Arquitecturas de nube con AWS

Ing. Fernando Lichtschein
Ing. Mora Villa Abrille

8. Conexión entre redes

UNIVERSIDAD AUSTRAL

Objetivos

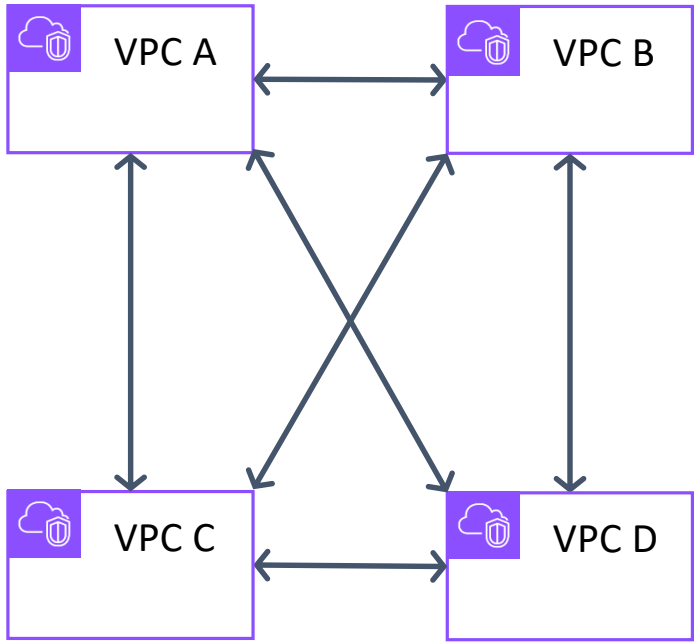
- Describir cómo se conecta una red *on-premises* con los servicios de AWS
- Explicar cómo se conectan múltiples VPC entre sí
- Conectar VPC mediante *peering*
- Describir cómo se pueden escalar VPC en la nube de AWS
- Aplicar los principios del Well-Architected Framework

Principios de arquitectura

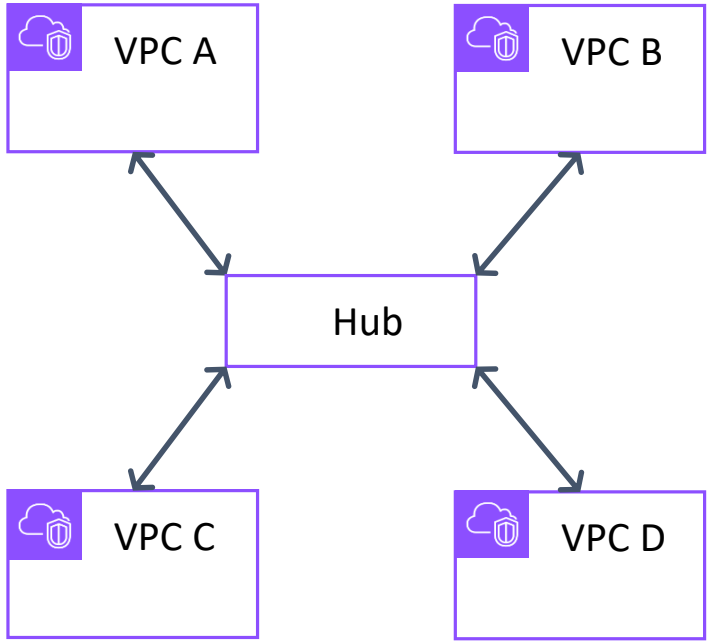
- Diseñar las conexiones aplicando medidas para la continuidad y asegurando un ancho de banda adecuado, para las aplicaciones *on-premises*, en la nube o hibridas.
- Seleccionar componentes de red que optimicen la *performance* y reduzcan los costos de transferencia de datos entre redes, para maximizar el valor.
- Proteger los datos en tránsito entre redes

Diseño de red con múltiples VPC

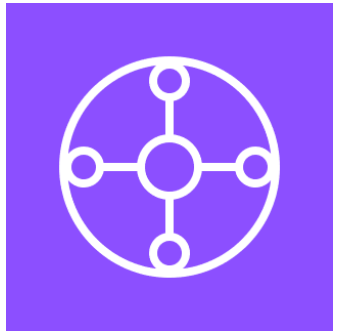
Arquitectura Full mesh



Arquitectura Hub-and-spoke



AWS Transit Gateway



- Es un *router* centralizado, regional para conectar VPCs y redes *on-premises* sobre la base de una arquitectura *hub-and-spoke*
- Es un servicio administrado por AWS que escala automáticamente en base al volumen del tráfico de red.
- Se puede conectar con otros Transit Gateways en otras regiones o cuentas de AWS.
- El costo depende de la cantidad de conexiones y de la cantidad de tráfico
- Tiene una función que publica logs: Transit Gateway Flow Logs

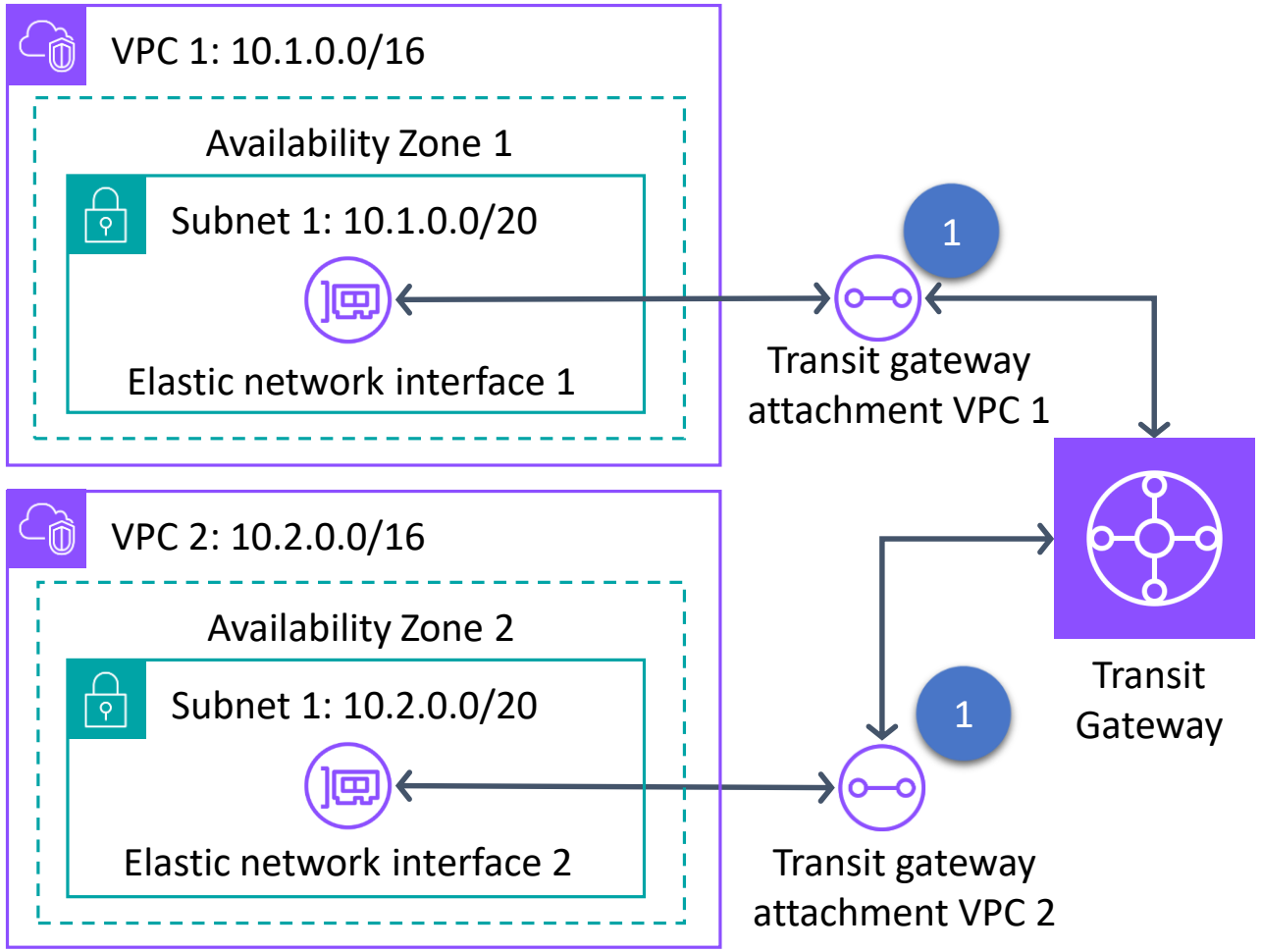
Ruteo con Transit Gateway entre VPCs

VPC 1 route table	
Destination	Target
10.1.0.0/16	local
10.0.0.0/8	Transit gateway ID

2

VPC 2 route table	
Destination	Target
10.2.0.0/16	local
10.0.0.0/8	Transit gateway ID

