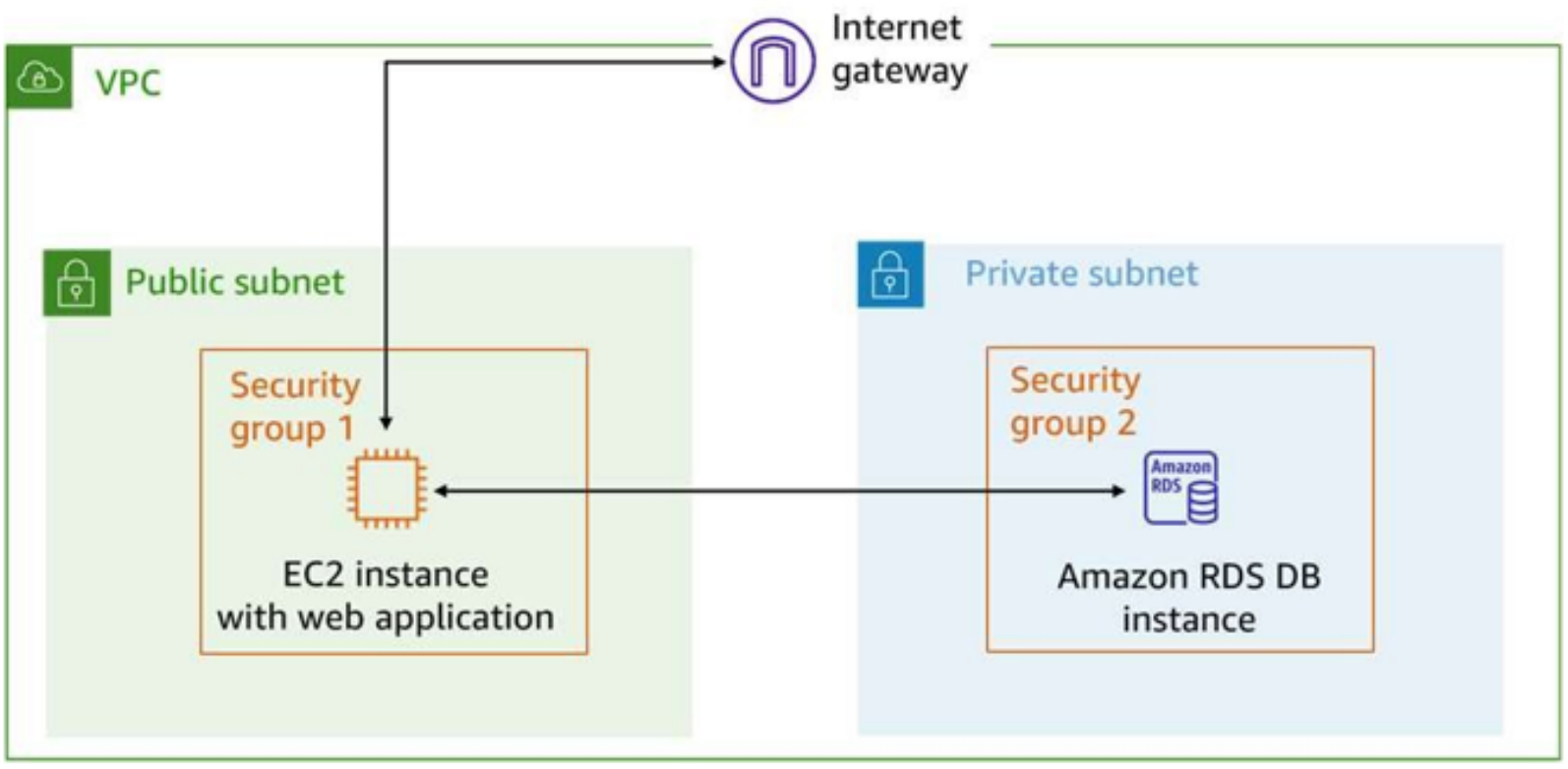
LECCIÓN 4: USO DE GRUPOS DE SEGURIDAD DE AWS Y USO DE ACL DE RED DE AWS

En esta lección se proporciona información sobre el uso de grupos de seguridad como parte de la seguridad de su infraestructura y el uso de listas de control de acceso a la red (ACL) como parte de la protección de su infraestructura.

