TRANSIT GATEWAY

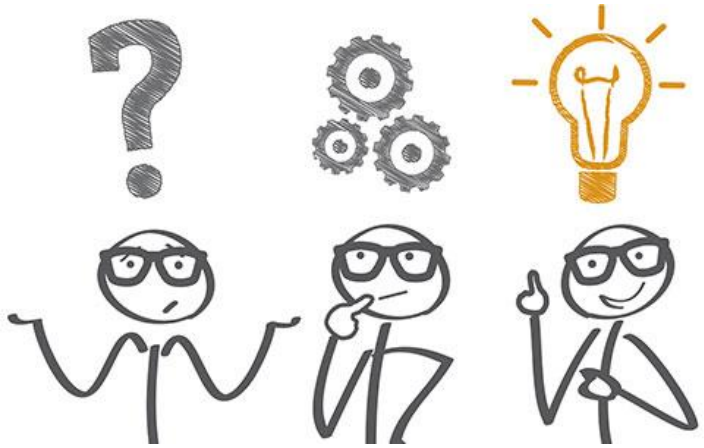
Uso en estrategias multi VPC en AWS

Carlos Cruzado
CLOUD SOLUTIONS ARCHITECT
/ccruzado

Resumen

- Multi cuentas en AWS
- Uso de multi VPC
- VPC Peering
- Transit Gateway
- Demo

Multi cuentas en AWS



Problema

Necesidad de segmentar servicios para para supervisar los costos, controlar el acceso y proporcionar una gestión ambiental más fácil

Solución

Uso de cuentas múltiples proporciona cuentas específicas para los servicios y usuarios dentro de una organización.

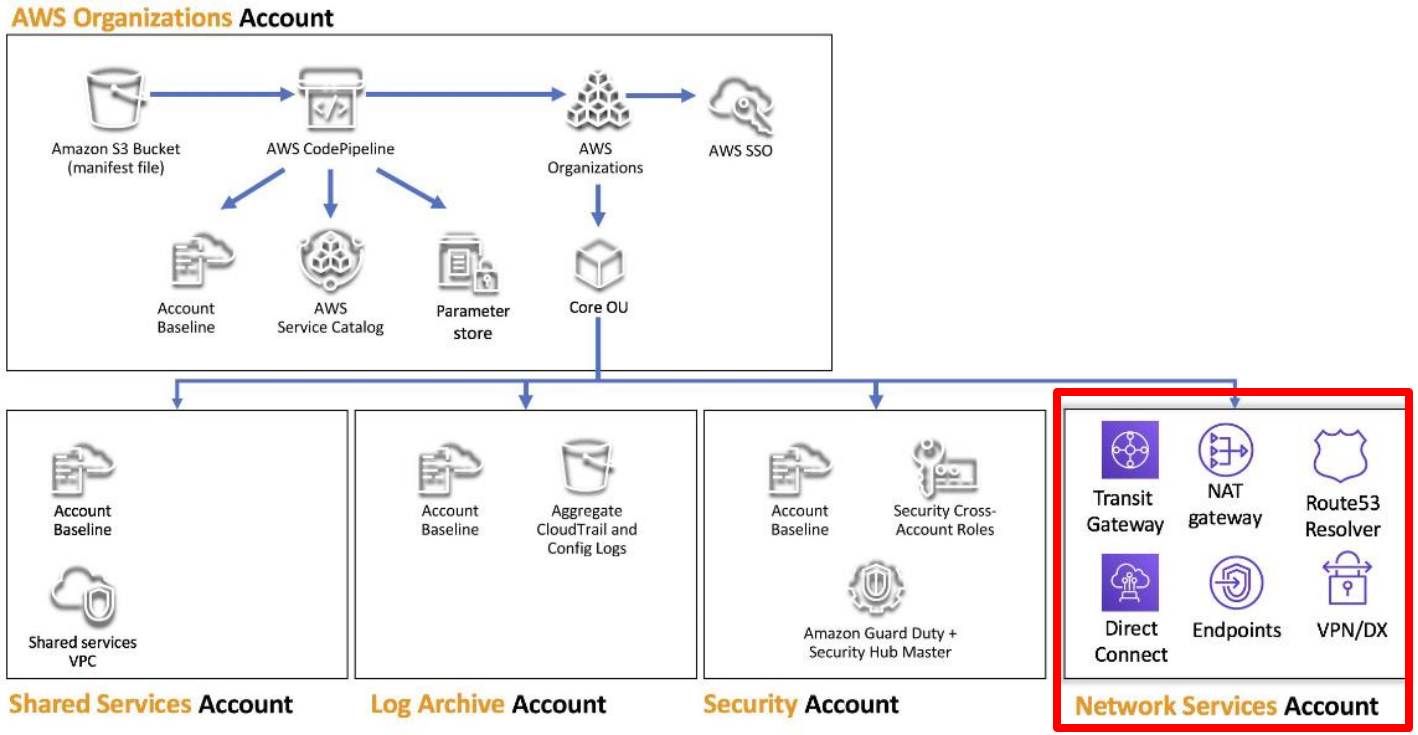
Como hacerlo

AWS proporciona herramientas para gestionar y configurar esta infraestructura, incluyendo **Landing Zone** y **Control Tower**

Multi cuentas en AWS

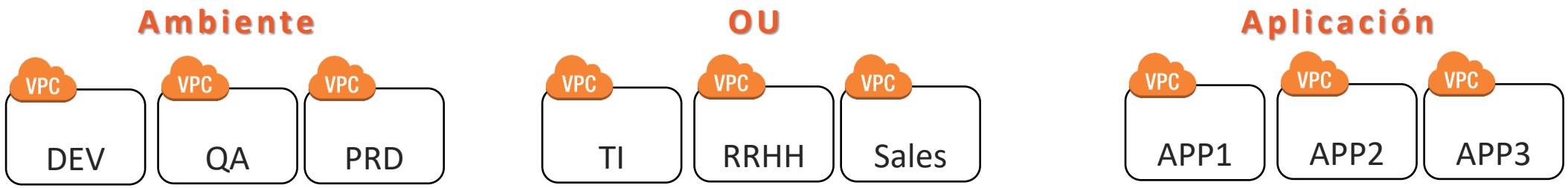
Landing Zone / Control Tower

Automatizar la configuración e integración de los múltiples servicios del AWS para proporcionar un entorno básico, altamente controlado y de múltiples cuentas con gestión de identidades y evaluaciones (IAM), gobernanza, seguridad de los datos, diseño de redes y registro.

