Arquitecturas de nube con AWS

Ing. Fernando Lichtschein
Ing. Mora Villa Abrille

7. Servicios de red

UNIVERSIDAD AUSTRAL

Objetivos

- Explicar el rol de una red privada virtual (VPC) en AWS
- Identificar los componentes de una VPC que se conectan a internet.
- Aislar y proteger recursos dentro del entorno de red
- Crear y monitorear una VPC con subredes, un internet Gateway, tablas de ruteo y un grupo de seguridad
- Aplicar los principios del AWS Well-Architected Framework para planificar y crear un entorno de red

Infraestructura física de AWS

Componentes y jerarquía

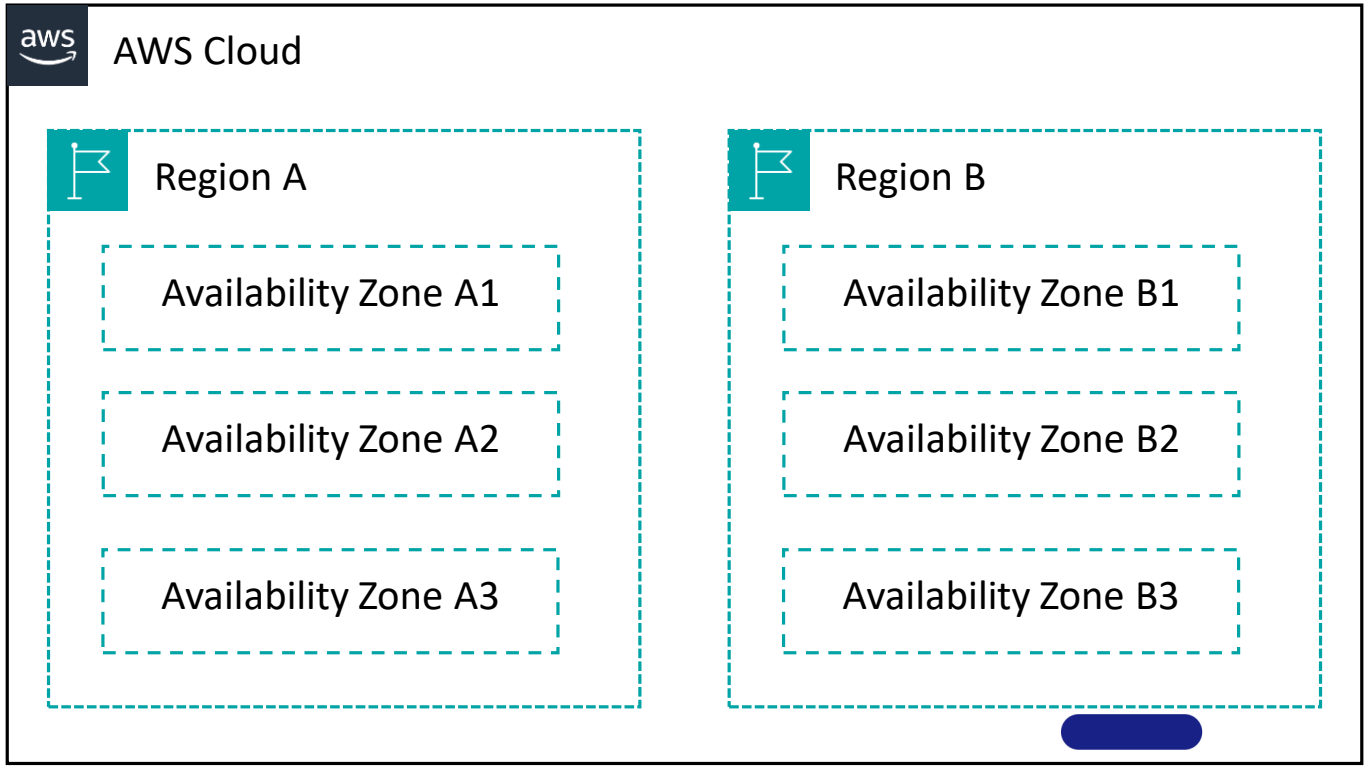
Los data centers de AWS tienen miles de servidores organizados en racks. Cada rack tiene routers de red y switches que direccionan el tráfico.

Los data centers se agrupan en Availability Zones (AZs).

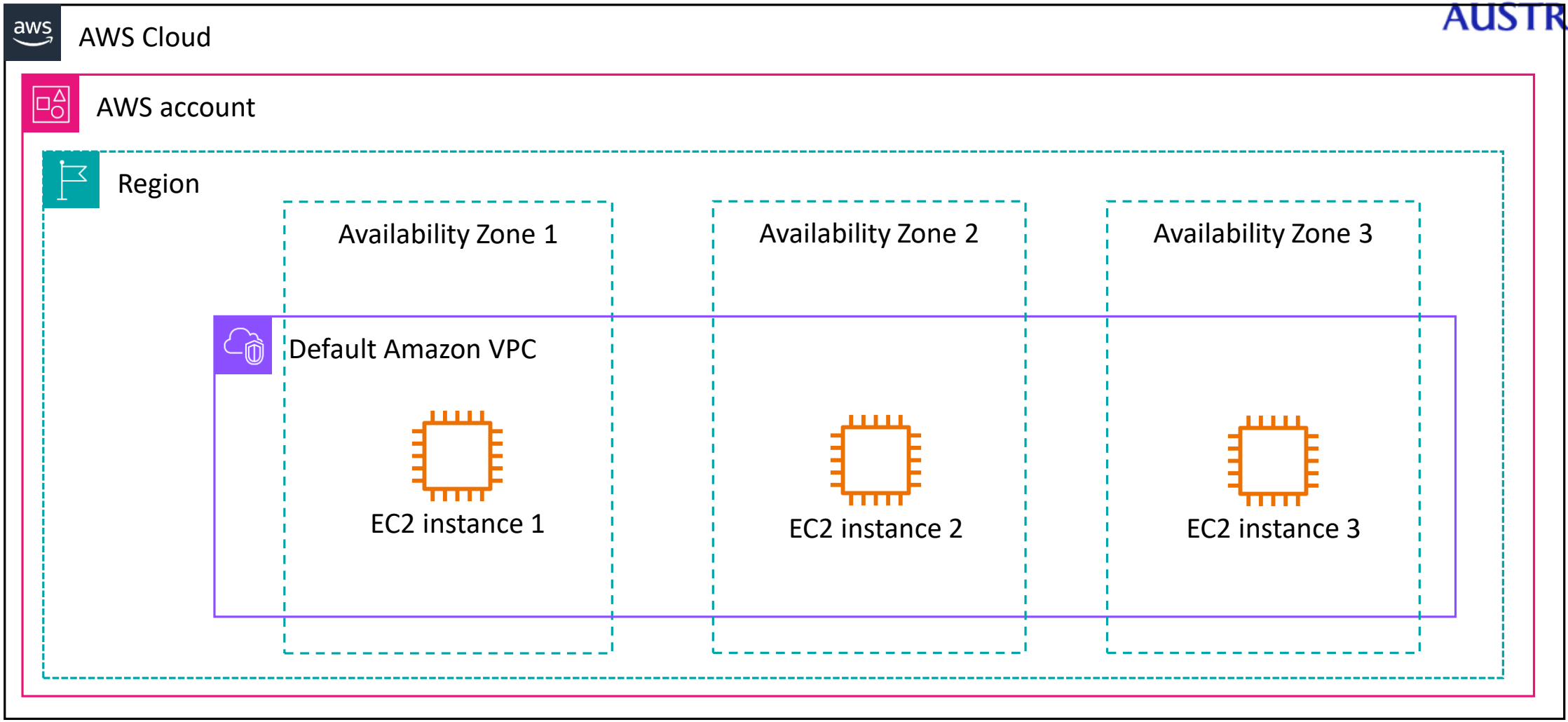
Las AZs se conectan en redes que tienen una latencia <10 milisegundos.

Las AZs están agrupadas en regiones.

