

REDES EN AWS

CONTENIDO

CONECTIVIDAD CON AWS	2
AMAZON VIRTUAL PRIVATE CLOUD (AMAZON VPC).....	2
PUERTA DE ENLACE DE INTERNET (INTERNET GATEWAY)	3
PUERTA DE ENLACE PRIVADA VIRTUAL (VIRTUAL PRIVATE GATEWAY)	4
AWS DIRECT CONNECT	5
LISTAS DE CONTROL DE ACCESO A REDES Y SUBREDES	6
SUBREDES.....	6
TRÁFICO DE RED EN UNA VPC	7
ACL DE RED.....	8
FILTRADO DE PAQUETES SIN ESTADO	9
GRUPOS DE SEGURIDAD	9
FILTRADO DE PAQUETES CON ESTADO.....	10
DIFERENCIA ENTRE ACL DE RED Y GRUPO DE SEGURIDAD	11
REDES GLOBALES	12
SISTEMA DE NOMBRES DE DOMINIO (DNS)	13
AMAZON ROUTE 53	13
AMAZON CLOUDFRONT	14
Ejemplo de cómo Amazon Route 53 y Amazon CloudFront entregan contenido.....	15
CONCLUSIONES.....	17

CONECTIVIDAD CON AWS

Si pensamos en nuestra cuenta AWS, las cosas ya deberían funcionar sin problemas. Aunque, ¿qué pasaría si tuviéramos a unos cuantos clientes ansiosos que quisieran conectarse directamente a nuestros servicios privados, en lugar de a los servicios que están delante?

No tiene sentido permitir que cada cliente interactúe con nuestros servicios, entonces, ¿qué hacemos? Amazon Virtual Private Cloud, o VPC, como se las conoce comúnmente.

Una VPC le permite aprovisionar de manera lógica, una sección aislada de la nube de AWS, donde puede iniciar recursos de AWS en una red virtual que usted defina. Estos recursos pueden ser públicos para que tengan acceso a Internet, o privados sin acceso a Internet, normalmente para servicios de backend como bases de datos o servidores de aplicaciones.

El agrupamiento público y privado de recursos se conoce como subredes, que son rangos de direcciones IP de la VPC.

Los servicios que queremos que interactúen con los clientes los ponemos en una subred pública, por ende, pueden comunicarse con los clientes o con Internet y los servicios privados que no queremos que interactúen con los clientes directamente, los ponemos en una subred privada.

AMAZON VIRTUAL PRIVATE CLOUD (AMAZON VPC)

Imagine los millones de clientes que utilizan los servicios de AWS, además, imagine los millones de recursos que han creado estos clientes, como las instancias de Amazon EC2. Sin límites en torno a todos estos recursos, el tráfico de red podría fluir entre ellos sin restricciones.

Un servicio de red que puede utilizar para establecer límites en torno a sus recursos de AWS es Amazon Virtual Private Cloud (Amazon VPC).

Dentro de una Virtual Private Cloud (VPC), puede organizar los recursos en subredes. Una subred es una sección de una VPC que puede contener recursos, como instancias de Amazon EC2.

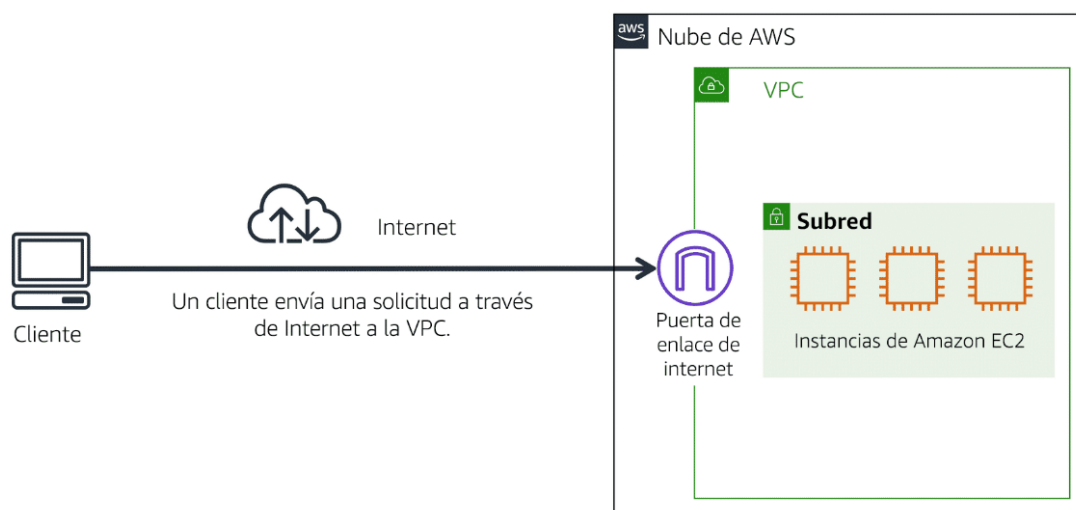
Una VPC o nube privada virtual es en esencia su propia red privada en AWS. Una VPC le permite definir su rango de IP privado para los recursos de AWS y colocar elementos como instancias de EC2 y ELB dentro de la VPC.