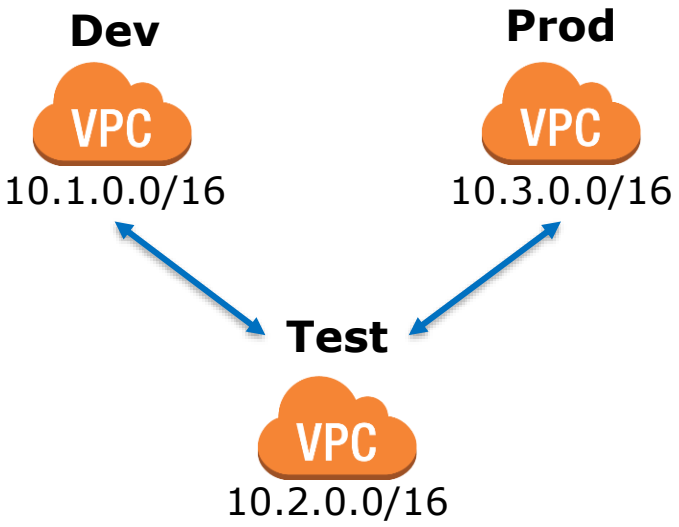


Multi VPC en AWS

- La mayoría de los clientes comienzan con unos pocos VPC para desplegar su infraestructura.
- El número de VPC que un cliente posee está generalmente relacionado con su número de cuentas, usuarios, y entornos escenificados (PRD, DEV, QA).
- A medida que aumenta el uso de la nube, se multiplica el número de usuarios, unidades de negocio, aplicaciones y regiones con las que el cliente interactúa, lo que da lugar a la creación de nuevos VPC.



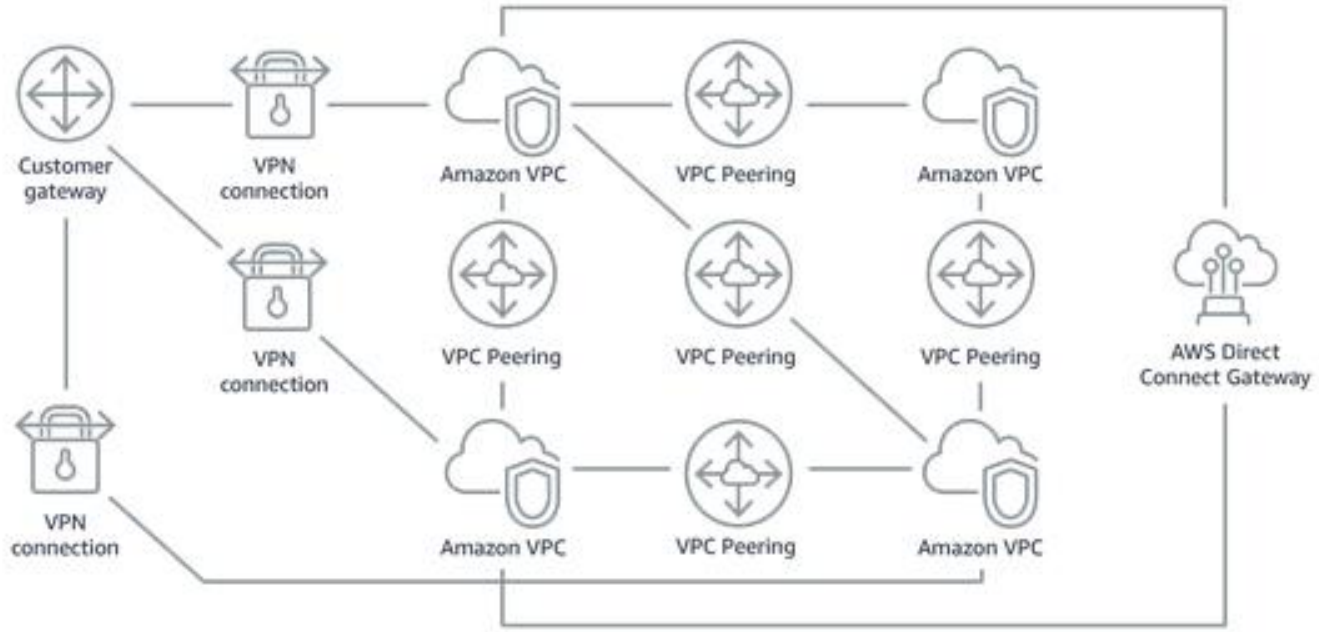
VPC Peering



- Usar direcciones IP privadas
- Soporte intra e inter regiones
- CIDR no deben sobreponerse
- No tiene transitividad
- Puede establecerse entre diferentes cuentas
- Conexiones altamente disponibles
- No hay cuellos de botella en el ancho de banda
- El tráfico siempre se mantiene en el backbone de AWS

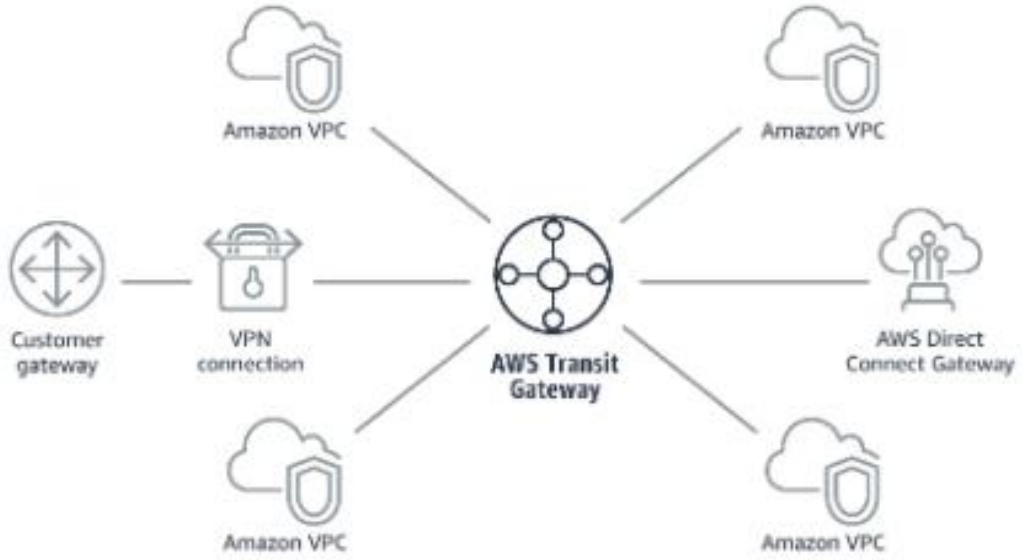
VPC Peering

Complejidad aumenta con la escala. Se debe dar mantenimiento las tablas de enrutamiento de cada VPC.