La latencia entre una región y otra es de decenas de milisegundos



Aislar recursos en una cuenta AWS



Amazon Virtual Private Cloud

Amazon VPC

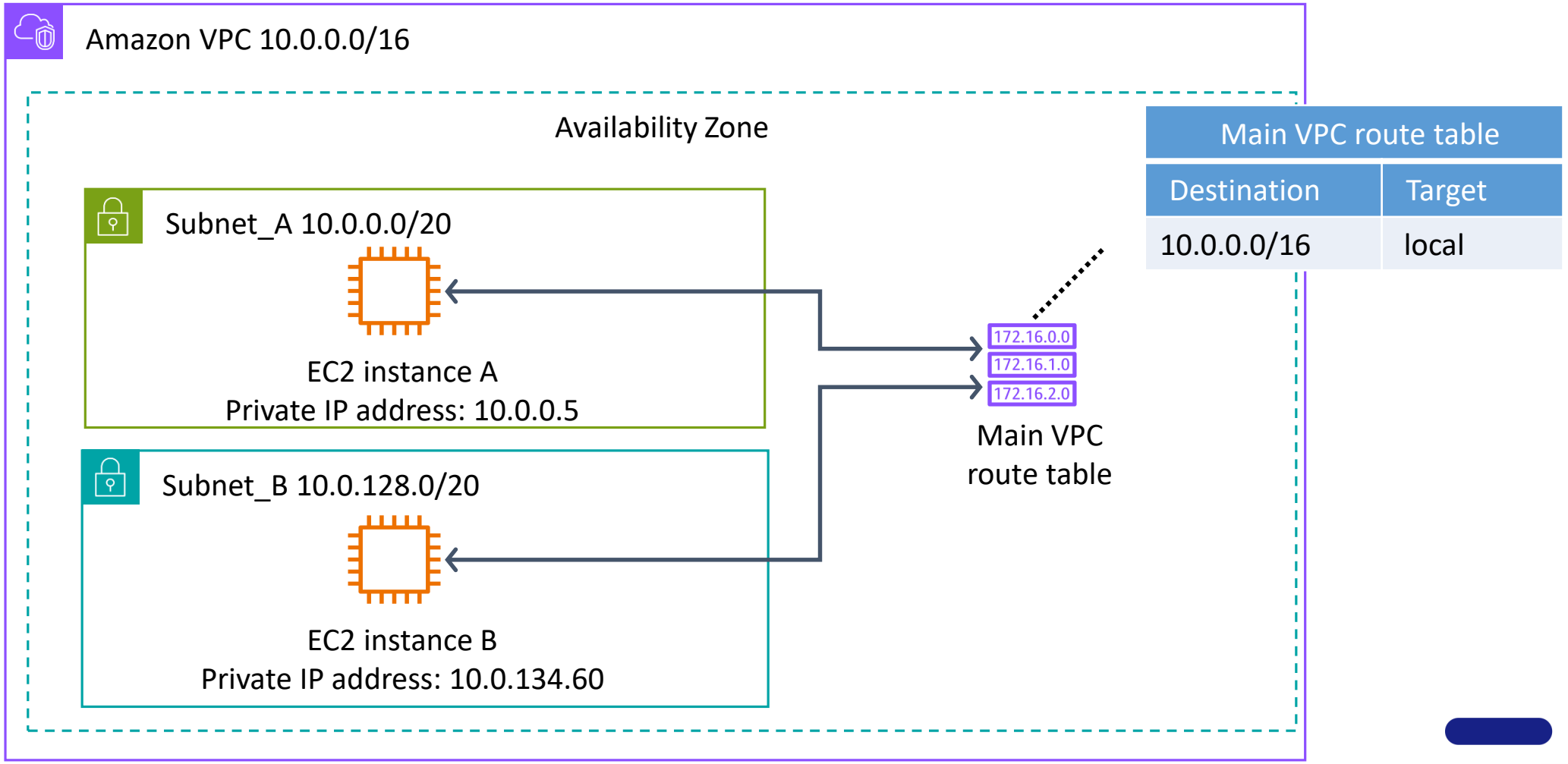
Es una red virtual definida por código, aislada lógicamente, similar a una red de un data center tradicional.

Pertenece a una región

Se puede personalizar para controlar el tráfico entrante y saliente.

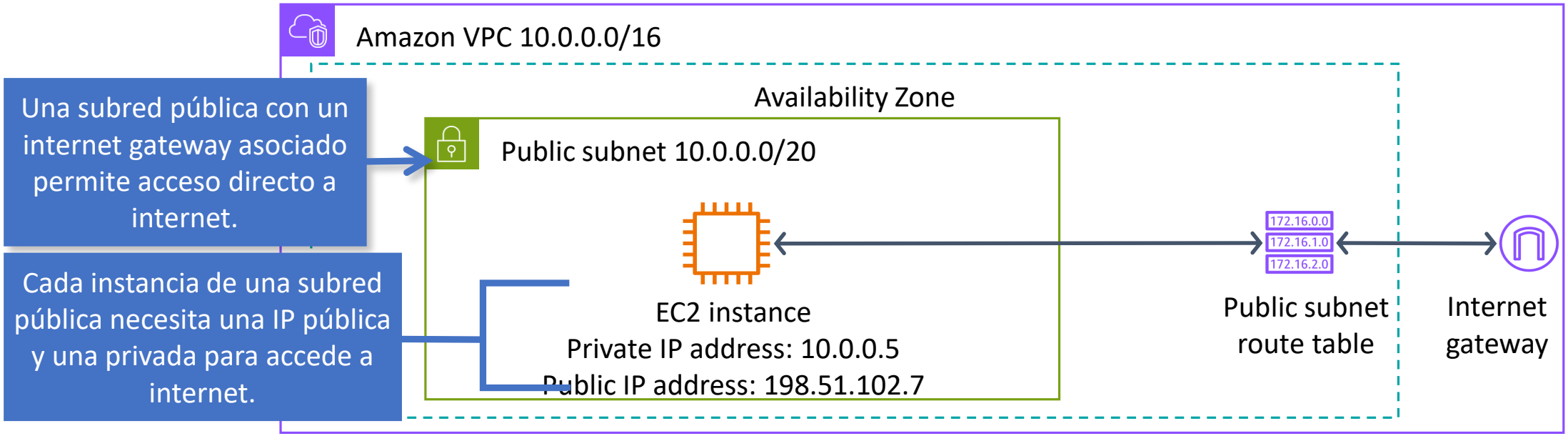
Se dimensiona mediante un rango de direcciones IP privadas: bloque CIDR (Classless Inter-Domain Routing block)

