Cloudshine
Enjoy the journey to the cloud

Cloud Essentials

Practico N° 5
Redes y entrega de contenido

Repaso

- Conceptos básicos de las redes
- Amazon VPC
- Redes de VPC
- Seguridad de VPC
- Amazon Route 53
- Amazon CloudFront

Direcciones IP

	192	.	0	.	2	.	0
Octetos	11000000		00000000		00000010		00000000
	8 bits		8 bits		8 bits		8 bits

32 bits

Dirección IPv4 (32 bits): 192.0.2.0

Dirección IPv6 (128 bits): 2600:1f18:22ba:8c00:ba86:a05e:a5ba:00FF

Cloudshine
Enjoy the journey to the cloud

Direccionamiento entre dominios sin clases (CIDR)

Identificador de red (prefijo de direccionamiento)

Identificador de host

192 . 0 . 2 . 0 / 24

11000000 | 00000000 | 00000010 | 00000000 hasta 11111111

Indica cuántos bits son estáticos

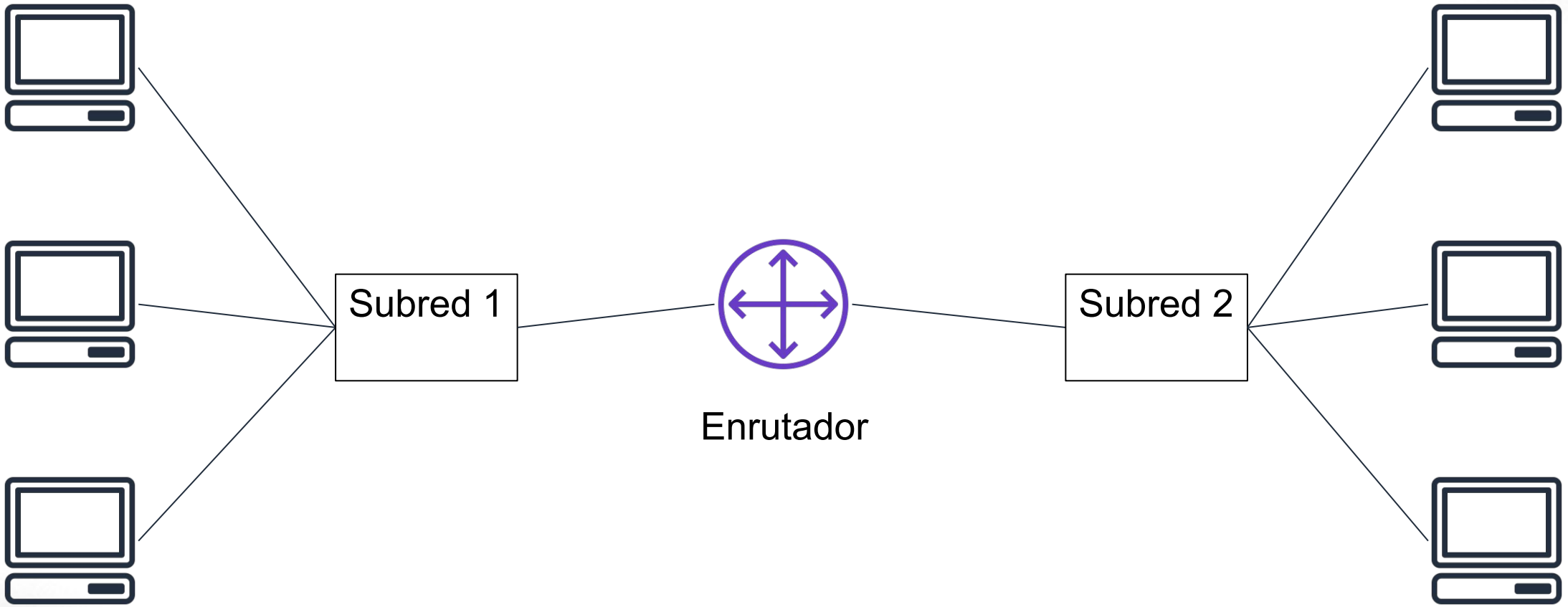
Estático | Estático | Estático | Flexible

192.0.2.0	Direccion de red
192.0.2.1	Dirección de router(o gateway)
192.0.2.2	Dirección de host
192.0.2.3	Dirección de host
***	
192.0.2.255	Dirección de broadcast

00000000
00000001
00000010
00000011
00000100
…
111111111

Cloudshine
Enjoy the journey to the cloud

Redes



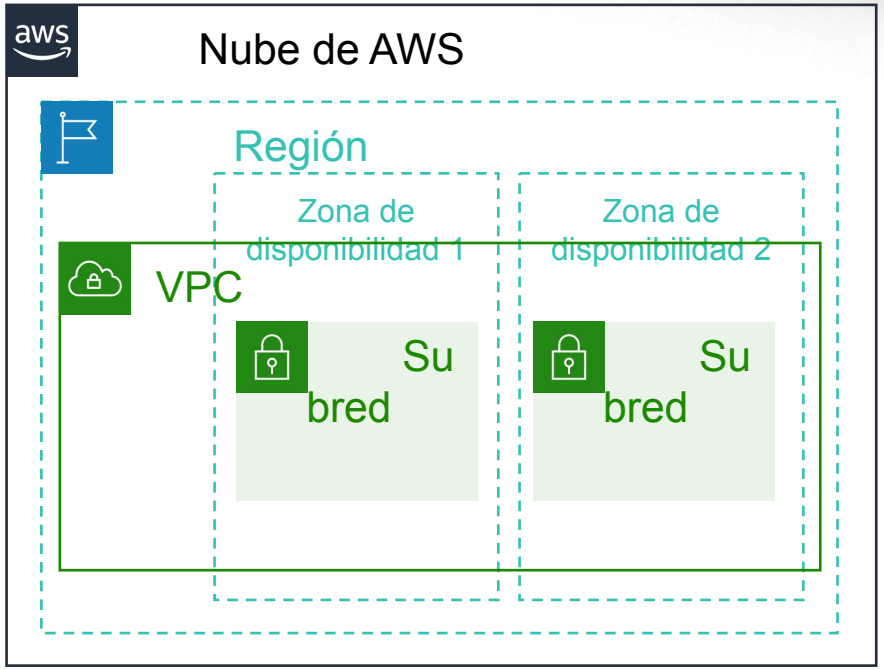
Modelo de interconexión de sistemas abiertos (OSI)

Capa	Número	Función	Protocolo/dirección
Aplicación	7	Es el medio por el que una aplicación obtiene acceso a una red informática	HTTP(S), FTP, DHCP, LDAP
Presentación	6	• Garantiza que la capa de aplicación pueda leer los datos • Cifrado	ASCI, ICA
Sesión	5	Permite un intercambio ordenado de datos	NetBIOS, RPC
Transporte	4	Proporciona protocolos para admitir la comunicación de host a host	TCP, UDP
Red	3	Direccionamiento y reenvío de paquetes (enrutadores)	IP
Enlace de datos	2	Transferir datos en la misma red LAN (concentradores y conmutadores)	MAC
Capa física	1	Transmisión y recepción de transmisiones de bits sin procesar a través de un medio físico	Señales (unos y ceros)

Amazon VPC

Características

- Sección de la nube de AWS aislada lógicamente
- Le permite controlar sus recursos de red virtual entre los que se cuentan los siguientes:
  - Selección del intervalo de direcciones IP
  - Creación de subredes
  - Configuración de tablas de enrutamiento y gateways de red
- Le permite utilizar varias capas de seguridad.
- Están dedicadas a su cuenta de AWS.
- Pertenecen a una única región de AWS y pueden abarcar varias zonas de disponibilidad.