Ahora no se limita a lanzar sus recursos en una VPC y seguir adelante, así como así. Los coloca en diferentes subredes, que son fragmentos de direcciones IP de la VPC que le permiten agrupar recursos. Las subredes, junto con las reglas de redes, controlan si los recursos están disponibles de forma pública o privada.

Hay formas de controlar el tráfico que entra en su VPC: Para algunas VPCs puede tener recursos orientados a internet a los que el público debería poder acceder, como un sitio web público, por ejemplo. Sin embargo, en otros escenarios es posible que tenga recursos que quiera que solo sean accesibles para aquellos que inicien sesión en su red privada; estos recursos podrían ser servicios internos como una aplicación de recursos humanos o una base de datos backend.

En primer lugar, hablemos de los recursos públicos. Para permitir que el tráfico de la Internet pública fluya dentro y fuera de la VPC, debe adjuntar lo que se denomina puerta de enlace a Internet, o IGW, a su VPC.

PUERTA DE ENLACE DE INTERNET (INTERNET GATEWAY)



Puerta de enlace de internet adjunta a una VPC que admite tres instancias de EC2. Una flecha conecta el cliente a la puerta de enlace de internet e indica que la solicitud del cliente obtuvo acceso a la VPC.

Para permitir que el tráfico público de internet acceda a su VPC, adjunte una puerta de enlace de internet a la VPC.

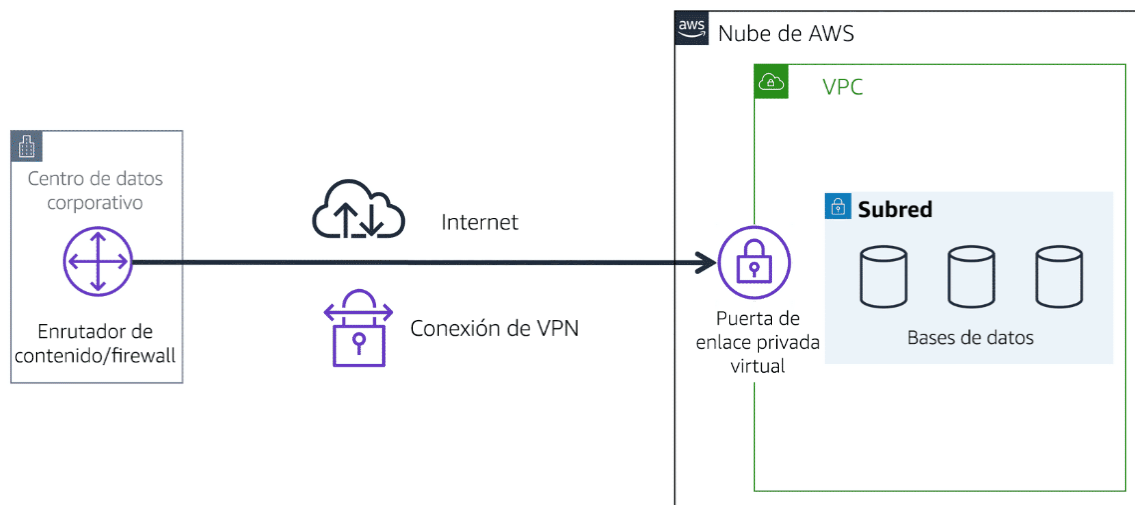
Una puerta de enlace de Internet es como una puerta abierta al público, sin ella, nadie puede acceder a los recursos ubicados dentro de la VPC.

Una puerta de enlace de Internet es una conexión entre una VPC e Internet. Puede considerar que una puerta de enlace de Internet es similar a una puerta que los clientes utilizan para entrar a una cafetería, sin ella los clientes no podrían entrar y pedir su café.

PUERTA DE ENLACE PRIVADA VIRTUAL (VIRTUAL PRIVATE GATEWAY)

A continuación, hablemos de una VPC con todos los recursos privados internos. No queremos que cualquier persona, desde cualquier lugar pueda acceder a estos recursos. Así que no queremos una puerta de enlace de Internet adjunta a nuestra VPC. En cambio, queremos una puerta de enlace privada que solo permita a las personas que provengan de una red aprobada, no de la Internet pública.