Tabla de rutas principal



Main VPC route table	
Destination	Target
10.0.0.0/16	local

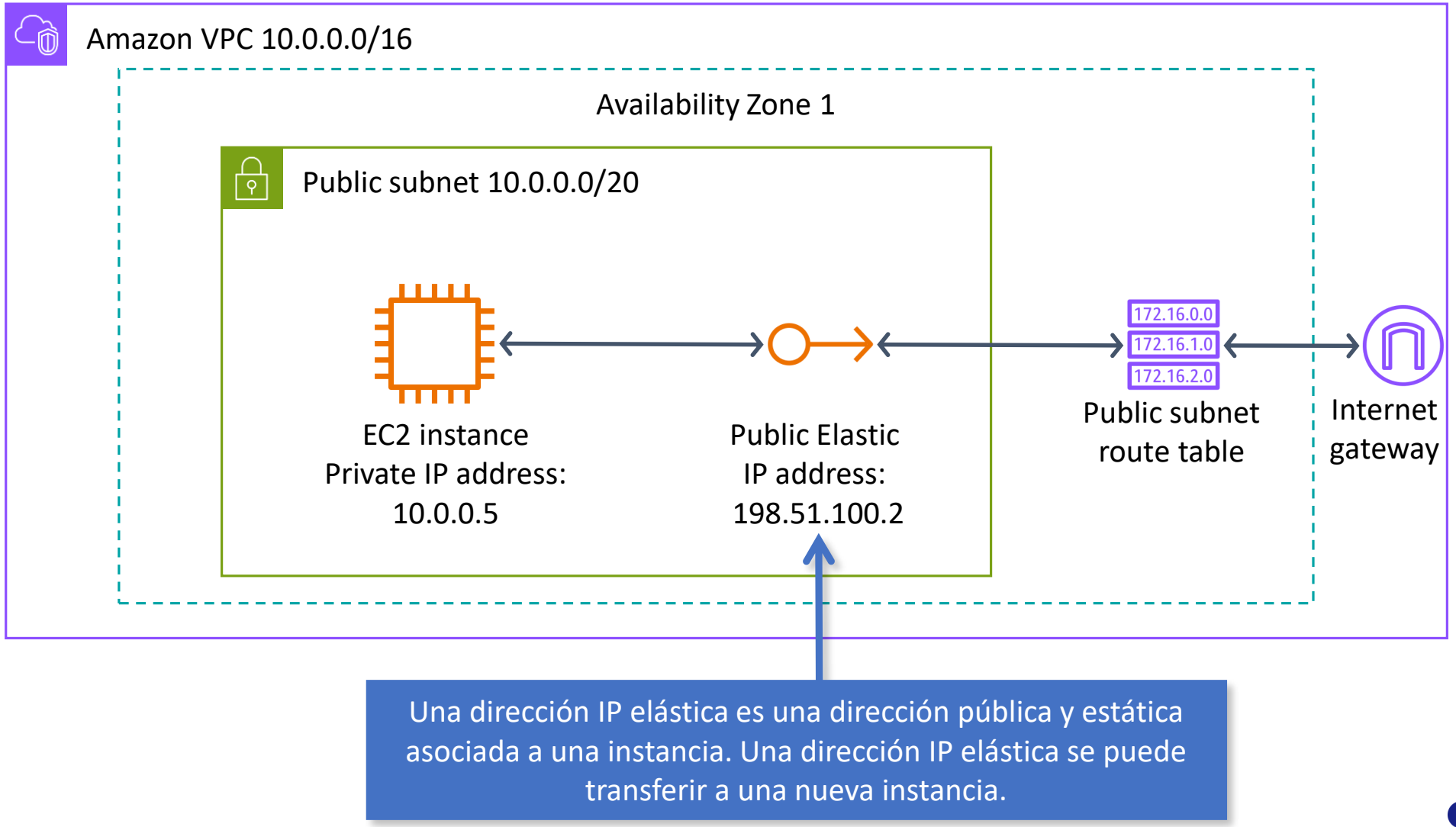
Subredes públicas



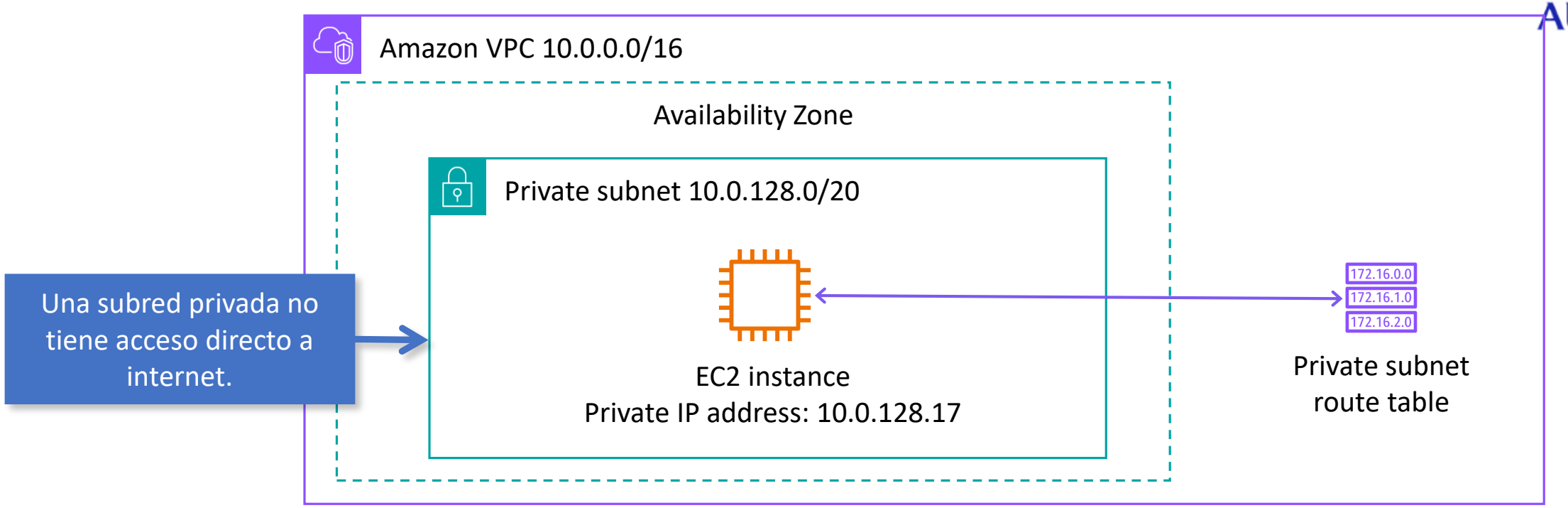
Main VPC route table	
Destination	Target
10.0.0.0/16	local

Public subnet route table	
Destination	Target
10.0.0.0/16	local
0.0.0.0/0	Internet gateway ID

Direcciones IP elásticas



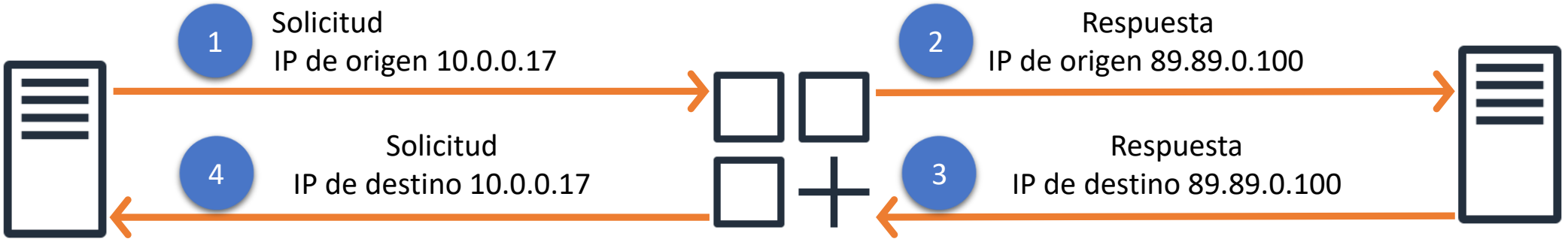
Subredes privadas



Main VPC route table	
Destination	Target
10.0.0.0/16	local

Private subnet route table	
Destination	Target
10.0.0.0/16	local

NAT IP mapping



Servidor de origen
Private IP: 10.0.0.17

Dispositivo NAT
Public IP: 89.89.0.100

Servidor de destino
Public IP: 190.50.20.87

Conexión de subredes privadas a internet

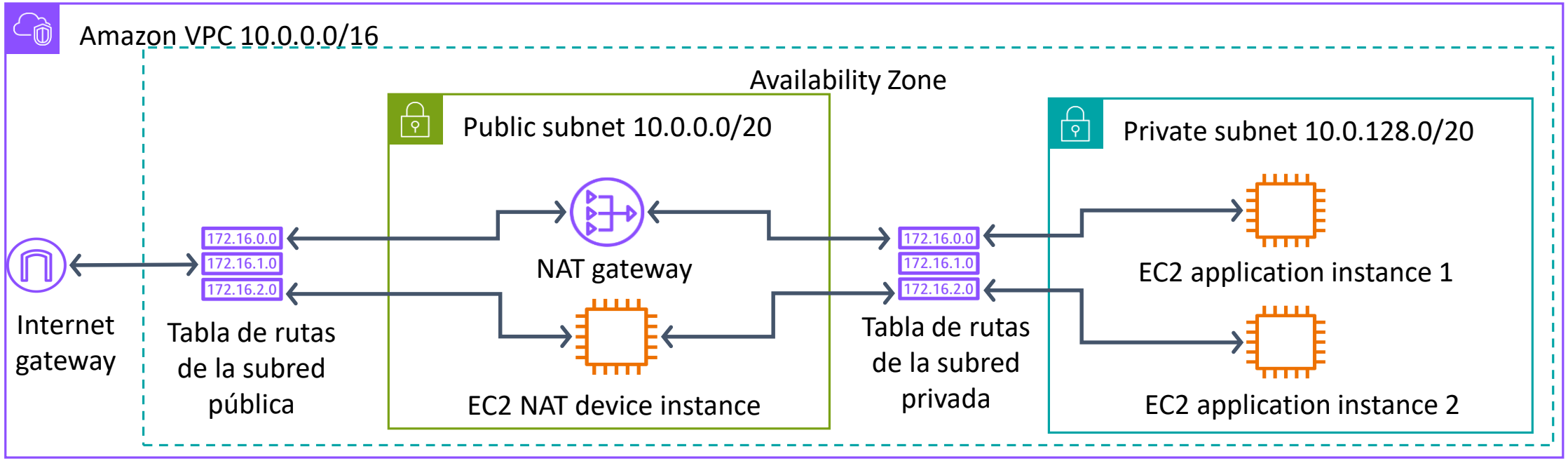


Tabla de rutas de la subred pública	
Destino	Objetivo
10.0.0.0/16	local
0.0.0.0/0	Internet gateway ID

Tabla de rutas de la subred privada	
Destino	Objetivo
10.0.0.0/16	local
0.0.0.0/0	NAT gateway ID

Actividad

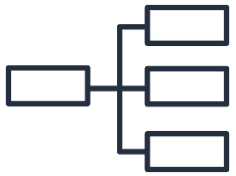
Selección de subredes

UNIVERSIDAD AUSTRAL

Actividad

Consigna

¿En qué subred se implementa cada uno de estos servicios?



Instancias que ejecutan procesos batch

Un NAT gateway o una instancia NAT

Instancias que ejecutan aplicaciones web

Instancias de bases de datos

Actividad

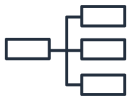
Consigna

¿En qué subred se implementa cada uno de estos servicios?

Instancias de bases de datos → Subred privada

Un NAT gateway o una instancia NAT → Subred privada

Instancias que ejecutan aplicaciones web → Pública o privada



Instancias que ejecutan procesos batch → Subred pública

Resumen

Una VPC es una red virtual, aislada lógicamente, definida por código.

Una subred pública con un internet Gateway brinda acceso a internet.

Una subred privada no tiene acceso directo a internet.

Un NAT Gateway permite que los recursos de una subred privada se conecten a internet.

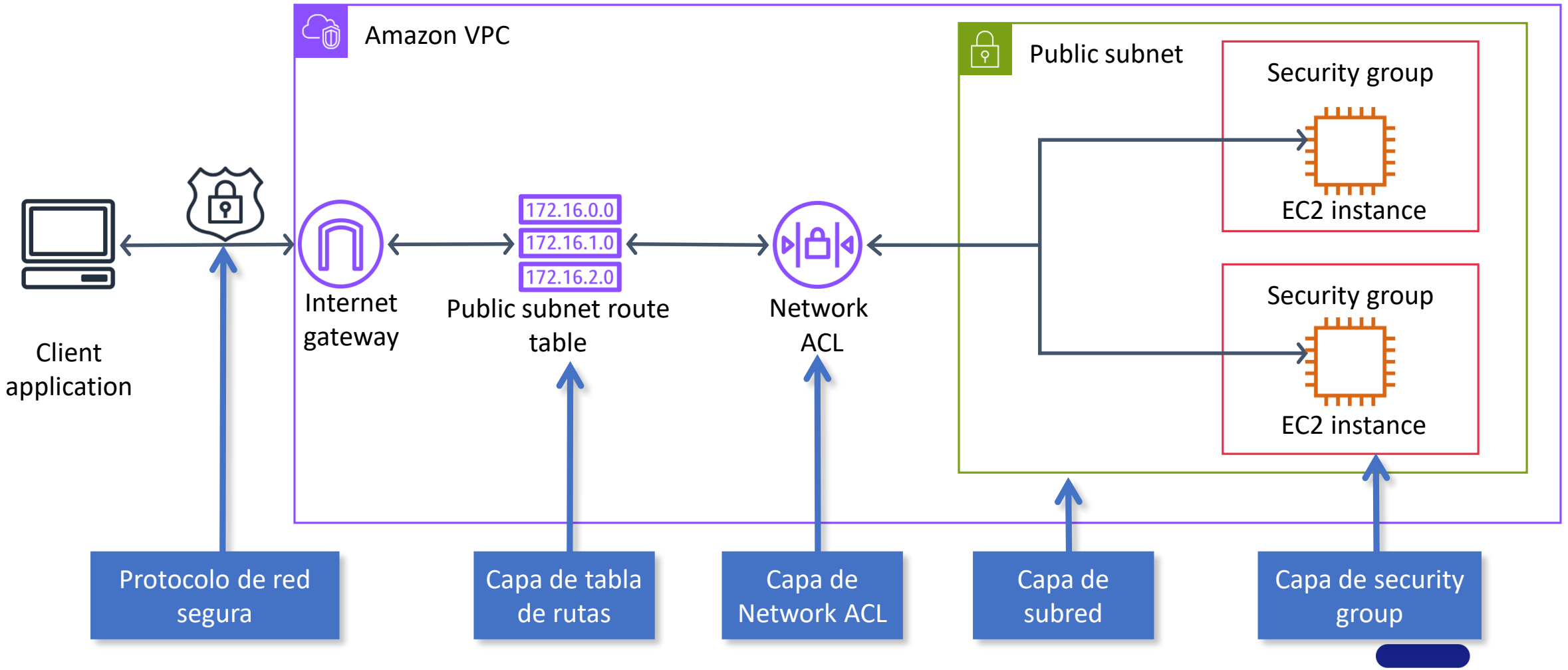
Las IP elásticas son direcciones estáticas, que se pueden transferir de una instancia a otra.

