LECCIÓN 4: PROTECCIÓN DEL ENTORNO DE RED DE AWS

Grupos de seguridad

- **Representan firewall con estado que controla el tráfico entrante y saliente a los recursos de AWS.**

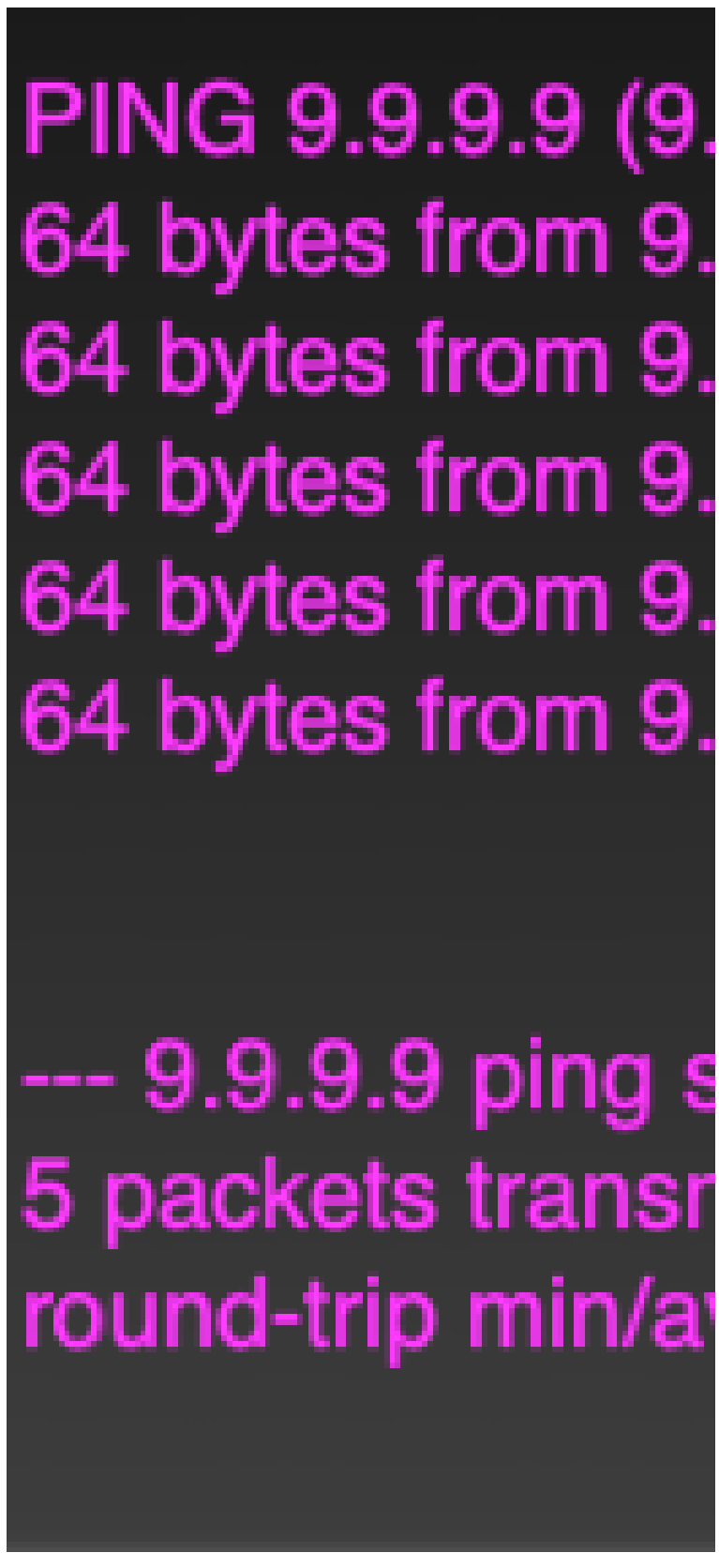
- **Funcionan en el nivel de la instancia o la interfaz de red.**

Ahora que sabe cómo diseñar e implementar un entorno de red, además de conectarlo a Internet, debe aislar sus aplicaciones y cargas de trabajo.