Esta puerta privada se llama puerta de enlace privada virtual y le permite crear una conexión de VPN entre una red privada, como su centro de datos en las instalaciones o red corporativa interna, a su VPC.



Una puerta de enlace privada virtual le permite establecer una conexión de red privada virtual (VPN) entre la VPC y una red privada, como un centro de datos en las instalaciones o una red corporativa interna. Una puerta de enlace privada virtual permite el tráfico hacia la VPC solo si procede de una red aprobada.

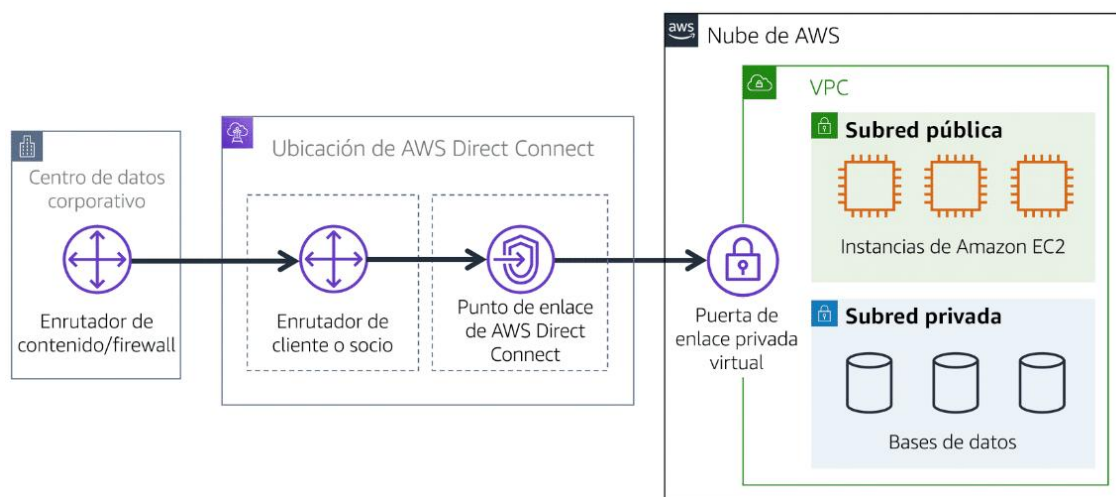
Para acceder a los recursos privados en una VPC, puede utilizar una puerta de enlace privada virtual. Así que, si quiere establecer una conexión de VPN cifrada a sus recursos internos privados de AWS, tendría que adjuntar una puerta de enlace privada virtual a la VPC.

La puerta de enlace privada virtual es el componente que permite el tráfico de internet protegido entre en la VPC.

Ahora bien, las conexiones de VPN son privadas y están cifradas, pero siguen usando una conexión a Internet normal que tiene ancho de banda compartido con muchas personas que utilizan Internet. El punto es que todavía quiere una conexión privada, pero quiere que sea dedicada y que no se comparta con nadie más, desea obtener la menor latencia posible con la mayor cantidad de seguridad posible. Con AWS, puede lograrlo con lo que se denomina AWS Direct Connect.

AWS DIRECT CONNECT

AWS Direct Connect es un servicio que le permite establecer una conexión privada dedicada entre su centro de datos y una VPC.



Un centro de datos corporativo une el tráfico de redes a una ubicación de AWS Direct Connect. Luego, ese tráfico se envía a una VPC a través de una puerta de enlace privada virtual. Todo el tráfico de red entre el centro de datos corporativo y la VPC fluye a través de esta conexión privada dedicada.

Direct Connect le permite establecer una conexión de fibra dedicada completamente privada desde su centro de datos a AWS, trabaja con un socio de Direct Connect en su área para establecer esta conexión porque AWS Direct Connect proporciona una línea física que conecta su red a su VPC de AWS.

Esto puede ayudarlo a satisfacer las altas necesidades regulatorias y de cumplimiento, así como evitar cualquier posible problema de ancho de banda.

La conexión privada que proporciona AWS Direct Connect le ayuda a reducir los costos de red y a aumentar la cantidad de ancho de banda que puede viajar a través de la red.

LISTAS DE CONTROL DE ACCESO A REDES Y SUBREDES

Puede imaginar su VPC como una fortaleza reforzada donde nada entra ni sale sin permiso explícito. Tiene una puerta de enlace que solo permite que el tráfico entre o salga de la VPC, pero eso solo cubre el perímetro y esa es solo una parte de la seguridad de red en la que debería centrarse como parte de su estrategia de TI.