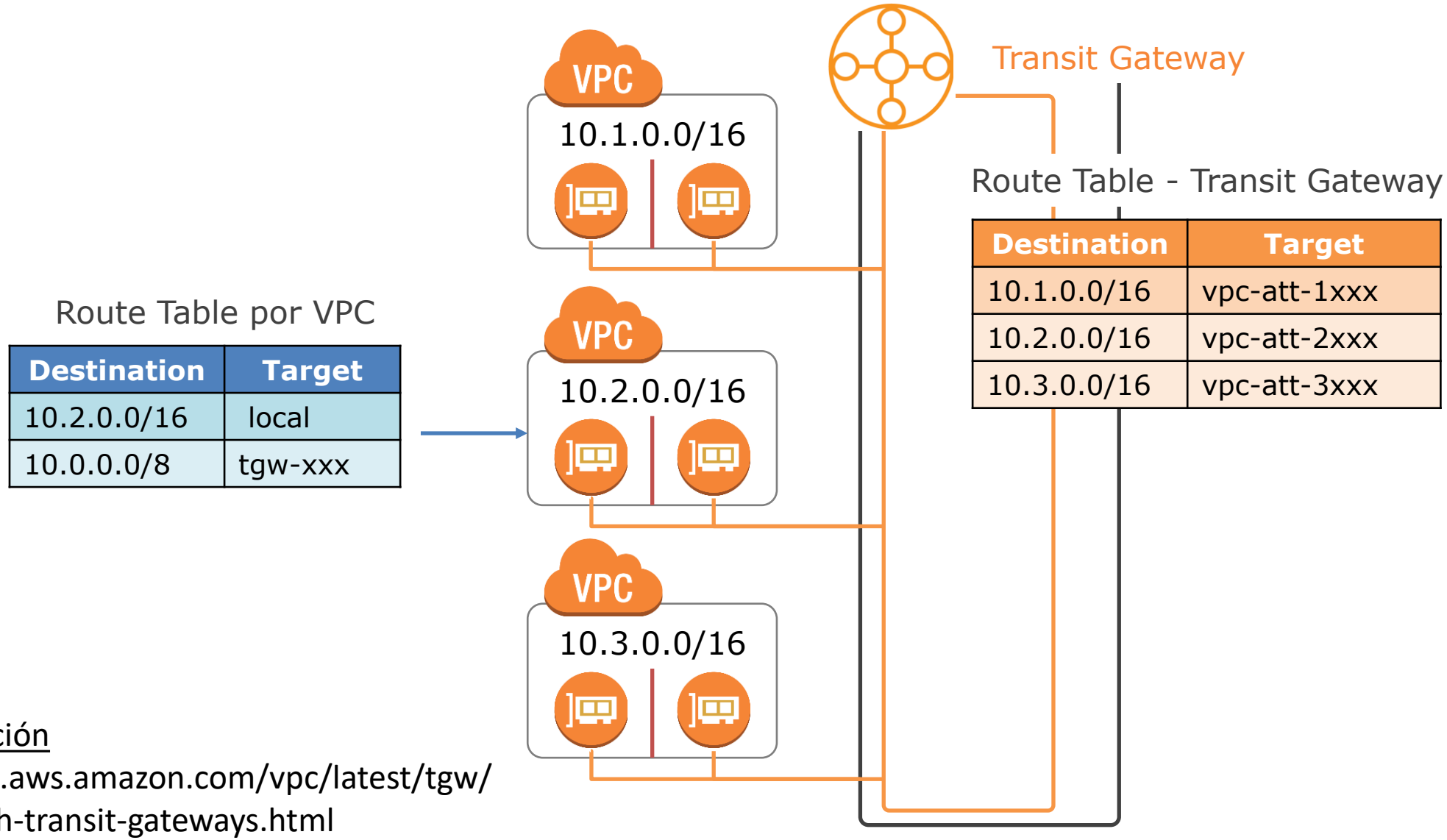


Transit Gateway

- Actúa como hub para que todo el trafico fluya entre las redes simplificando la conectividad
- Servicio de enrutamiento totalmente gestionado, altamente disponible y flexible
- Soporte intra e inter regiones, conexiones VPN y Direct Connect.