Recursos de red

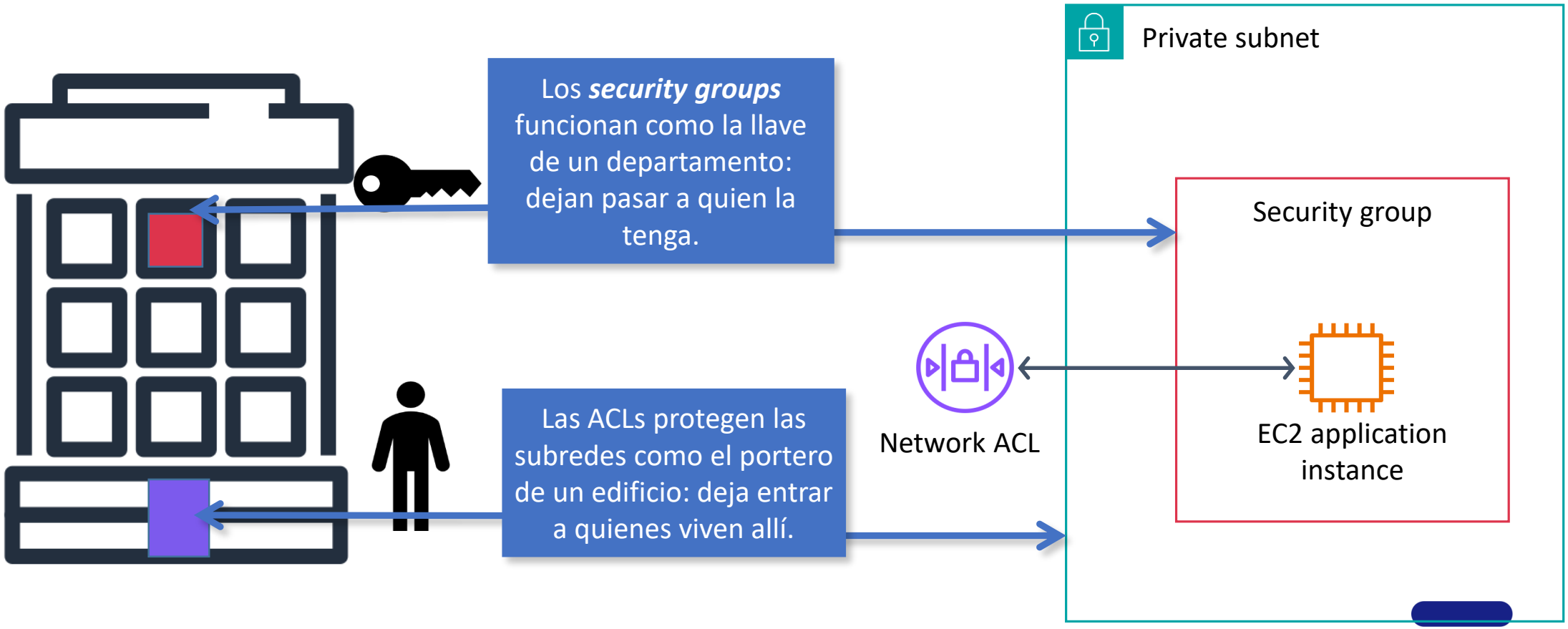
Seguridad

UNIVERSIDAD AUSTRAL

Capas de seguridad de defensa



Security groups y ACLs



Security groups

Son *stateful*.

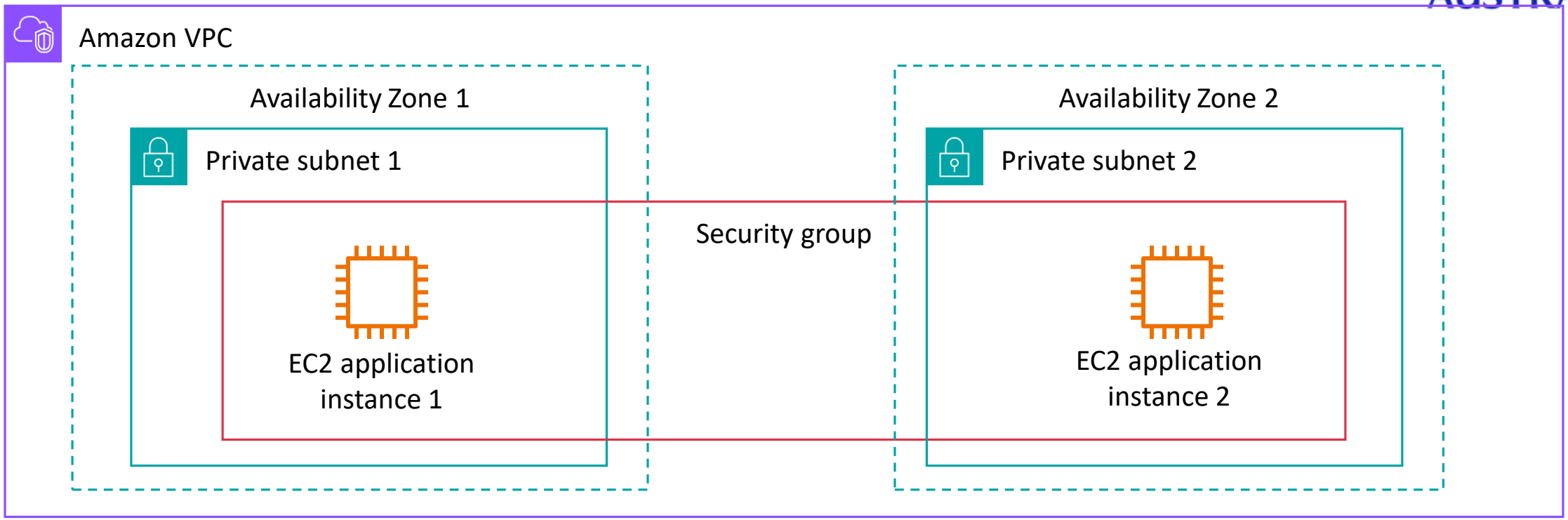
Actúan al nivel de una instancia o una interfaz de red.

Se pueden aplicar en múltiples AZ.

Se definen reglas para permitir tráfico, protocolos y rangos de puertos.

Los recursos que tienen los mismos requisitos de seguridad ***deberían*** asociarse al mismo security group.

Grupos de seguridad

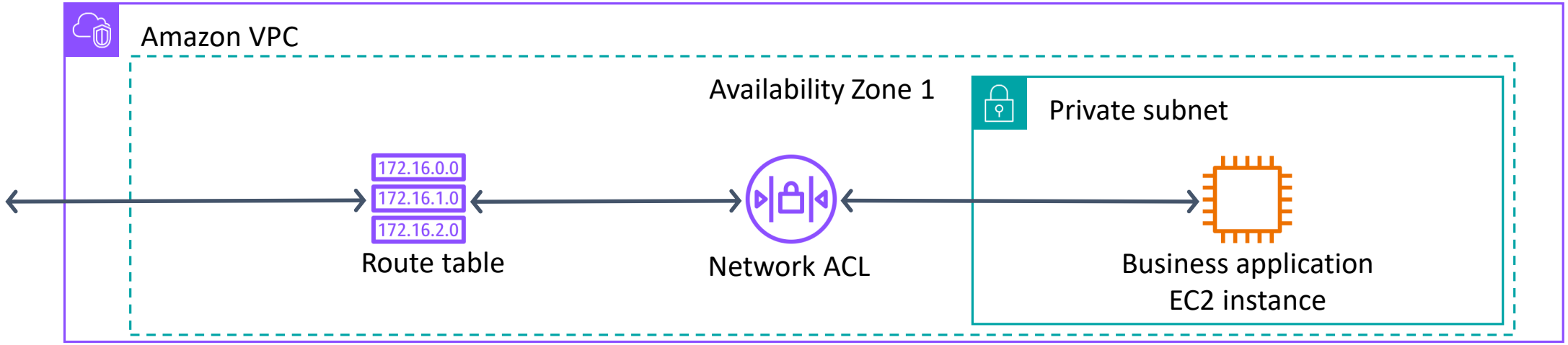


Inbound security group rule			
Source	**Traffic type**	**Protocol**	**Port range**
Load balancer security group ID	HTTPS	TCP	443

Network ACLs

- Funcionan como firewalls ***stateless***
- Controlan el tráfico entrante y saliente de una o más ***subredes***
- Una subred puede tener una única ACL
- Una ACL se puede aplicar a varias subredes
- Las reglas entrantes y salientes pueden permitir o denegar el tráfico
- Deniegan por *default* el tráfico no incluido en otras reglas