Puede lograr el aislamiento mediante la implementación de las instancias EC2 que alojan la aplicación o la carga de trabajo en un grupo de seguridad asociado a la VPC.

Los grupos de seguridad representan firewall con estado que actúa en el nivel de la instancia o la interfaz de red.

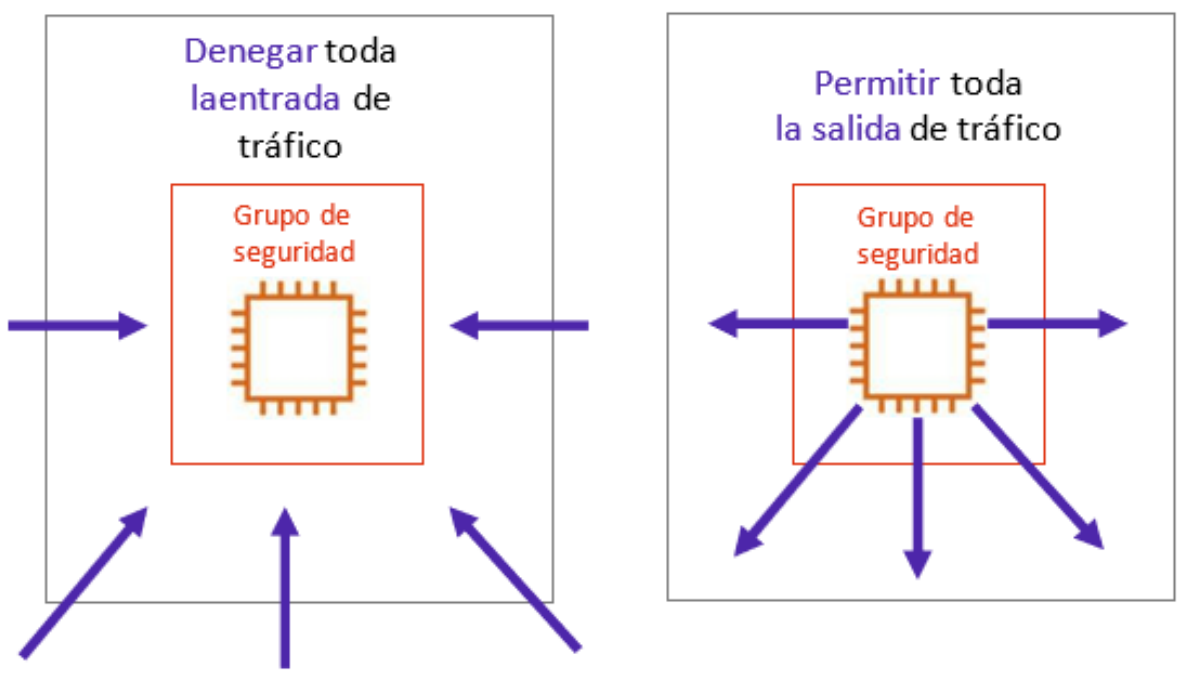
Con estado significa que el tráfico de retorno se admite de manera automática, independientemente de las reglas. Por ejemplo, supongamos que inicia un comando ping del protocolo de mensaje de control de Internet (ICMP) en la instancia desde su equipo personal. Si las reglas de entrada del grupo de seguridad permiten el tráfico de ICMP, se realiza un seguimiento de la información sobre la conexión (incluida la información del puerto). No se realiza un seguimiento del tráfico de respuesta de la instancia por el comando ping como una nueva solicitud. En cambio, se realiza un seguimiento de dicho tráfico como una conexión establecida. Está permitido el tráfico saliente de la instancia, incluso si las reglas de salida del grupo de seguridad restringen el tráfico ICMP saliente.