Transit Gateway

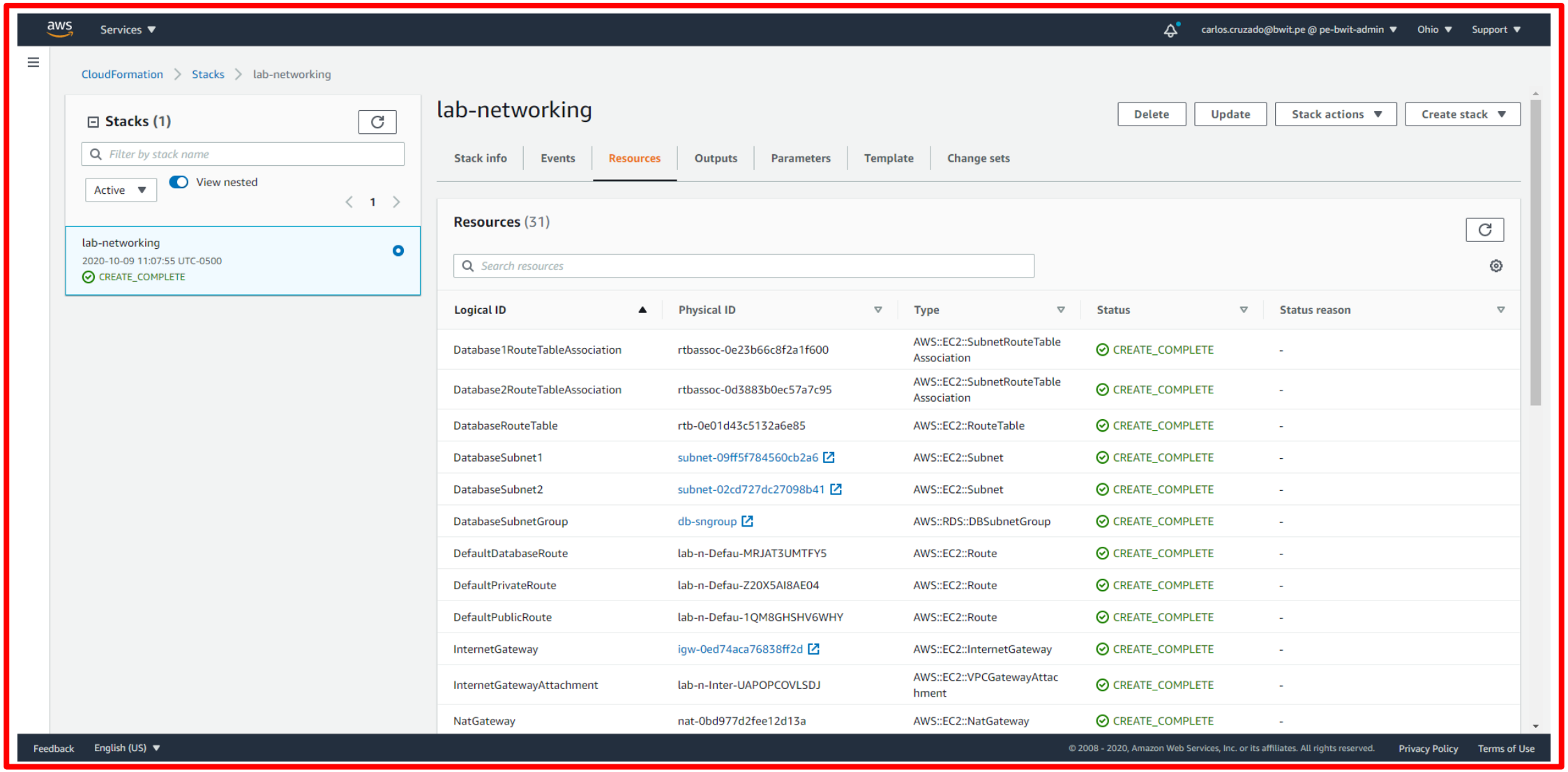


Documentación
https://docs.aws.amazon.com/vpc/latest/tgw/working-with-transit-gateways.html