AWS tiene una amplia gama de herramientas que cubren todas las capas de seguridad: Protección de red, seguridad de aplicaciones, identidad de usuario, autenticación y autorización, denegación de servicio distribuido o prevención DDoS, integridad de datos, cifrado y mucho más.

Vamos a hablar de algunos aspectos de la protección de red y analizar lo que sucede dentro de la VPC.

SUBREDES

Una subred es una sección de una VPC en la que se pueden agrupar recursos en función de las necesidades operativas o de seguridad. Las subredes pueden ser públicas o privadas.

Las **subredes públicas** contienen recursos a los que el público debe tener acceso, como el sitio web de una tienda en línea.

Las **subredes privadas** contienen recursos a los que solo se debe tener acceso a través de la red privada, como una base de datos que contiene la información personal de los clientes y los historiales de pedidos.

En una VPC, las subredes se pueden comunicar entre sí. Por ejemplo, podría tener una aplicación que incluya instancias de Amazon EC2 de una subred pública que se comuniquen con bases de datos ubicadas en una subred privada.



La única razón técnica para utilizar subredes en una VPC es controlar el acceso a las puertas de enlace, las subredes públicas tienen acceso a la puerta de enlace de Internet, mientras que las subredes privadas no.

TRÁFICO DE RED EN UNA VPC

Cuando un cliente solicita datos de una aplicación alojada en la nube de AWS, la solicitud se envía como un paquete. Un paquete es una unidad de datos enviada a través de Internet o de una red.

Entra en una VPC a través de una puerta de enlace de Internet. Antes de que un paquete pueda entrar o salir de una subred, comprueba los permisos. Estos permisos indican quién envió el paquete y cómo intenta comunicarse con los recursos de una subred.

Las subredes también pueden controlar los permisos de tráfico. Los paquetes son mensajes de Internet y cada paquete que cruza los límites de la subred se verifica con algo llamado lista de control de acceso de red o ACL de red.

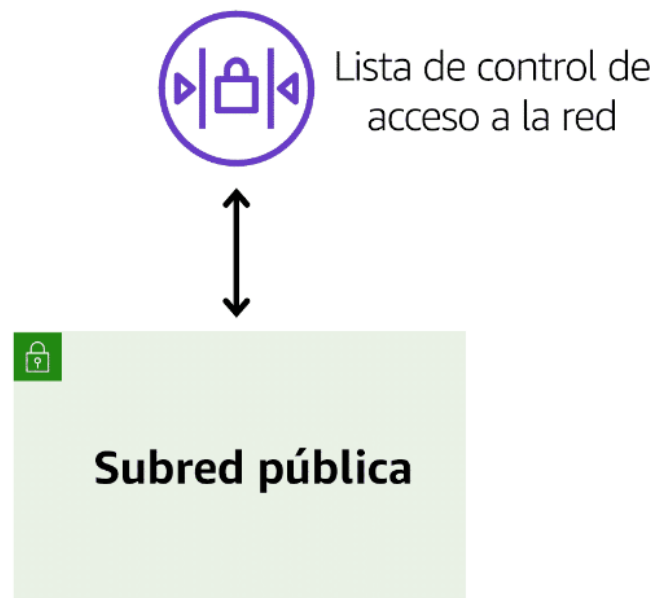
El componente de VPC que comprueba los permisos de paquetes para las subredes es una lista de control de acceso (ACL) a la red.

ACL DE RED

Una ACL de red es un firewall virtual que controla el tráfico entrante y saliente a nivel de la subred.

La verificación que hace la lista de control de acceso de red o ACL de red sirve para ver si el paquete tiene permisos para salir de la subred o entrar, en función de quién la envió y cómo intenta comunicarse.

Puede pensar en las ACL de red como oficiales de control de pasaportes. Si está en la lista aprobada, puede pasar, si no está en la lista o bien si está explícitamente en la lista de no entrar, entonces lo bloquean. Las ACL de red verifican el tráfico que entra a una subred o sale, tal como el control de pasaportes.



Cada cuenta de AWS incluye una ACL de red predeterminada. Al configurar la VPC, puede usar la ACL de red predeterminada de su cuenta o crear ACL de red personalizadas.