Grupos de seguridad (1 de 2)



El diagrama de una VPC con una subred pública y otra privada. La subred pública contiene una instancia de EC2 que está protegida por el grupo de seguridad 1. La subred privada contiene una instancia de base de datos de Amazon Relational Database Service (Amazon RDS) protegida por el grupo de seguridad 2. Se permite la comunicación entre los dos grupos de seguridad, e Internet puede comunicarse con el grupo de seguridad 1.

Un grupo de seguridad actúa como un firewall virtual para una instancia de EC2 y controla el tráfico entrante y saliente de la instancia. Los grupos de seguridad funcionan al nivel de la instancia, no al nivel de la subred. Por lo tanto, cada instancia en la subred de VPC puede ser asignada a distintos conjuntos de grupos de seguridad.

En el nivel más básico, un grupo de seguridad es una forma de filtrado del tráfico hacia las instancias.

Grupos de seguridad (2 de 2)

- Los grupos de seguridad tienen reglas que controlan el tráfico de entrada y de salida de la instancia.
- De forma predeterminada, los grupos de seguridad deniegan todo el tráfico entrante y permiten todo el tráfico saliente. Esto se considera *con estado.*

Entrada

Origen	Protocolo	Intervalo de puertos	Descripción
sg-xxxxxxxx	Todos	Todos	Permite el tráfico de entrada de las interfaces de red asignadas al mismo grupo de seguridad.

Salida

Destino	Protocolo	Intervalo de puertos	Descripción
0.0.0.0/0	Todos	Todos	Permite todo el tráfico IPv4 de salida.
::/0	Todos	Todos	Permite todo el tráfico IPv6 de salida.

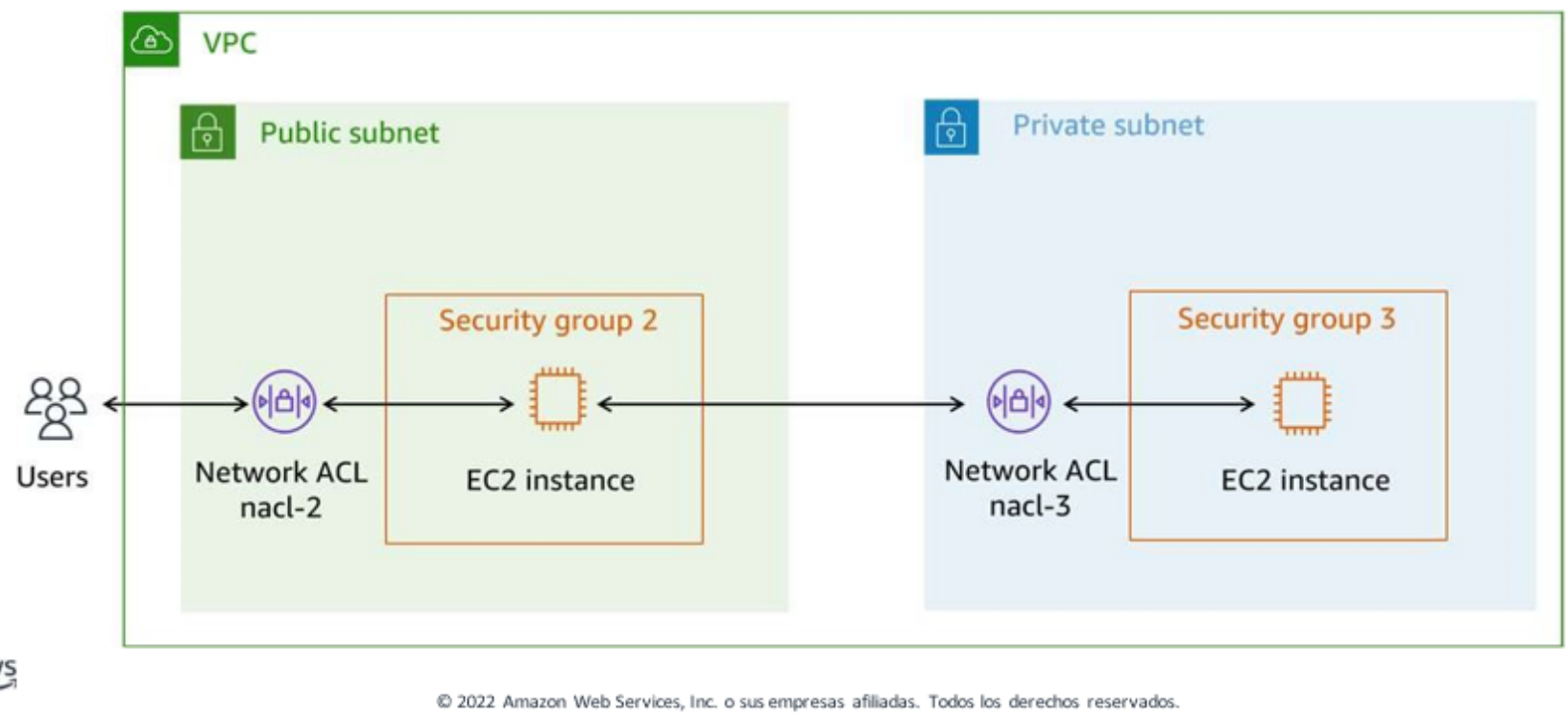
Cuando se crea un grupo de seguridad, este no tiene ninguna regla de entrada. Por lo tanto, el tráfico entrante que se origina desde otro host a su instancia no está permitido hasta que agregue reglas de entrada al grupo de seguridad.

