Lectura 2.7: Enrutamiento y seguridad de Amazon VPC

La tabla de ruta principal

Cuando crea una VPC, AWS crea una tabla de rutas denominada tabla de rutas principal. Una tabla de rutas contiene un conjunto de reglas, denominadas rutas, que se utilizan para determinar hacia dónde se dirige el tráfico de red. AWS asume que cuando crea una nueva VPC con subredes, desea que el tráfico fluya entre ellas. Por lo tanto, la configuración predeterminada de la tabla de rutas principal es permitir el tráfico entre todas las subredes de la red local. A continuación se muestra un ejemplo de una tabla de rutas principal:

Destination	Target	Status	Propagated
10.2.0.0/16	local	active	No

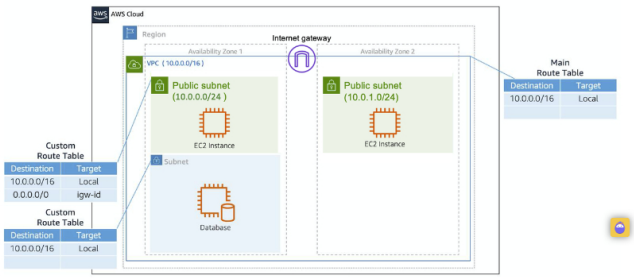
Hay dos partes principales en esta tabla de rutas.

- El destino, que es un rango de direcciones IP donde desea que vaya su tráfico. En el ejemplo de enviar una carta, necesita un destino para enrutar la carta al lugar adecuado. Lo mismo es cierto para el tráfico de enrutamiento. En este caso, el destino es el rango de IP de nuestra red VPC.
- El destino, que es la conexión a través de la cual enviar el tráfico. En este caso, el tráfico se enruta a través de la red VPC local.

Tablas de rutas personalizadas

Si bien la tabla de enrutamiento principal controla el enrutamiento de su VPC, es posible que desee ser más granular acerca de cómo enruta su tráfico para subredes específicas. Por ejemplo, su aplicación puede consistir en una interfaz y una base de datos. Puede crear subredes separadas para estos recursos y proporcionar diferentes rutas para cada uno de ellos.

Si asocia una tabla de rutas personalizada con una subred, la subred la usará en lugar de la tabla de rutas principal. De manera predeterminada, cada tabla de ruteo personalizada que cree tendrá la ruta local dentro de ella, lo que permitirá que la comunicación fluya entre todos los recursos y subredes dentro de la VPC.



Proteja sus subredes con ACL de red

Piense en una ACL de red como un firewall a nivel de subred. Una ACL de red le permite controlar qué tipo de tráfico puede entrar o salir de su subred. Puede configurar esto configurando reglas que definen lo que desea filtrar. Aquí hay un ejemplo.

Entrante					
Regla #	**Tipo**	**Protocolo**	**rango de puertos**	**Fuente**	**Permiten negar**
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
Saliente					
Regla #	**Tipo**	**Protocolo**	**rango de puertos**	**Fuente**	**Permiten negar**
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

La ACL de red predeterminada, que se muestra en la tabla anterior, permite que todo el tráfico entre y salga de su subred. Para permitir que los datos fluyan libremente a su subred, este es un buen punto de partida. Sin embargo, es posible que desee restringir los datos a nivel de subred. Por ejemplo, si tiene una aplicación web, puede restringir su red para permitir el tráfico HTTPS y el tráfico del protocolo de escritorio remoto (RDP) a sus servidores web.

Entrante					
Regla #	**IP de origen**	**Protocolo**	**Puerto**	**Permiten negar**	**Comentarios**
100	Todo el tráfico IPv4	TCP	443	PERMITIR	Permite el tráfico HTTPS entrante desde cualquier lugar
130	192.0.2.0/24	TCP	3389	PERMITIR	Permite el tráfico RDP entrante a los servidores web desde el rango de direcciones IP públicas de su red doméstica (a través de la puerta de enlace de Internet)
*	Todo el tráfico IPv4	Todo	Todo	DENEGAR	Deniega todo el tráfico entrante que aún no haya sido manejado por una regla anterior (no modificable)
Saliente					
Regla #	**IP de destino**	**Protocolo**	**Puerto**	**Permiten negar**	**Comentarios**
120	0.0.0.0/0	TCP	1025-65535	PERMITIR	Permite respuestas salientes a clientes en Internet (atendiendo a personas que visitan los servidores web en la subred)

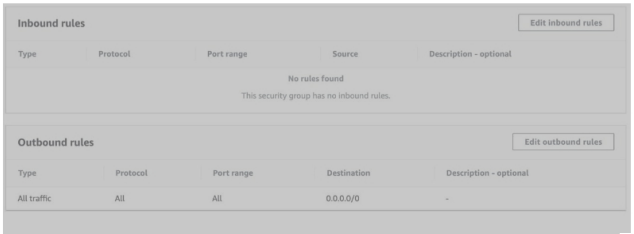
					web en la subred)
*	0.0.0.0/0	Todo	Todo	DENEGAR	Deniega todo el tráfico saliente que no haya sido controlado por una regla anterior (no modificable)

