntos de enlace de interfaz le permiten conectarse a servicios que funcionan con tecnología de AWS PrivateLink. El propietario del servicio es su proveedor. Como la entidad principal que crea el punto de enlace de interfaz, usted es el consumidor del servicio. Para obtener una lista completa de los servicios compatibles con los puntos de enlace de interfaz, consulte VPC Endpoints — Interface Endpoints.

UN PUNTO DE ENLACE DE GATEWAY

Es una gateway que especifica como el objetivo de una ruta en la tabla de enrutamiento. La ruta es para el tráfico que tiene como destino un servicio de AWS compatible. Amazon S3 y Amazon DynamoDB son compatibles con los puntos de enlace de gateway.

No se aplican cargos por el procesamiento de datos ni cargos por hora derivados del uso de puntos de enlace de la VPC de gateway. Sin embargo, se le facturará cada hora en que su punto de enlace de la VPC permanezca aprovisionado en cada zona de disponibilidad, independientemente del estado de su asociación al servicio. Esta facturación por hora de su punto de enlace de la VPC terminará cuando lo elimine. La facturación por hora también parará si el propietario del servicio de punto de enlace rechaza la asociación de su punto de enlace de la VPC a su servicio. Después de eso, el servicio se borra.

CONFIGURACIÓN DE UN PUNTO DE ENLACE DE INTERFAZ



Para configurar un punto de enlace de interfaz, siga estos pasos generales desde la consola de Amazon VPC:

1 . Especifique el nombre del servicio de AWS, el servicio de punto de enlace o el servicio de AWS Marketplace al que desea conectarse.

3. Elija una subred de la VPC que utilizará el punto de enlace de interfaz. Cuando crea un punto de enlace de interfaz para un servicio en la VPC, se crea una interfaz de red de punto de enlace en la subred seleccionada. La interfaz de red de punto de enlace tiene una dirección IP privada que sirve como punto de entrada para el tráfico que tiene como destino el servicio.

5. Especifique los grupos de seguridad que se asociarán a la interfaz de red. Las reglas de los grupos de seguridad controlan el tráfico que proviene de los recursos de su VPC y tiene como destino la interfaz de red de punto de enlace. Si no se especifica un grupo de seguridad, se utilizará el grupo de seguridad predeterminado para la VPC.

2. Elija la VPC en la que desea crear el punto de enlace de interfaz. Puede especificar más de una subred en diferentes zonas de disponibilidad (según lo admita el servicio). Esto ayuda a garantizar que el punto de enlace de interfaz sea resiliente a errores de la zona de disponibilidad. En tal caso, se crea una interfaz de red de punto de enlace en cada subred que especifique.