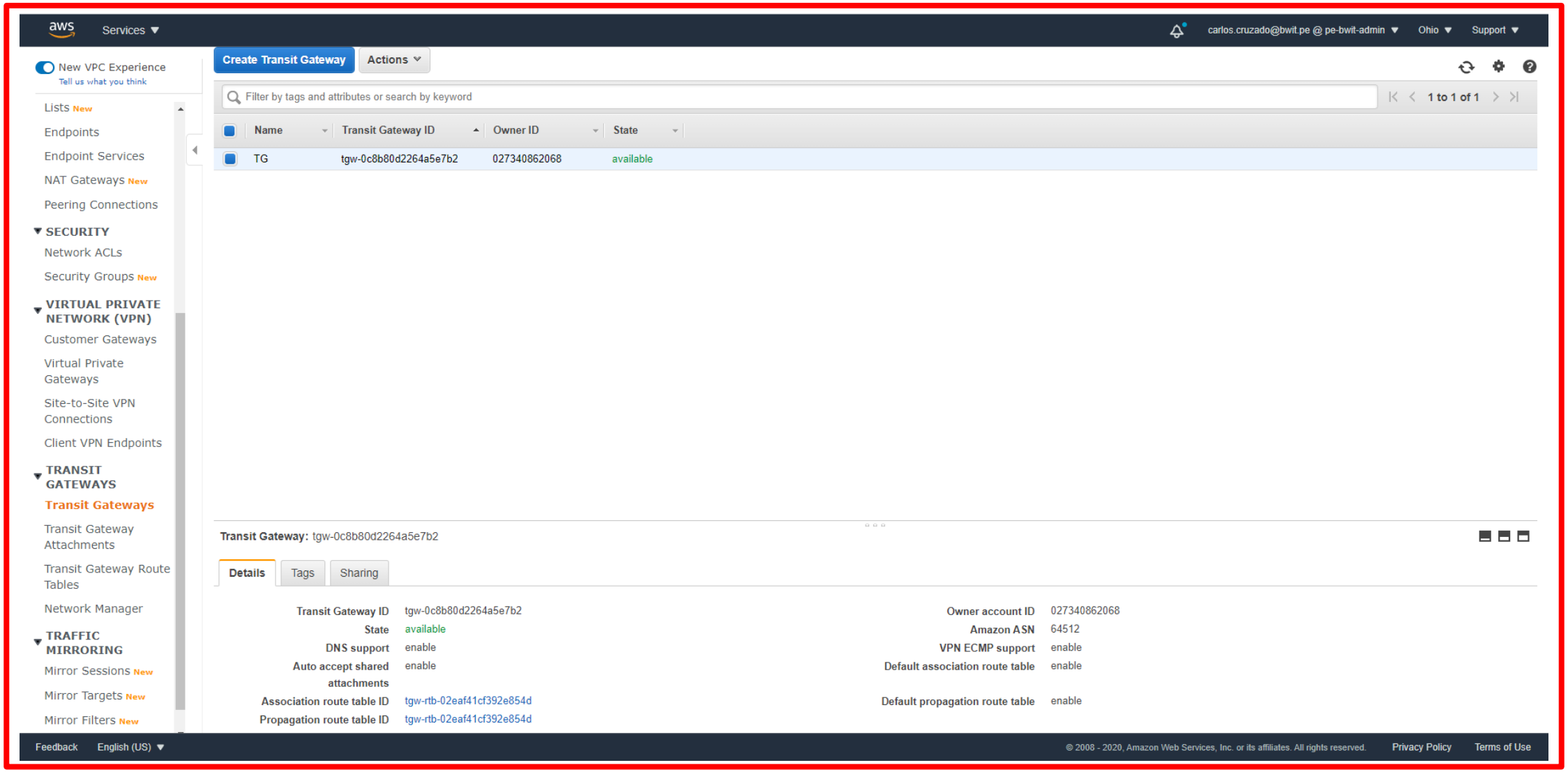
Demo

Creación de Transit Gateway

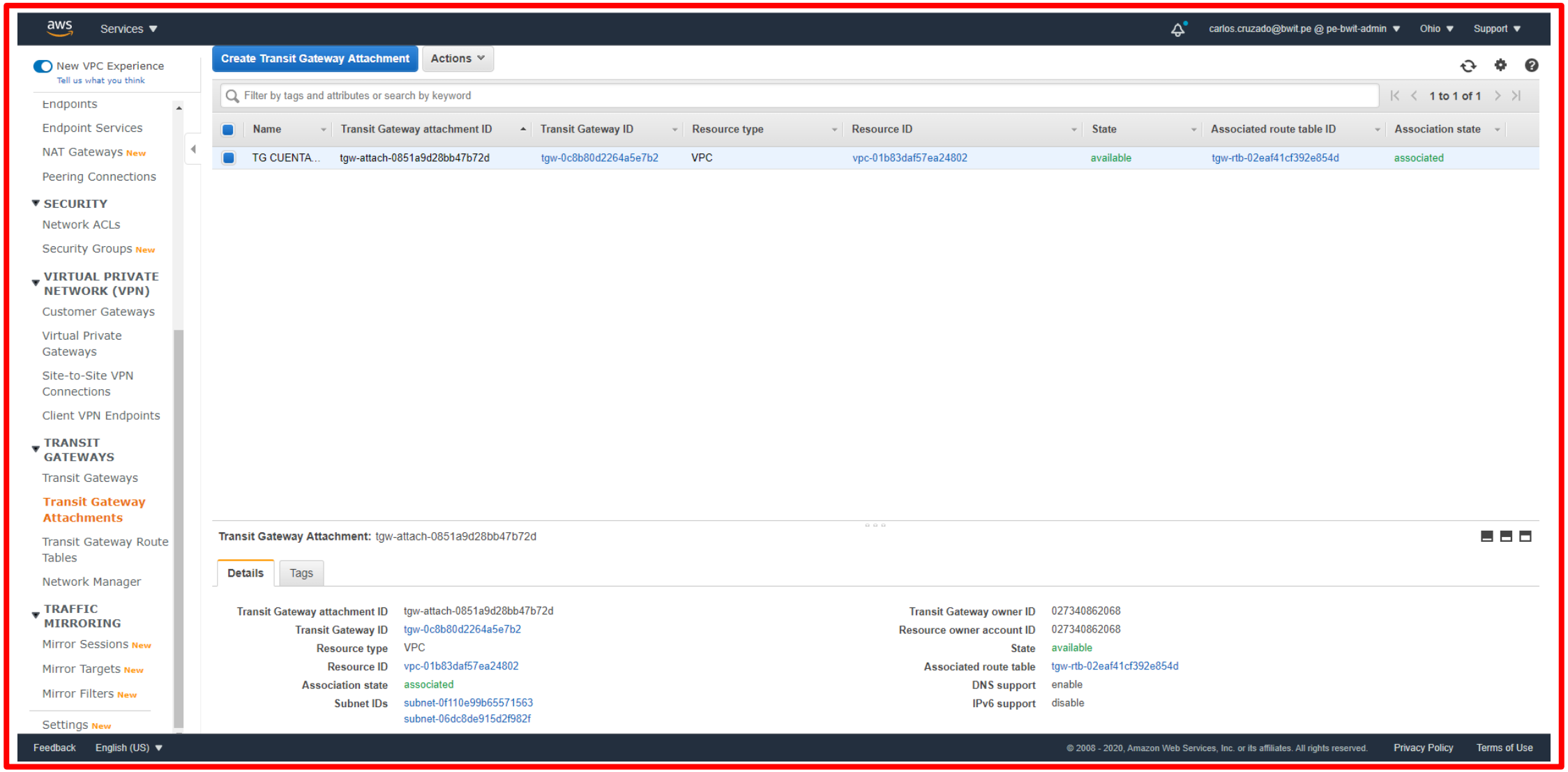
- Creación de VPC en diferentes cuentas
- Creación de Transit Gateway
- Creación de EC2