2



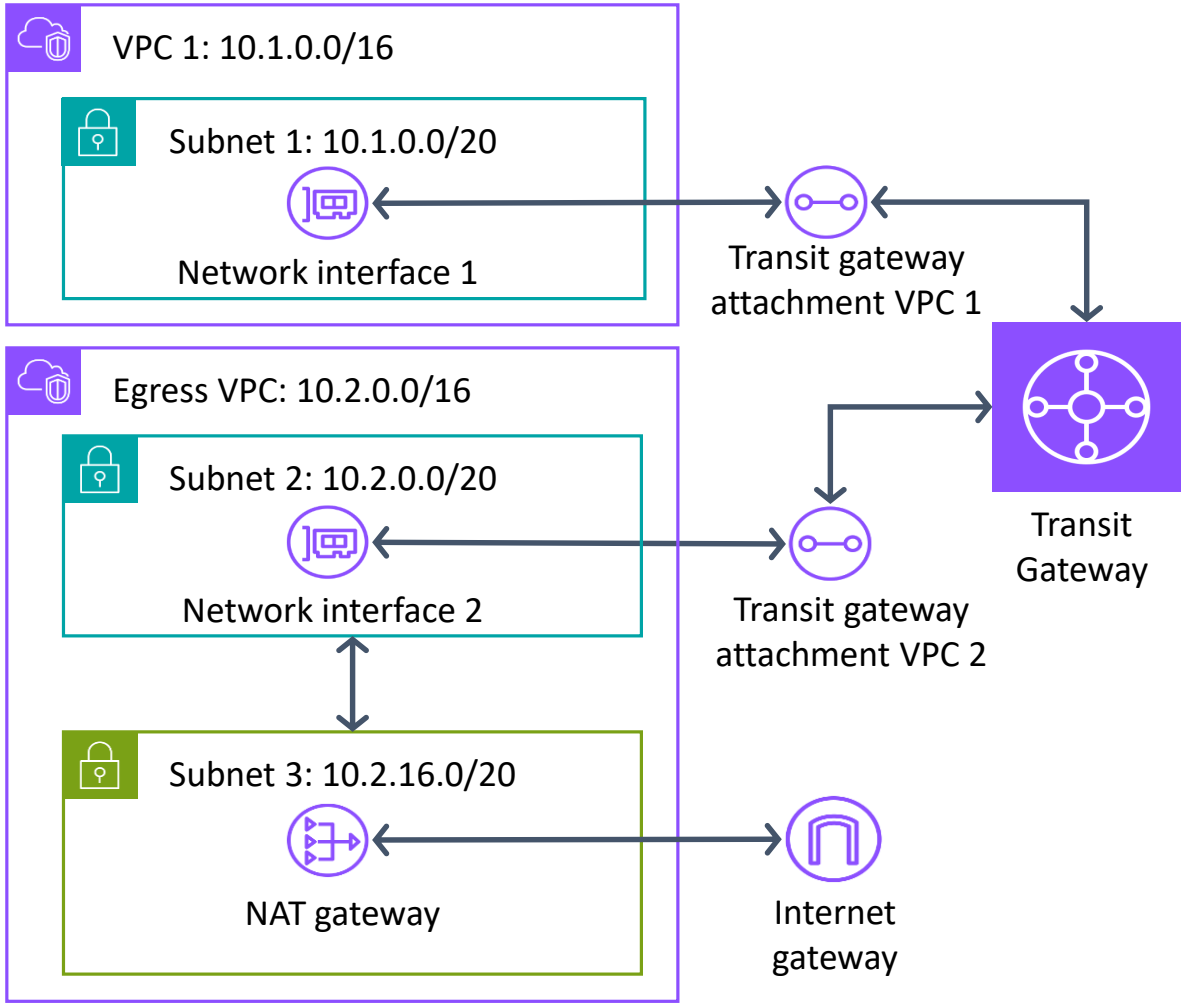
3

Transit gateway route table	
Destination	Target
10.1.0.0/16	Transit gateway attachment VPC 1 ID
10.2.0.0/16	Transit gateway attachment VPC 2 ID

Tráfico saliente entre VPC

VPC 1 route table	
Destination	Target
10.1.0.0/16	local
0.0.0.0/0	Transit gateway ID

Subnet 2 route table	
Destination	Target
10.1.0.0/16	local
0.0.0.0/0	NAT gateway ID

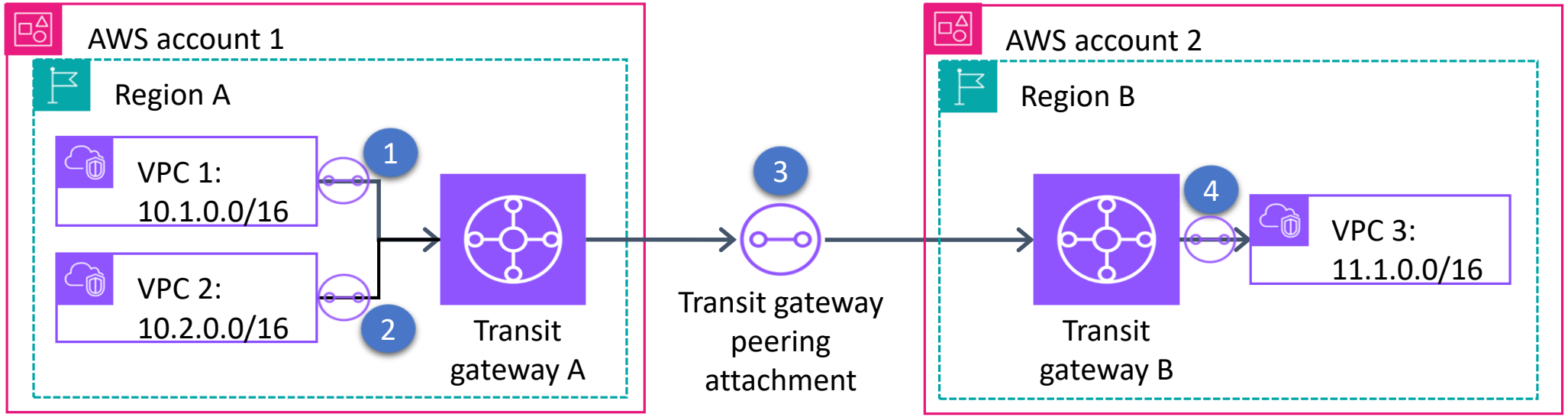


Transit gateway route table	
Destination	Target
10.1.0.0/16	Transit gateway attachment VPC 1 ID
10.2.0.0/16	Transit gateway attachment VPC 2 ID

Egress VPC route table	
Destination	Target
10.2.0.0/16	local
10.1.0.0/16	Transit gateway ID
0.0.0.0/0	Internet gateway ID

Conexión de dos Transit Gateways

Peering



Transit gateway A route table	
Destination	Target
10.1.0.0/16	Transit gateway attachment VPC 1 ID 1
10.2.0.0/16	Transit gateway attachment VPC 2 ID 2
11.1.0.0/16	Transit gateway peering attachment ID 3

Transit gateway B route table	
Destination	Target
11.1.0.0/16	Transit gateway attachment VPC 3 ID 4
10.1.0.0/16	Transit gateway peering attachment ID 3
10.2.0.0/16	Transit gateway peering attachment ID 3

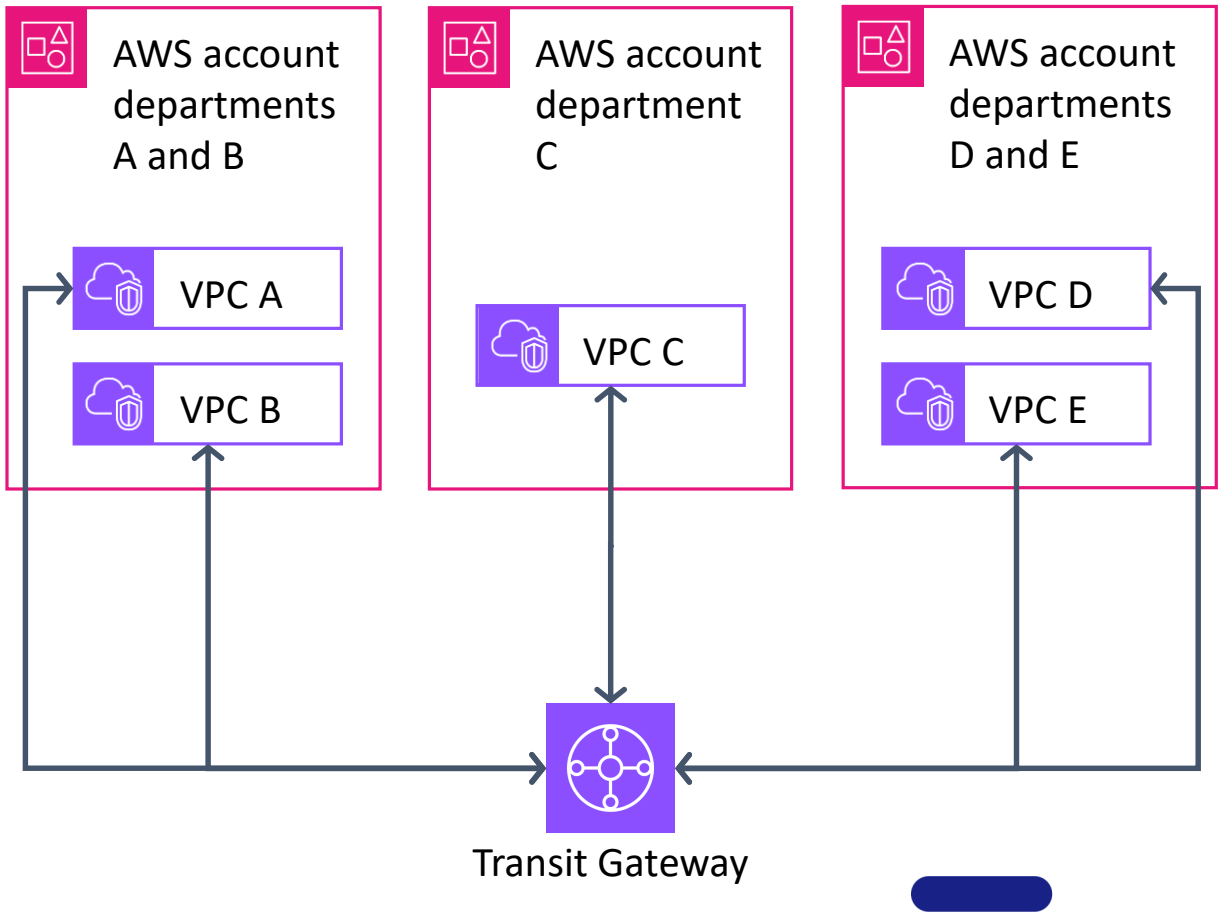
Caso de uso

Escenario:

Una compañía tiene múltiples departamentos de IT, cada uno posee su propia VPC.