Subredes

- Son el intervalo de direcciones IP que dividen una VPC.
- Pertenecen a una única zona de disponibilidad.
- Se clasifican como públicas o privadas.

Cloudshine
Enjoy the journey to the cloud

Direccionamiento IP

- En la creacion de una VPC se asigna un bloque CIDR (un intervalo de direcciones IPv4 privadas).
- No puede cambiar el intervalo de direcciones después de crear la VPC.
- El bloque de CIDR IPv4 más grande es /16.
- El bloque de CIDR IPv4 más pequeño es /28.
- También se admite IPv6
- Los bloques de CIDR de subredes no se pueden superponer.

Direcciones IP reservadas

Direcciones IP para el bloque de CIDR 10.0.0.0/24	Reservadas para
10.0.0.0	Dirección de red
10.0.0.1	Comunicación interna
10.0.0.2	Resolución del sistema de nombres de dominio (DNS)
10.0.0.3	Uso futuro
10.0.0.255	Dirección de transmisión de la red

Cloudshine
Enjoy the journey to the cloud

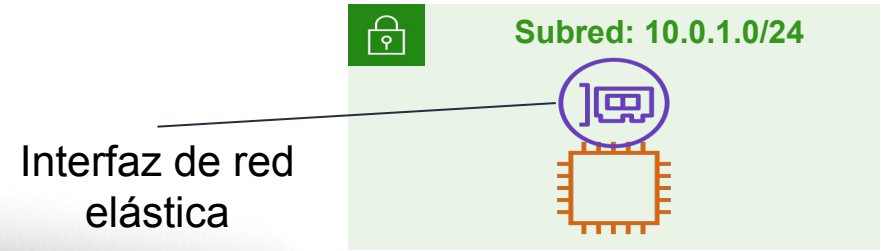
Más detalles sobre direccionamiento y redes

Tipos de direcciones IP públicas

- **Dirección IPv4 pública**
  - Se asigna manualmente a través de una dirección IP elástica.
  - Se asigna de manera automática a través de la configuración de asignación automática de direcciones IP públicas en el nivel de subred.
  - Creación de subredes
  - Configuración de tablas de enrutamiento y gateways de red
- **Dirección IP elástica**
  - Está asociada a una cuenta de AWS.
  - Se puede asignar y reasignar en cualquier momento.
  - Podría implicar costos adicionales.

Interfaz de red elástica

- Es una interfaz de red virtual
  - Se asocia a una instancia
  - Se puede desconectar y asociar a otra instancia
- Sus atributos se mantienen, por lo que si se cambia de instancia estos también se asocian
- Cada instancia de la VPC ya tiene una interfaz de red predeterminada con una IPv4 privada



Cloudshine
Enjoy the journey to the cloud

Tablas de enrutamiento y rutas

- **Tabla de enrutamiento:** Conjunto de reglas (o rutas) que se configura para dirigir el tráfico de red de su subred.
- **Ruta**: Especifica un destino y un objetivo.
- De forma predeterminada, cada tabla de enrutamiento contiene una ruta local para la comunicación dentro de la VPC.
- Cada subred debe estar asociada a una tabla de enrutamiento (solamente a una).

Tabla de enrutamiento principal (predeterminada)

Destino	Objetivo
10.0.0.0/16	local

Bloque de CIDR de la VPC

Cloudshine
Enjoy the journey to the cloud

Gateway de Internet

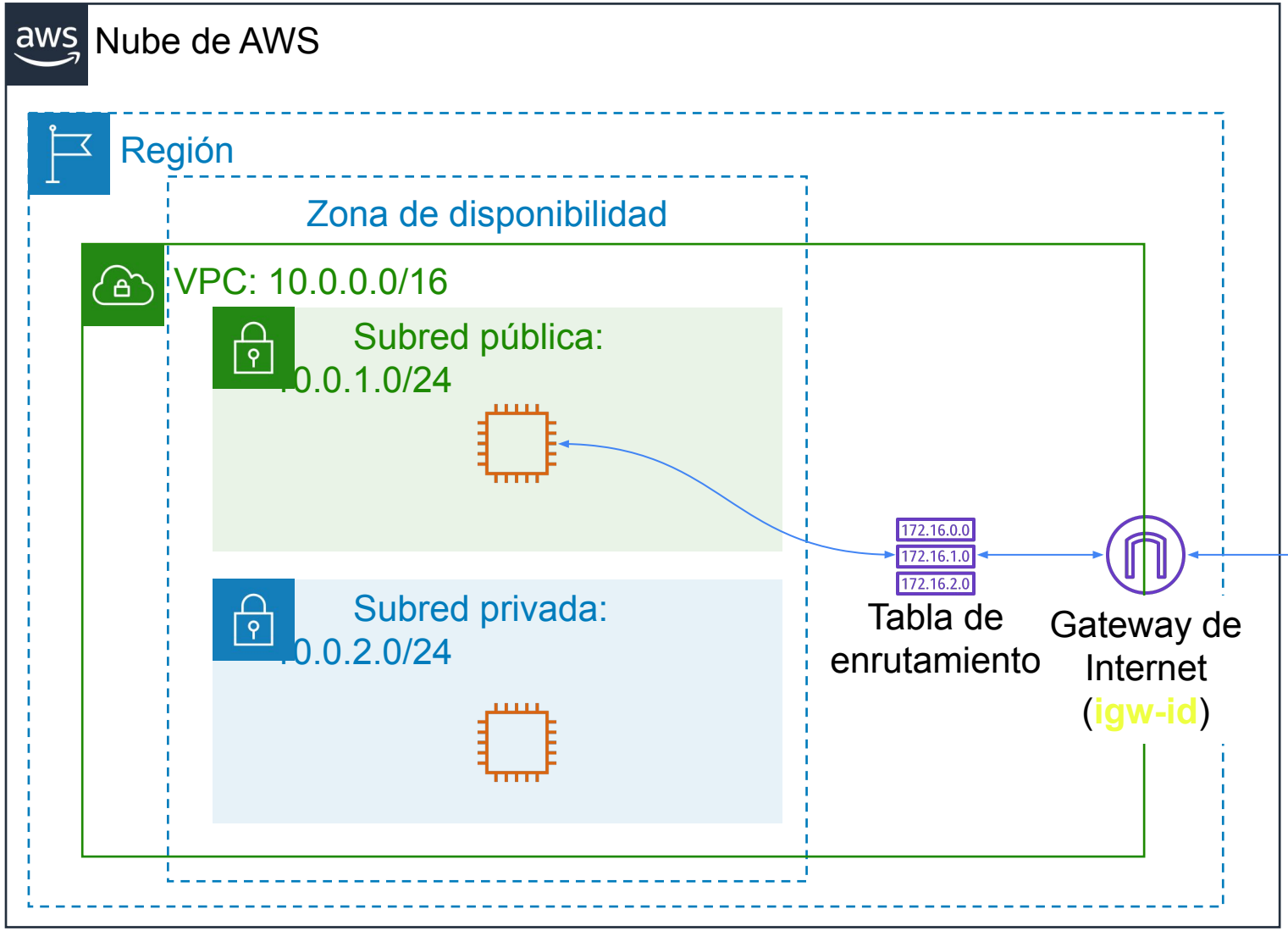


Tabla de enrutamiento de subred pública

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

Gateway de traducción de direcciones de red (NAT Gateway)