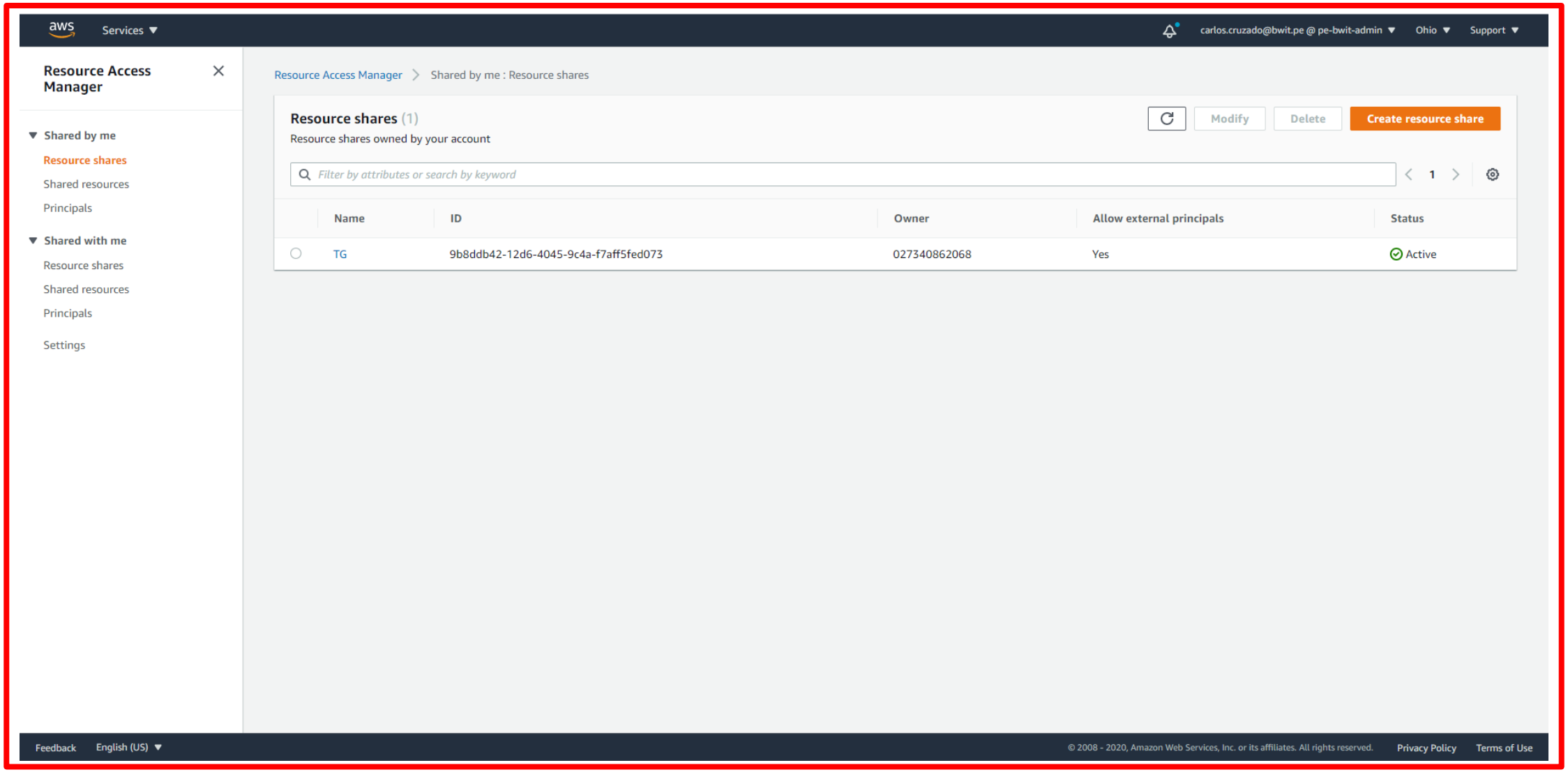
1. Creación de VPC en diferentes cuentas