Network ACL



Rule number	Source	Traffic type	Protocol	Port range	Deny or allow
Inbound ACL rules					
100	188.7.55.9/32	HTTPS	TCP	443	Allow
*	0.0.0.0/0	All traffic	All	All	Deny

Outbound ACL rules					
100	0.0.0.0/0	HTTPS	TCP	443	Allow
*	0.0.0.0/0	All traffic	All	All	Deny

Network ACLs

- Funcionan como firewalls ***stateless***
- Controlan el tráfico entrante y saliente de una o más ***subredes***
- Una subred puede tener una única ACL
- Una ACL se puede aplicar a varias subredes
- Las reglas entrantes y salientes pueden permitir o denegar el tráfico
- Deniegan por *default* el tráfico no incluido en otras reglas

Network ACL vs Security groups

Security groups	Network ACLs
Operan a nivel de recursos	Opera a nivel de la subred
Permiten tráfico	Especifica reglas que *permiten* o *deniegan* tráfico
Las reglas son *stateful*	Las reglas son *stateless*.
Se evalúan todas las reglas	Las reglas se evalúan en orden. La evaluación termina cuando se aplica una regla
Ningún tráfico entrante está permitido por *default*	Todo el tráfico entrante está permitido por *default*
Todo el tráfico saliente está permitido por *default*	Todo el tráfico saliente está permitido por *default*

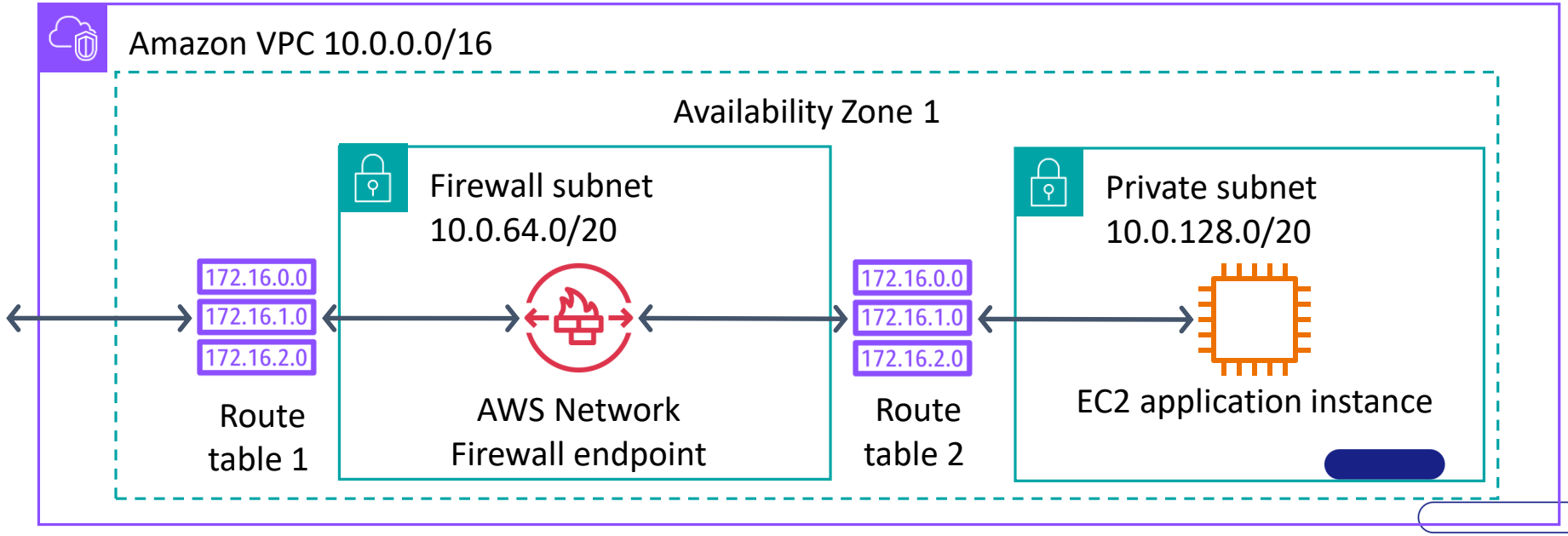
El tráfico de respuesta se permite automáticamente.

Se aplican las reglas de las ACL al tráfico de respuesta

Firewalls de red

Brinda funciones de firewall de red y servicio de IDS/IPS

Para proteger los recursos de una subred, se puede dirigir el tráfico externo a través de un AWS Network Firewall

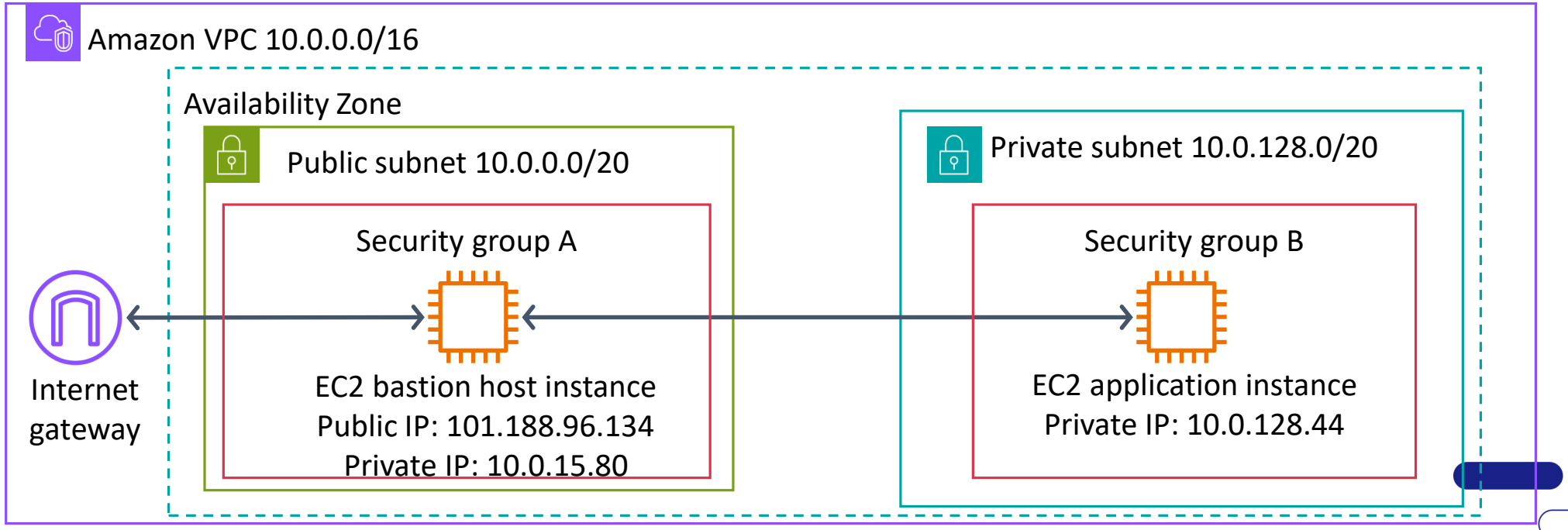


Administración de recursos

Bastion hosts

Security Group A inbound rule			
Source	Type	**Protocol**	Port range
IP address range	SSH	TCP	22

Security Group B inbound rule			
Destination	**Traffic type**	Protocol	Port range
Security group A	SSH	TCP	22



Resumen

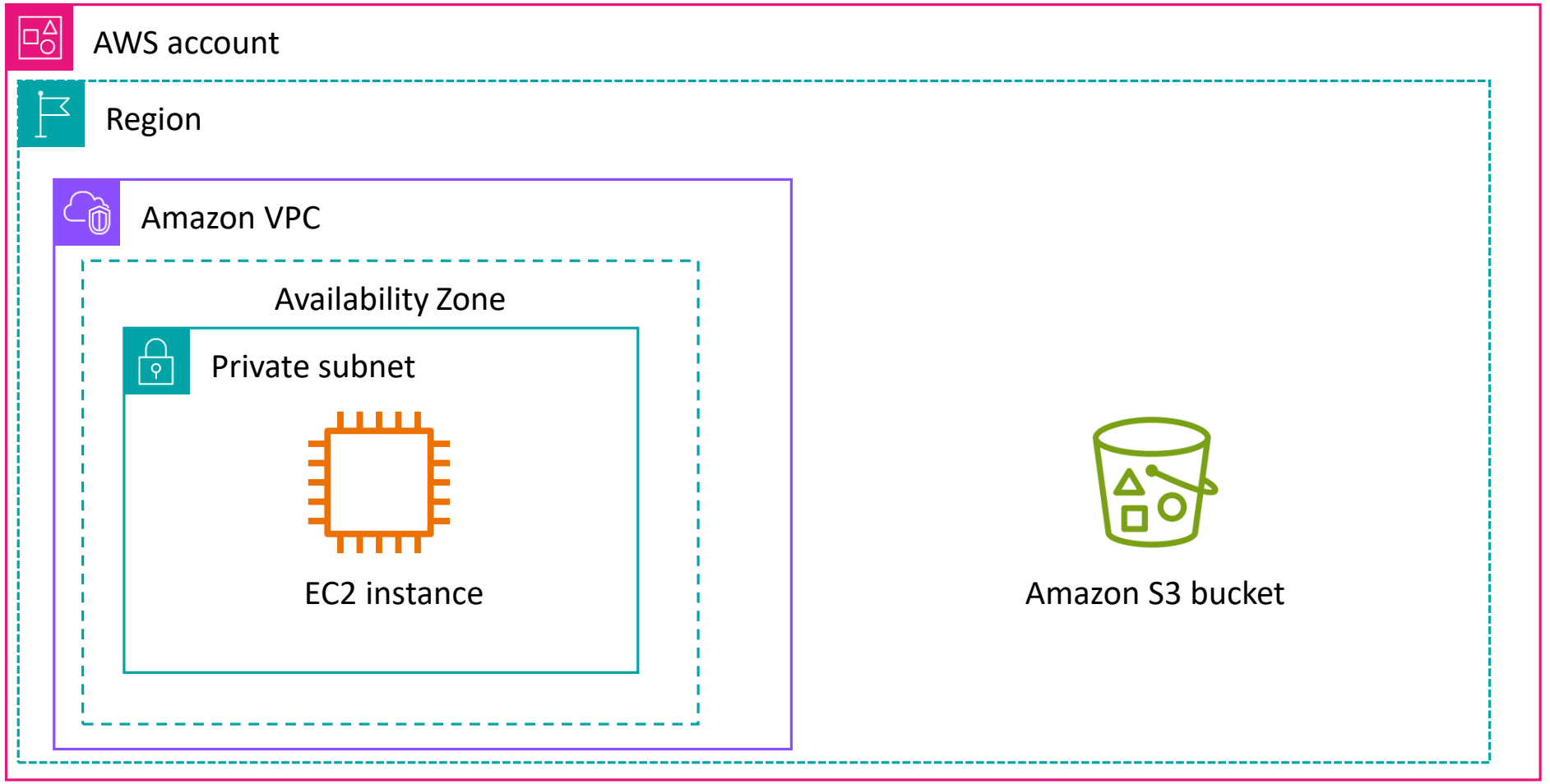
- Infraestructura segura de AWS con múltiples capas de defensa.
- Un grupo de seguridad en una VPC especifica el tráfico permitido hacia o desde los recursos de AWS. Es un grupo *stateful*.
- Una ACL de red permite o deniega tráfico entrante o saliente específico a nivel de subred. No tiene estado.
- El tráfico de VPC externo se rutea a través de AWS Network Firewall para agregar una capa adicional de seguridad del tráfico.
- Los *host* bastión se utilizan para administrar recursos de subred privada desde un entorno local.