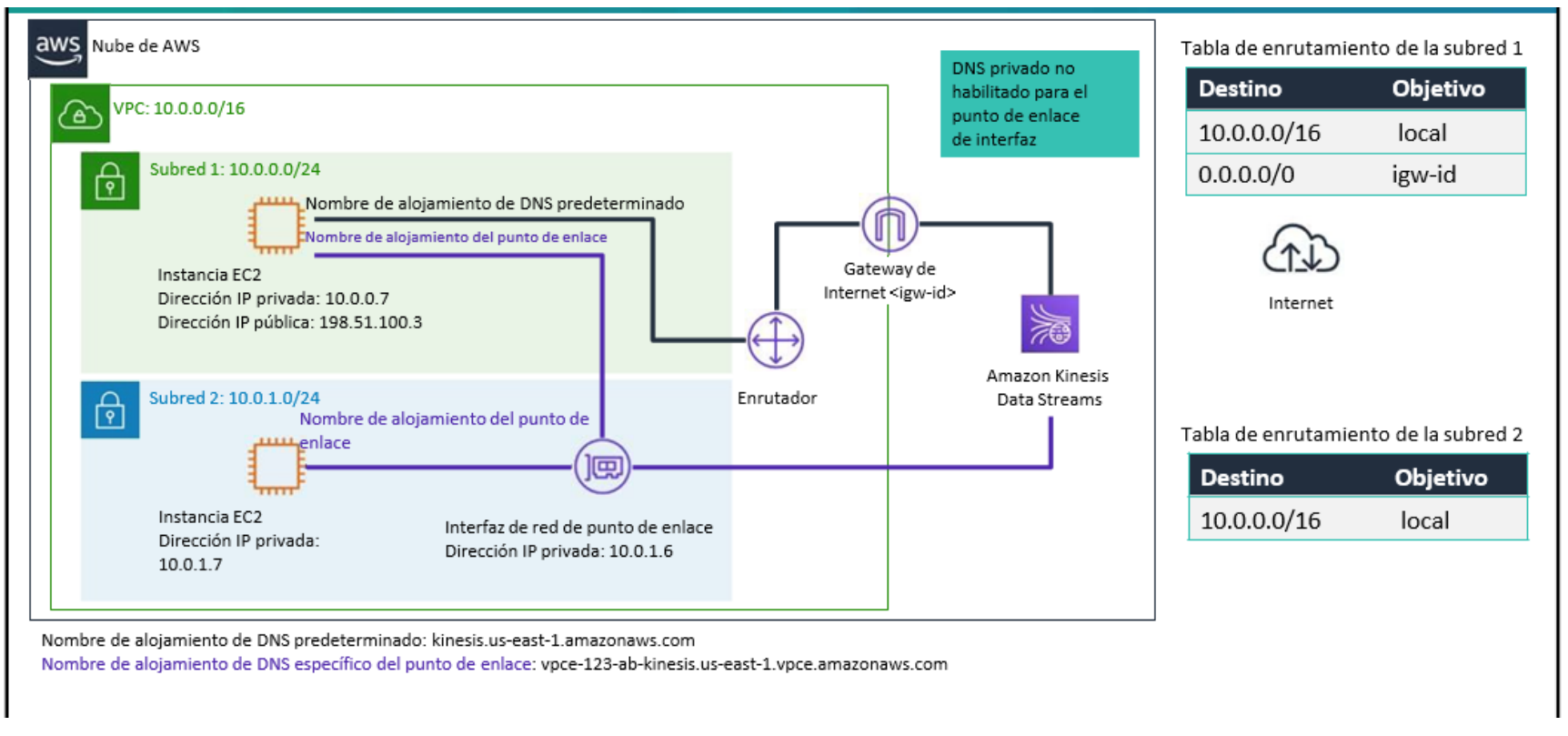
4. (Opcional) Habilite el sistema de nombres de dominio (DNS) privado para el punto de enlace. Hacer esto le permite realizar solicitudes al servicio utilizando su nombre de alojamiento de DNS predeterminado (que está habilitado de forma predeterminada para los puntos de enlace que se hayan creados para los servicios de AWS y los servicios de socios de AWS Marketplace).

Los servicios no pueden presentar solicitudes a los recursos de su VPC a través del punto de enlace. Un punto de enlace solo proporciona respuestas al tráfico que se haya iniciado desde recursos de la VPC.

Para obtener más información sobre cómo crear puntos de enlace de interfaz, consulte los siguientes recursos:

- Creación de un punto de enlace de interfaz

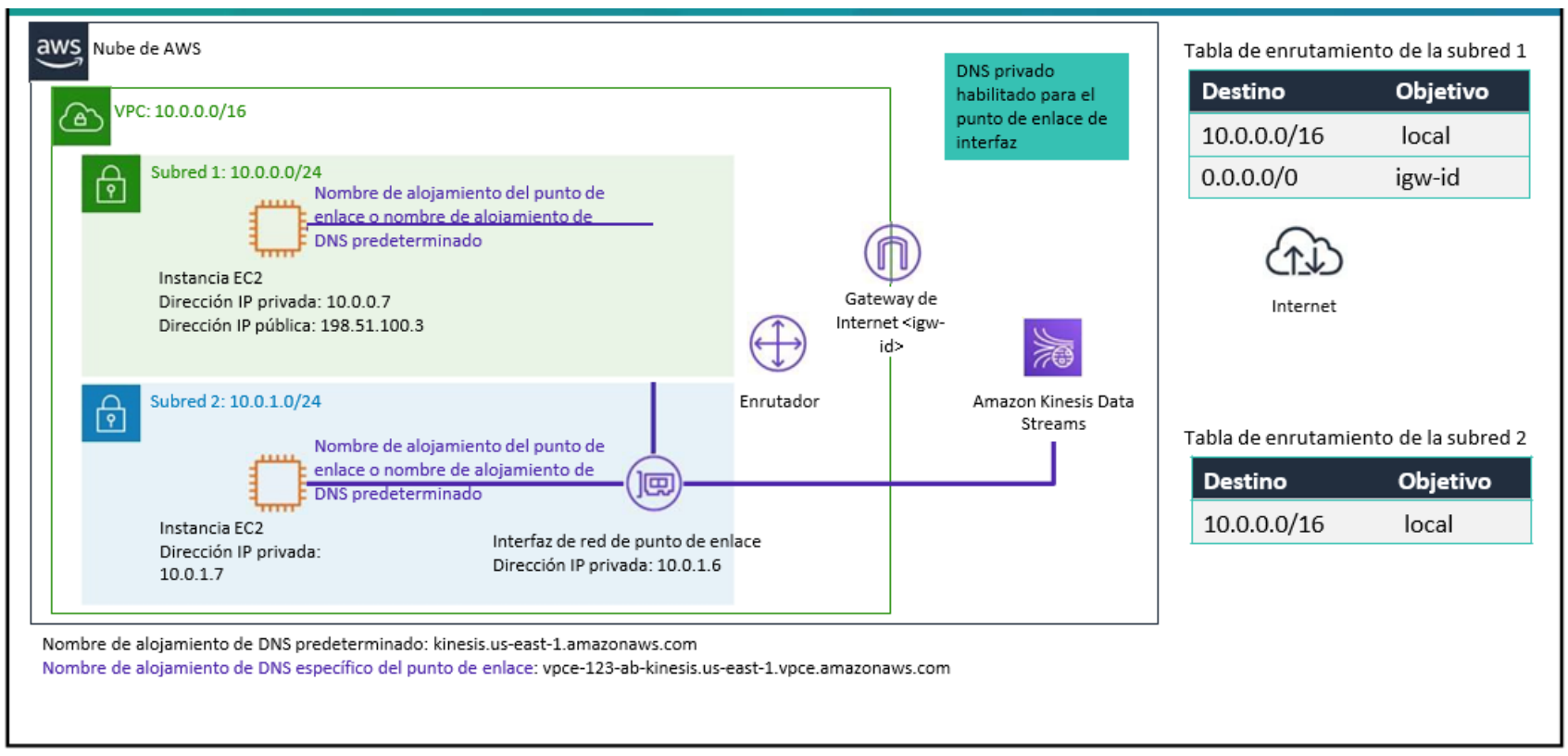
EJEMPLO DE USO DE LOS PUNTOS DE ENLACE DE LA VPC (1 DE 2)