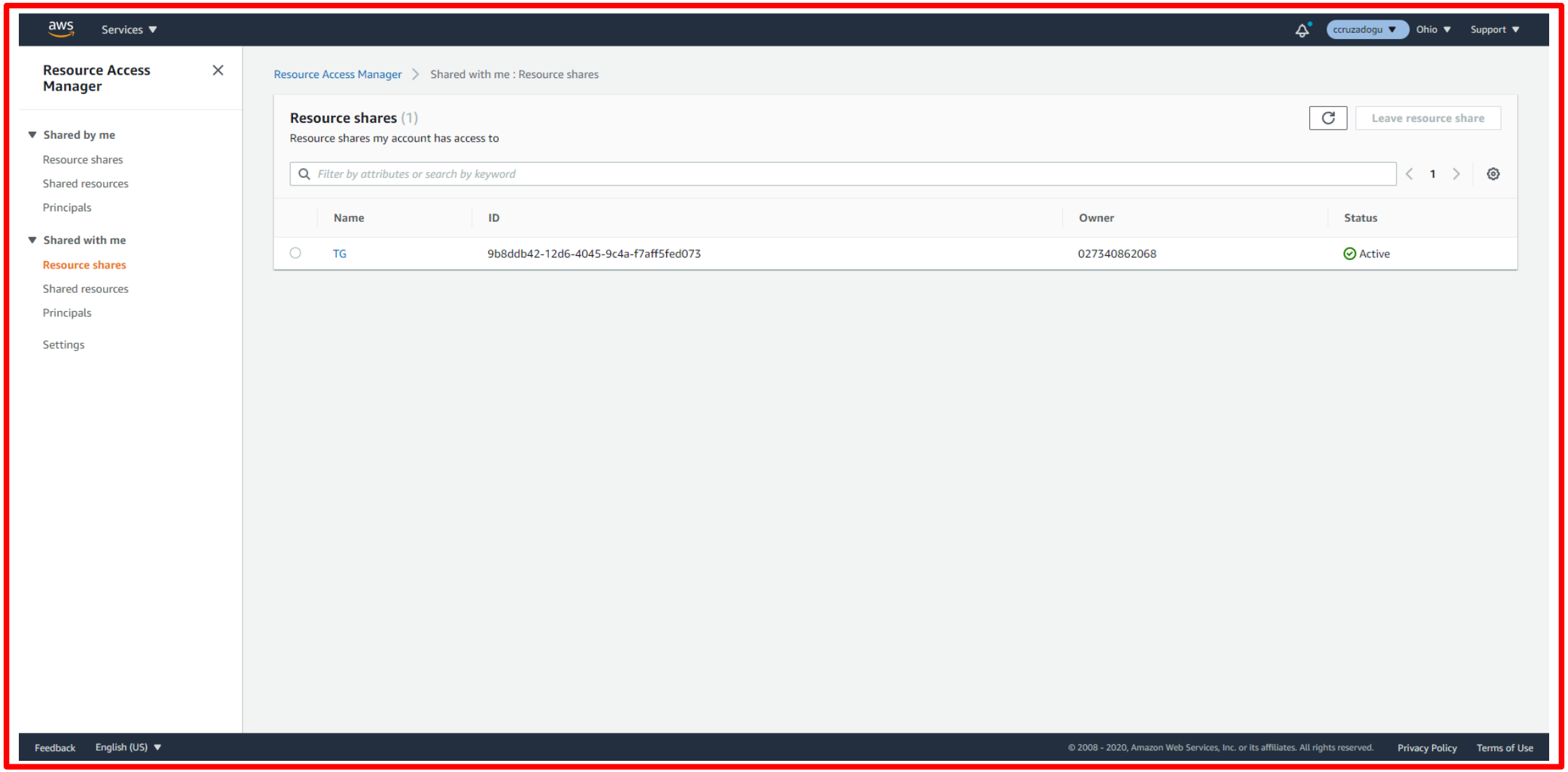
2. Crear Transit Gateway



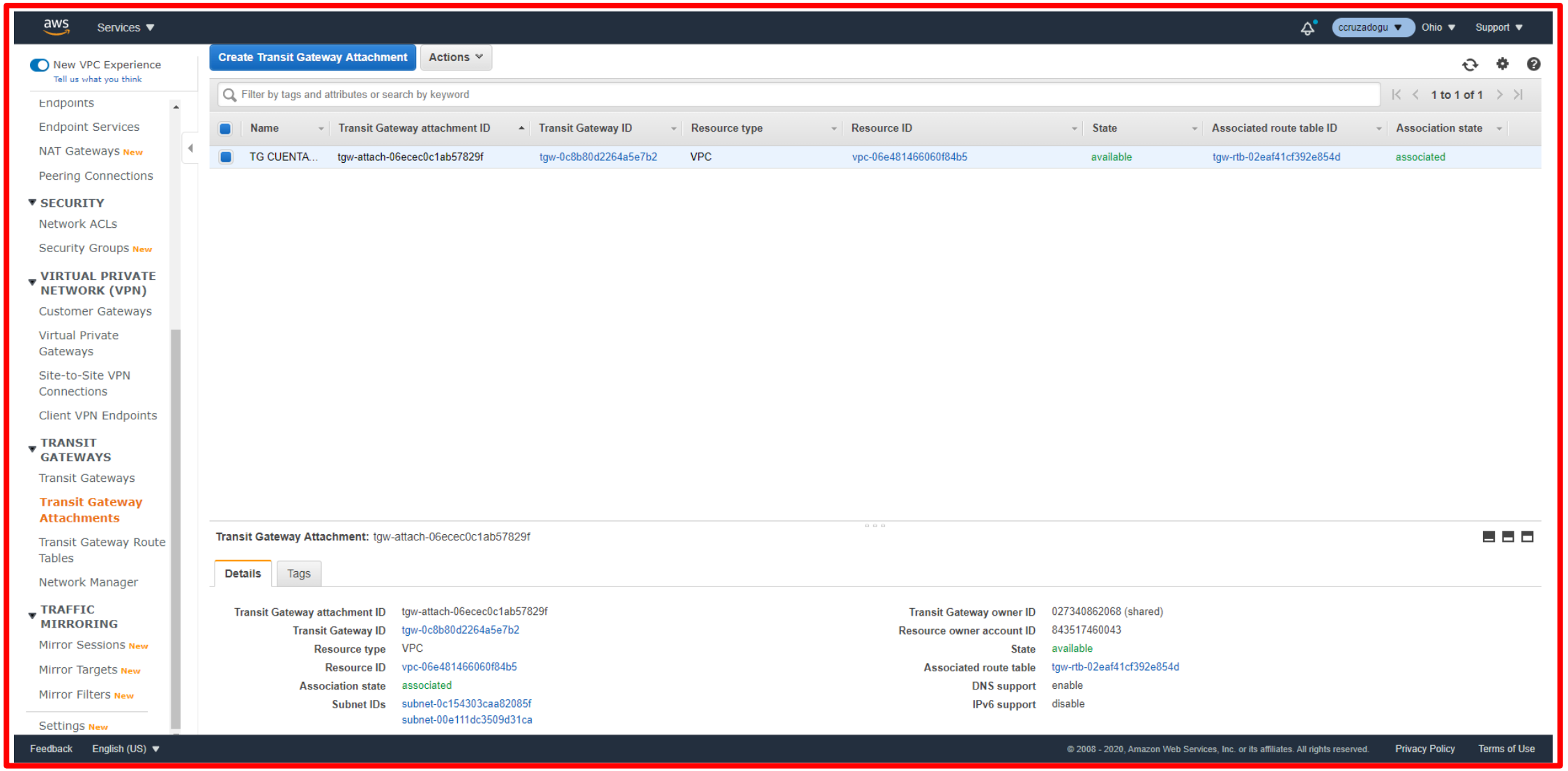
3. Crear Transit Gateway Attachment



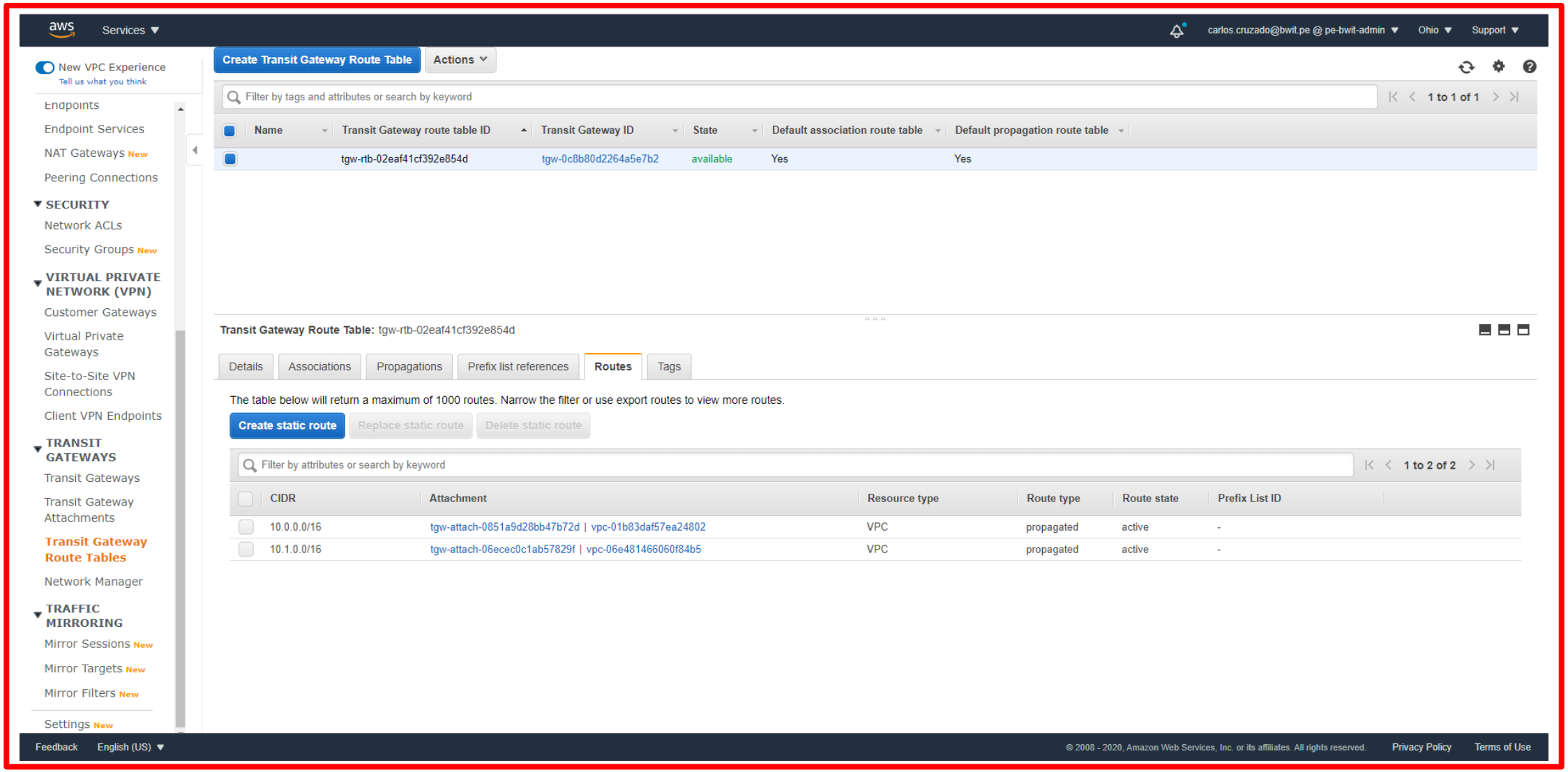
4. Compartir Transit Gateway con Resource Access Manager (RAM)



