COLOMBIA POTENCIA DE LA VIDA

TIC

LECCIÓN 4:
CONEXIÓN DE LAS VPC EN AWS CON LA INTERCONEXIÓN DE VPC

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

CONEXIÓN DE VPC

Por lo general, aislar algunas de las cargas de trabajo se considera una práctica recomendada.

Sin embargo, es posible que tenga que transferir datos entre dos o más VPC.

Por lo general, aislar las cargas de trabajo en VPC individuales se considera una práctica recomendada. Por ejemplo, cuando su empresa o arquitectura sean lo suficientemente grandes, es posible que deba separar elementos lógicos, ya sea por seguridad o necesidades de la arquitectura, o bien, por simplicidad. Sin embargo, puede ser muy conveniente tener conectividad entre las VPC para situaciones en las que necesite transferir datos entre ellas.

INTERCONEXIÓN DE VPC

Se establece una conexión de red directa entre dos VPC.

No se necesitan gateway, conexiones de VPN ni dispositivos de red independientes.

Las conexiones cuentan con alta disponibilidad.

No hay puntos únicos de error ni cuellos de botella en el ancho de banda.

El tráfico siempre permanece en la red troncal global de AWS.

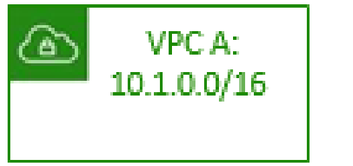
Una interconexión de VPC es una conexión de red directa entre dos VPC que permite dirigir el tráfico entre ellas de forma privada. Las instancias de cualquiera de las VPC pueden comunicarse entre sí como si estuvieran en la misma red. Puede crear una interconexión de VPC entre sus propias VPC, con una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

Puede establecer relaciones de interconexión entre VPC de diferentes regiones de AWS. La interconexión de VPC entre regiones ofrece una forma sencilla y rentable de compartir recursos entre regiones o de replicar datos para conseguir redundancia geográfica. Los datos transferidos a través de interconexiones de VPC entre regiones se cobran según las tarifas estándar de transferencia de datos entre regiones.

La interconexión de VPC entre regiones permite que los recursos de VPC se comuniquen entre sí mediante direcciones IP privadas, sin la necesidad de recurrir a gateways, conexiones de VPN ni dispositivos de red independientes. Algunos ejemplos de recursos de VPC incluyen las instancias de Amazon Elastic Compute Cloud (Amazon EC2), las bases de datos de Amazon Relational Database Service (Amazon RDS) y las funciones de AWS Lambda que se ejecutan en diferentes regiones.

El tráfico permanece en el espacio de direcciones IP privadas. Todo el tráfico entre regiones se cifra sin un punto único de error ni cuello de botella en el ancho de banda. El tráfico
siempre permanece en la red troncal global de AWS. El tráfico nunca pasa por el Internet público, lo que reduce la cantidad de amenazas, como ataques comunes y ataques de denegación de servicio distribuidos (DDoS).

ESTABLECIMIENTO DE LA INTERCONEXIÓN DE VPC



Interconexión
(PCX-1)

Tabla de enrutamiento de la VPC A

Destino	Objetivo
10.1.0.0/16	local
10.2.0.0/16	PCX-1

Tabla de enrutamiento de la VPC B

Destino	Objetivo
10.2.0.0/16	local
10.1.0.0/16	PCX-1

Para establecer una interconexión de VPC, el propietario de la VPC solicitante (o VPC local) envía una solicitud al propietario de la VPC del mismo nivel. Para activar la conexión, el propietario de la VPC del mismo nivel debe aceptar la solicitud de interconexión de VPC.

Para permitir el flujo del tráfico entre las VPC del mismo nivel utilizando direcciones IP privadas, debe agregar una ruta a una o más tablas de enrutamiento de la VPC. Esta ruta debe llevar al intervalo de direcciones IP de la VPC del mismo nivel. El propietario de la VPC del mismo nivel agrega una ruta a una de sus tablas de enrutamiento de la VPC que lleva al intervalo de direcciones IP de la VPC.