Cuando crea un punto de enlace de interfaz, se generan nombres de alojamiento de DNS específicos del punto de enlace que puede utilizar para comunicarse con el servicio. Para los servicios de AWS y los servicios de socios de AWS Marketplace, la opción de DNS privado (habilitada de forma predeterminada) asocia una zona alojada privada a la VPC. La zona alojada contiene un registro definido para el nombre de DNS predeterminado correspondiente al servicio (por ejemplo, kinesis.us-east-1.amazonaws.com) que se convierte en las direcciones IP privadas de las interfaces de red de punto de enlace de la VPC. Esto habilita a su aplicación a realizar solicitudes al servicio utilizando su nombre de alojamiento de DNS predeterminado, en lugar de los nombres de alojamiento de DNS específicos del punto de enlace. Esto permite que las aplicaciones existentes realicen solicitudes a un servicio de AWS a través del punto de enlace de interfaz, sin necesidad de ningún cambio de configuración.

En este ejemplo, hay un punto de enlace de interfaz para Amazon Kinesis Data Streams y una interfaz de red de punto de enlace en la subred 2. **NO** se ha habilitado el DNS privado para el punto de enlace de interfaz. Las instancias de cualquiera de las subredes pueden enviar solicitudes a Amazon Kinesis Data Streams a través del punto de enlace de interfaz usando un nombre de alojamiento de DNS específico del punto de enlace. Las instancias de la subred 1 pueden comunicarse con Amazon Kinesis Data Streams a través del espacio de dirección IP pública en la región de AWS mediante el nombre de alojamiento de DNS predeterminado que corresponde al servicio.

EJEMPLO DE USO DE LOS PUNTOS DE ENLACE DE LA VPC (2 DE 2)



Aquí, se ha habilitado el DNS privado para el punto de enlace. Las instancias de cualquiera de las subredes pueden enviar solicitudes a Amazon Kinesis Data Streams a través del punto de enlace de interfaz usando el nombre de alojamiento de DNS predeterminado o el nombre de alojamiento de DNS específico del punto de enlace.

Para obtener más información sobre este ejemplo, consulte DNS privado para puntos de enlace de interfaz.