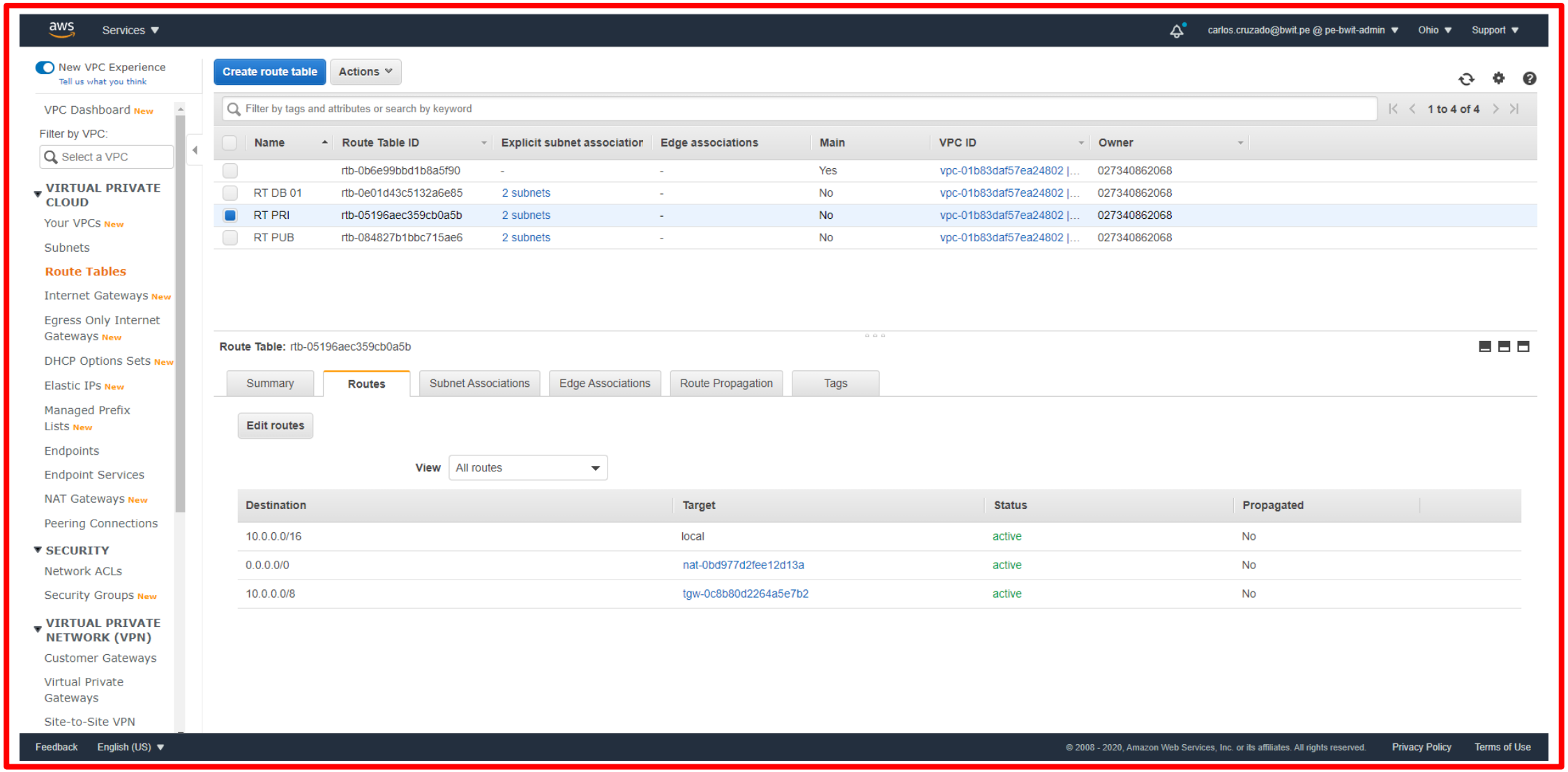
5. Aceptar el recurso de Transit Gateway en la otra cuenta



6. Crear Transit Gateway Attachment en cuenta adicional



7. Verificar el Transit Gateway Route Table



8. Modificar Route Table para comunicarse entre VPC a través de Transit Gateway

Preguntas?