COLOMBIA POTENCIA DE LA VIDA

TIC

Lección 3

VPC networking

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

Universidad Tecnológica de Pereira

Ahora que ha aprendido acerca de los componentes básicos de una VPC, puede comenzar a enrutar el tráfico de maneras interesantes. En esta sección, aprenderá sobre diferentes opciones de redes.

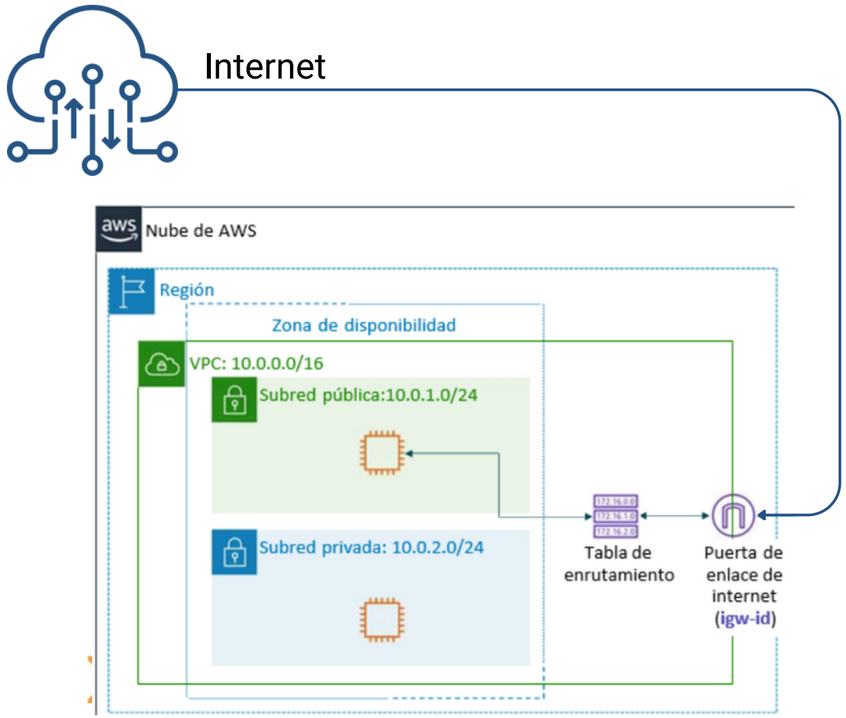


Tabla de enrutamiento de subred pública

Destino	Objetivo
10.0.0.0/16	local
0.0.0.0/0	igw-id

Una puerta de enlace de internet es un componente de la VPC de alta disponibilidad, redundante y escalable que permite la comunicación entre las instancias en la VPC e Internet. Una puerta de enlace de internet tiene dos funciones: proporcionar un objetivo en las tablas de enrutamiento de VPC para el tráfico que se puede enrutar a través de Internet y traducir direcciones de red para instancias a las cuales se les asignan direcciones IPv4 públicas.

Para que una subred sea pública, puede adjuntar una puerta de enlace de Internet a su VPC y agregar una ruta a la tabla de enrutamiento para enviar tráfico no local a través de la puerta de enlace de Internet a Internet (0.0.0.0/0).

Para obtener más información sobre, consulte puertas de enlace de internet, vea Puertas de enlace de Internet en la documentación de AWS en https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Internet_Gateway.html

Puerta de enlace de traducción de direcciones de red (NAT)