Algunas VPC están dentro de la misma cuenta de AWS, y otras están en cuentas distintas.

Queremos conectar todas las VPC para que tengan acceso a los recursos de las demás. La compañía está evaluando la posibilidad de agregar nuevas cuentas en el futuro.



Actividad

Configurar tablas de rutas de la VPC

UNIVERSIDAD AUSTRAL

Actividad

Consigna

¿Qué rutas debemos agregar a las tablas de rutas de las VPC si queremos que las cinco estén totalmente conectadas?

VPC ID	VPC CIDR	Transit gateway VPC attachment ID	VPC route table ID	VPC route table destination	VPC route table target
vpc-a	10.1.0.0/16	tgw-attach-vpc-a	rtb-vpc-a	?	?
vpc-b	10.2.0.0/16	tgw-attach-vpc-b	rtb-vpc-a	?	?
vpc-c	10.3.0.0/16	tgw-attach-vpc-c	rtb-vpc-a	?	?
vpc-d	10.4.0.0/16	tgw-attach-vpc-d	rtb-vpc-a	?	?
vpc-e	10.5.0.0/16	tgw-attach-vpc-e	rtb-vpc-a	?	?

Actividad

Consigna

2. Configurar la tabla de rutas tgw-1 del Transit Gateway.

Transit gateway route table destination	Transit gateway route table target
?	?
?	?
?	?
?	?
?	?

Actividad

Solución parte 1

VPC ID	VPC CIDR	Transit gateway VPC attachment ID	VPC route table ID	VPC route table destination	VPC route table target
vpc-a	10.1.0.0/16	tgw-attach-vpc-a	rtb-vpc-a	10.0.0.0/8	tgw-1
vpc-b	10.2.0.0/16	tgw-attach-vpc-b	rtb-vpc-a	10.0.0.0/8	tgw-1
vpc-c	10.3.0.0/16	tgw-attach-vpc-c	rtb-vpc-a	10.0.0.0/8	tgw-1
vpc-d	10.4.0.0/16	tgw-attach-vpc-d	rtb-vpc-a	10.0.0.0/8	tgw-1
vpc-e	10.5.0.0/16	tgw-attach-vpc-e	rtb-vpc-a	10.0.0.0/8	tgw-1

Actividad

Solución parte 2

Transit gateway route table destination	Transit gateway route table target
10.1.0.0/16	tgw-attach-vpc-a
10.2.0.0/16	tgw-attach-vpc-b
10.3.0.0/16	tgw-attach-vpc-c
10.4.0.0/16	tgw-attach-vpc-d
10.5.0.0/16	tgw-attach-vpc-e

Resumen

Un Transit Gateway es un router centralizado regional que conecta VPCs.

Los Transit Gateways de distintas regiones o cuentas se pueden conectar entre sí

Un Transit Gateway soporta miles de conexiones.

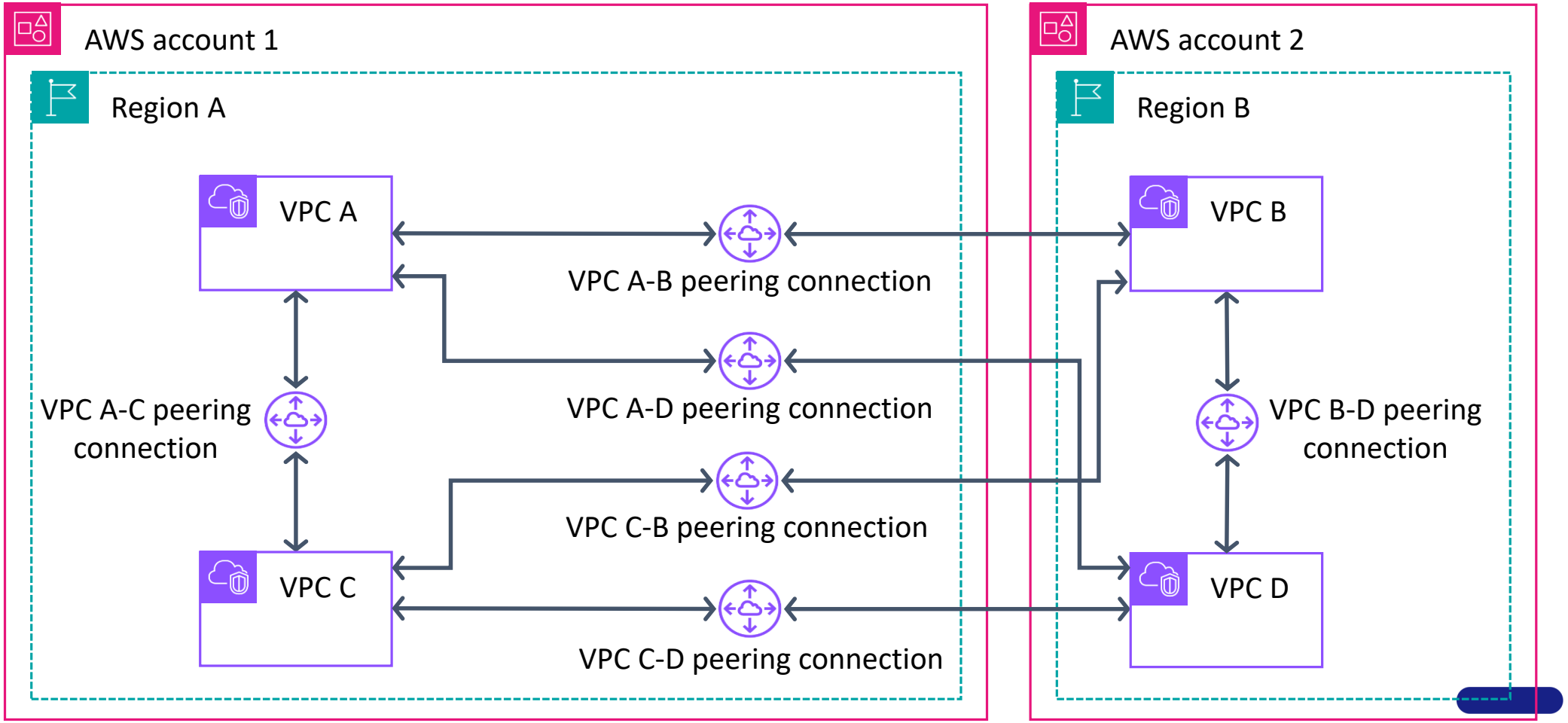
Transit Gateway tiene costo por hora, que depende de:

- El número de conexiones
- La cantidad de tráfico

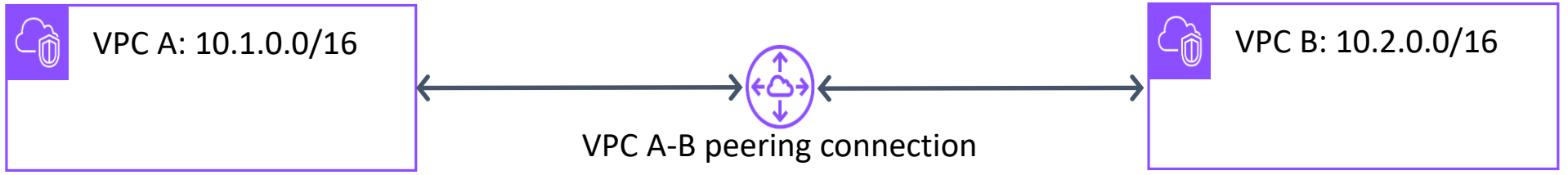
VPC peering

UNIVERSIDAD AUSTRAL

Arquitecturas *mesh* con VPC Peering



¿Cómo establecer una conexión?

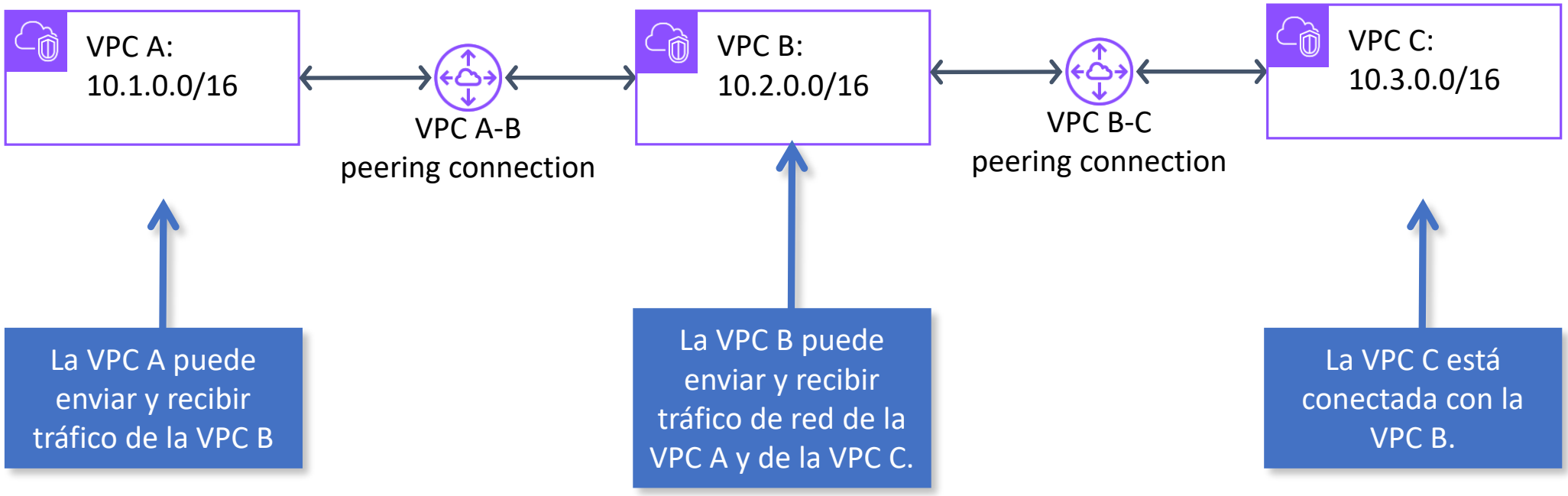


VPC A route table	
Destination	Target
10.1.0.0/16	local
10.2.0.0/16	VPC A-B peering connection ID