Las reglas del grupo de seguridad controlan el tráfico entrante y saliente correspondiente a sus recursos de AWS. Debe configurar estas reglas de manera muy estricta para restringir el
tráfico y permitir el acceso solo según sea necesario. El tráfico se puede restringir con cualquier protocolo de Internet, puerto de servicio y dirección IP de origen o destino (dirección IP individual o bloque de CIDR).

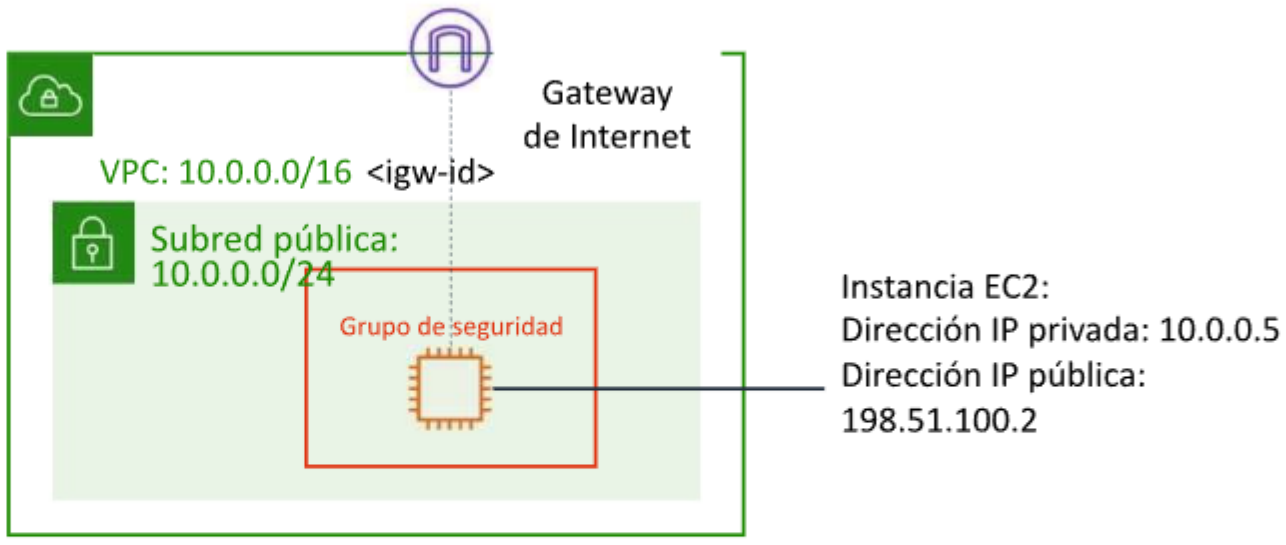
No se realiza un seguimiento de todos los flujos de tráfico. Considere la posibilidad de incorporar una regla de grupo de seguridad que permita flujos del protocolo de control de transmisión (TCP) o el protocolo de datagramas de usuario (UDP) para todo el tráfico (es decir, 0.0.0.0/0). También hay una regla correspondiente en la otra dirección que permite el tráfico de respuesta. En este caso, no se realiza un seguimiento de ese flujo de tráfico. Por ello, se autoriza el flujo del tráfico de respuesta en función de la regla de entrada o salida que permita dicho tráfico, y no en función de la información de seguimiento.

Grupos de seguridad predeterminados



Cuando crea un grupo de seguridad, este carece de reglas de entrada. Esto significa que debe agregar reglas de entrada al grupo de seguridad para permitir el tráfico entrante que proceda de otro alojamiento hacia su instancia. De forma predeterminada, en los grupos de seguridad se incluye una regla de salida con la que se permite todo el tráfico saliente. Es posible quitar esta regla y agregar reglas de salida que permitan solo tráfico saliente específico. Si el grupo de seguridad no tiene reglas de salida, no se permitirá el tráfico saliente que proceda de su instancia.