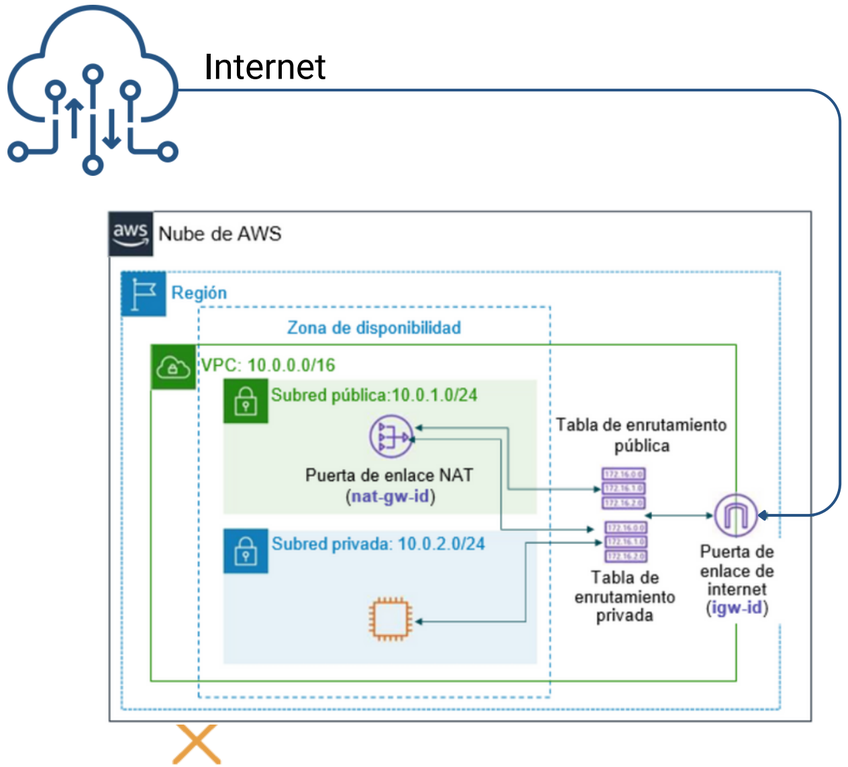


Tabla de enrutamiento de subred pública

Destino	Objetivo
10.0.0.0/16	local
0.0.0.0/0	igw-id

Tabla de enrutamiento de subred privada

Destino	Objetivo
10.0.0.0/16	local
0.0.0.0/0	nat-gw-id

Una puerta de enlace de traducción de direcciones de red (NAT) habilita las instancias de una subred privada a conectarse a Internet o a otros servicios de AWS, pero 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 cuando la cree. 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.

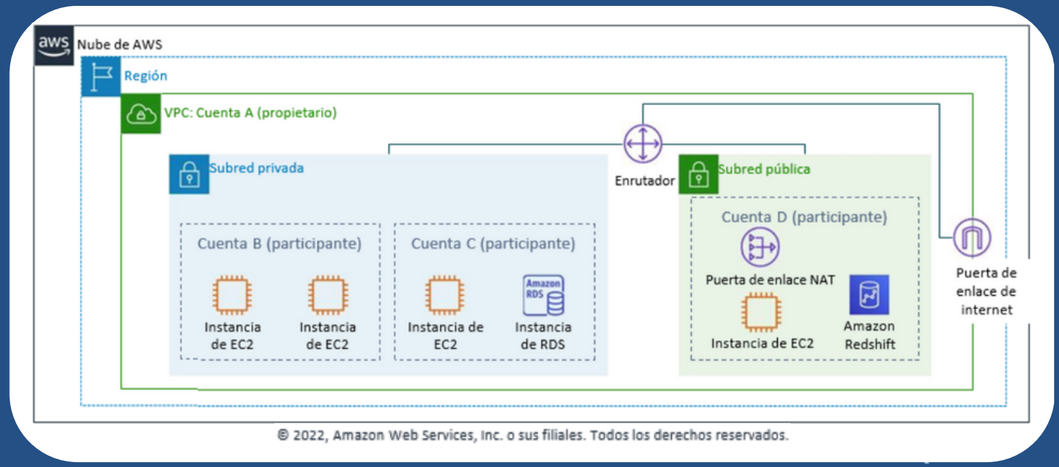
También puede utilizar una instancia NAT en una subred pública de su VPC en lugar de una puerta de enlace NAT. Sin embargo, una puerta de enlace NAT es un servicio NAT administrado que ofrece mayor disponibilidad, mayor ancho de banda y menos esfuerzo administrativo. Para los casos prácticos habituales,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

Consulte la documentación de AWS para más información sobre

- Puertas de enlace de 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
- Diferencias entre puertas de enlace NAT e instancias de NAT https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-comparison.html

Uso compartido de VPC

El uso compartido de VPC permite a los clientes compartir subredes con otras cuentas de AWS en la misma organización en AWS Organizations. El uso compartido de VPC permite que varias cuentas de AWS creen sus recursos de aplicaciones, como instancias de Amazon EC2, bases de datos de Amazon Relational Database Service (Amazon RDS), clústeres de Amazon Redshift y funciones de Lambda en VPC administradas compartidas.