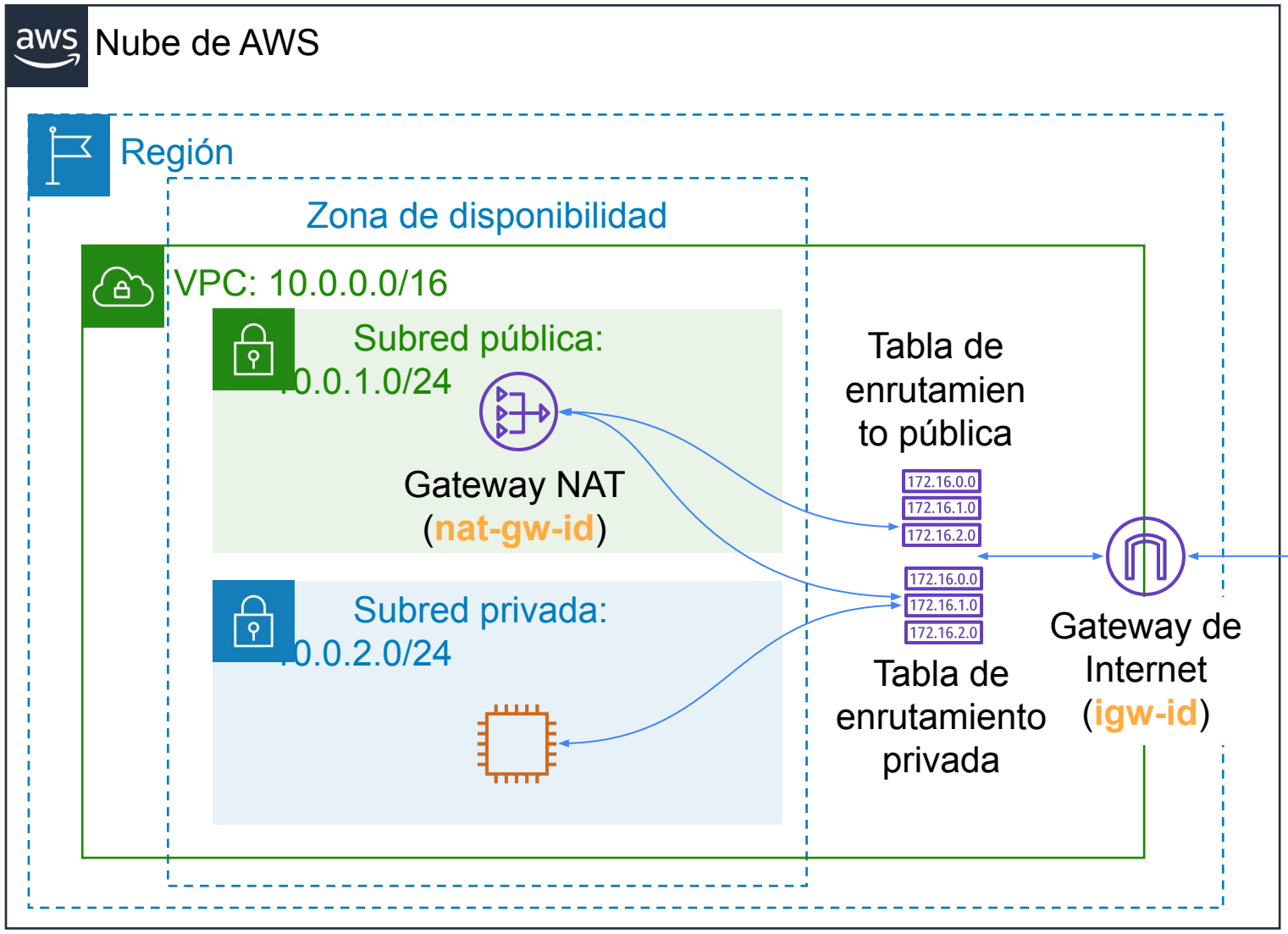


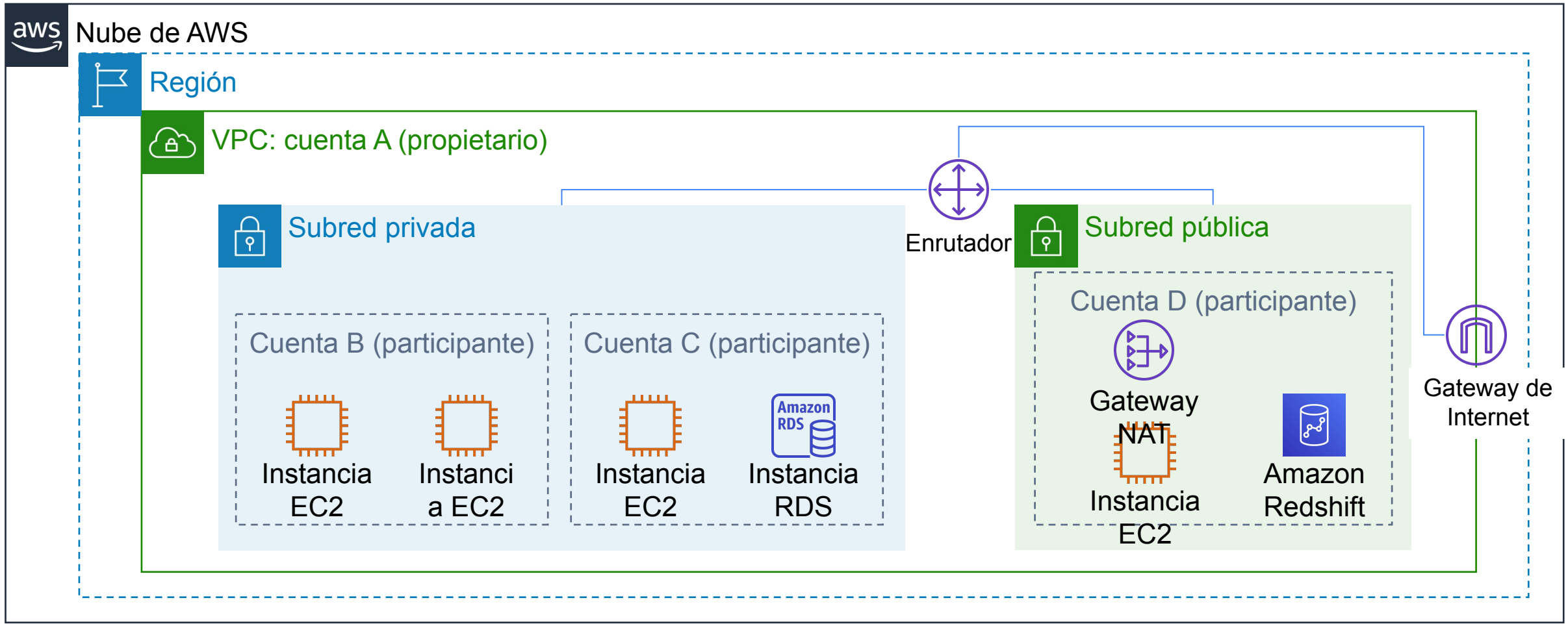
Tabla de enrutamiento de subred pública

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

Uso compartido de VPC(VPC-sharing)