Tenga en cuenta que en el ejemplo anterior de ACL de red, permite el rango de entrada 443 y el rango de salida 1025-65535. Eso es porque HTTP usa el puerto 443 para iniciar una conexión y responderá a un puerto efímero. Las ACL de red se consideran sin estado, por lo que debe incluir los puertos de entrada y salida utilizados para el protocolo. Si no incluye el rango de salida, su servidor respondería pero el tráfico nunca abandonaría la subred.

Dado que las ACL de red están configuradas de manera predeterminada para permitir el tráfico entrante y saliente, no necesita cambiar su configuración inicial a menos que necesite capas de seguridad adicionales.

Proteja sus instancias EC2 con grupos de seguridad

La siguiente capa de seguridad es para sus instancias EC2. Aquí, puede crear un firewall llamado grupo de seguridad. La configuración predeterminada de un grupo de seguridad bloquea todo el tráfico entrante y permite todo el tráfico saliente.

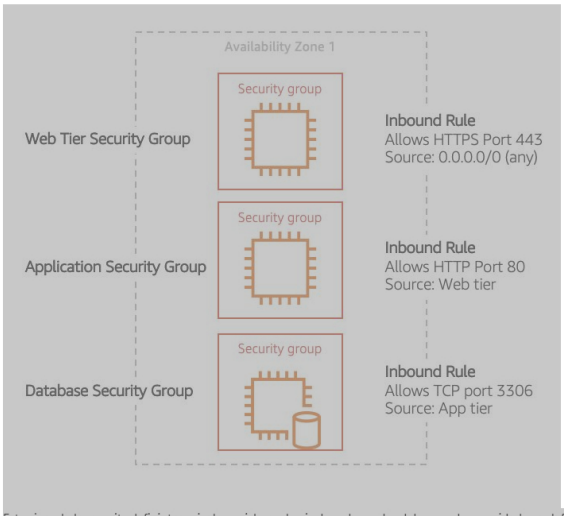


Quizás se esté preguntando: "¿Esto no bloquearía todas las instancias EC2 para que no recibieran la respuesta de las solicitudes de los clientes?" Bueno, los grupos de seguridad tienen estado, lo que significa que recordarán si una conexión fue iniciada originalmente por la instancia EC2 o desde el exterior y permiten que el tráfico responda temporalmente sin tener que modificar las reglas de entrada.

Si desea que su instancia EC2 acepte tráfico de Internet, deberá abrir puertos de entrada. Si tiene un servidor web, es posible que deba aceptar solicitudes HTTP y HTTPS para permitir ese tipo de tráfico a través de su grupo de seguridad. Puede crear una regla de entrada que permita el puerto 80 (HTTP) y el puerto 443 (HTTPS) como se muestra a continuación.

Reglas de entrada			
Tipo	**Protocolo**	**rango de puertos**	**Fuente**
HTTP (80)	TCP (6)	80	0.0.0.0/0
HTTP (80)	TCP (6)	80	::/0
HTTPS (443)	TCP (6)	443	0.0.0.0/0
HTTPS (443)	TCP (6)	443	::/0

Aprendió en una unidad anterior que las subredes se pueden usar para segregar el tráfico entre las computadoras en su red. Los grupos de seguridad se pueden utilizar para hacer lo mismo. Un patrón de diseño común es organizar sus recursos en diferentes grupos y crear grupos de seguridad para que cada uno controle la comunicación de red entre ellos.



Este ejemplo le permite definir tres niveles y aislar cada nivel con las reglas del grupo de seguridad que defina. En este caso, solo permite el tráfico de Internet al nivel web a través de HTTPS, el nivel web al nivel de aplicación a través de HTTP y el nivel de aplicación al nivel de base de datos a través de MySQL. Esto es diferente de los entornos locales tradicionales, en los que aísla grupos de recursos a través de la configuración de VLAN. En AWS, los grupos de seguridad le permiten lograr el mismo aislamiento sin vincularlo a su red.

Recursos :

- *Sitio externo:* AWS: Tablas de ruta
- *Sitio externo:* AWS: opciones de enrutamiento de ejemplo
- *Sitio externo:* AWS: trabajar con tablas de enrutamiento
- *Sitio externo:* AWS: ACL de red
- *Sitio externo:* AWS: grupos de seguridad para su VPC
- *Sitio externo:* AWS: Alojo un sitio web en una instancia EC2. ¿Cómo permito que mis usuarios se conecten en HTTP (80) o HTTPS (443)?