En este modelo, la cuenta propietaria de la VPC (propietario) comparte una o más subredes con otras cuentas (participantes) que pertenecen a la misma organización en AWS Organizations. Después de compartir una subred, los participantes pueden ver, crear, modificar y eliminar los recursos de su aplicación en las subredes que se comparten con ellos. Los participantes no pueden ver, modificar ni eliminar recursos que pertenezcan a otros participantes o al propietario de la VPC.

El uso compartido de VPC ofrece varios beneficios:

- Separación de funciones: estructura de VPC, enrutamiento y asignación de direcciones IP controlados centralmente
- Propiedad: los propietarios de aplicaciones siguen siendo propietarios de recursos, cuentas y grupos de seguridad.
- Grupos de seguridad: los participantes que comparten VPC pueden hacer referencia a los ID de grupo de seguridad de cada uno
- Eficiencias: mayor densidad en subredes, uso eficiente de VPN y AWS Direct Connect
- Sin límites estrictos: se pueden evitar los límites estrictos; por ejemplo, 50 interfaces virtuales por conexión de AWS Direct Connect a través de una arquitectura de red simplificada.
- Costos optimizados: los costos se pueden optimizar mediante la reutilización de puertas de enlace NAT, puntos finales de interfaz de VPC y tráfico dentro de la zona de disponibilidad.

El uso compartido de VPC le permite desacoplar cuentas y redes. Tiene menos VPC, más grandes y administradas de forma centralizada. Las aplicaciones altamente interconectadas se benefician automáticamente de este enfoque.

Interconexión de VPC

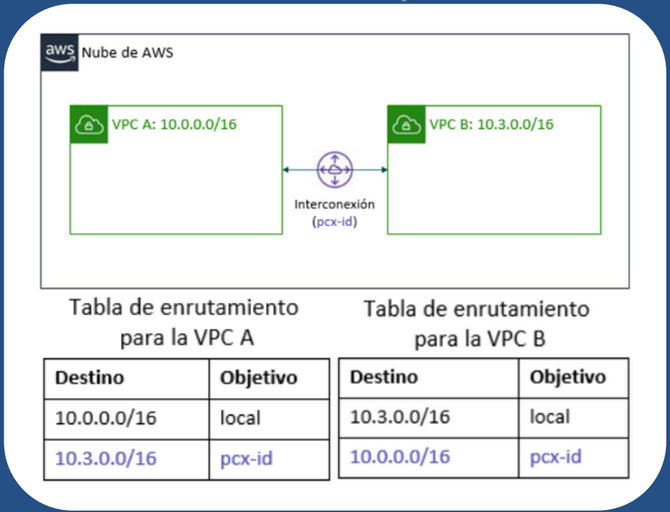


Tabla de enrutamiento para la VPC A

Destino	Objetivo
10.0.0.0/16	local
10.3.0.0/16	pcx-id

Tabla de enrutamiento para la VPC B

Destino	Objetivo
10.3.0.0/16	local
10.0.0.0/16	pcx-id

Puede conectar VPC en su propia cuenta de AWS, entre cuentas de AWS o entre regiones de AWS.
Restricciones:

- Los espacios IP no se pueden superponer.
- La interconexión transitiva no está admitida.
- Puede tener solo un recurso de interconexión entre dos VPC.

Una interconexión de VPC es una conexión de redes entre dos VPC que le permite dirigir el tráfico entre ellas de forma privada. Las instancias en cualquiera de las VPC se pueden comunicar entre sí como si estuvieran en la misma red. Puede crear una interconexión de VPC entre sus propias VPC, con una VPC en otra cuenta de AWS o con una VPC en una región de AWS diferente.

Cuando configura la interconexión, crea reglas en su tabla de enrutamiento que permiten que las VPC se comuniquen entre sí a través del recurso de interconexión. Por ejemplo, suponga que tiene dos VPC. En la tabla de enrutamiento para la VPC A, establece que el destino sea la dirección IP de la VPC B y que el objetivo sea el ID del recurso de interconexión. En la tabla de enrutamiento para la VPC B, establece que el destino sea la dirección IP de la VPC A y que el objetivo sea el ID del recurso de interconexión.