Interconexión de VPC (VPC peering)

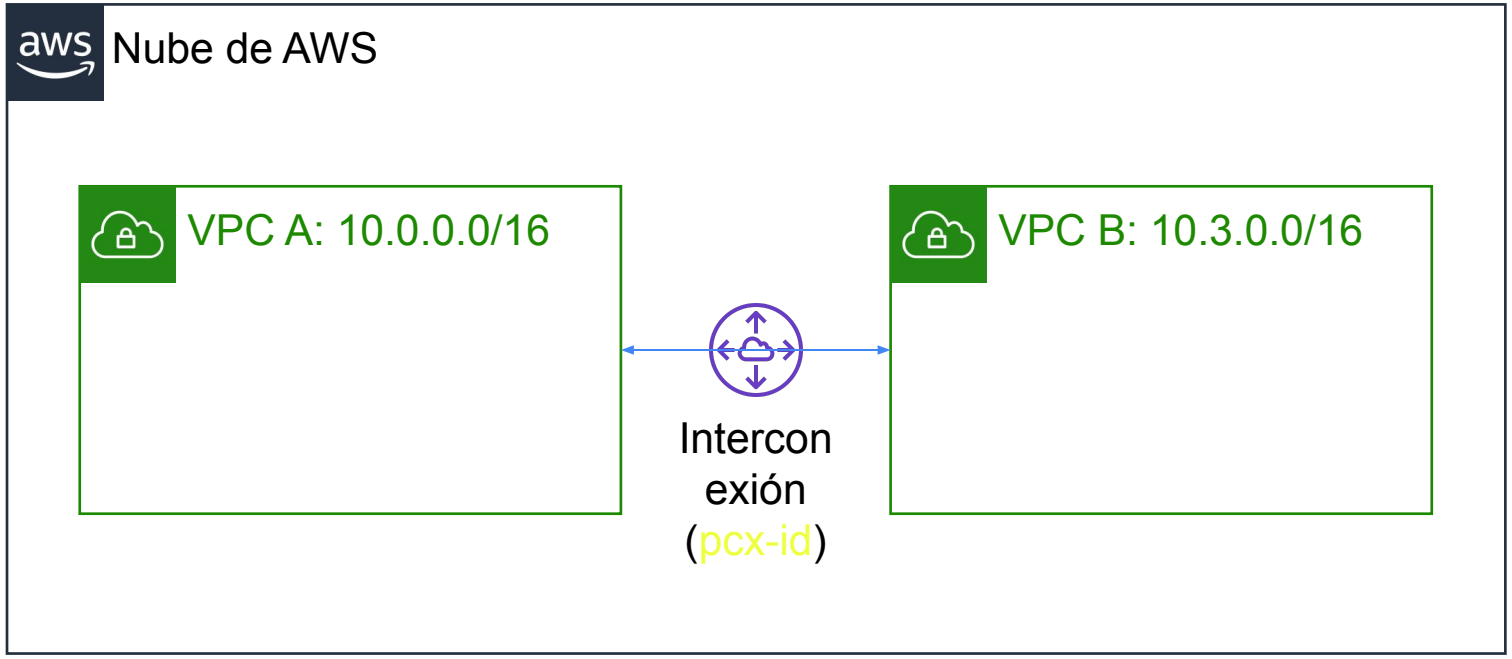


Tabla de enrutamiento para VPC A

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

Tabla de enrutamiento para VPC B

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

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

Restricciones:

- Los espacios IP no se pueden superponer.
- No se admite la interconexión transitiva.
- Solo puede tener un recurso de interconexión entre las mismas dos VPC.