Es posible que también tenga que actualizar las reglas del grupo de seguridad que se han asociado a la instancia para que el tráfico desde y hacia la VPC del mismo nivel no se vea restringido.

RESTRICCIONES EN LA INTERCONEXIÓN DE VPC

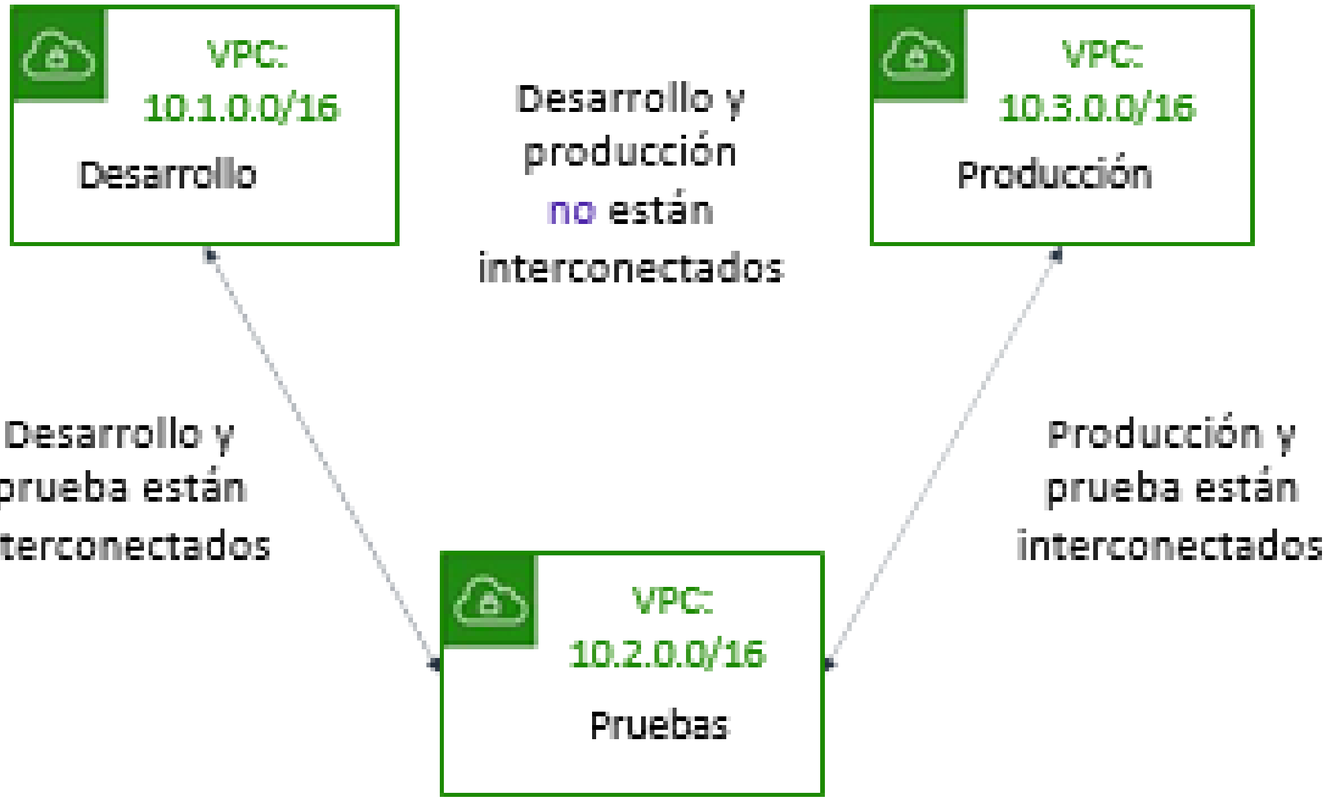
Se usan direcciones IP privadas

Se pueden establecer entre cuentas diferentes de AWS

No se pueden tener bloques de CIDR superpuestos

Solo se puede tener un recurso de interconexión entre dos VPC cualquiera

No se admiten relaciones de interconexión transitivas


VPC:
10.1.0.0/16
Desarrollo
Desarrollo y producción no están interconectados
VPC:
10.3.0.0/16
Producción
Desarrollo y prueba están interconectados
Producción y prueba están interconectados
VPC:
10.2.0.0/16
Pruebas