ESTOS SON ALGUNOS DE LOS APRENDIZAJES CLAVE DE ESTA PARTE DE LA LECCIÓN 5 DE LA UNIDAD 2:

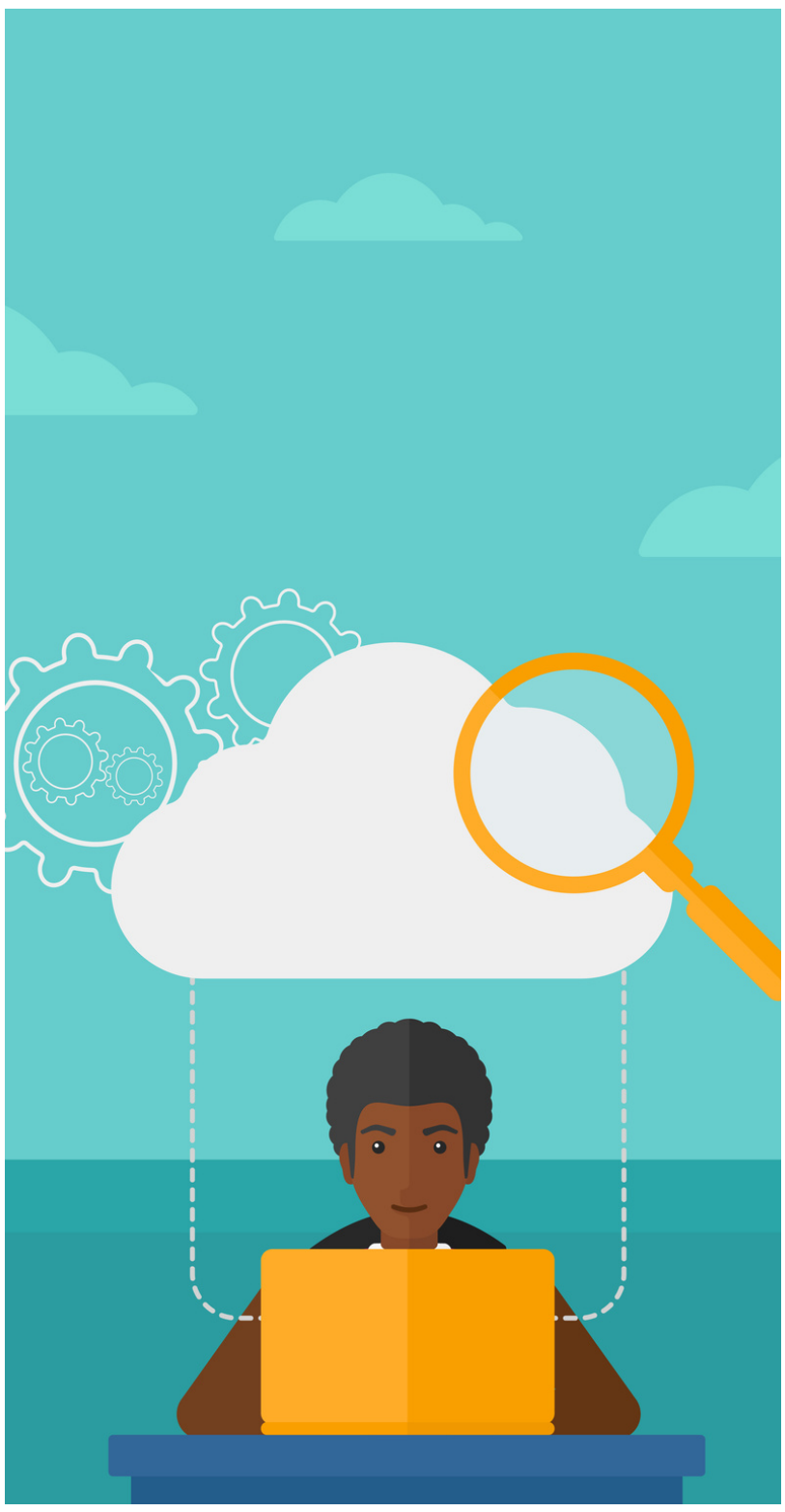
Un punto de enlace de la VPC le permite conectar de forma privada la VPC con servicios de AWS compatibles y servicios de punto de enlace de la VPC que funcionan con tecnología de AWS PrivateLink.

Los puntos de enlace de la VPC no requieren una gateway de Internet, un dispositivo NAT, una conexión de VPN ni una conexión de AWS Direct Connect.

Existen dos tipos de punto de enlace de la VPC: los puntos de enlace de interfaz y los puntos de enlace de gateway.

RESUMEN DE LA UNIDAD

A modo de resumen, en este módulo, aprendió a hacer lo siguiente:



Describir cómo conectar una red en las instalaciones a la nube de AWS

Describir cómo conectar las VPC en la nube de AWS

Conectar las VPC en la nube de AWS mediante la interconexión de VPC

Describir cómo escalar las VPC en la nube de AWS

Describir cómo conectar las VPC a servicios de AWS compatibles