AWS Site-to-Site VPN

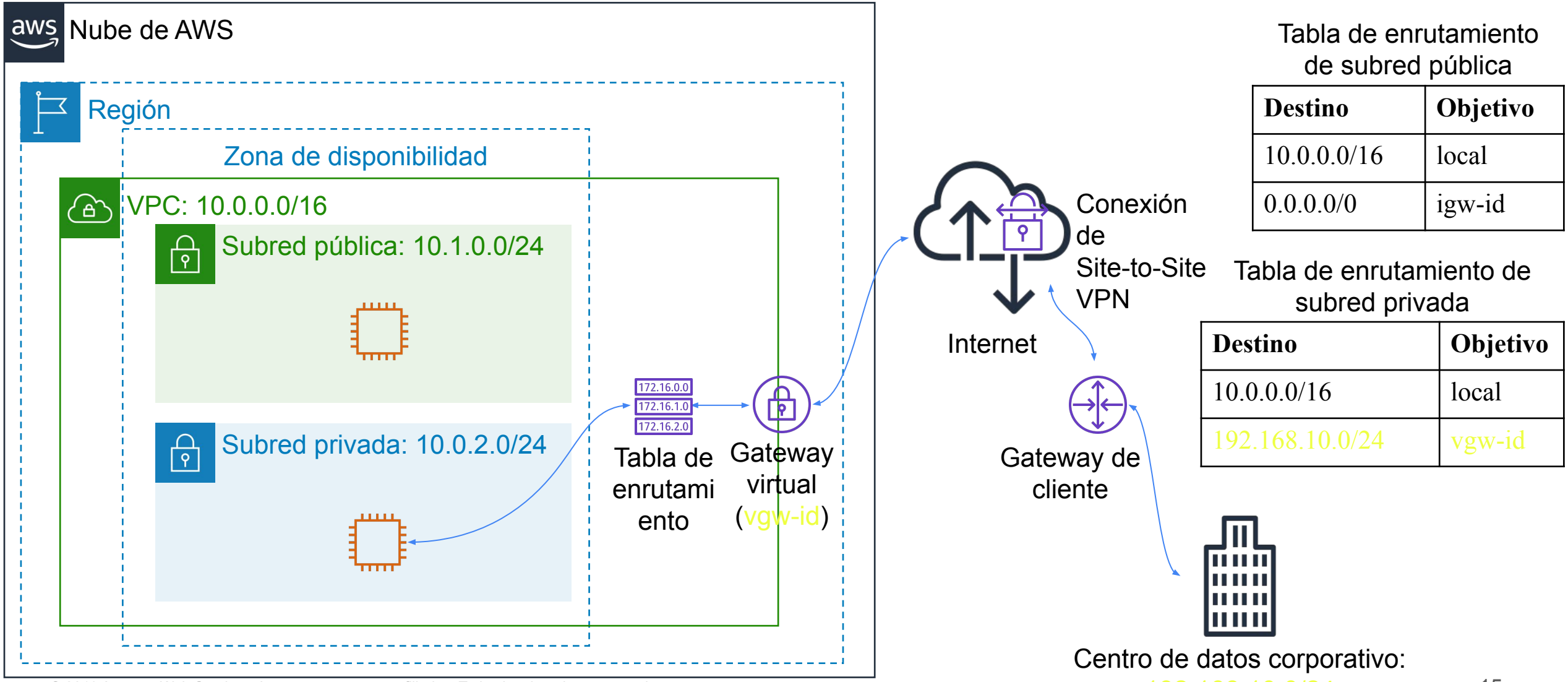


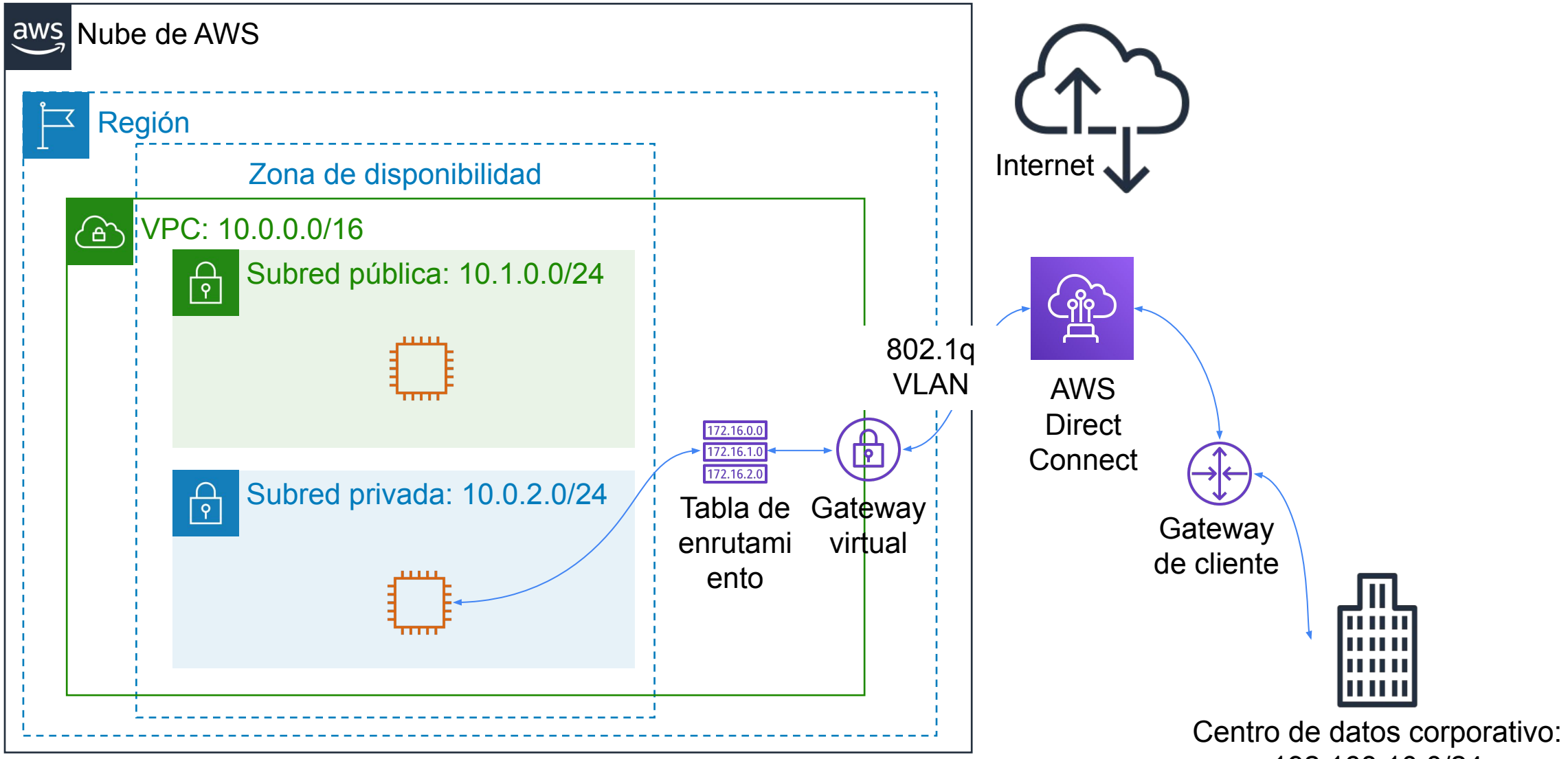
Tabla de enrutamiento de subred pública

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

AWS Direct Connect



Puntos de enlace VPC (VPC endpoint)