Conexión a servicios administrados de AWS

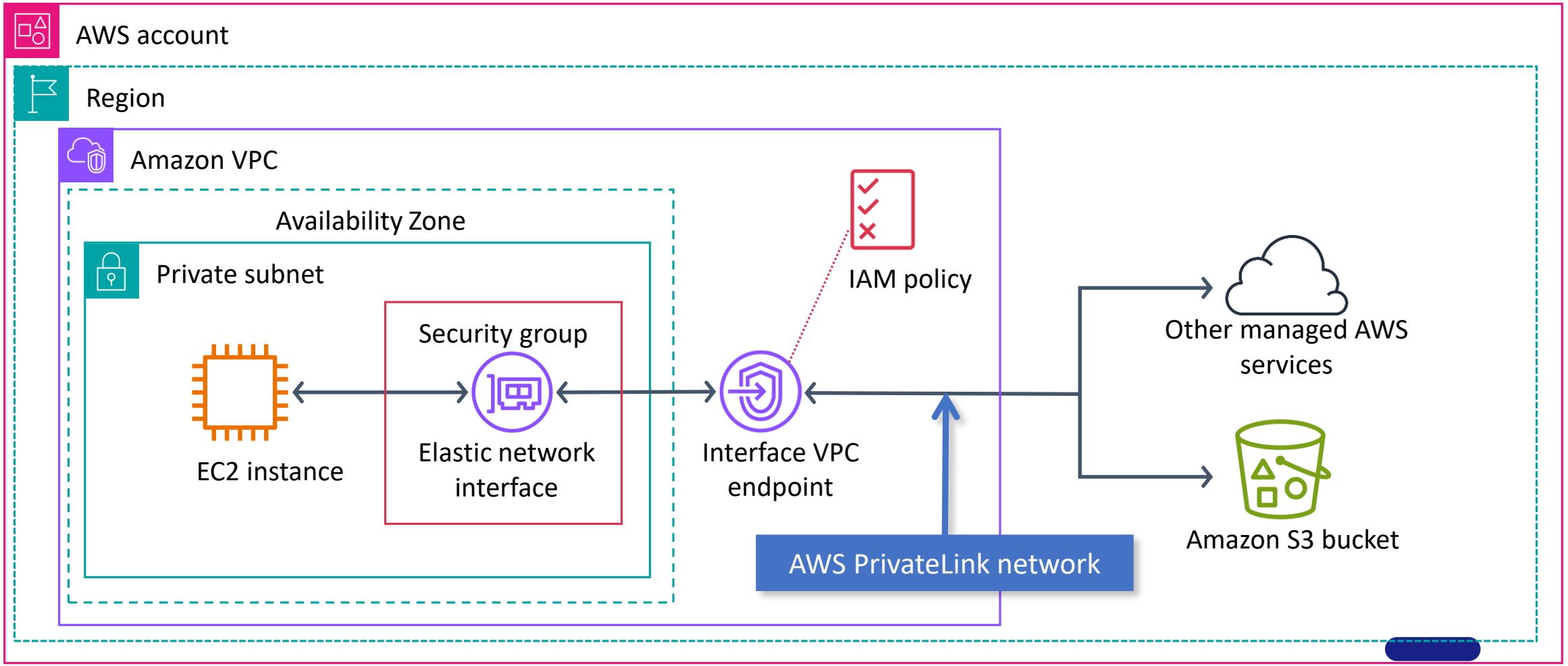
Creación de un entorno de red

UNIVERSIDAD AUSTRAL

Conexión a recursos gestionados

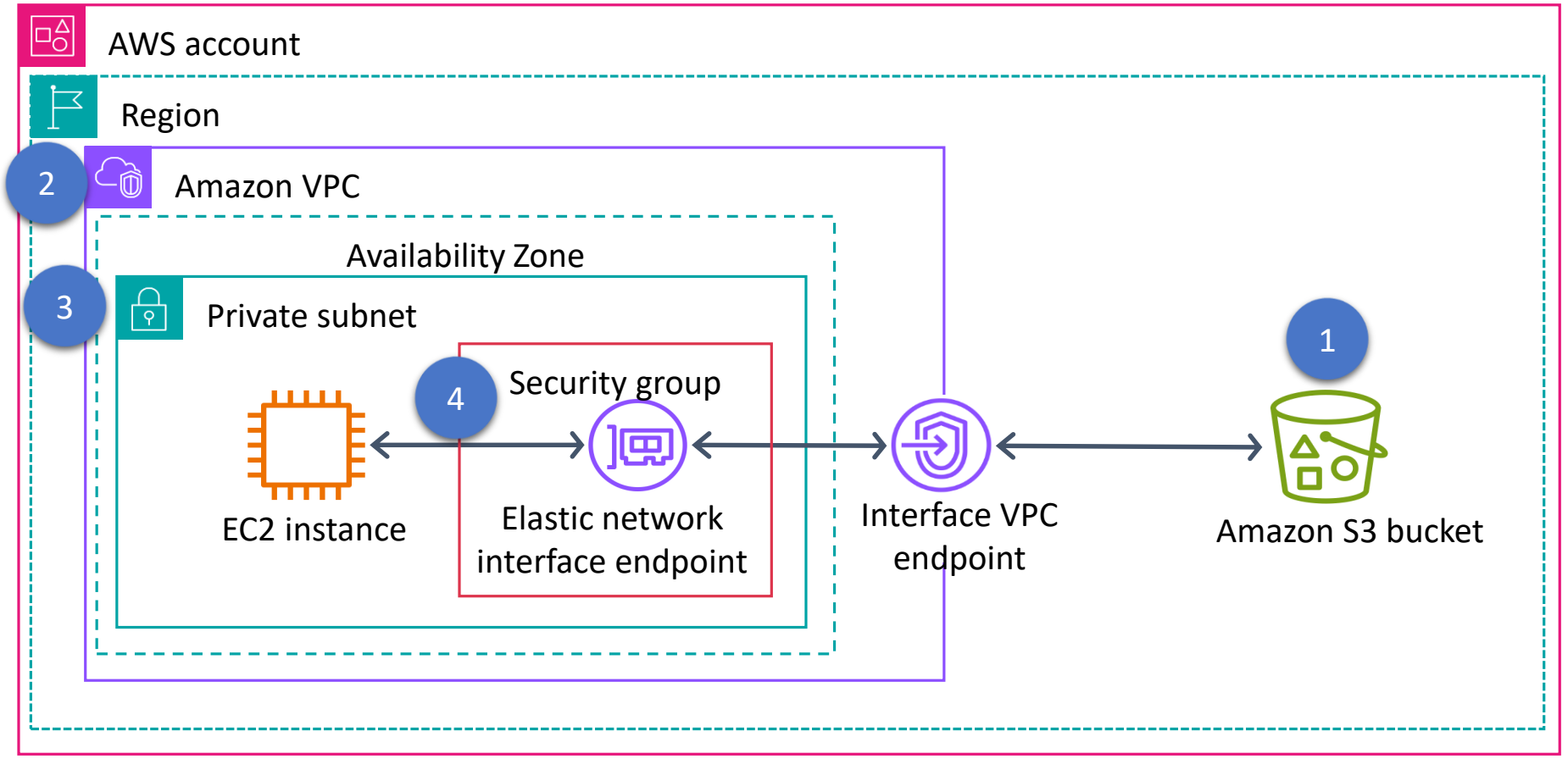


Endpoints de interface VPC



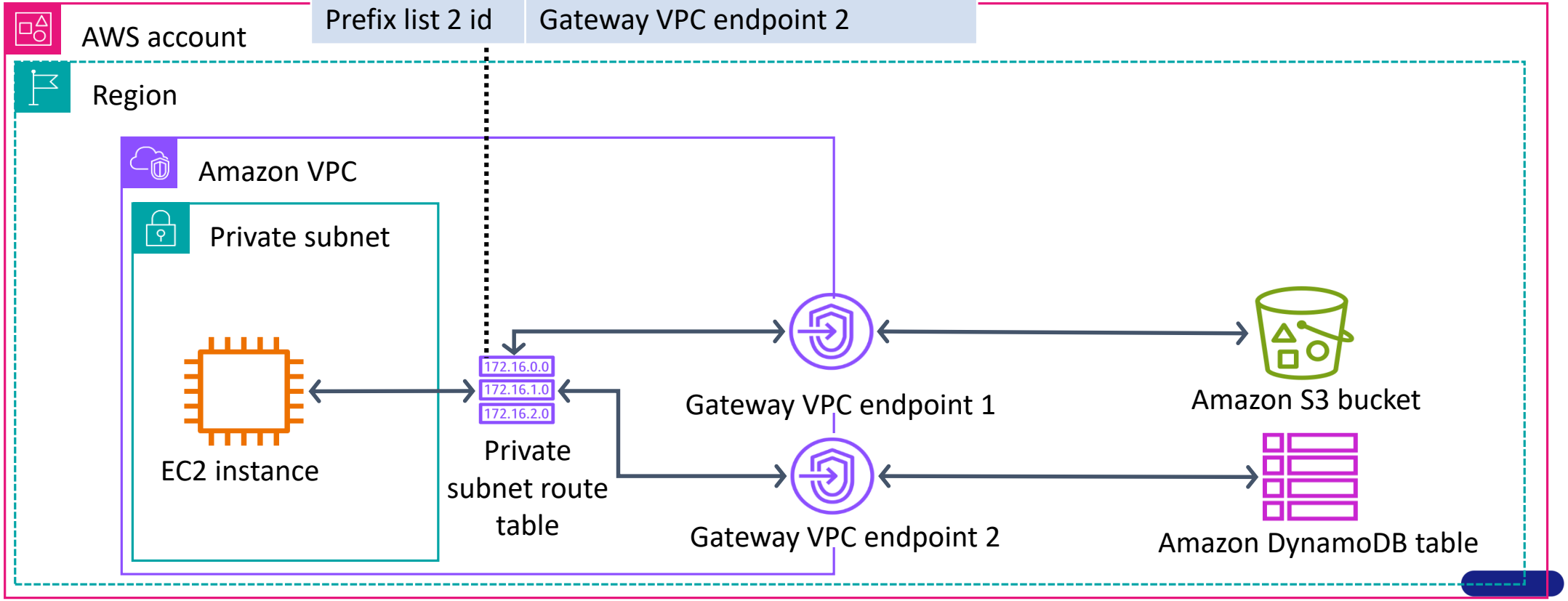
Endpoints de interface VPC

Configuración



Gateway VPC endpoints

Tablas de rutas de redes privadas	
Destino	Objetivo
Prefix list 1 id	Gateway VPC endpoint 1
Prefix list 2 id	Gateway VPC endpoint 2

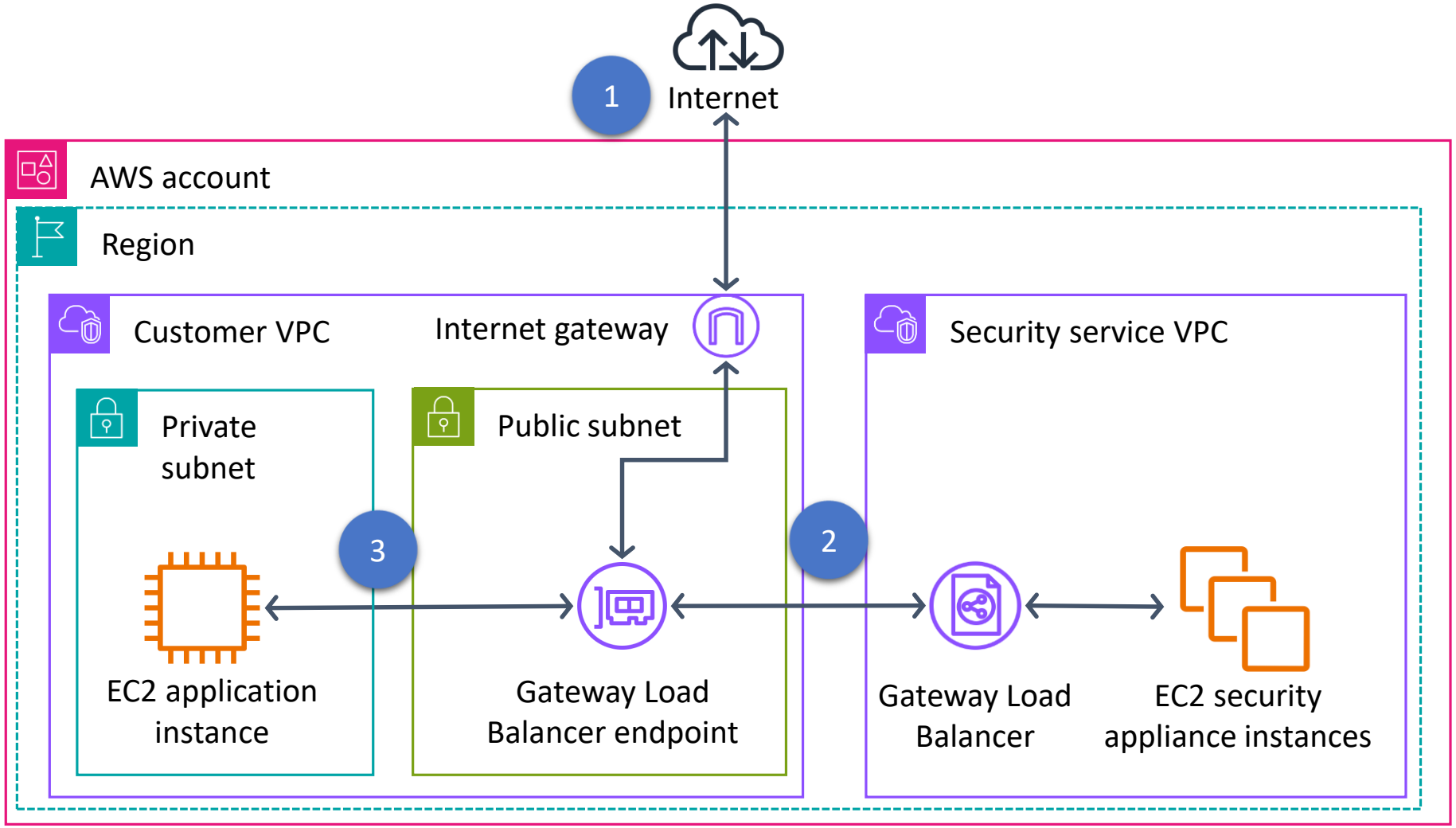


Gateway VPC endpoints

Factor	Endpoints de Interface VPC	Endpoints de Gateway VPC
Amazon S3 access point	IP Privada de una subred en una VPC	IP públicas de Amazon S3
On-premises	Permite conectarse	No
Otra región de AWS	Permitido	No
Costo	Tiene costo	Sin costo
Ancho de banda	Hasta 10 Gbps por AZ Escala automáticamente hasta 100 Gbps.	Sin límite
Tamaño del paquete	Máximo: 8500 bytes.	Sin límite

Gateway Load Balancer

Endpoints



Conexión de servicios gestionados

Resumen

- Los recursos de VPC pueden acceder a los servicios administrados de AWS mediante *endpoints* de VPC.
- Un *endpoint* utiliza AWS PrivateLink para acceder a los servicios administrados de AWS. Esto genera costos y presenta limitaciones de rendimiento.
- Un Gateway VPC *endpoint* se integra directamente con Amazon S3 y Amazon DynamoDB. No genera costos ni tiene limitaciones de rendimiento.
- Los *endpoints* de Gateway Load Balancer se utilizan con Gateway Load Balancers para inspeccionar el tráfico con dispositivos de seguridad.