De forma predeterminada, un grupo de seguridad incluye una regla de salida que permite todo el tráfico saliente. Puede quitar la regla y agregar reglas de salida que solo permitan tráfico saliente específico. Si un grupo de seguridad no tiene ninguna regla de salida, el tráfico saliente que se origina en su instancia no está permitido.

Los grupos de seguridad son grupos con estado, lo que significa que la información de estado se mantiene incluso después de procesar una solicitud. Entonces, si envía una solicitud desde su instancia, se permite el tráfico de respuesta para esa solicitud para que fluya independientemente de las reglas de grupo de seguridad de entrada. Las respuestas para permitir el tráfico entrante se encuentran permitidas a fin de circular, independientemente de las reglas de salida.
Todas las reglas se evalúan antes de decidir si se permite el tráfico.

En las tablas de la diapositiva, se indica que el tráfico entrante está permitido desde cualquier interfaz de red asignada al mismo grupo de seguridad. Se permite todo el tráfico de salida.

Para más información, consulte Control Traffic to Resources Using Security Groups (Control del tráfico a los recursos mediante grupos de seguridad) en la Guía del usuario sobre Amazon VPC en https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html



El diagrama que muestra cómo funcionan las ACL de red. Una VPC contiene una subred pública y una subred privada. Cada subred contiene una instancia de EC2. Una ACL de red en cada subred controla el tráfico hacia las instancias y desde estas.

Una lista de control de acceso a la red (ACL) es una capa opcional de seguridad para su VPC. Una ACL de red actúa como un firewall para controlar el tráfico que entra y sale de una o varias subredes. Para agregar otra capa de seguridad a su VPC, puede configurar ACL de red con reglas similares a las de su grupo de seguridad.

Cada subred en su VPC se debe asociar a una ACL de red. Si no asocia una subred de forma explícita a una ACL de red, la subred se asociará de forma automática a la ACL de red predeterminada. Puede asociar una ACL de red a varias subredes; sin embargo, una subred se puede asociar sólo a una ACL de red por vez. Cuando se asocia una ACL de red a una subred, se elimina la asociación anterior.

Comparar grupos de seguridad y ACL de red

Atributo	Grupos de seguridad	ACL de red
Alcance	Nivel de instancia o interfaz	Nivel de subred
Reglas admitidas	Solo reglas de permiso	Reglas de permiso y de denegación
Estado	Con estado (el tráfico de retorno se permite automáticamente, independientemente de las reglas)	Sin estado (el tráfico de retorno debe estar explícitamente permitido por reglas)
Orden de las reglas	Se evalúan todas las reglas antes de decidir si se permite el tráfico	Las reglas se evalúan por orden numérico antes de tomar la decisión de permitir el tráfico

A continuación, se resumen las diferencias entre los grupos de seguridad y las ACL de red:

Los grupos de seguridad actúan a nivel de instancia o interfaz, pero las ACL de red actúan a nivel de subred.