La interconexión de VPC tiene algunas restricciones:

- Los intervalos de direcciones IP no pueden superponerse.
- La interconexión transitiva no está admitida. Por ejemplo, suponga que tiene tres VPC: A, B y C. La VPC A está conectada a la VPC B y la VPC A está conectada a la VPC C. Sin embargo, la VPC B no está conectada a la VPC C implícitamente. Para conectar la VPC B a la VPC C, debe establecer explícitamente esa conectividad.
- Puede tener sólo un recurso de interconexión entre dos VPC.

Para obtener más información acerca de las interconexiones de VPC, consulte Interconexiones de VPC en https://docs.aws.amazon.com/vpc/latest/peering/vpc-peering-basics.htm

AWS Site-to-Site VPN

De manera predeterminada, las instancias que usted inicia en una VPC no pueden comunicarse con una red remota. Para conectar su VPC a su red remota (que significa, crear una red privada virtual o conexión VPN), usted debe:

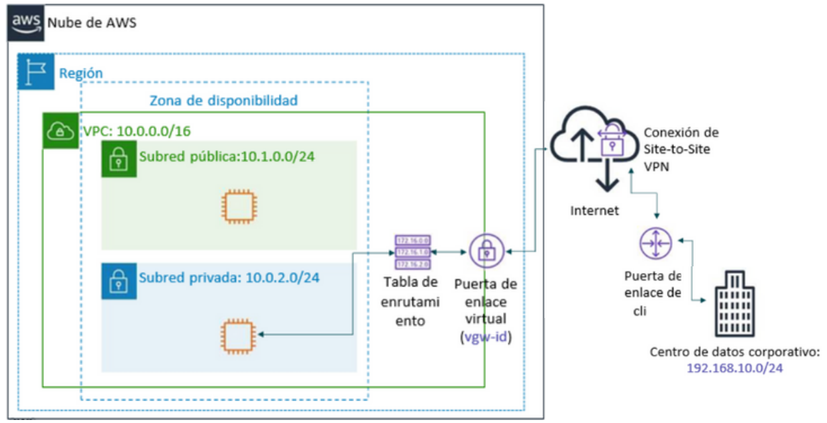


Tabla de enrutamiento de subred pública

Destino	Objetivo
10.0.0.0/16	local
0.0.0.0/0	igw-id

Tabla de enrutamiento de subred privada

Destino	Objetivo
10.0.0.0/16	local
192.168.10.0/24	vgw-id

1. Crear un nuevo dispositivo de puerta de enlace (llamado una puerta de enlace de red privada virtual (VPN)) y adjuntar a su VPC.

2. Definir la configuración del dispositivo VPN o la puerta de enlace del cliente. La puerta de enlace de cliente no es un dispositivo sino un recurso de AWS que brinda información sobre su dispositivo VPN a AWS.

3 Crear una tabla de enrutamiento personalizada para dirigir el tráfico del centro de datos corporativo a la puerta de enlace VPN. También debe actualizar las reglas del grupo de seguridad. (Aprenderá sobre los grupos de seguridad en la siguiente sección).

4 Establecer una conexión Site-to-Site VPN de AWS para enlazar los dos sistemas.

5 Configure el enrutamiento para pasar el tráfico a través de la conexión.

Para obtener más información sobre AWS Site-to-Site VPN y otras opciones de conectividad VPN, consulte Conexiones de VPN en la documentación de AWS en https://docs.aws.amazon.com/vpc/latest/userguide/vpn-connections.html