VPC B route table	
Destination	Target
10.2.0.0/16	local
10.1.0.0/16	VPC A-B peering connection ID

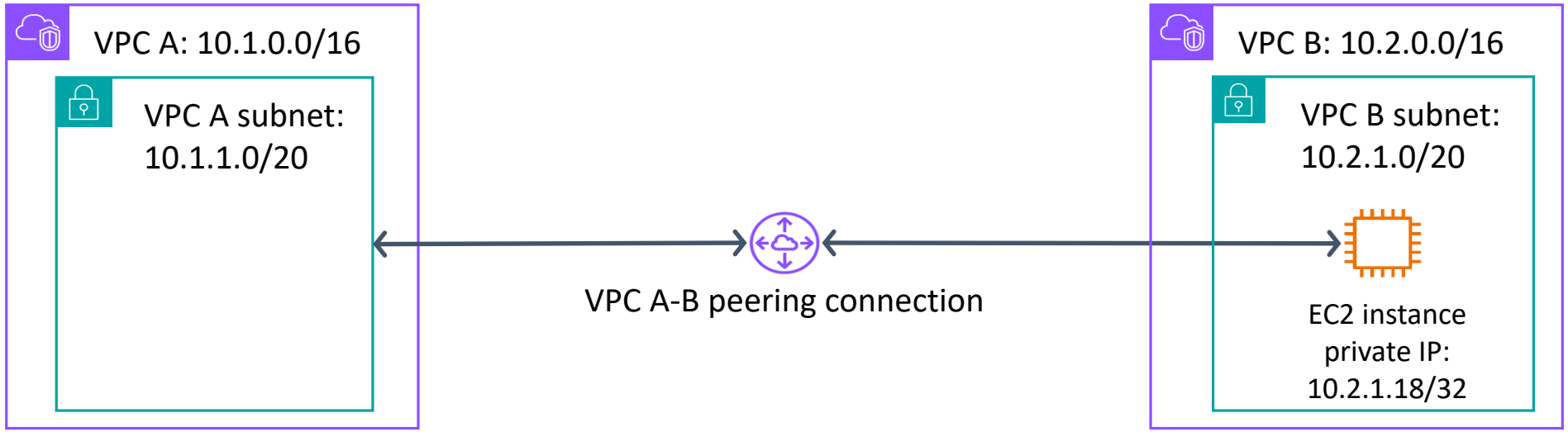
VPC peering connections

No son transitivas



VPC peering connections

Uso de rutas específicas

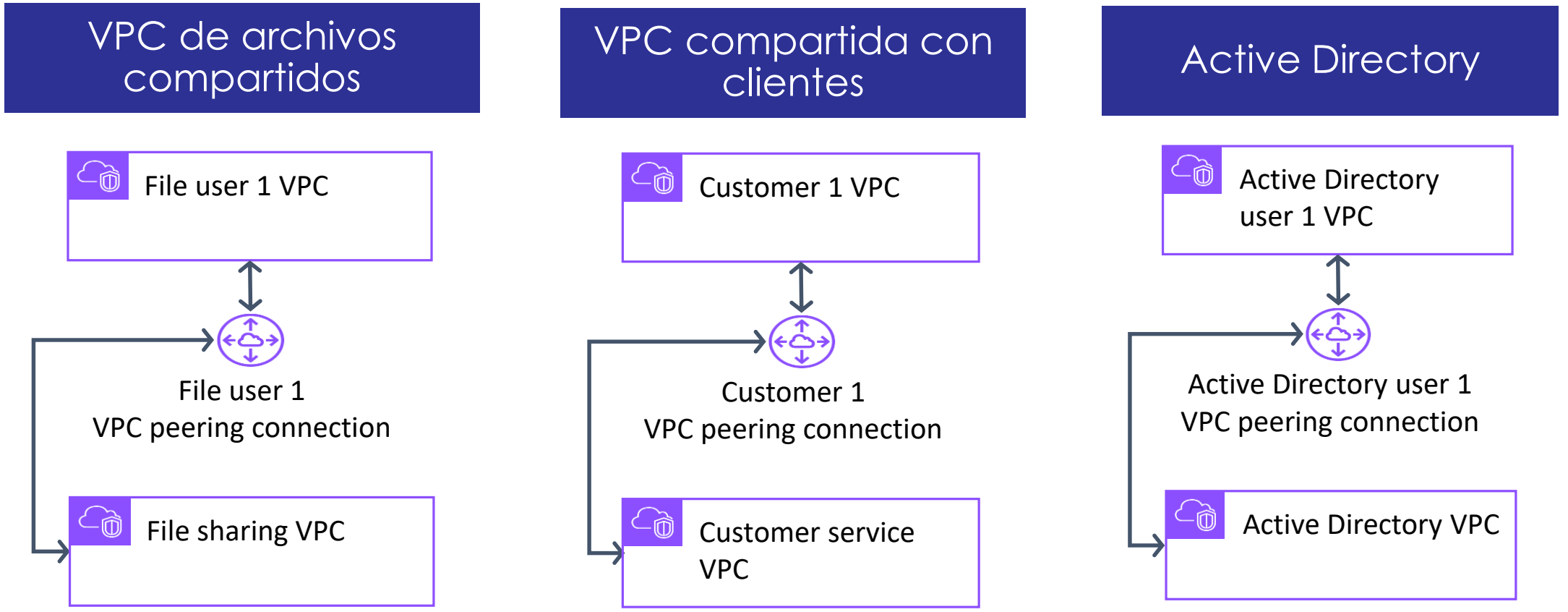


VPC A subnet route table	
Destination	Target
10.1.0.0/16	local
10.2.1.18/32	VPC A-B peering connection ID

VPC B subnet route table	
Destination	Target
10.2.0.0/16	local
10.1.1.0/20	VPC A-B peering connection ID