Grupos de seguridad personalizados

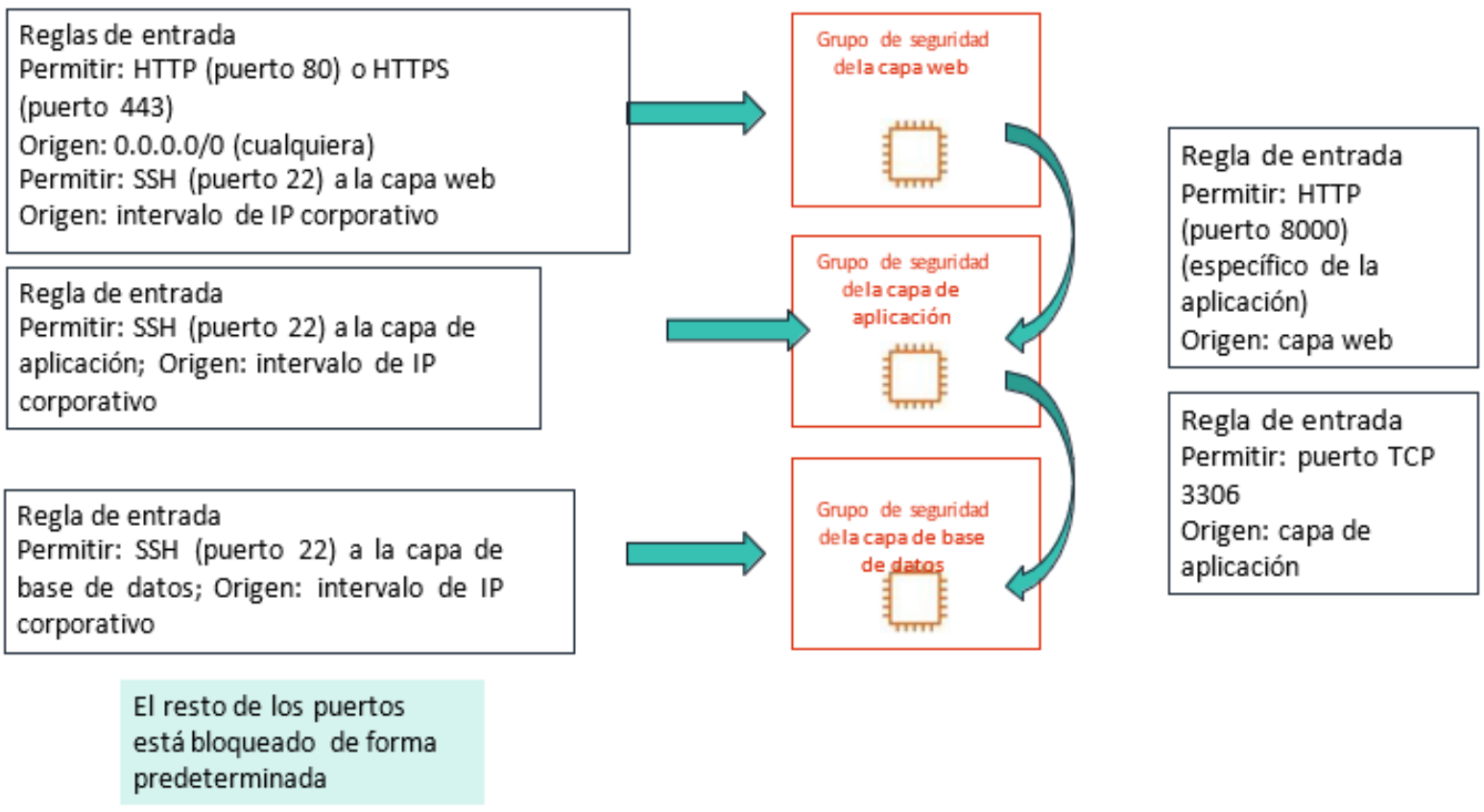


Entrada				
Tipo	Protocolo	Intervalo de puertos	Origen	Destino
HTTP	TCP	80	Cualquier lugar	Permitir acceso web

Al crear un grupo de seguridad personalizado, tienes la capacidad de definir reglas de permiso para el tráfico, pero no puedes especificar reglas de denegación directamente. Por ejemplo, al configurar una subred pública para alojar instancias de una aplicación web, el paso final implica la creación de un grupo de seguridad que permita el tráfico HTTP hacia esas instancias.