COLOMBIA POTENCIA DE LA VIDA

TIC

Presionar cada tema para ver si contenido

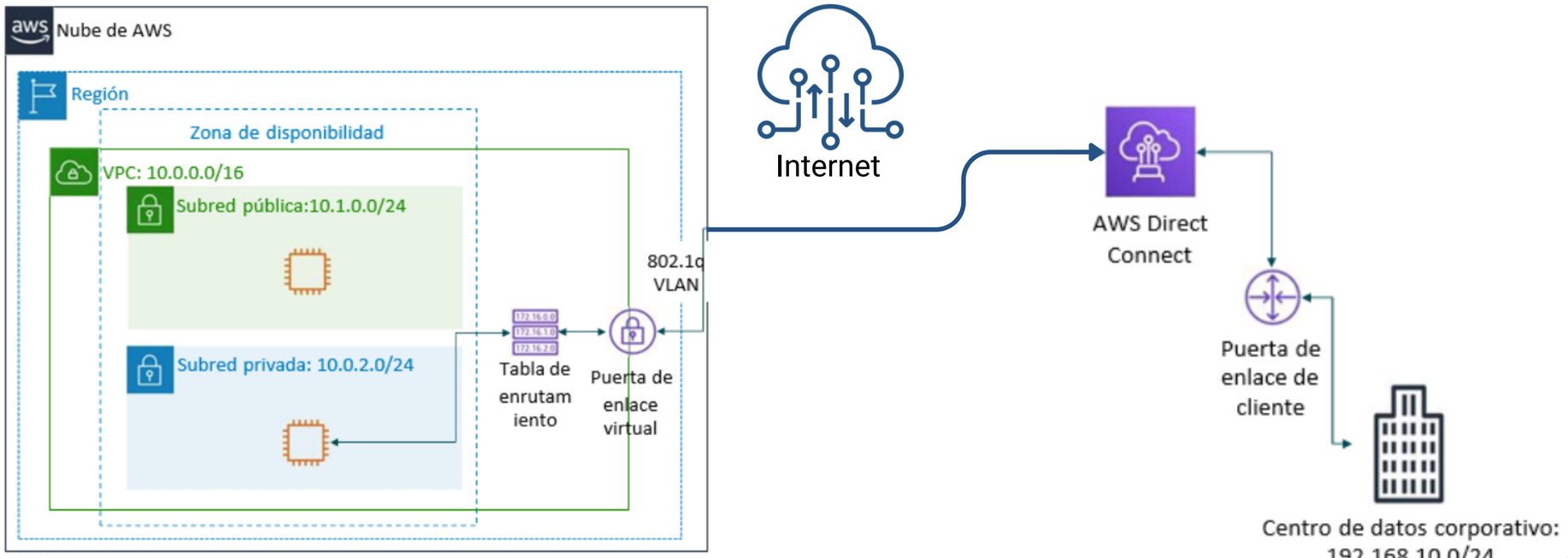
- AWS Direct Connect
- Puntos de enlace de VPC
- AWS Transit Gateway
- Actividad
- Puntos clave

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

Universidad Tecnológica de Pereira

AWS Direct Connect



+INFO

Uno de los desafíos de una conexión de VPN es el rendimiento de la red. El rendimiento se puede ver afectado de forma negativa si su centro de datos está ubicado lejos de su región de AWS. Para este tipo de situaciones, AWS ofrece AWS Direct Connect o DX. AWS Direct Connect le permite establecer una conexión de red dedicada y privada entre su red y una de las ubicaciones de DX. Esta conexión privada puede reducir los costos de red, mejorar el rendimiento del ancho de banda y proporcionar una experiencia de red más uniforme que las conexiones basadas en Internet. DX utiliza redes de área local virtual (VLAN) 802.1q de estándar abierto.

Para obtener más información sobre DX, consulte la página de productos de AWS Direct Connect en https://aws.amazon.com/directconnect/