Monitoreo de red

Otras consideraciones

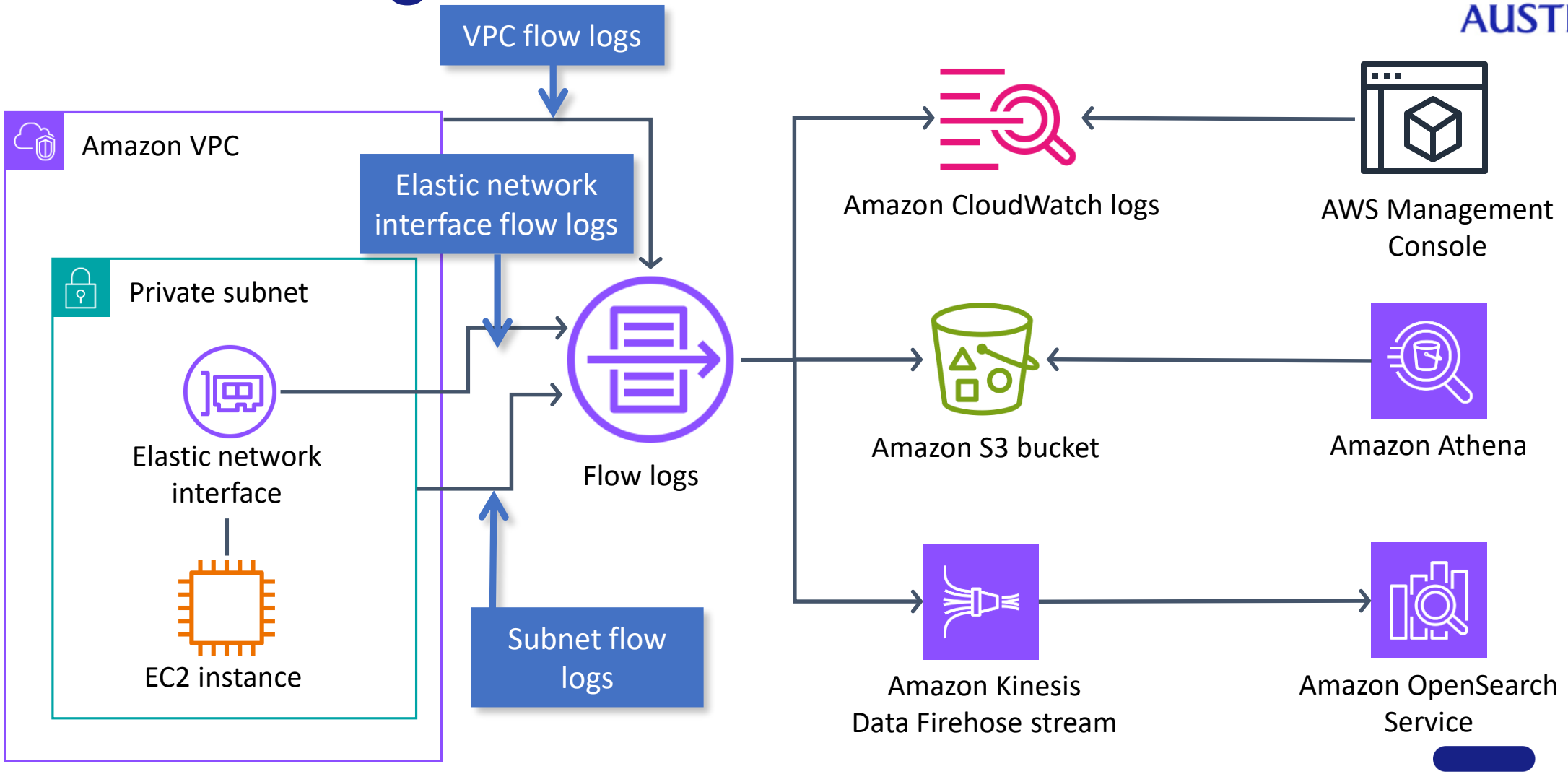
UNIVERSIDAD AUSTRAL

Resolución de problemas de red

Escenarios

- Tiempos de respuesta muy lentos en instancias EC2
- Imposibilidad de acceso a través de SSH
- No se aplican parches a las instancias de base de datos de EC2

VPC Flow logs



Permisos sobre flow logs

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateFlowLogs",
        "ec2:DescribeFlowLogs",
        "ec2:DeleteFlowLogs"
      ],
      "Resource": "*"
    }
  ]
}
```

La política de IAM otorga a los usuarios permisos para crear, describir y eliminar registros de flujo.

Ejemplo de flow log (1 de 2)

Field name	Field description	Example value
version	Versión de los registros de flujo de VPC	2
account-id	Cuenta de AWS del propietario de la red	123456789010
interface-id	Interfaz de red de tráfico	eni-1235b8ca123456789
srcaddr	Dirección de origen para el tráfico entrante o interfaz de dirección de red para el tráfico saliente	172.31.16.139
dstaddr	Dirección de destino para el tráfico saliente o dirección de interfaz de red para el tráfico entrante	172.31.16.21
srcport	Puerto de origen del tráfico	20641
dstport	Puerto de destino del tráfico	22
protocol	Número de protocolo de IANA de tráfico	6 (TCP)

Ejemplo de flow log (2 de 2)

Field name	Field description	Example value
packets	Cantidad de paquetes transferidos	20
bytes	Cantidad de bytes transferidos	4249
start	Tiempo Unix en segundos del primer paquete recibido	1418530010
end	Tiempo Unix en segundos del último paquete recibido	1418530070
action	Aceptar o rechazar el indicador de éxito o fracaso del enrutamiento del tráfico	ACCEPT
log-status	Estado del registro de flujo: OK, NODATA, SKIPDATA	OK

Resolución de problemas en VPC

Otras herramientas

Reachability Analyzer

Permite probar la conectividad entre un recurso de origen y un recurso de destino en una VPC.

Network Access Analyzer

Identificar accesos de red no deseados a los recursos de AWS.

Traffic Mirroring

Hace una copia del tráfico de red y la envía a soluciones de seguridad y monitoreo.

Monitoreo de red

Resumen

- VPC Flow Logs captura información sobre el tráfico de red en una VPC.
- Los registros incluyen todos los flujos dentro de un intervalo
- Reachability Analyzer permite chequear si dos recursos de una VPC tienen conectividad
- Network Access Analyzer permite identificar accesos no deseados a los recursos de una cuenta de AWS
- Traffic Mirroring permite copiar el tráfico de red y enviarlo a herramientas de seguridad y monitoreo

Well-Architected Framework

Aplicado a la red

UNIVERSIDAD AUSTRAL

Well-Architected Framework

Pilares

Reliability

Security

Performance Efficiency

Cost Optimization

Well-Architected Framework

Planificar la topología de red

Asegurarse de asignar direcciones IP para permitir la expansion de los servicios

Well-Architected Framework

Protección de la infraestructura – Protección de redes

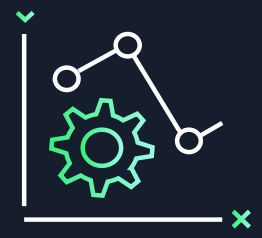
Crear capas de red

Controlar el tráfico en todas las capas.

Implementar medidas de protección e inspección

Well-Architected Framework

Performance

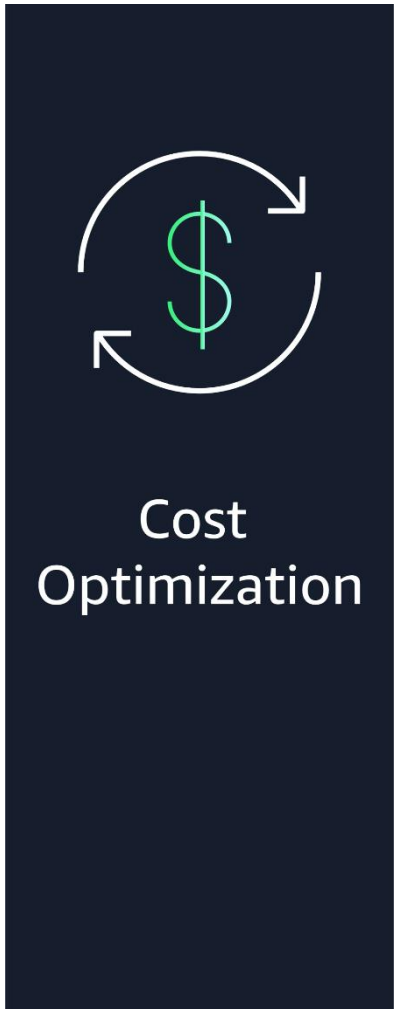


Performance efficency

- Entender el impacto de las redes en la performance
- Evaluar las funciones de red disponibles
- Elegir protocolos de red que aumenten la performance

Well-Architected Framework

Optimización de costos



Tomar en cuenta los costos para elegir las regiones

Errores en el diseño de la red

Identificar los errores de diseño de este escenario

- La empresa A, basada en Europa, vende calzado.
- La mayoría de los clientes de la compañía está en Estados Unidos.
- La compañía implementó sus servidores web y sus servidores de bases de datos en la región de AWS de Irlanda, en una única VPC con una subred pública.
- La VPC tiene una *netmask* de /27 con 32 direcciones IP. La subred tiene una *netmask* de /28 con 16 direcciones IP disponibles.
- El grupo de seguridad de los servidores web y de base de datos permite tráfico de internet hacia los servidores.
- La compañía A proyecta un rápido crecimiento en el futuro cercano.

Errores en el diseño de la red

Identificar los errores de diseño de este escenario

Patrones	Antipatrones
VPC grandes con subredes públicas y privadas grandes	VPC pequeña con subredes pequeñas
Grupos de seguridad estrictos organizados en capas según el uso del servidor	Grupos de seguridad permisivos
Sin acceso directo a las bases de datos	Acceso directo a bases de datos
Región de AWS cercana a los clientes	Región de AWS lejos de los clientes

Café Web

Challenge

UNIVERSIDAD AUSTRAL

Café Challenge

Resumen

En este laboratorio, harás lo siguiente:

- Asegurar el servidor de aplicaciones.
- Trasladar la instancia de la aplicación a una subred privada. Configurar un *bastion host* en una subred pública. Configurar un grupo de seguridad para cada instancia.
- Permitir que el servidor de aplicaciones descargue parches de Internet configurando una puerta de enlace NAT en la subred pública.
- Agregar reglas de Network ACL para aumentar la seguridad.

Módulo 7. Servicios de red

Resumen

- Explicar la función de una nube privada virtual (VPC) en la red en la nube de Amazon Web Services (AWS).
- Identificar los componentes de una VPC que pueden conectar un entorno de red de AWS a Internet.
- Aislar y proteger los recursos dentro de un entorno de red de AWS.
- Crear y monitorear una VPC con subredes, un Internet Gateway, tablas de rutas y security groups.
- Aplicar los principios de AWS Well-Architected Framework a la planificación y creación de un entorno de red.

Muchas gracias.

www.austral.edu.ar

UNIVERSIDAD AUSTRAL