Es importante tener en cuenta que todas las reglas en un grupo de seguridad se evalúan en conjunto antes de determinar si se permite o no el tráfico.

Encadenamiento de grupos de seguridad

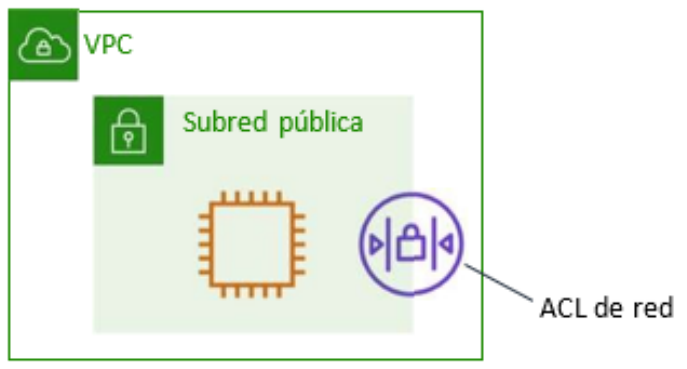


La mayoría de las organizaciones que operan en la nube utilizan grupos de seguridad para establecer reglas de acceso para cada función dentro de una aplicación. En un ejemplo típico de una aplicación de tres capas, estos grupos de seguridad están organizados en una cadena, con reglas de entrada y salida diseñadas para permitir el flujo de tráfico solo de la capa superior a la inferior y viceversa. Esta configuración asegura que cualquier brecha de seguridad en una capa no permita automáticamente el acceso desde la red a todos los recursos.

Los grupos de seguridad pueden personalizarse para aplicar reglas específicas a diferentes tipos de instancias. Por ejemplo, en una arquitectura de tres capas para una aplicación web, el grupo de seguridad para los servidores web podría tener los puertos 80 (HTTP) o 443 (HTTPS) abiertos al tráfico desde Internet. El grupo para los servidores de aplicaciones podría permitir el acceso al puerto 8000 (específico de la aplicación) solo desde el grupo de servidores web. Mientras tanto, el grupo para los servidores de base de datos podría tener el puerto 3306 (MySQL) abierto solo para el grupo de servidores de aplicaciones. Todos estos grupos también podrían permitir el acceso administrativo al puerto 22 (SSH), pero únicamente desde la red corporativa del cliente. Este enfoque garantiza que las aplicaciones puedan ser desplegadas con un alto nivel de seguridad.

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

- Actúan en el nivel de subred
- Permiten todo el tráfico entrante y saliente de forma predeterminada
- Representan firewall sin estado que requiere reglas explícitas para el tráfico entrante y saliente