Puntos de enlace de VPC

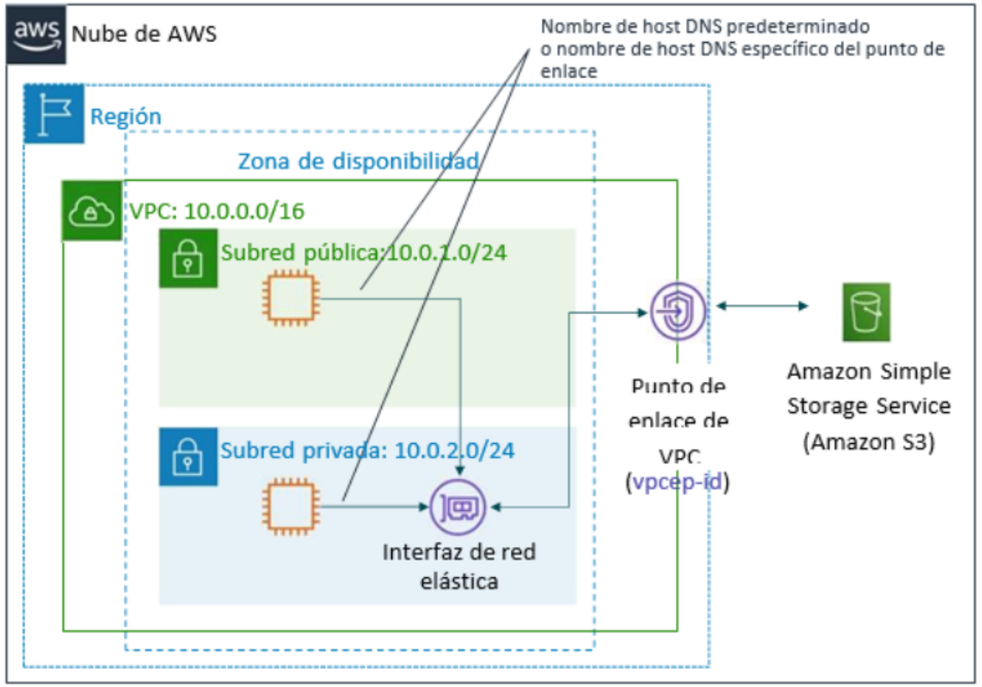


Tabla de enrutamiento de subred pública

Destino	Objetivo
10.0.0.0/16	local
ID de Amazon S3	vpcep-id

Dos tipos de puntos de enlace:

- Puntos de enlace de interfaz (con tecnología de AWS PrivateLink)
- Puntos de enlace de puertas de enlace (Amazon S3 y Amazon DynamoDB)

+INFO

Un punto de enlace de la VPC es un dispositivo virtual que le permite conectar de forma privada su VPC a los servicios de AWS compatibles y a los servicios de punto de enlace de la VPC con tecnología de AWS PrivateLink. La conexión a estos servicios no requiere puerta de enlace de internet, dispositivo NAT, conexión VPN ni conexión AWS Direct Connect. 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.

COLOMBIA POTENCIA DE LA VIDA

TIC

Hay dos tipos de puntos de conexión de la VPC:

Un punto de enlace de la VPC (punto de enlace de interfaz), le permite conectarse a servicios con tecnología de AWS PrivateLink. Estos servicios incluyen algunos servicios de AWS, servicios alojados por otros clientes y socios de AWS y red de socios de AWS (APN) en sus propias VPC (denominados servicios de punto de enlace) y servicios de socios de AWS Marketplace y APN compatibles. El propietario del servicio es el proveedor del servicio y usted, como director que crea el punto final de la interfaz, es el consumidor del servicio. Se le cobra por crear y usar un punto de enlace de interfaz en un servicio. Se aplican tarifas de uso por horas y tarifas de procesamiento de datos.

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

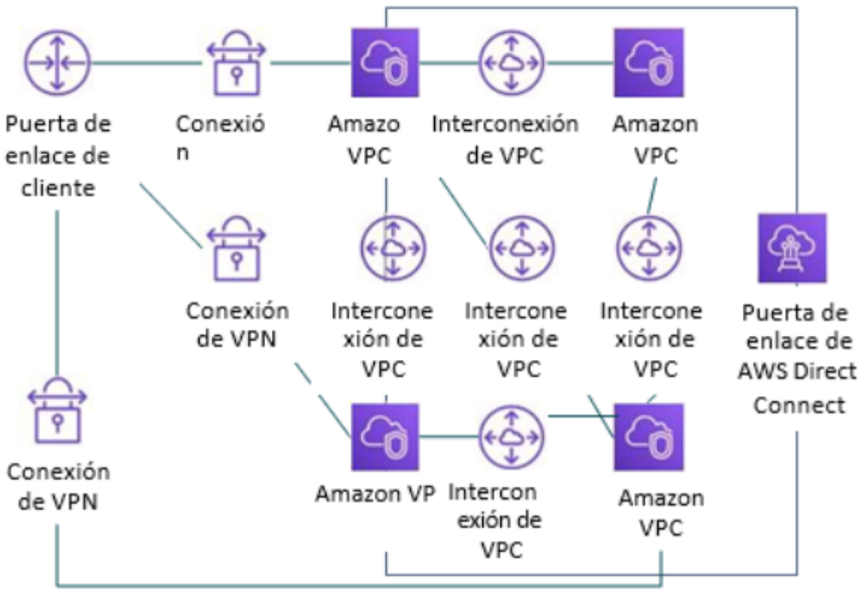
UTP Universidad Tecnológica de Pereira

Puntos de enlace de puerta de enlace: el uso de puntos de enlace de puerta de enlace no genera ningún cargo adicional. Se aplicará la tarifa estándar por la transferencia de datos y por el uso de recursos.