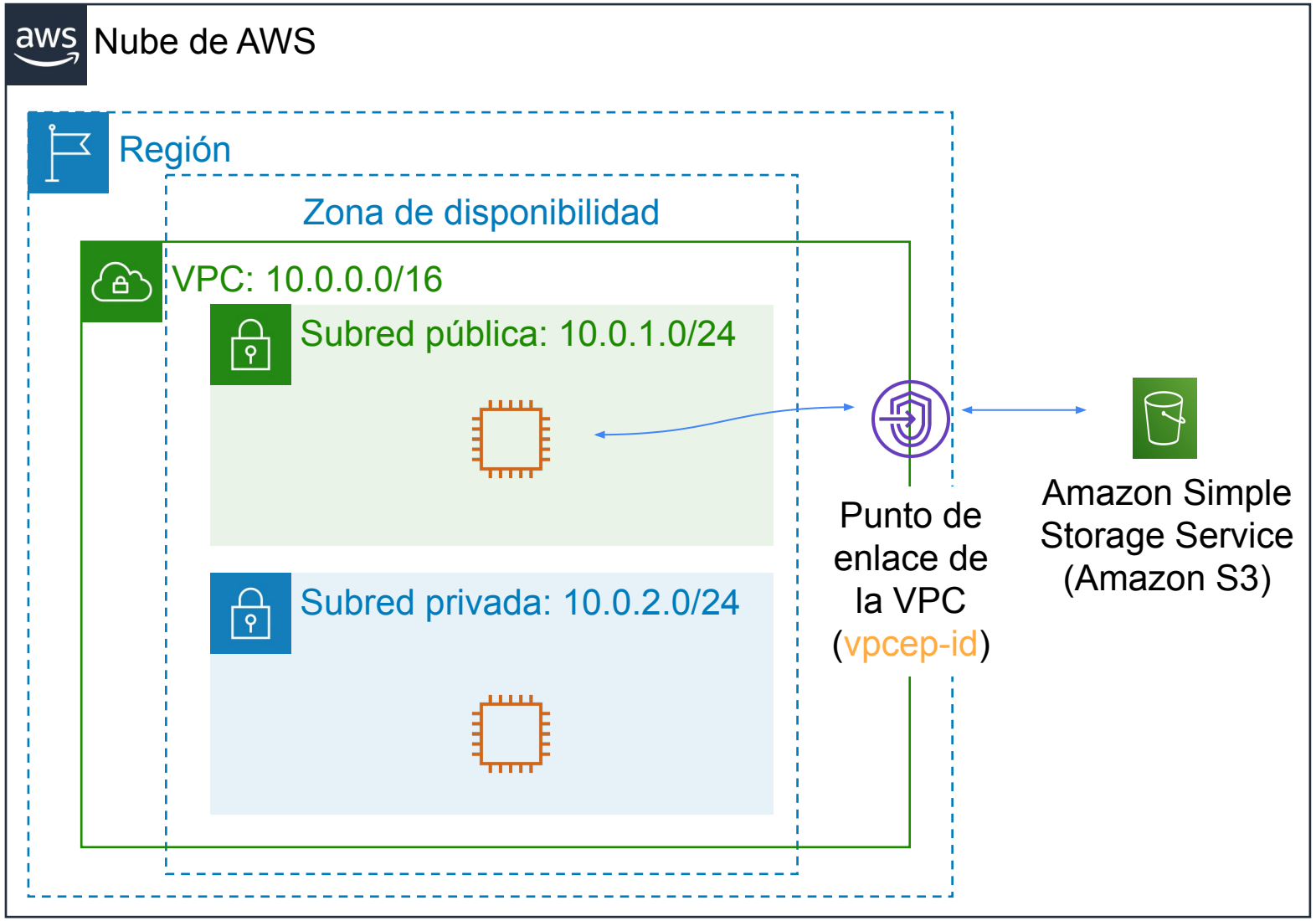


Tabla de enrutamiento de subred pública

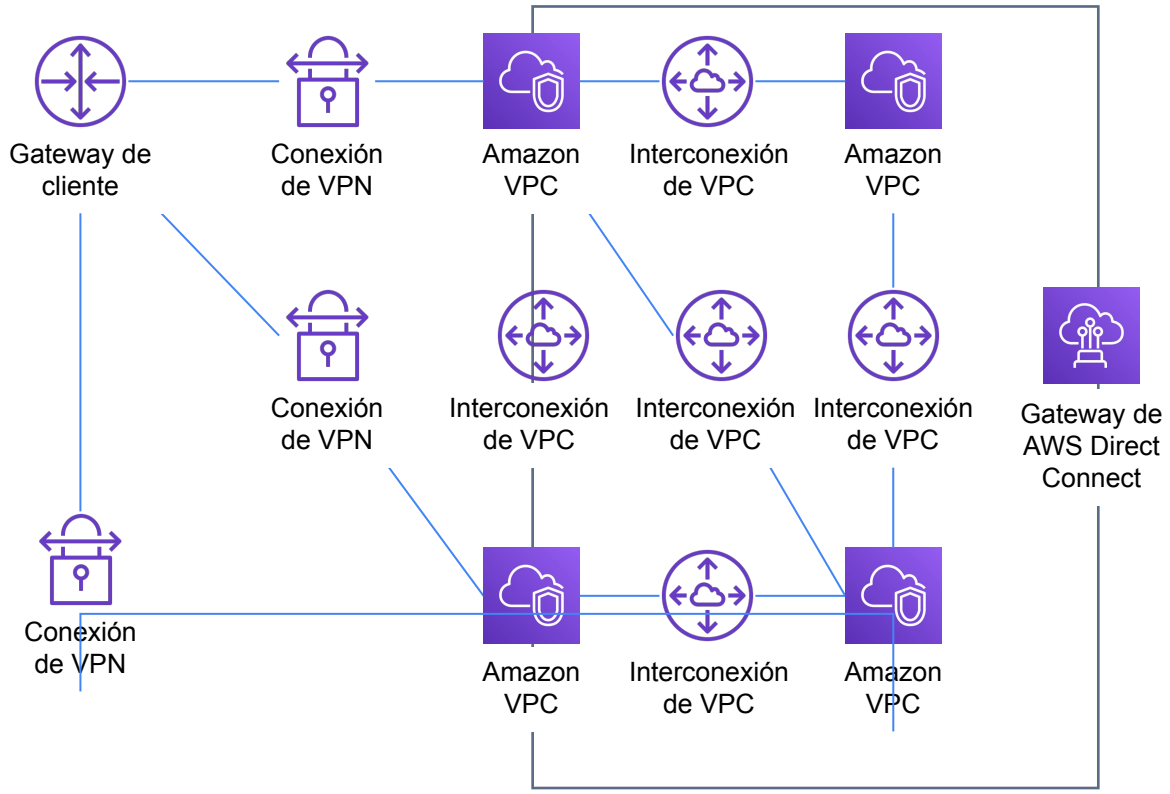
Destino	Objetivo
10.0.0.0/16	local
ID de Amazon S3	vpcep-id

Dos tipos de puntos de enlace:

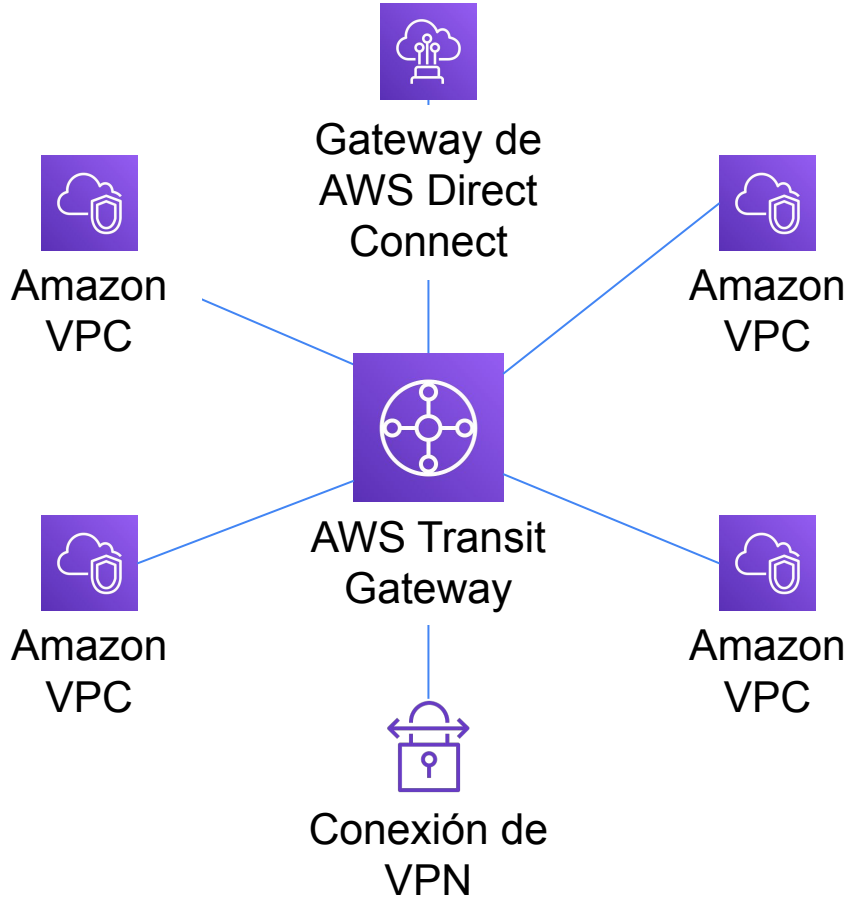
- **Puntos de enlace de** interfaz (con tecnología de AWS PrivateLink)
- **Puntos de enlace de** gateway (Amazon S3 y Amazon DynamoDB)