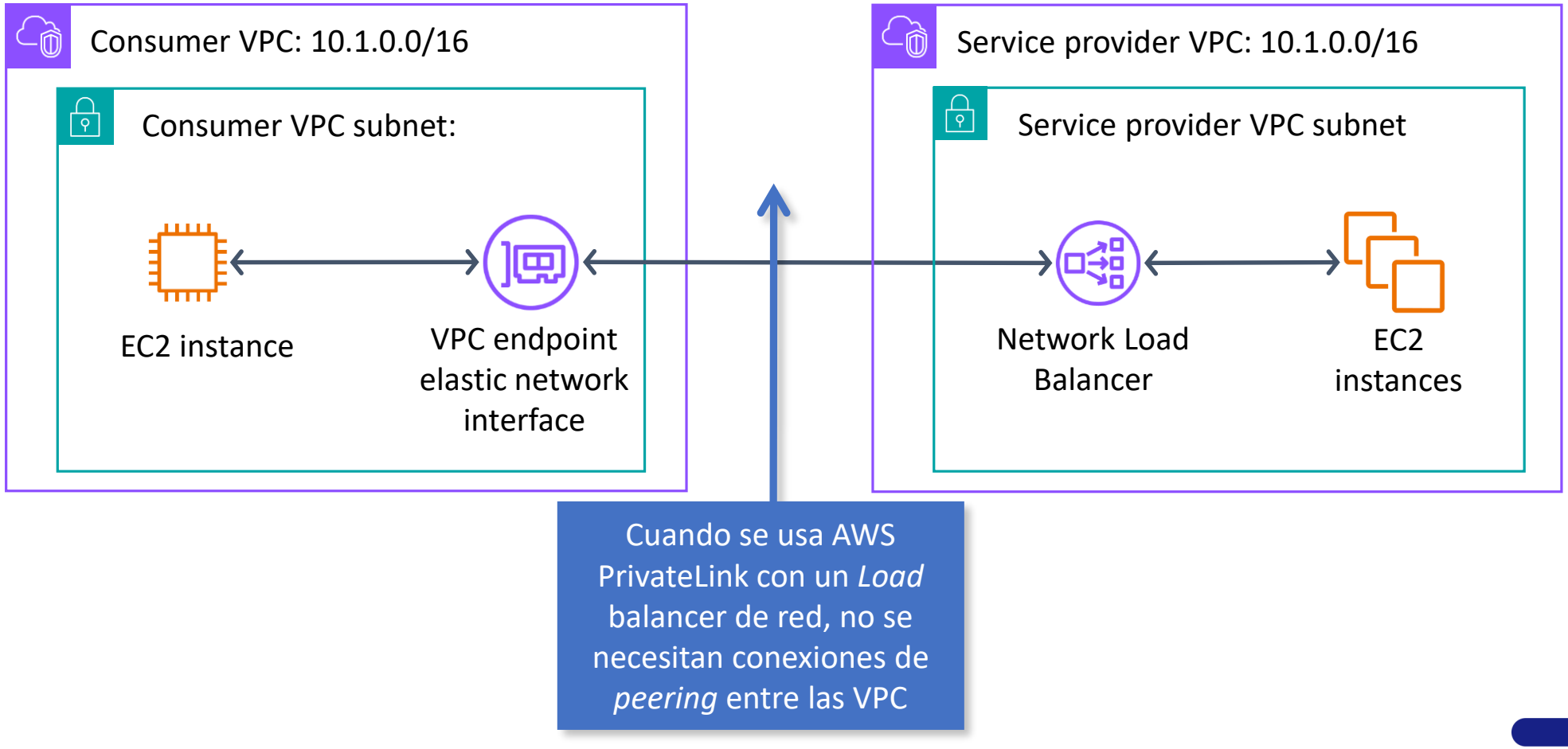
Caso de uso

Conexión a una VPC para acceder a recursos centralizados



Conexión de VPC con AWS Private Link

Arquitectura



Resumen

- VPC *peering* establece una conexión de red uno-a-uno entre dos VPC para brindar rutas de tráfico de red privadas.
- No tiene costo, pero sí existen cargos por transferir datos entre AZ o entre regiones.
- Permite el tráfico de red entre cuentas y regiones diferentes de AWS.
- No admite relaciones transitivas entre VPC.
- Si los bloques de Classless Inter-Domain Routing (CIDR) de las VPC se superponen, hay que usar PrivateLink con un Network Load Balancer para establecer la conexión

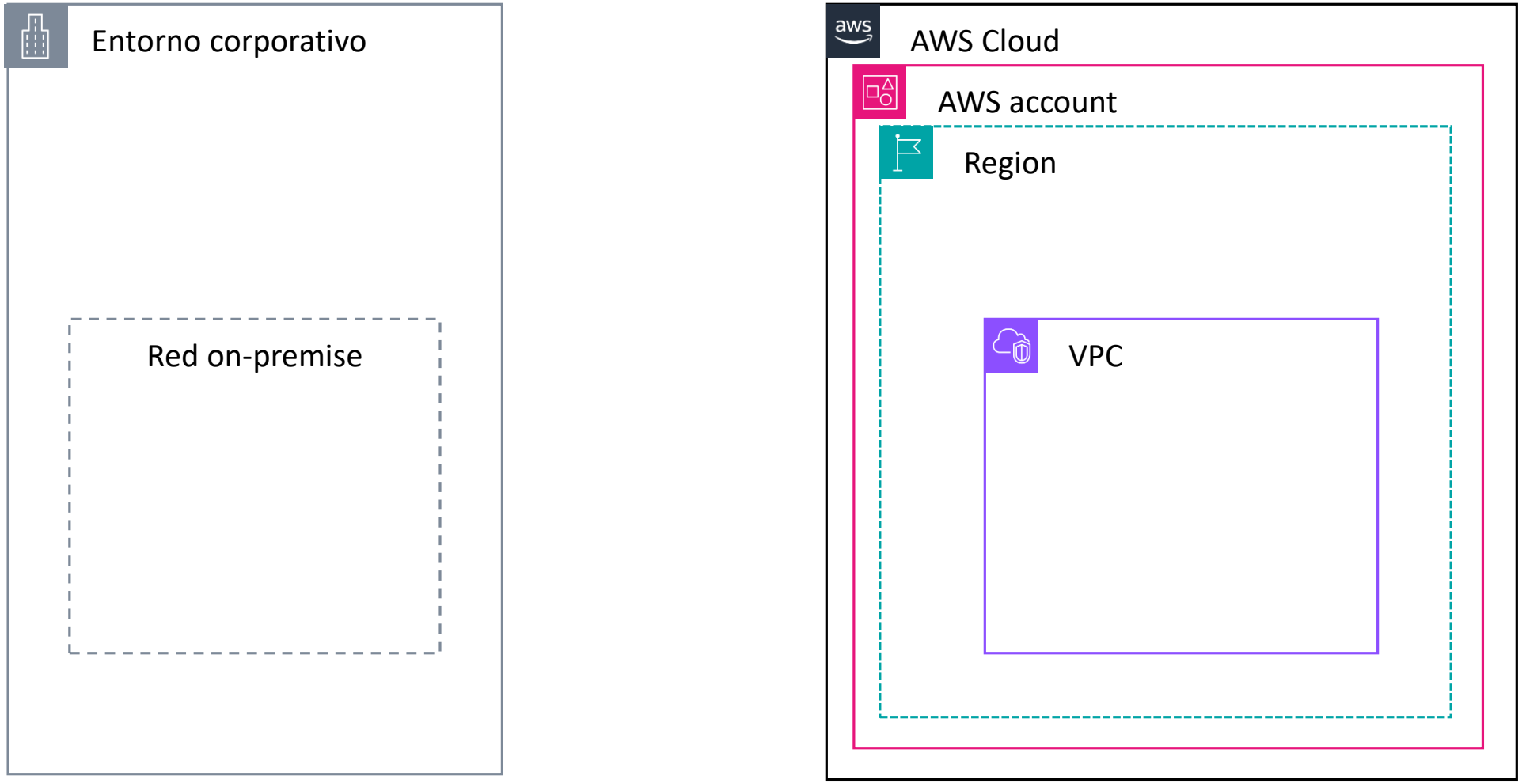
Conexión de redes remotas

Site-to-site VPN

UNIVERSIDAD AUSTRAL

Conexión de instalaciones on-premise

A una VPC



Conexión de servicios gestionados

Resumen

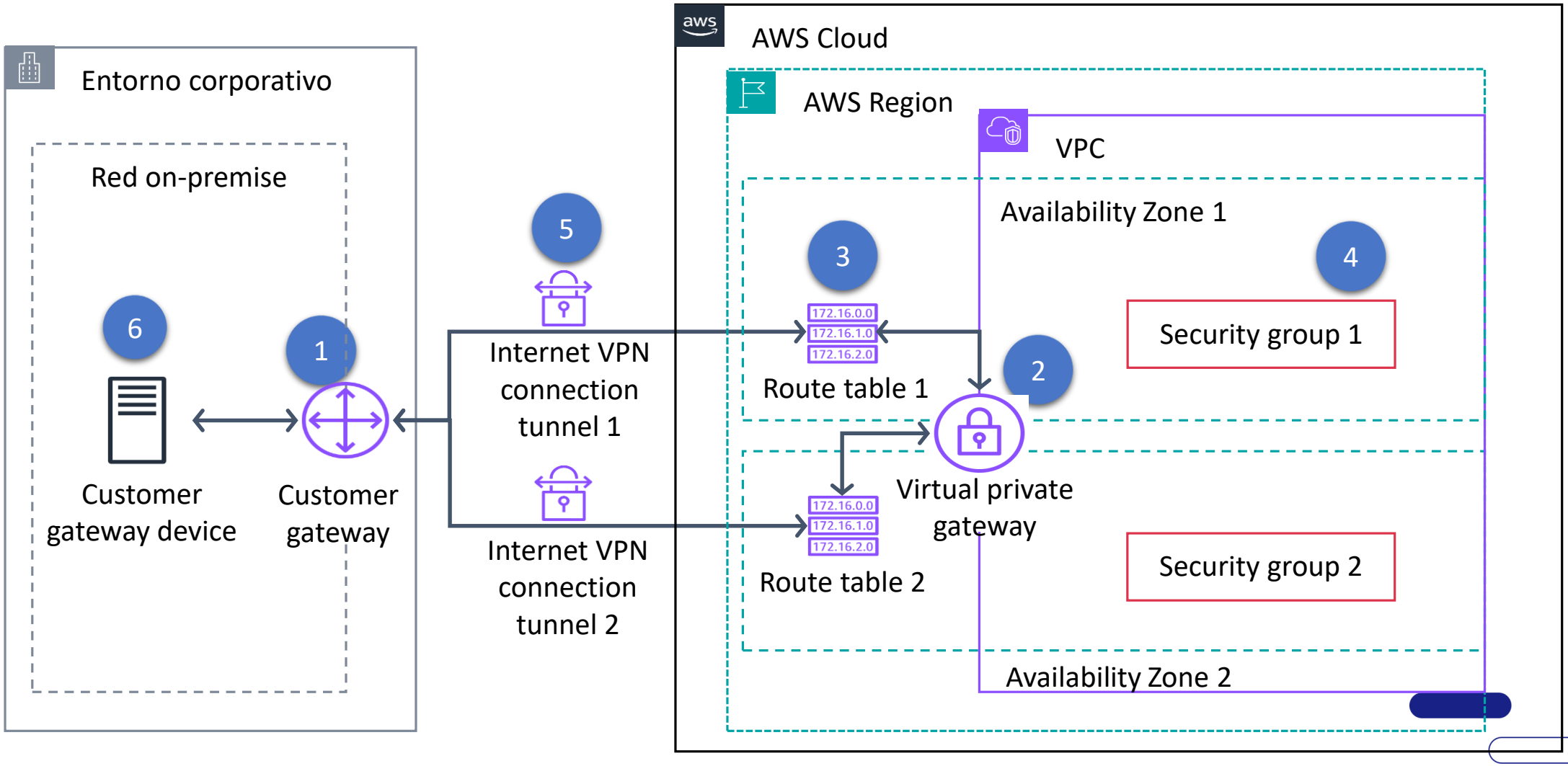
Site-to-Site VPN

Crea una conexión segura entre un *Gateway* en las instalaciones del cliente con un *Gateway* privado virtual de AWS o un Transit Gateway.