Por defecto, la ACL de red predeterminada de su cuenta permite todo el tráfico entrante y saliente, pero usted puede modificarla y agregar sus propias reglas. En el caso de las ACL de red personalizadas, se deniega todo el tráfico entrante y saliente hasta que agregue reglas para especificar qué tráfico permitir. Además, todas las ACL de red tienen una regla de denegación explícita. Esta regla garantiza que, si un paquete no coincide con ninguna de las demás reglas de la lista, el paquete se deniega.

FILTRADO DE PAQUETES SIN ESTADO

Las ACL de red realizan el filtrado de paquetes sin estado. No recuerdan nada y comprueban los paquetes que cruzan el borde de la subred en cada sentido: Entrante y saliente.

Recuerde el ejemplo anterior de un viajero que quiere ingresar a un país diferente, es similar a enviar una solicitud desde una instancia de Amazon EC2 a internet.

La lista se verifica cuando se entra en un país y al salir de él, pero no porque le permitieron entrar quiere decir que le permitan salir. Igual sucede en las ACL, el tráfico autorizado se puede enviar, mientras que el tráfico potencialmente dañino, como los intentos de obtener el control de un sistema mediante solicitudes administrativas, se bloquea antes de hacer contacto con su objetivo. No puede atacar lo que no puede tocar.

Cuando una respuesta de paquete para esa solicitud vuelve a la subred, la ACL de red no recuerda la solicitud anterior. La ACL de red comprueba la respuesta del paquete con la lista de reglas para determinar si se permite o se deniega.

Un control sin estado significa que siempre revisan su lista.

Ahora bien, una vez que un paquete entró en una subred, se deben evaluar sus permisos para los recursos de la subred, como las instancias de Amazon EC2.

El componente de VPC que corrobora los permisos de los paquetes para una instancia de Amazon EC2 es un grupo de seguridad

GRUPOS DE SEGURIDAD

Las ACL suenan como una gran seguridad, pero no responden a todos los problemas de control de red, porque una ACL de red solo evalúa un paquete si cruza un límite dentro o fuera de la subred, no evalúa si un paquete puede alcanzar o no una instancia de EC2 específica.

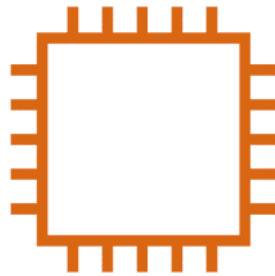
A veces habrá varias instancias de EC2 en la misma subred, pero pueden tener reglas diferentes en torno a quién puede enviar los mensajes y a qué puerto se les permite enviar esos mensajes, por lo que también necesita seguridad de red a nivel de instancia.

Para resolver las preguntas de acceso a nivel de instancia, están los grupos de seguridad. Cada instancia de EC2 cuando se inicia, llega automáticamente con un grupo de seguridad y, de forma predeterminada, el grupo de seguridad no permite nada de tráfico en la instancia. Todos los puertos se bloquean, todas las direcciones IP que envían paquetes se bloquean.

El mecanismo es muy seguro, pero quizás no sea muy útil si desea que una instancia pueda aceptar tráfico desde el exterior, como por ejemplo un mensaje desde una instancia de frontend o un mensaje de Internet.

Obviamente se puede modificar el grupo de seguridad para que acepte un tipo específico de tráfico. En el caso de un sitio web, lo que se quiere es que se acepte el tráfico basado en la web o https, pero no otros tipos de tráfico como un sistema operativo o solicitudes de administración.

Grupo de seguridad



Instancias de Amazon EC2

Un grupo de seguridad es un firewall virtual que controla el tráfico entrante y saliente de una instancia de Amazon EC2.

De forma predeterminada, un grupo de seguridad deniega todo el tráfico entrante y permite todo el tráfico saliente. Puede añadir reglas personalizadas para configurar qué tráfico debe permitirse, cualquier otro tipo de tráfico será denegado.

Si tiene varias instancias de Amazon EC2 en la misma VPC, puede asociarlas al mismo grupo de seguridad o utilizar grupos de seguridad distintos para cada instancia.

FILTRADO DE PAQUETES CON ESTADO

Los grupos de seguridad realizan el filtrado de paquetes con estado, es decir, recuerdan las decisiones anteriores que se tomaron para los paquetes entrantes.

Considere el mismo ejemplo de envío de una solicitud desde una instancia de Amazon EC2 a internet.

Cuando una respuesta de paquete para esa solicitud vuelve a la instancia, el grupo de seguridad recuerda la solicitud anterior y el grupo de seguridad permite que la respuesta continúe, independientemente de las reglas del grupo de seguridad de entrada.