AWS Transit Gateway

De esto:



A esto:



Seguridad de VPC

Security groups

- Funciona como un **firewall virtual** de la instancia para **controlar el tráfico** de entrada y de salida.
- Actúan al **nivel de la instancia**, pero no en el de la subred.
- Cada instancia de la subred de su VPC puede asignarse a un conjunto de grupos de seguridad diferente.
- Tienen **reglas** que controlan el tráfico de entrada y de salida
- Por defecto **deniegan** todo el **tráfico de entrada** y **permiten** todo el **tráfico de salida**.
- Tienen **estado**

Entrada				
Tipo	Protocolo	Intervalo de puertos	Origen	Descripción
Todo el tráfico	Todo	Todo	sg-xxxxxxxx	
Salida				
Tipo	Protocolo	Intervalo de puertos	Origen	Descripción
Todo el tráfico	Todo	Todo	sg-xxxxxxxx	

Cloudshine
Enjoy the journey to the cloud

Grupos de seguridad

Security groups

- **Personalizados**
  - Puede especificar **reglas de permiso**, pero no reglas de denegación.
  - Todas las **reglas se evalúan antes** de decidir si se permite el tráfico o no.

Entrada				
Tipo	Protocolo	Intervalo de puertos	Origen	Descripción
HTTP	TCP	80	0.0.0.0/0	Todo el tráfico web
HTTPS	TCP	443	0.0.0.0/0	Todo el tráfico web
SSH	TCP	22	54.24.12.19/32	Dirección de la oficina
Salida				
Tipo	Protocolo	Intervalo de puertos	Origen	Descripción
Todo el tráfico	Todo	Todo	0.0.0.0/0	
Todo el tráfico	Todo	Todo	::/0	

Cloudshine
Enjoy the journey to the cloud

Listas de control de acceso a la red (ACL de red)

- Las ACL de red funcionan en el **nivel de la subred**
- Tiene **reglas** de entrada y de salida **independientes**, y cada regla puede **permitir o denegar** tráfico.
- Por defecto **permiten todo** el tráfico IPv4 de entrada y de salida.
- No tienen **estado**.

Entrada					
N.º de regla	Tipo	Protocolo	Intervalo de puertos	Origen	Permitir/Denegar
100	Todo el tráfico IPv4	Todo	Todo	0.0.0.0/0	PERMITIR
*	Todo el tráfico IPv4	Todo	Todo	0.0.0.0/0	DENEGAR
Salida					
N.º de regla	Tipo	Protocolo	Intervalo de puertos	Origen	Permitir/Denegar
100	Todo el tráfico IPv4	Todo	Todo	0.0.0.0/0	PERMITIR
*	Todo el tráfico IPv4	Todo	Todo	0.0.0.0/0	DENEGAR

Cloudshine
Enjoy the journey to the cloud

Listas de control de acceso a la red (ACL de red)

- **Personalizadas**:
  - Las ACL de red personalizadas **deniegan todo** el tráfico de entrada y de salida hasta que se agregan reglas.
  - Puede especificar **reglas de permiso y de denegación**.
  - Las reglas se evalúan según el **orden numérico**, comenzando por el número más bajo.

Entrada					
N.º de regla	Tipo	Protocolo	Intervalo de puertos	Origen	Permitir/Denegar
103	SSH	TCP	22	0.0.0.0/0	PERMITIR
100	HTTPS	TCP	443	0.0.0.0/0	PERMITIR
*	Todo el tráfico IPv4	Todo	Todo	0.0.0.0/0	DENEGAR
Salida					
N.º de regla	Tipo	Protocolo	Intervalo de puertos	Origen	Permitir/Denegar
103	SSH	TCP	22	0.0.0.0/0	PERMITIR
100	HTTPS	TCP	443	0.0.0.0/0	PERMITIR
*	Todo el tráfico IPv4	Todo	Todo	0.0.0.0/0	DENEGAR

Comparación entre grupos de seguridad y ACL de red

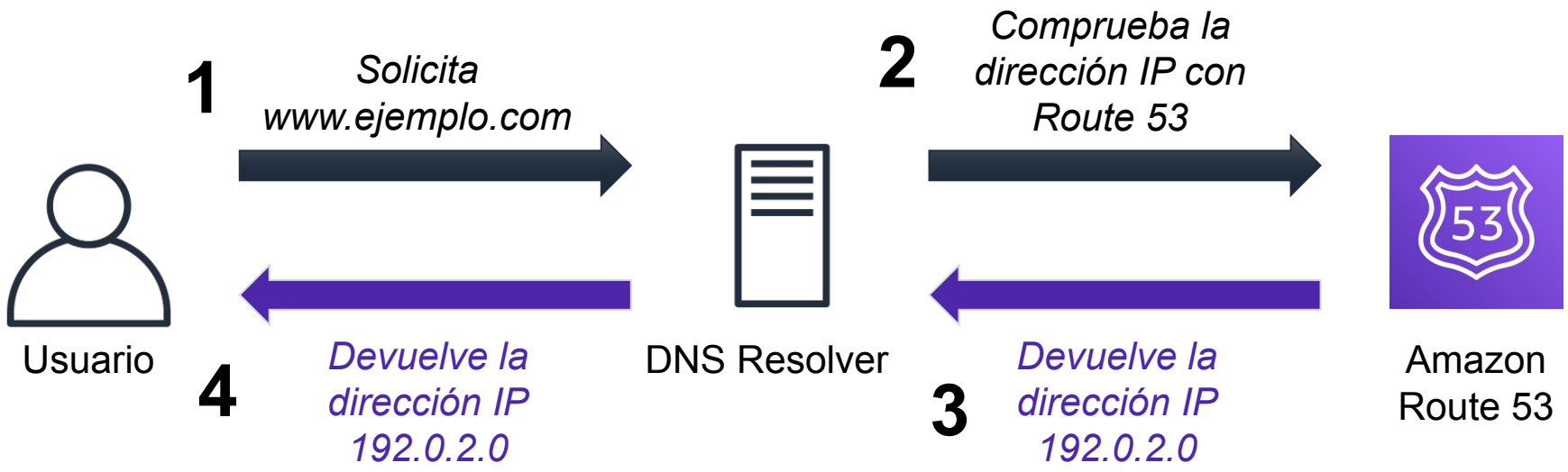
Atributo	Grupos de seguridad	ACL de red
Alcance	Nivel de la instancia	Nivel de la subred
Reglas admitidas	Solo reglas de permiso	Reglas de permiso y de denegación
Estado	Con estado (el tráfico de retorno se permite automáticamente, sin importar las reglas)	Sin estado (las reglas deben permitir de forma explícita el tráfico de retorno)
Orden de las reglas	Todas las reglas se evalúan antes de decidir si se permite el tráfico	Las reglas se evalúan según el orden numérico antes de decidir si se permite el tráfico

Amazon Route 53

Características

- Es un **servicio web de DNS** (Sistema de nombres de dominio) de gran disponibilidad y escalabilidad.
- Se utiliza para redirigir a los usuarios finales a las aplicaciones en Internet mediante la traducción de nombres (como www.ejemplo.com) en direcciones IP numéricas (como 192.0.2.1)
- Compatible con IPv4 e IPv6.
- Conecta las solicitudes de los usuarios a la infraestructura que se ejecuta en AWS y también fuera de AWS.
- Se utiliza para comprobar el **estado de los recursos.**
- Cuenta con una característica para el **flujo de tráfico**.
- Permite **registrar** nombres de dominio.