COLOMBIA POTENCIA DE LA VIDA

TIC

EXISTEN ALGUNAS RESTRICCIONES QUE DEBE TENER EN CUENTA AL ESTABLECER INTERCONEXIONES DE VPC:

Las interconexiones de VPC se pueden establecer entre diferentes cuentas de AWS. El bloque de CIDR de la VPC del mismo nivel no puede superponerse con el de la VPC solicitante.

Solo puede tener un recurso de interconexión entre dos VPC cualquiera.

No se admite la interconexión transitiva. Por ejemplo, en el diagrama, las VPC de desarrollo y prueba están interconectadas, y las de producción y prueba también. Sin embargo, esto no significa que la VPC de producción esté conectada a la VPC de desarrollo. De forma predeterminada, la interconexión de VPC no permite que la VPC de producción se conecte a la de desarrollo, a menos que estén explícitamente establecidas en el mismo nivel. Por lo tanto, usted controla qué VPC pueden comunicarse entre sí.

Para obtener más información sobre las restricciones de la interconexión de VPC, consulte Limitaciones de interconexión de VPC.

CONSIDERACIONES PARA INTERCONECTAR VARIAS VPC

CUANDO CONECTE VARIAS VPC, TENGA EN CUENTA LOS SIGUIENTES PRINCIPIOS DE DISEÑO DE REDES:

Solo debe conectar las VPC esenciales

Asegúrese de que su solución pueda escalar

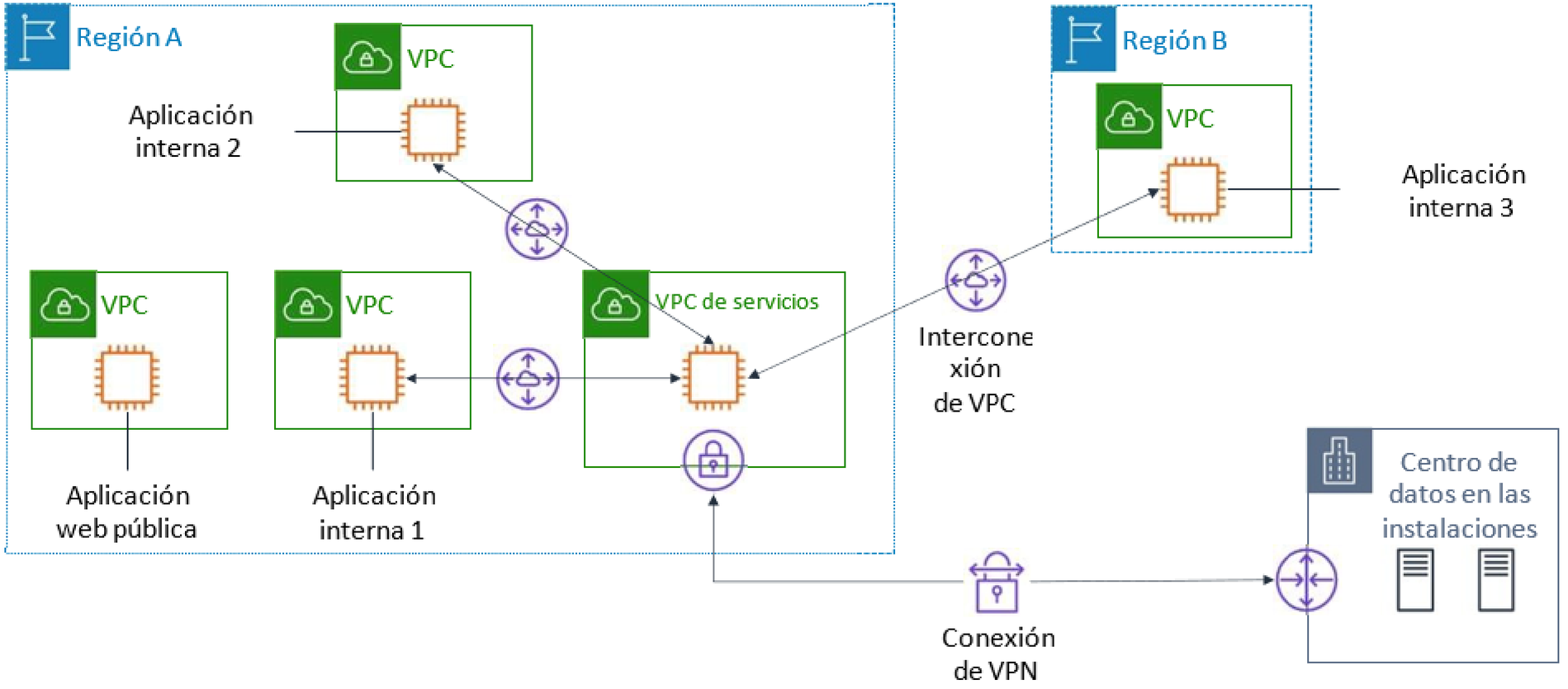
Conecte solo aquellas VPC que realmente deben comunicarse entre sí