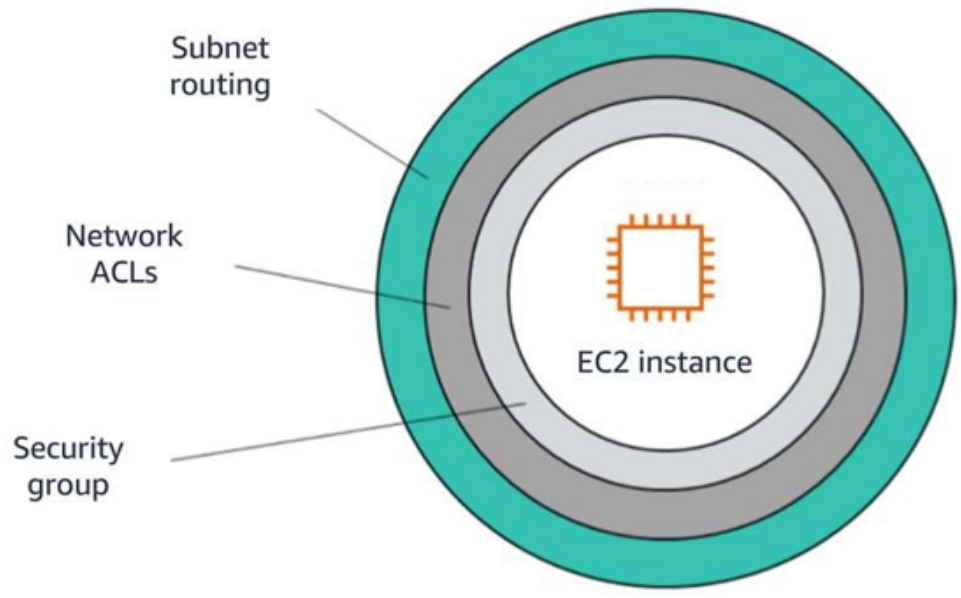
Los grupos de seguridad solo admiten reglas de permiso, pero las ACL de red admiten tanto reglas de permiso como de denegación.

Los grupos de seguridad tienen estado, pero las ACL de red no.

Para los grupos de seguridad, se evalúan todas las reglas antes de tomar la decisión de permitir el tráfico. En las ACL de red, las reglas se evalúan por orden numérico antes de tomar la decisión de permitir el tráfico.

Características de seguridad de VPC

- Grupos de seguridad
- ACL de red
- Subredes
- Tablas de enrutamiento



Nota: VPC Flow Logs puede registrar la actividad hasta el nivel de interfaz.

La instancia de EC2 está rodeada de capas de seguridad. La capa más cercana a la instancia es un grupo de seguridad. La siguiente capa son las ACL de red. La capa exterior, y más alejada, es el enrutamiento de subredes.

Entre las funciones de seguridad de la VPC se incluyen las siguientes:

Los grupos de seguridad funcionan como firewalls virtuales de sus instancias de EC2 para controlar el tráfico entrante y saliente.

Las ACL de red proporcionan una capa opcional de seguridad para su VPC. Actúan como firewalls para controlar el tráfico que entra y sale de una o varias subredes.

Las subredes hacen que las redes sean más eficientes. Mediante la subred, el tráfico de red puede recorrer una distancia más corta sin pasar por enrutadores innecesarios para llegar a su destino.