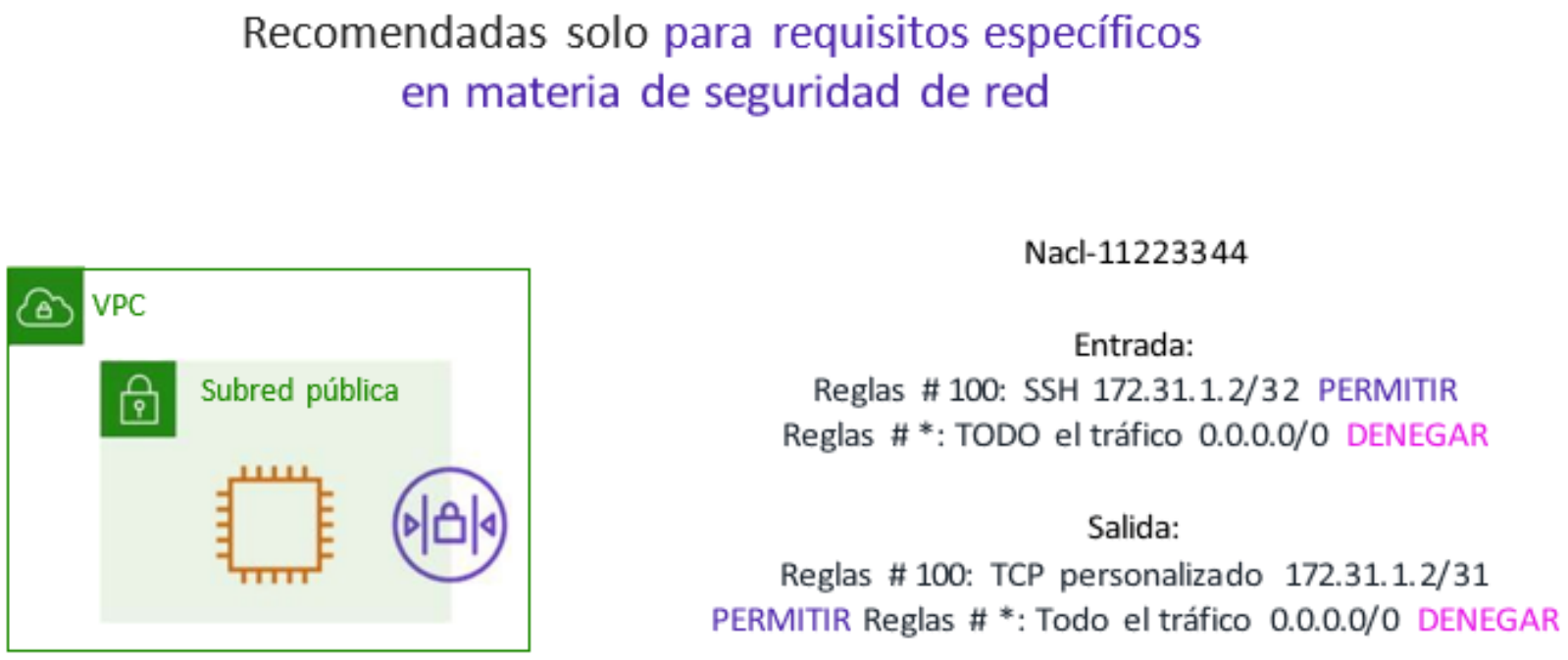
Una lista de control de acceso a la red (ACL de red) es una capa de seguridad opcional para su VPC. Actúa como firewall para controlar el tráfico que entra y sale de una o más subredes. Para agregar una capa de seguridad adicional a su VPC, puede configurar ACL de red con reglas similares a sus grupos de seguridad.

Cada subred de su VPC debe estar asociada a una ACL de red. Si no asocia una subred de forma explícita a una ACL de red, la subred se asociará automáticamente a la ACL de red predeterminada. Puede asociar una ACL de red a varias subredes. Sin embargo, una subred solo puede asociarse a una ACL de red a la vez. Cuando se asocia una ACL de red a una subred, se elimina la asociación anterior.

Una ACL de red tiene reglas de entrada y de salida independientes, y cada regla puede permitir o denegar tráfico. Su VPC incluye automáticamente una ACL de red predeterminada y modificable. De forma predeterminada, permite todo el tráfico IPv4 de entrada y salida, además, si corresponde, del tráfico IPv6.