Para este ejemplo, imagine que se encuentra en un edificio de apartamentos con un portero que recibe a los huéspedes en el vestíbulo. Puede considerar a los invitados como paquetes y al portero como un grupo de seguridad. A medida que llegan los invitados, el portero revisa una lista para asegurarse de que pueden entrar en el edificio. Sin embargo, el portero no vuelve a comprobar la lista cuando los invitados salen del edificio

El portero verificará una lista para asegurarse de que alguien tenga permitido entrar al edificio, pero no se molestará en verificar la lista al salir. Con los grupos de seguridad, se permite la entrada de tráfico específico y, de forma predeterminada, se permite toda la salida de tráfico.

DIFERENCIA ENTRE ACL DE RED Y GRUPO DE SEGURIDAD

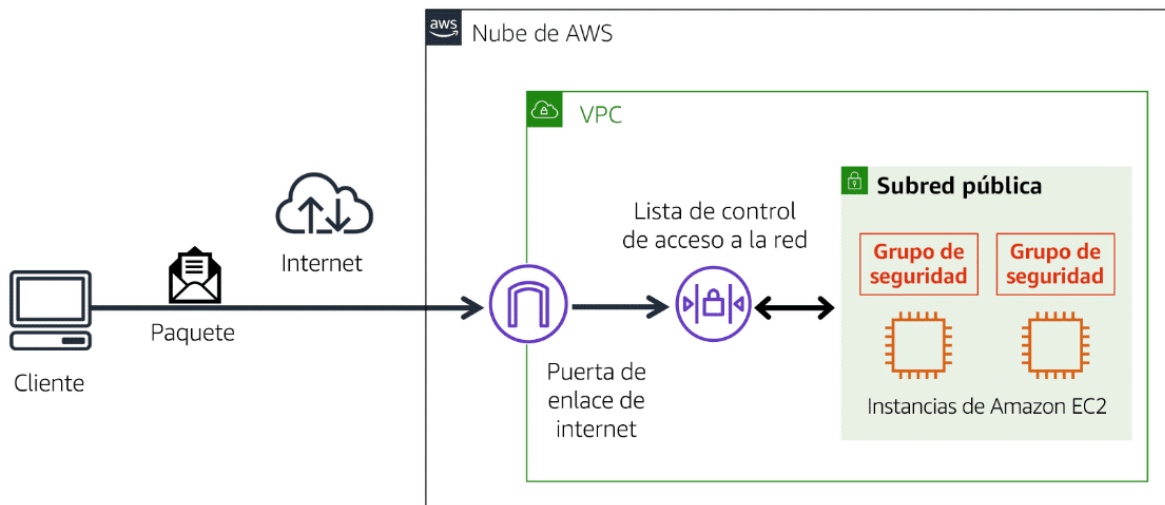
Si las ACL de red son nuestro control de pasaportes, un grupo de seguridad es como el portero de su edificio y el edificio es la instancia de EC2 en este caso.

De forma predeterminada, se permite todo el tráfico saliente de un grupo de seguridad, pero a la ACL de red no le importa lo que permitió el grupo de seguridad. Tiene su propia lista de quién puede pasar y quién no.

Son dos mecanismos diferentes, cada uno haciendo exactamente el mismo trabajo: Dejar entrar paquetes buenos y mantener afuera los paquetes malos.

La diferencia clave entre un grupo de seguridad y una ACL de red es que el grupo de seguridad cuenta con estado, lo que significa, que tiene algún tipo de memoria cuando se trata de a quién permite la entrada o la salida, y la ACL de red no tiene estado, es decir, que no recuerda nada y comprueba cada paquete que cruza su frontera, independientemente de cualquier circunstancia.

Puede parecer que nos hemos esforzado mucho en hacer que un paquete vaya de una instancia a otra y vuelva y puede que le preocupe la sobrecarga de red que esto pueda generar, pero la realidad es que todos estos intercambios ocurren al instante como parte del funcionamiento real de las redes de AWS.



Un paquete viaja por internet desde un cliente hasta la puerta de enlace de internet e ingresa a la VPC. El paquete atraviesa la lista de control de acceso a la red y accede a la subred pública, en la que se ubican dos instancias de EC2.

REDES GLOBALES

Hemos hablado mucho sobre cómo interactúa con su infraestructura de AWS, pero, ¿cómo interactúan sus clientes con la infraestructura de AWS? Si tiene un sitio web alojado en AWS, los clientes suelen ingresar a él desde el navegador, pulsan enter y el sitio se abre.

Entonces, ¿cómo logran los clientes acceder a nuestro sitio web? AWS tiene dos servicios que pueden ayudarnos con esto. El primero es Route 53, que es el servicio de nombres de dominio de AWS, o DNS, y tiene una alta disponibilidad y escalabilidad.