Resolución de DNS con Amazon Route 53



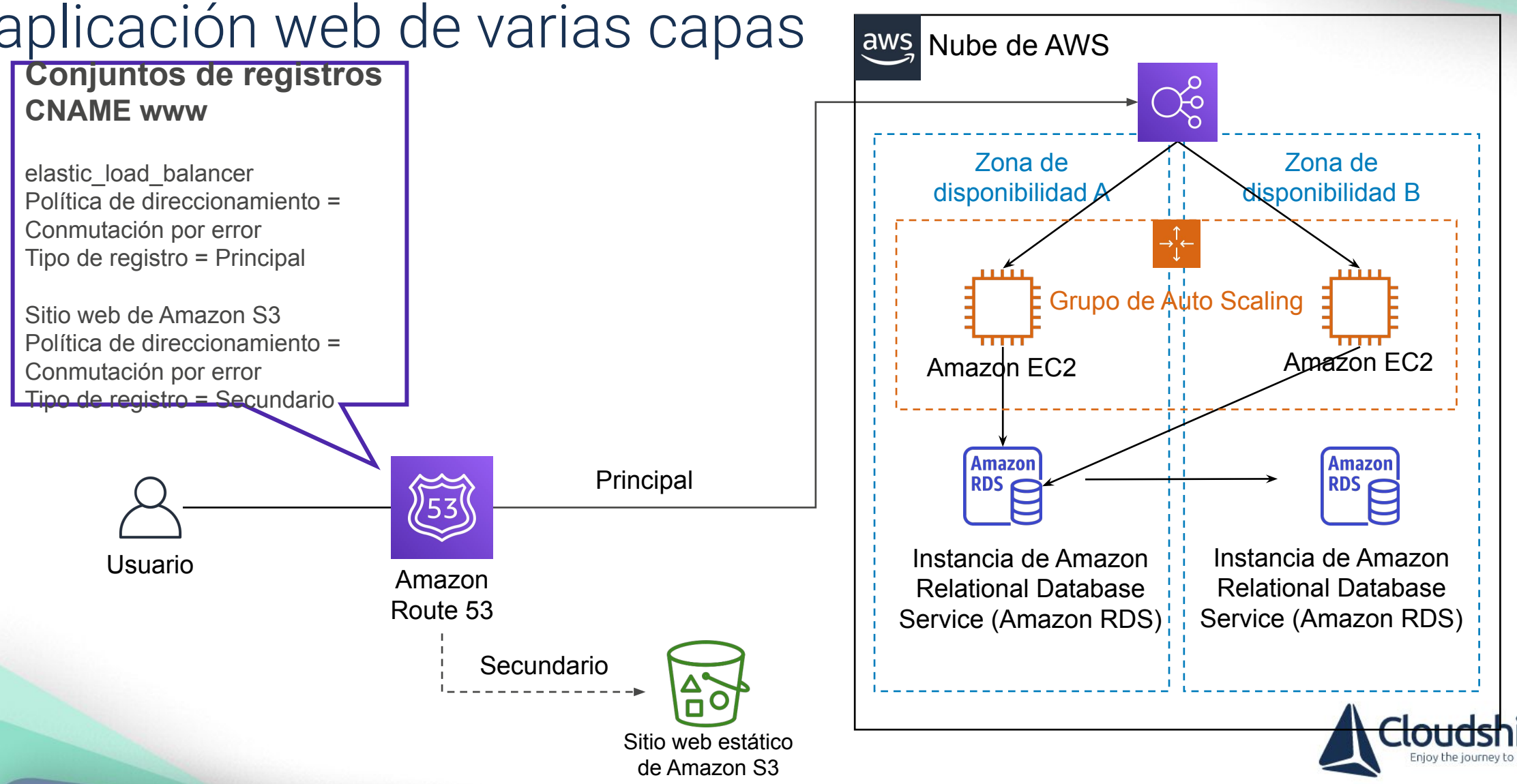
Cloudshine
Enjoy the journey to the cloud

Direccionamiento admitido por Amazon Route 53

- **Direccionamiento sencillo**: entornos de un solo servidor.
- **Direccionamiento de turno rotativo ponderado**: ponderaciones a los conjuntos de registros de recursos para especificar la frecuencia.
- **Direccionamiento basado en la latencia**: para mejorar las aplicaciones con nivel mundial.
- **Direccionamiento por geolocalización**: dirigir el tráfico en función de la ubicación de los usuarios.
- **Direccionamiento por geoproximidad**: dirigir el tráfico en función de la ubicación de los recursos.
- **Direccionamiento de respuesta con varios valores**: responda a consultas DNS con hasta ocho registros en buen estado que se seleccionan al azar.
- **Direccionamiento tras conmutación por error**: realice la conmutación por error a un sitio de copia de seguridad si ya no se puede acceder al sitio principal.
    - Configuración de las situaciones de copia de seguridad y de conmutación por error para sus propias aplicaciones
    - Habilitación de las arquitecturas en varias regiones de alta disponibilidad en AWS
    - Creación de comprobaciones de estado

Cloudshine
Enjoy the journey to the cloud

Conmutación por error a nivel de DNS para una aplicación web de varias capas



Cloudshine
Enjoy the journey to the cloud

Amazon CloudFront

¿Qué es un CDN?

- Es un sistema distribuido a nivel mundial de servidores de **almacenamiento en caché**.
- Almacena en caché copias de archivos solicitados habitualmente (**contenido estático**).
- Acelera la entrega de contenido dinámico, mejora el rendimiento y el escalado de las aplicaciones.

Características

- Servicio de **CDN** rápido, mundial y seguro
- Red global de **ubicaciones de borde y cachés** de borde regionales
- Modelo de autoservicio
- Precios de pago por uso

Beneficios De Amazon CloudFront

- Rapidez y alcance mundial
- Seguridad en el borde
- Alta capacidad de programación
- Integración total con AWS
- Rentabilidad

¿Cómo se paga por CloudFront?

- Transferencia **saliente** de datos
- Cantidad de solicitudes HTTP(S)
- Solicitudes de anulación
- Capa de conexión segura (SSL) personalizada con IP dedicada

Cloudshine
Enjoy the journey to the cloud

Gracias

Cloudshine
Enjoy the journey to the cloud