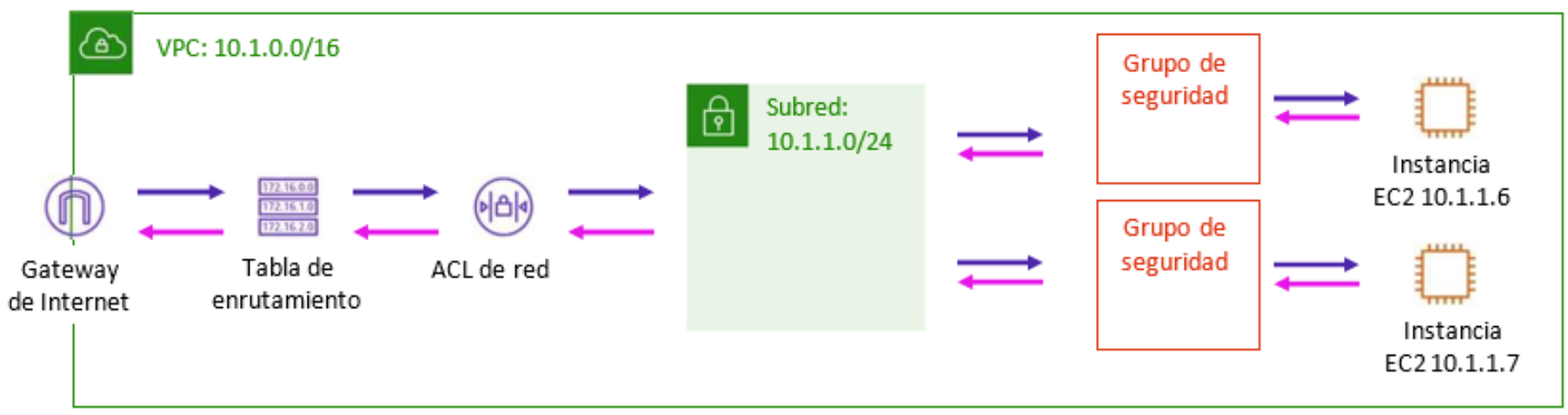
Las ACL de red no tienen estado, lo que significa que no se mantiene información sobre las solicitudes después de procesarlas. Las reglas deben permitir de forma explícita el tráfico de retorno.

ACL de red personalizadas



Tienes la opción de generar una Lista de Control de Acceso a la Red (ACL) personalizada y vincularla a una subred específica. Por defecto, todas las ACL de red personalizadas bloquean completamente el tráfico entrante y saliente hasta que configures reglas específicas.

Estructuración de su infraestructura con varias capas de defensa



Como medida recomendada, es fundamental asegurar tu infraestructura con múltiples capas de protección. Cuando ejecutas tu infraestructura dentro de una VPC, tienes el control sobre qué instancias están directamente expuestas a Internet. Puedes establecer grupos de seguridad y Listas de Control de Acceso a la Red (ACL) para fortalecer aún más la seguridad de tu infraestructura a nivel de instancia y subred, respectivamente. Además, es crucial proteger las instancias con un firewall a nivel del sistema operativo y seguir otras mejores prácticas en materia de seguridad.

Al implementar tanto ACL de red como grupos de seguridad como parte de una estrategia de defensa en profundidad para controlar el tráfico, cualquier error en la configuración de uno de estos controles no pondrá en riesgo tu infraestructura al exponerla a tráfico no deseado.

Revisión: creación de una subred pública

Para crear una subred pública que permita la comunicación entre instancias de la VPC e Internet, debe hacer lo siguiente:

Asocie una gateway de Internet a la VPC.

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

Dirija la tabla de enrutamiento de la subred de su instancia a la gateway de Internet.

Asegúrese de que las instancias tengan direcciones IP públicas o elásticas.

Grupo de seguridad

Asegúrese de que los grupos de seguridad y las ACL de red permitan el flujo de tráfico relevante.

A modo de revisión, para crear una subred pública que permita la comunicación entre instancias de la VPC e Internet, debe hacer lo siguiente:

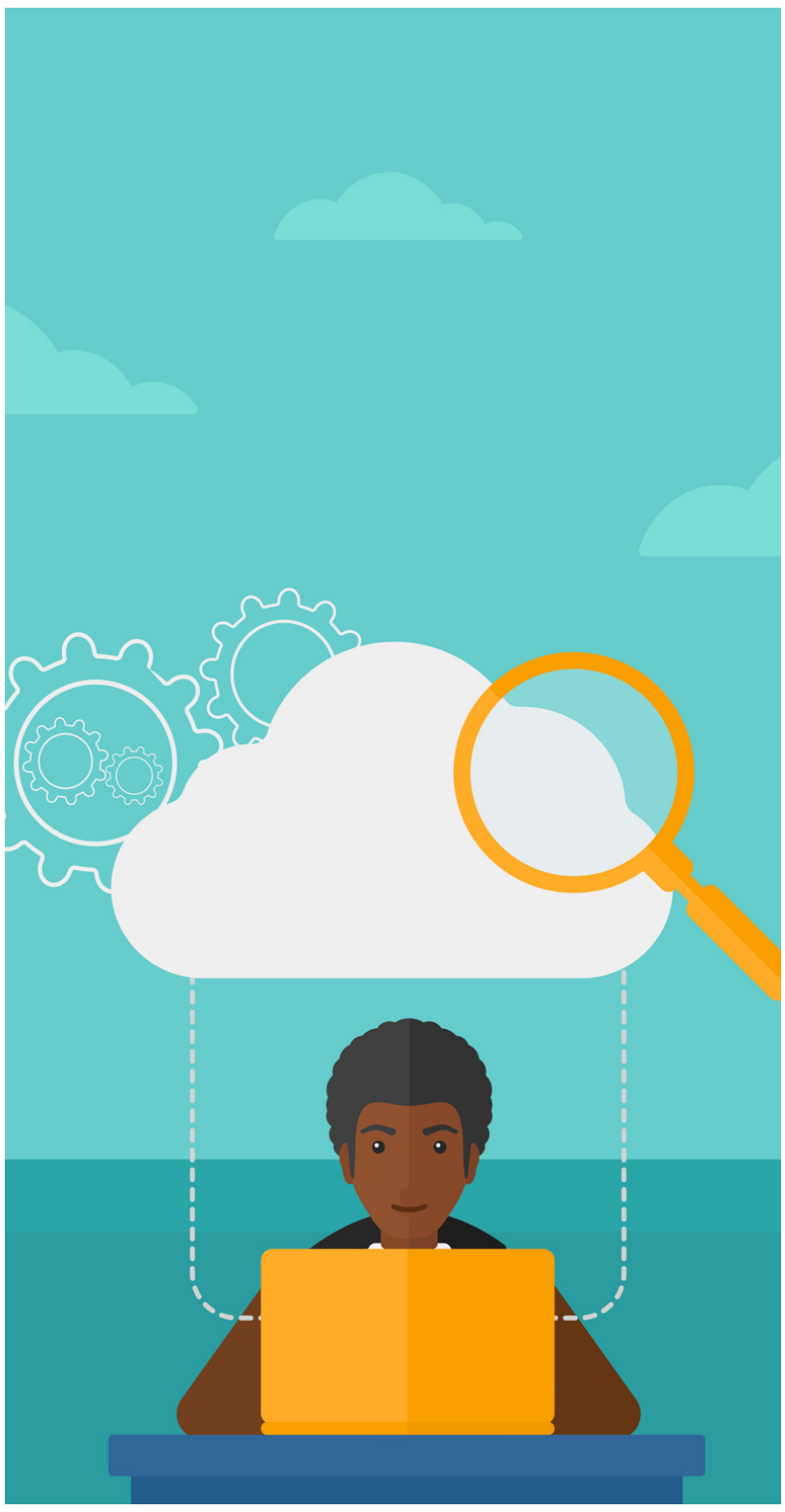
Asociar una gateway de Internet a la VPC

Agregar una ruta a la tabla de enrutamiento de la subred que dirija el tráfico con destino a Internet a la gateway de Internet

Asegurarse de que las instancias tengan direcciones IP públicas o elásticas

Asegurarse de que los grupos de seguridad y las ACL de red permitan el flujo de tráfico relevante

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



Los grupos de seguridad son firewall con estado que actúan en el nivel de la instancia.

Las ACL de red son firewall sin estado que actúan en el nivel de subgrupo.

Cuando establece reglas de entrada y salida para permitir que el tráfico fluya desde la capa superior hasta la capa inferior de la arquitectura, puede encadenar los grupos de seguridad de manera que se aíslen los casos de violación a la seguridad.

Debe estructurar su infraestructura con varias capas de defensa.