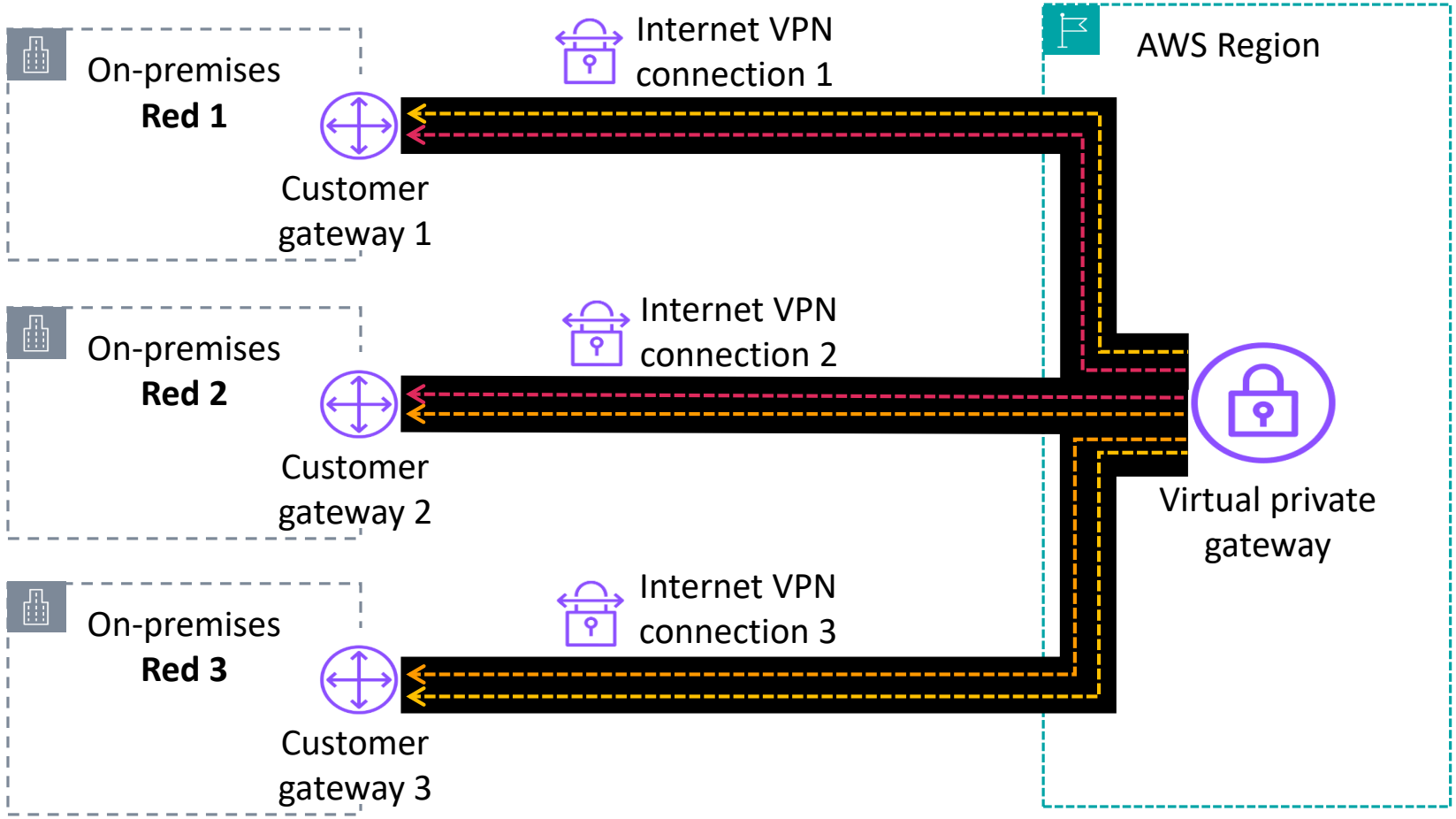
Crea dos túneles IPsec para cada conexión a través de múltiples AZ.

Hay costo por cada hora de conexión de VPN

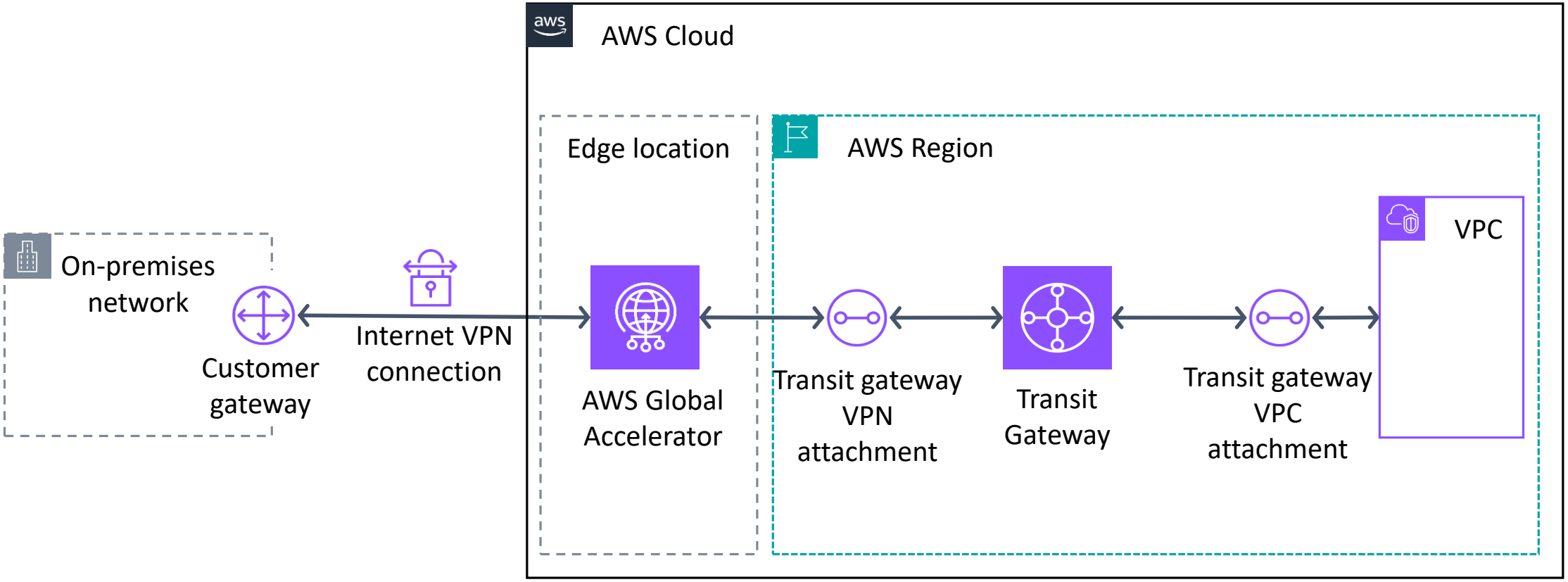
Conexión VPN site-to-site



AWS VPN CloudHub



AWS Global Accelerator

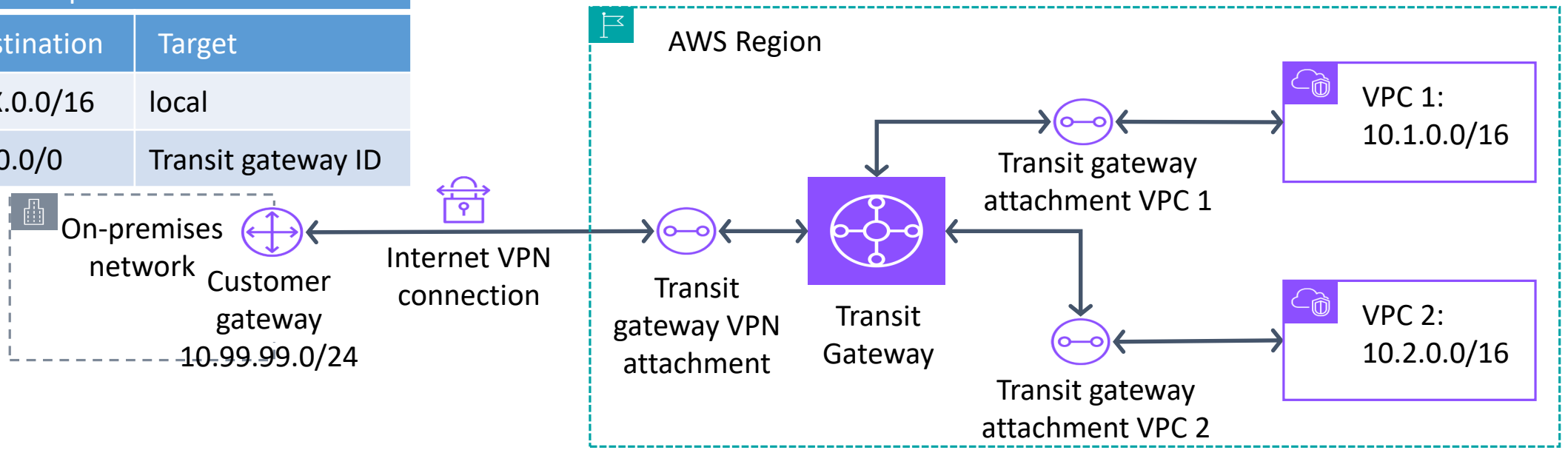


https://speedtest.globalaccelerator.aws/#/

Aislar VPC con acceso por VPN

Transit Gateway

On-premises route table	
Destination	Target
10.X.0.0/16	local
0.0.0.0/0	Transit gateway ID



Transit gateway VPN route table	
Destination	Target
10.1.0.0/16	Transit gateway attachment VPC 1 ID
10.2.0.0/16	Transit gateway attachment VPC 2 ID

Transit gateway VPC route table	
Destination	Target
10.99.99.0/24	Transit gateway VPN attachment ID

Resumen

Conexión con instalaciones propias

- **Site-to-site VPN** crea una conexión segura entre un gateway on-premises del cliente y un Virtual Private Gateway (o un Transit Gateway) de AWS.
- Múltiples redes on-premises se pueden conectar a un único Virtual Private Gateway.
- Global Accelerator permite acelerar las conexiones site-to-site.
- Se pueden configurar múltiples tablas de rutas en Transit Gateway para aislar las VPC que brindan acceso completo a través de VPN.