Pero, ¿qué es DNS? Piense en DNS como un servicio de traducción que, en lugar de traducir entre idiomas, traduce los nombres de sitios web en direcciones IP, o Internet Protocol - Protocolo de Internet, que los equipos de cómputo pueden leer. Por ejemplo, cuando ingresamos la dirección de un sitio web en nuestro navegador, se pone en contacto con Route 53 para obtener la dirección IP del sitio, digamos 192.1.1.1, y luego dirige ese equipo o navegador a esa dirección.

El segundo es Amazon CloudFront, que puede ayudar a acelerar la entrega de activos de sitios web a los clientes.

Vamos a verlos más a detalle.

SISTEMA DE NOMBRES DE DOMINIO (DNS)

Supongamos que AnyCompany tiene un sitio web alojado en la nube de AWS. Los clientes introducen la dirección web en su navegador y acceden al sitio web. Esto ocurre debido a la resolución del sistema de nombres de dominio (DNS). La resolución de DNS implica un solucionador de DNS del cliente que se comunica con un servidor DNS de la empresa.

Puede considerar el DNS como la guía telefónica de internet. La resolución de DNS es el proceso de traducir el nombre de dominio a una dirección IP.

Un cliente se conecta a un solucionador de DNS que busca el dominio y el solucionador envía la solicitud al servidor de DNS, que envía la dirección IP al solucionador.



En este ejemplo, supongamos que quiere visitar el sitio web de AnyCompany:

1. Cuando ingresa el nombre del dominio en el navegador, esta solicitud se envía a un solucionador de DNS del cliente.
2. El solucionador de DNS del cliente pide al servidor de DNS de la empresa la dirección IP que corresponde al sitio web de AnyCompany.
3. El servidor DNS de la empresa responde y proporciona la dirección IP del sitio web de AnyCompany: 192.0.2.0.

AMAZON ROUTE 53

Amazon Route 53 es un servicio web de DNS que ofrece a los desarrolladores y a las empresas una forma fiable de dirigir a los usuarios finales a aplicaciones de Internet alojadas en AWS.

Amazon Route 53 conecta las solicitudes de los usuarios a la infraestructura que funciona en AWS (como las instancias de Amazon EC2 y los equilibradores de carga). Puede dirigir a los usuarios a una infraestructura fuera de AWS.

Otra característica de Route 53 es la capacidad de administrar los registros de DNS de los nombres de dominio. Puede registrar nuevos nombres de dominio directamente en Route 53. También puede transferir registros de DNS de nombres de dominio existentes administrados por otros registradores de dominios. Esto le permite administrar todos los nombres de dominio en una única ubicación.

Route 53 puede dirigir el tráfico a diferentes puntos de enlace utilizando varias políticas de enrutamiento diferentes, como el enrutamiento basado en latencia, geolocalización, DNS, geo proximidad y Weighted Round Robin.

Si hablamos de la geolocalización DNS, significa que dirigimos el tráfico según la ubicación del cliente, por ejemplo, el tráfico procedente de Norteamérica se dirige a la región de Oregón y el tráfico en Irlanda se dirige a la región de Dublín.

Incluso puede usar Route 53 para registrar nombres de dominio y así poder comprar y administrar sus propios nombres de dominio directamente en AWS.

AMAZON CLOUDFRONT

Hablando de sitios web, hay otro servicio que puede ayudar a acelerar la entrega de activos de sitios web a los clientes: Amazon CloudFront, que es un servicio de entrega de contenido.

En clases anteriores hablamos de ubicaciones perimetrales (edge locations), estas ubicaciones ofrecen contenido lo más cerca posible de los clientes y una parte de eso es la red de entrega de contenido, o CDN. Recordemos que una CDN es una red que ayuda a entregar contenido perimetral a los usuarios en función de su ubicación geográfica.

Almacenar copias de datos en caché más cerca de los clientes de todo el mundo utiliza el concepto de redes de entrega de contenido o CDN. Las CDN se utilizan comúnmente, y en AWS, la CDN se llama Amazon CloudFront. Amazon CloudFront es un servicio que ayuda a entregar datos, video, aplicaciones y APIs a clientes de todo el mundo con baja latencia y altas velocidades de transferencia. Amazon CloudFront utiliza las denominadas ubicaciones de borde en todo el mundo, para ayudar a acelerar la comunicación con los usuarios, sin importar el lugar donde se encuentren.