Asegúrese de que la solución que elija pueda escalar en función de sus necesidades de conectividad de la VPC actuales y futuras.

EJEMPLO: INTERCONEXIÓN DE VPC PARA RECURSOS COMPARTIDOS

Aquí, se muestra un ejemplo de cómo puede utilizar la interconexión de VPC para recursos compartidos.

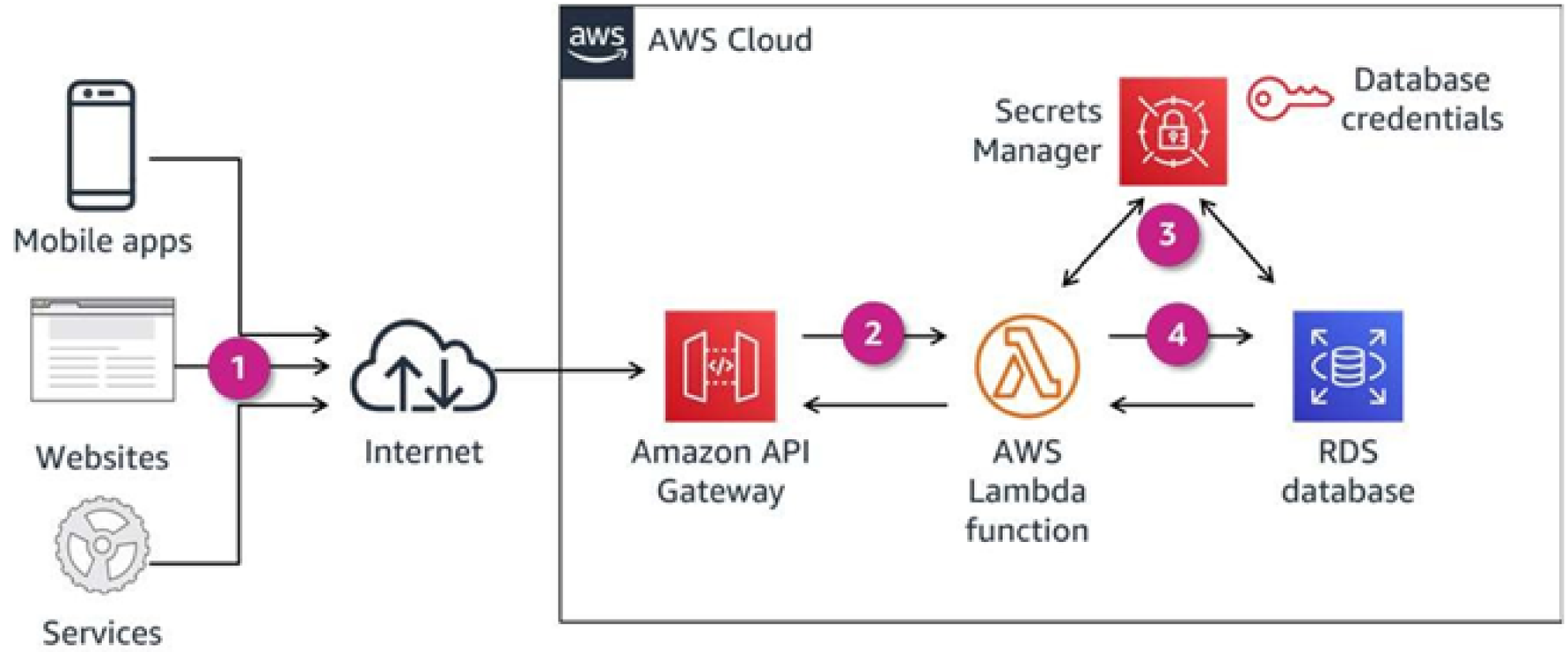
En este ejemplo, las VPC de cada departamento de una empresa están interconectadas con una VPC de servicios compartida. Esta VPC contiene conexiones a Microsoft Active Directory, herramientas de análisis de la seguridad, herramientas de monitoreo y registro, y muchas otras capacidades. También proporciona un proxy mediante el cual las VPC de los departamentos pueden acceder a algunos recursos en las instalaciones. La interconexión de VPC permite que las aplicaciones de la empresa que se encuentren en distintas VPC accedan a la VPC de servicios compartida, pero permanezcan aisladas entre sí. En este ejemplo, también observe que se estableció una interconexión de VPC entre VPC de regiones diferentes.


Región A
VPC
Aplicación interna 2
VPC
VPC
VPC de servicios
Aplicación web pública
Aplicación interna 1
Región B
VPC
Aplicación interna 3
Interconexión de VPC
Centro de datos en las instalaciones
Conexión de VPN

AWS Secrets Manager es un servicio que simplifica la administración de datos confidenciales. Los datos confidenciales pueden ser credenciales de base de datos, contraseñas, claves de API de terceros e incluso texto arbitrario. Puede almacenar y controlar el acceso a estos datos confidenciales de forma centralizada con la consola, la CLI de AWS o la API y los SDK.

Con Secrets Manager, puede eliminar las credenciales codificadas de forma rígida (incluidas las contraseñas) de su código fuente y evitar almacenar las credenciales en un archivo de configuración. En su lugar, utiliza una llamada API a Secrets Manager para recuperar el dato confidencial mediante programación. Esto ayuda a garantizar que los datos confidenciales no puedan ser vulnerados si alguien examina el código, ya que simplemente no están ahí. Además, puede configurar Secrets Manager de forma que rote los datos confidenciales automáticamente de acuerdo con la programación que especifique. Por lo tanto, puede reemplazar datos confidenciales a largo plazo por datos confidenciales a corto plazo, lo que ayuda a reducir significativamente el riesgo de que haya una vulneración.