Conexión de redes remotas

AWS Direct Connect

UNIVERSIDAD AUSTRAL

AWS Direct Connect

Direct Connect

Es una conexión de VLAN (virtual local area network) dedicada, privada que extiende la red on-premises para incluir recursos de AWS.

Brinda una experiencia de red consistente, con rendimiento predecible y mayor ancho de banda.

AWS Direct Connect

Casos de uso

Entornos híbridos

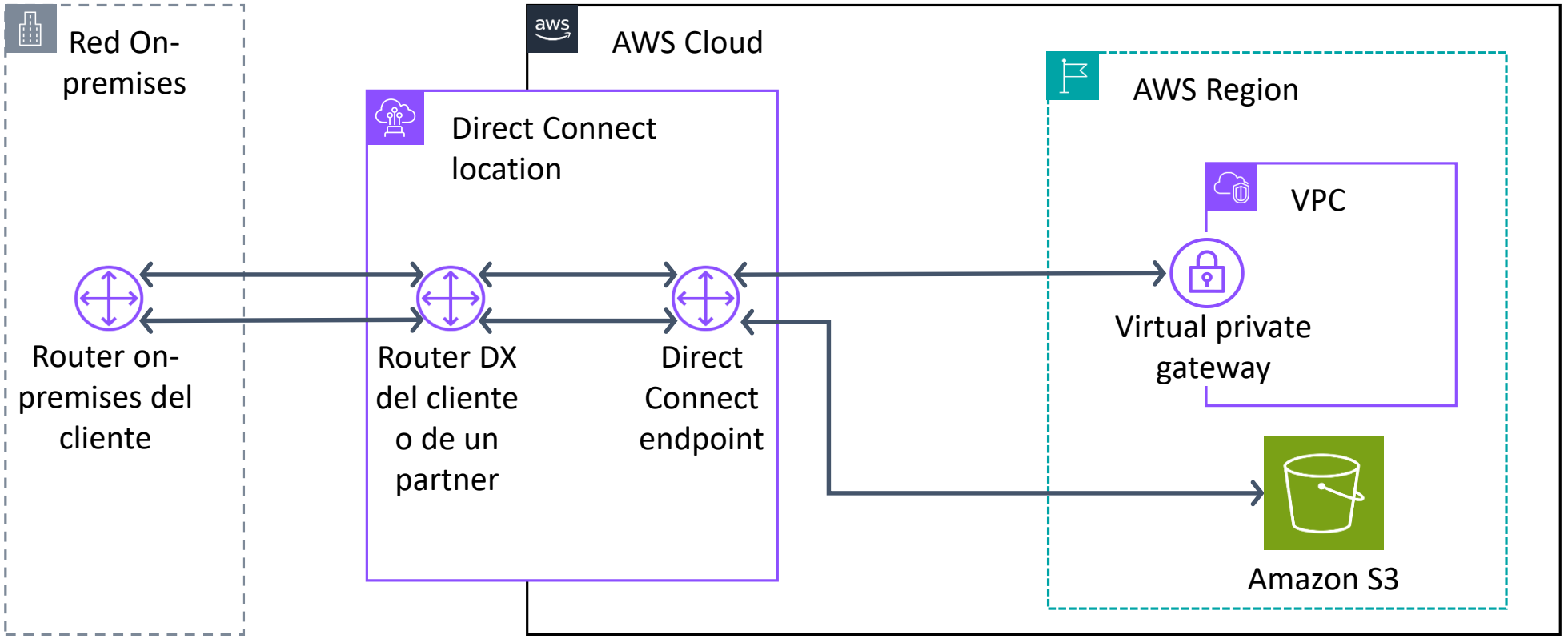
Volúmenes de datos grandes

Rendimiento de red predecible

Seguridad y cumplimiento

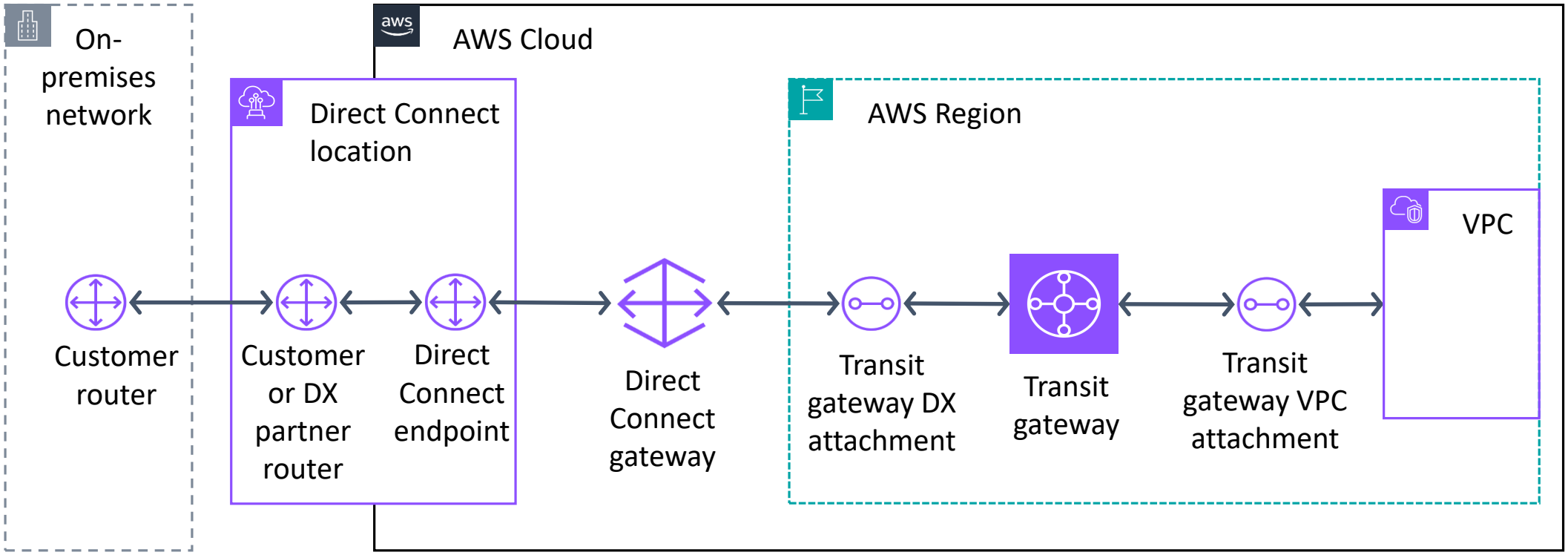
AWS Direct Connect

Extensión de una red *on-premises*



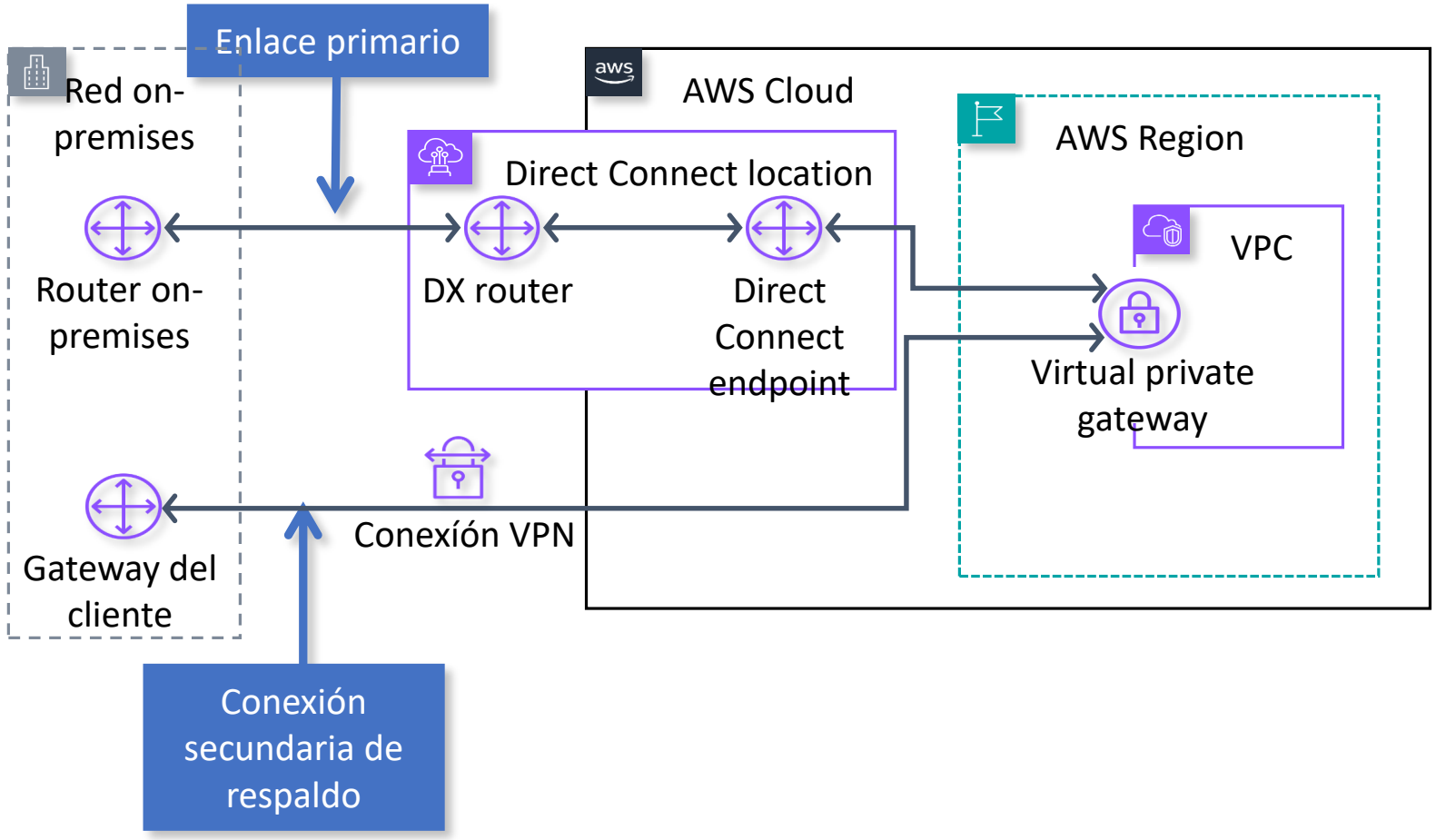
AWS Direct Connect

Con Transit Gateway



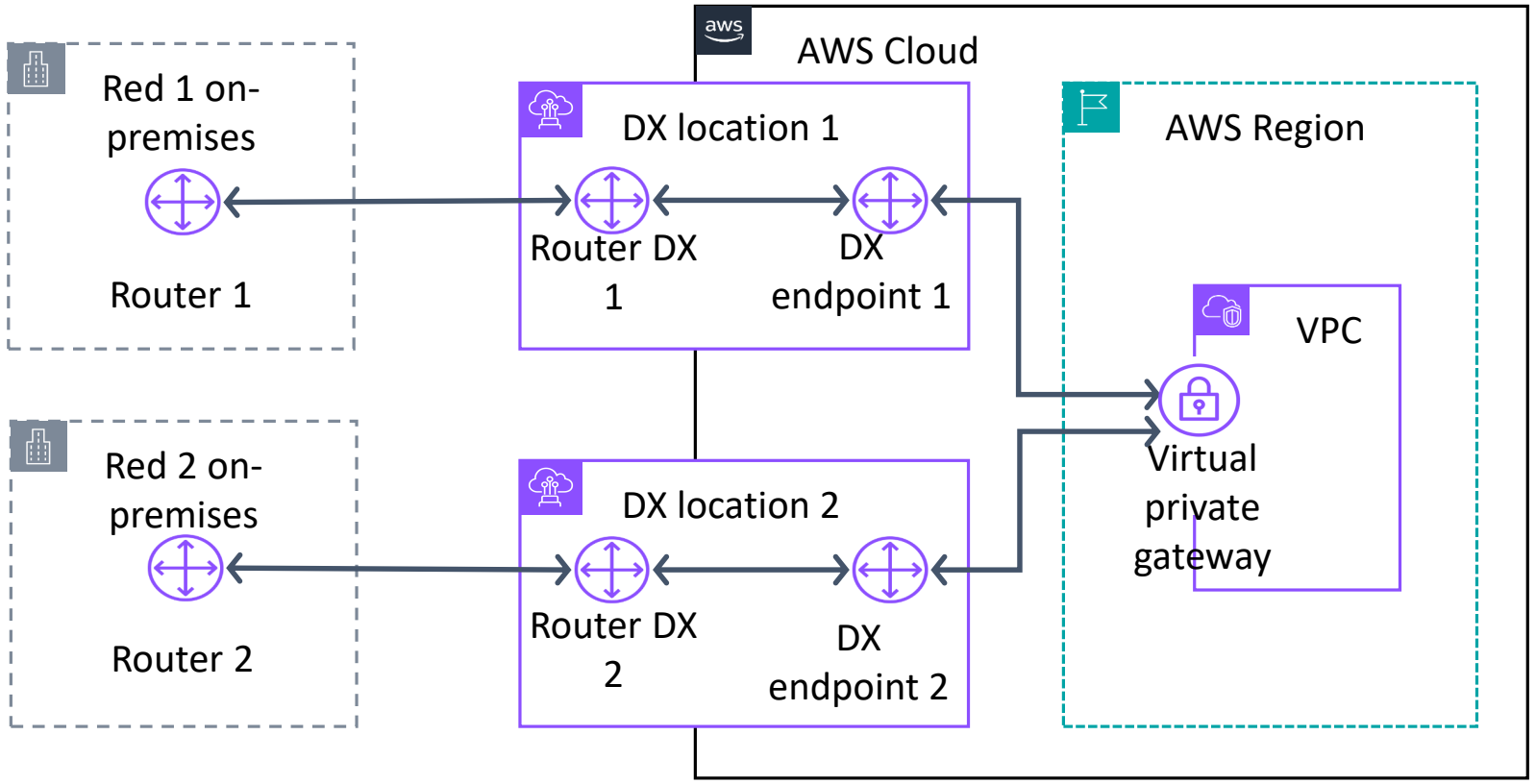
AWS Direct Connect

Alta disponibilidad



AWS Direct Connect

Alta resiliencia con múltiples ubicaciones



Direct Connect

Resumen

Direct Connect es una conexión VLAN dedicada, privada que extiende una red on-premises para incluir recursos de AWS:

- Usa una interfaz privada para conectar una ubicación de Direct Connect con un *Gateway* privado virtual.
- Usa una interfaz pública para conectar una ubicación de Direct Connect a servicios de AWS que lo soportan.
- Usa una interfaz de tránsito para conectar una ubicación de Direct Connect a un *transit Gateway* a través de Direct Connect Gateway.

Se puede usar una VPN como conexión secundaria para crear alta disponibilidad.

El uso de varias ubicaciones de Direct Connect permite mejorar la resiliencia de varias redes *on-premises*.

Well-Architected Framework

Aplicado a la conexión entre redes

UNIVERSIDAD AUSTRAL

Well-Architected Framework

Pilares

Reliability

Security

Performance Efficiency

Cost Optimization

Well-Architected Framework

Planificar la topología de red

Crear enlaces redundantes entre las redes privadas de la nube y las instalaciones *on-premises*

Elegir topologías *hub-and-spoke* en lugar de implementar topologías mesh muchos a muchos

Well-Architected Framework

Protección de redes

Controlar el tráfico en todas las capas

Protección de datos en tránsito

Autenticar las comunicaciones de red

Cifrado

Well-Architected Framework

Performance

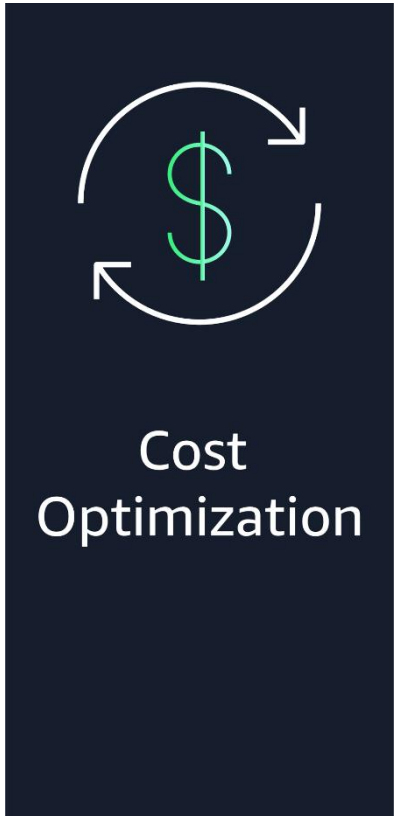
Performance efficency