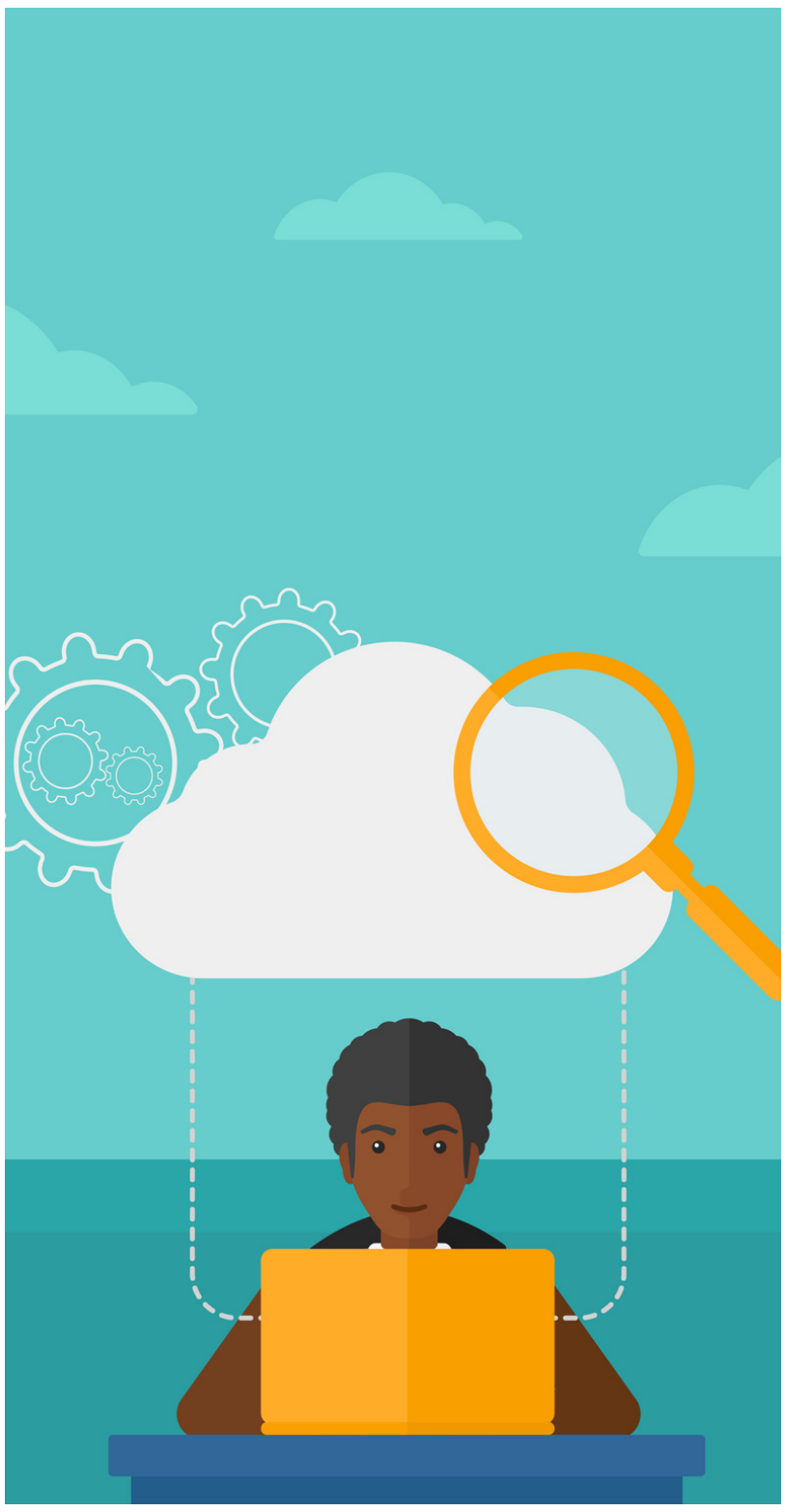
Las tablas de enrutamiento controlan a dónde se dirige el tráfico de la red.

Con la función VPC Flow Logs, puede capturar información sobre el tráfico IP que entra y sale de las interfaces de red de su VPC. Puede publicar datos de registro de flujo en Registros de Amazon CloudWatch o Amazon Simple Storage Service (Amazon S3). Una vez creado un registro de flujo, puede recuperar y visualizar sus datos en el destino elegido.

Puede crear un registro de flujo para una VPC, una subred o una interfaz de red. Si crea un registro de flujo para una subred o VPC, se supervisan todas las interfaces de red de dicha VPC o subred. Los datos de registro de flujo para una interfaz de red supervisada se registran como registros de flujo, que son eventos de registro que constan de campos que describen el flujo de tráfico.

Para más información, consulte Logging IP Traffic Using VPC Flow Logs (Registro de tráfico IP mediante registros de flujo de VPC) en la Guía del usuario de Amazon VPC en https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html

Estos son algunos de los aprendizajes clave de esta sección de la unidad



Una ACL de red es una capa opcional de seguridad para su VPC y actúa como un firewall para controlar el tráfico a nivel de subred.

Cada subred en su VPC se debe asociar a una ACL de red.

Las ACL de red no tienen estado, lo que significa que las respuestas para el tráfico entrante están sujetas a las reglas para el tráfico saliente, y viceversa.

Las reglas se evalúan por orden numérico antes de tomar la decisión de permitir el tráfico.