USO DE SECRETS MANAGER



COLOMBIA POTENCIA DE LA VIDA

TIC

LABORATORIO GUIADO: TAREAS

CREAR UNA INTERCONEXIÓN DE VPC ENTRE DOS VPC

CONFIGURAR TABLAS DE ENRUTAMIENTO PARA ENVIAR TRÁFICO A LA INTERCONEXIÓN

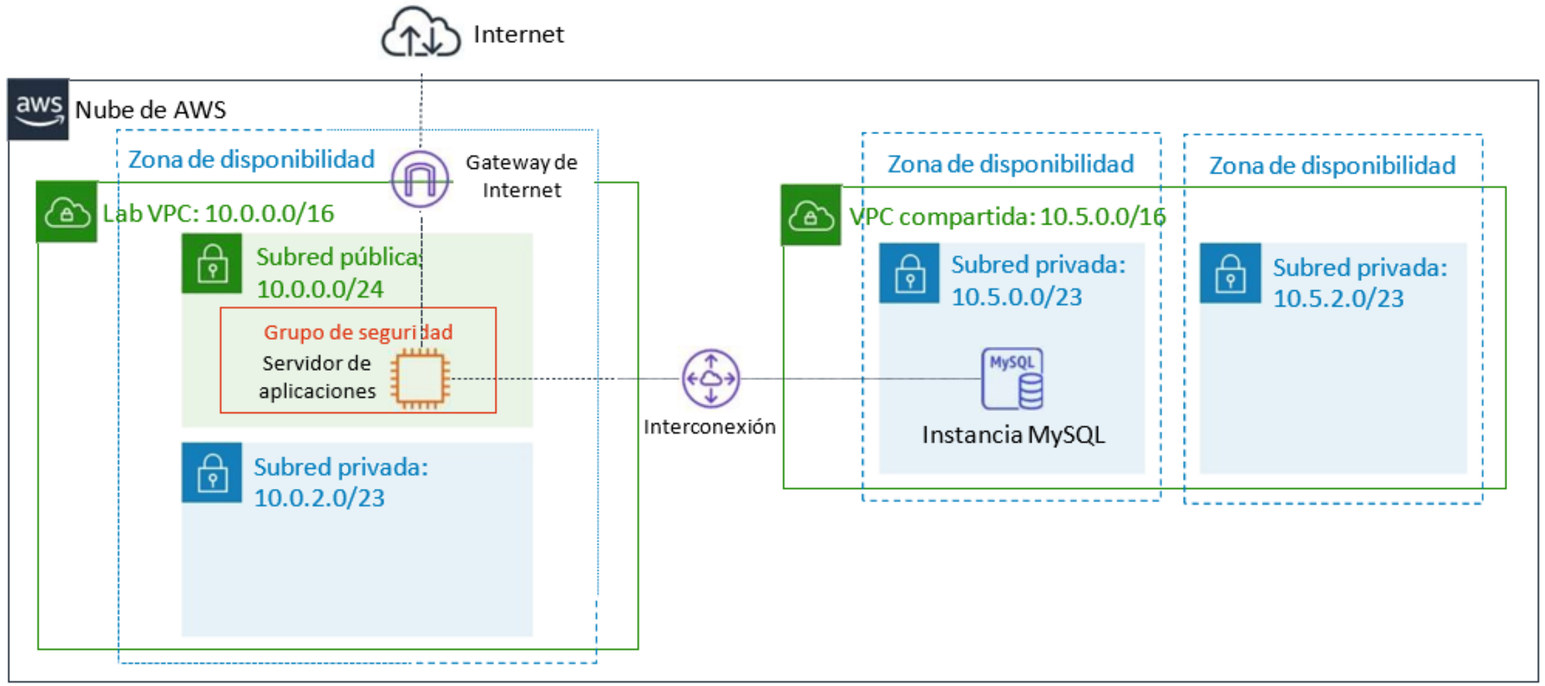
PROBAR LA INTERCONEXIÓN

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

UTP Universidad Tecnológica de Pereira

LABORATORIO GUIADO: PRODUCTO FINAL



EN EL DIAGRAMA, SE RESUME LO QUE HABRÁ CREADO DESPUÉS DE TERMINAR EL LABORATORIO.