Para obtener más información acerca de los puntos de enlace de VPC, consulte Puntos de enlace de VPC en la documentación de AWS en https://docs.aws.amazon.com/vpc/latest/privatelink/concepts.html

AWS Transit Gateway

Desde este...



Hasta este...

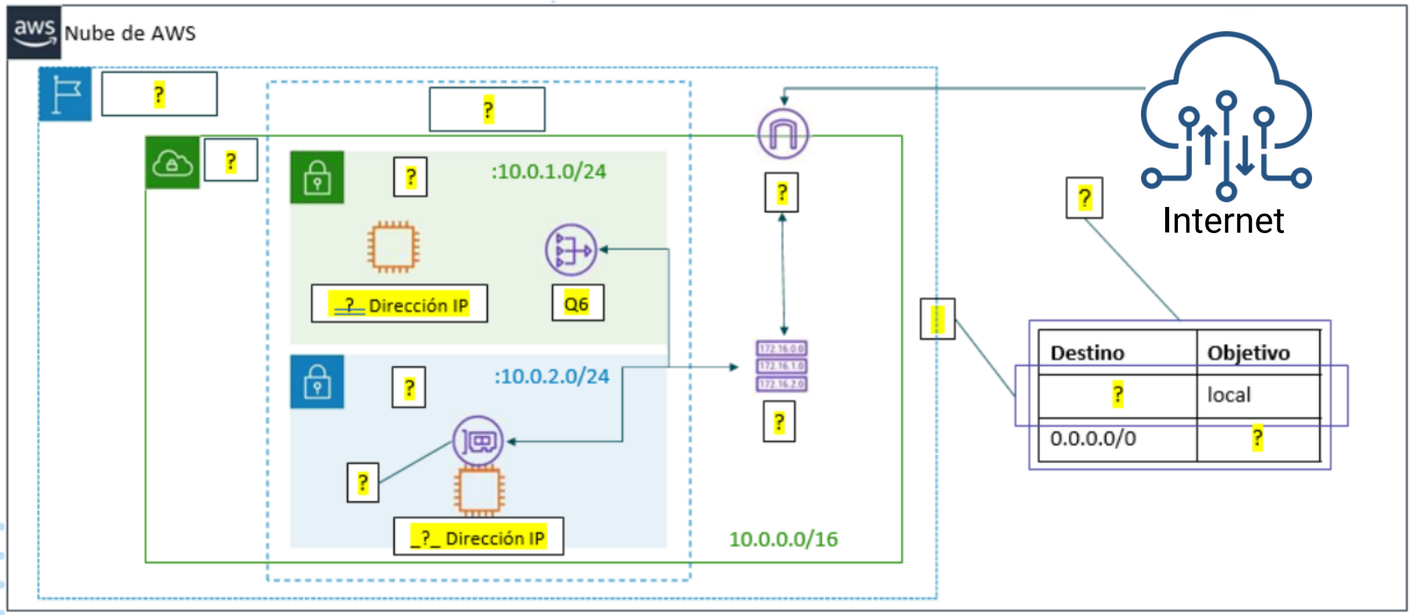
+INFO

Puede configurar sus VPC de varias maneras y aprovechar numerosas opciones de conectividad y puertas de enlace. Estas opciones y puertas de enlace incluyen AWS Direct Connect (a través de puertas de enlace DX), puertas de enlace NAT, puertas de enlace de Internet, interconexión de VPC, etc. No es raro encontrar clientes de AWS con cientos de VPC distribuidas en cuentas y regiones de AWS para atender múltiples líneas de negocios, equipos, proyectos, etc. Las cosas se vuelven más complejas cuando los clientes comienzan a configurar la conectividad entre sus VPC. Todas las opciones de conectividad son estrictamente punto a punto, por lo que la cantidad de conexiones de VPC a VPC puede crecer rápidamente. A medida que aumenta la cantidad de cargas de trabajo que se ejecutan en AWS, debe poder escalar sus redes en múltiples cuentas y VPC para mantenerse al día con el crecimiento.

Si bien puede utilizar interconexión de VPC para conectar pares de VPC, la administración de la conectividad punto a punto en muchas VPC, sin la capacidad para centralizar la administración de las políticas de conectividad, puede ser costosa en términos operativos y difícil. Para conectividad en las instalaciones, debe asociar el VPN a cada VPC individual. Esta solución puede ser de lenta creación y difícil administración cuando hay cientos de VPC.