Elegir conexiones dedicadas o VPN apropiadas para el tamaño de las cargas de trabajo

Elegir la ubicación de las cargas de trabajo en función de los requerimientos de red

Well-Architected Framework

Optimización de costos



Elegir los componentes que optimicen el costo de transferencia de datos

Implementar servicios que reduzcan el costo de transferencia de datos

Módulo 8. Conexión de redes

Resumen

- Describir cómo se puede conectar una red *on-premises* con la nube de AWS
- Describir cómo conectar múltiples VPC en la nube de AWS
- Conectar VPC usando VPC peering
- Describir el escalamiento de VPC en la nube de AWS
- Aplicar el AWS Well-Architected Framework a este proceso

Sample exam question

An application running on Amazon EC2 instances in a virtual private cloud (VPC) processes sensitive information stored on Amazon S3. The information is accessed by using an Amazon S3 public Regional endpoint over the internet. The security team is concerned that the internet connectivity to Amazon S3 is a security risk. Which solution will resolve the security concern with the most efficient network route?

Identify the key words and phrases before continuing.

The following are the key words and phrases:

- EC2 instances in a VPC
- Sensitive information
- Internet connectivity to Amazon S3 is a security risk
- Most efficient network route

Sample exam question: Response choices

An application running on Amazon EC2 instances in a virtual private cloud (VPC) processes sensitive information stored on Amazon S3. The information is accessed by using an Amazon S3 public regional endpoint over the internet. The security team is concerned that the internet connectivity to Amazon S3 is a security risk. Which solution will resolve the security concern with the most efficient network route?

Choice	Response
A	Access the data through an internet gateway.
B	Access the data through a virtual private network (VPN) connection.
C	Access the data through a NAT gateway.
D	Access the data through a VPC endpoint for Amazon S3.

Sample exam question: Answer

The answer is D.

Choice	Response
A	
B	
C	
D	Access the data through a VPC endpoint for Amazon S3.

Muchas gracias.

www.austral.edu.ar

UNIVERSIDAD AUSTRAL