Para resolver este problema, puede usar AWS Transit Gateway para simplificar su modelo de redes. Con AWS Transit Gateway, solo debe crear y administrar una única conexión desde la puerta de enlace central a cada VPC, centro de datos en las instalaciones u oficina remota en su red. Una puerta de enlace de tránsito actúa como un centro que controla la manera en la que el tráfico se enruta a todas las redes conectadas, que funcionan como radios. Este sistema radial simplifica de manera significativa la administración y reduce los costos operativos porque cada red solo debe conectarse a la gateway de tránsito y a ninguna otra red. Cualquier VPC nueva se conecta a la puerta de enlace de tránsito y queda disponible automáticamente para cualquier otra red que esté conectada a la puerta de enlace de tránsito. Esta facilidad de conectividad simplifica la capacidad de escalar su red a medida que crece.

Actividad: Etiquetar este diagrama



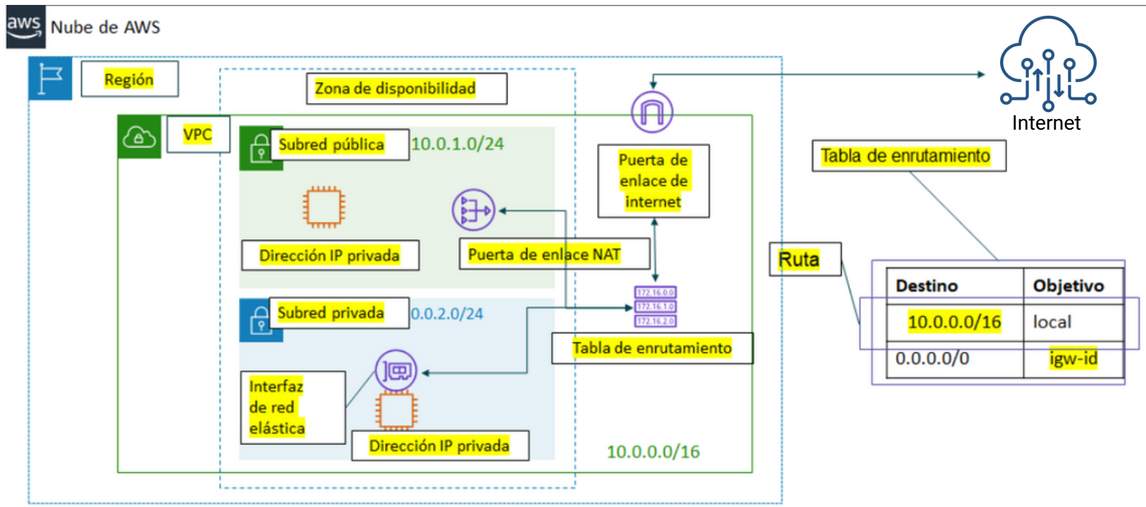
Vea si puede reconocer los diferentes componentes de red de VPC que conoció al etiquetar este diagrama de red

+INFO

Ahora, mire lo bien que lo hizo.

Actividad: solución

Ahora que sabe cómo diseñar una VPC, mire la demostración en para aprender a utilizar el asistente de VPC para configurar una VPC con subredes públicas y privadas.



Puntos clave

Los puntos clave de esta lección de la unidad 2 incluyen:

- Demostración registrada de Amazon VPC
- Puerta de enlace a Internet: conecta su VPC a Internet
- Puerta de enlace NAT: habilitas instancias en una subred privada para conectarse a Internet
- Punto de enlace de VPC: conecta de forma privada su VPC a los servicios de AWS compatibles
- Interconexión de VPC: conecta su VPC a otras VPC
- Uso compartido de VPC: permite que varias cuentas de AWS creen sus recursos de aplicaciones en Amazon VPC compartidas y administradas de forma centralizada.
- AWS Site-to-Site VPN: conecta su VPC a redes remotas
- AWS Direct Connect: conecta su VPC a una red remota mediante una conexión de red dedicada
- AWS Transit Gateway: una alternativa de conexión central y periférica a la interconexión de VPC
- Puede utilizar el VPC Wizard para implementar su diseño.

INICIO