Volvamos al ejemplo de Norteamérica, ahora comparado con Irlanda, digamos que tenemos un usuario en Seattle que quiere acceder a un sitio web. Para acelerar esto, alojamos el sitio en Oregón e implementamos nuestros activos web estáticos como

imágenes y GIF, en CloudFront en América del Norte. Esto significa que obtienen contenido lo más cerca posible de ellos, Norteamérica, en este caso, cuando acceden al sitio.

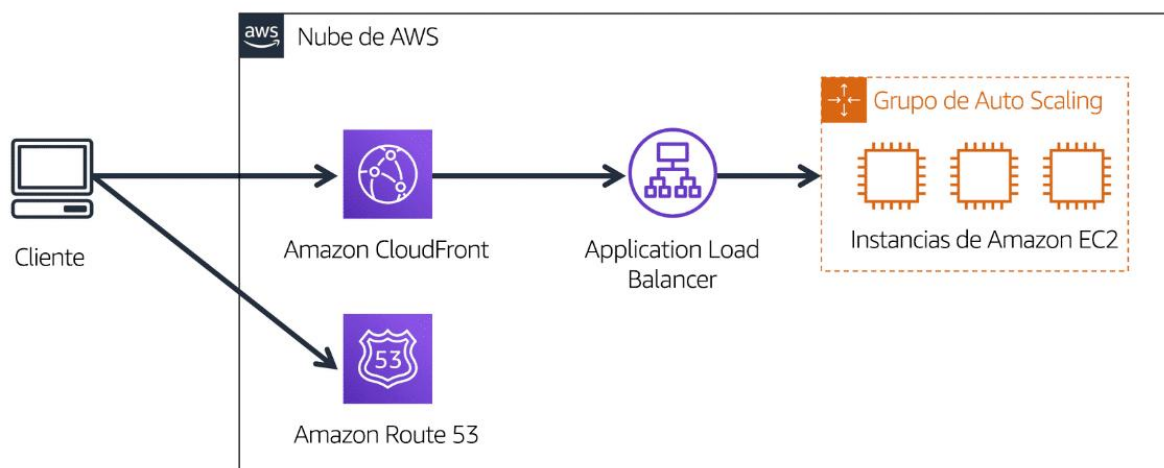
Pero para nuestros usuarios irlandeses no tiene sentido entregar esos activos fuera de Oregón, ya que la latencia no es favorable. Por lo tanto, implementamos esos mismos activos estáticos en CloudFront, pero esta vez en la región de Dublín.

Eso significa que pueden acceder al mismo contenido, pero desde un lugar más cercano a ellos, lo que a su vez mejora la latencia.

Las ubicaciones de borde de AWS ejecutan Amazon CloudFront para ayudar a acercar el contenido a sus clientes, sin importar en qué parte del mundo estén.

Ejemplo de cómo Amazon Route 53 y Amazon CloudFront entregan contenido

En el siguiente ejemplo se describe cómo Route 53 y Amazon CloudFront trabajan conjuntamente para entregar contenido a los clientes.



Supongamos que la aplicación de AnyCompany funciona en varias instancias de Amazon EC2. Estas instancias se encuentran en un grupo de Auto Scaling que se adjunta a un equilibrador de carga de aplicaciones.

1. Un cliente solicita datos de la aplicación si accede al sitio web de AnyCompany.

2. Amazon Route 53 utiliza la resolución de DNS para identificar la dirección IP correspondiente de AnyCompany.com, 192.0.2.0. Esta información se devuelve al cliente.
3. La solicitud del cliente se envía a la ubicación perimetral más cercana a través de Amazon CloudFront.
4. Amazon CloudFront se conecta al Application Load Balancer, que envía el paquete entrante a una instancia de Amazon EC2.

CONCLUSIONES

- Las redes solían ser el dominio exclusivo de los genios de la topología. Con AWS, las redes ahora se simplifican y se resumen para responder a la sencilla pregunta de quiénes deberían poder comunicarse entre sí. Siempre que pueda responder a esa pregunta, podrá configurar su red en AWS.
- Las VPC permiten aprovisionar de manera lógica una sección aislada de la nube de AWS, donde se lanzan los recursos de AWS en una red virtual definida. Dichos recursos pueden ser públicos para que tengan acceso a Internet, o privados sin acceso a Internet.
- Las listas de control de acceso a la red (ACL) de una cuenta de AWS son sin estado y permiten todo el tráfico entrante y saliente; mientras que los grupos de seguridad realizan el filtrado de paquetes con estado, deniegan todo el tráfico entrante y permite todo el tráfico saliente.
- Es fundamental entender la diferencia entre un grupo de seguridad y una ACL de red: El grupo de seguridad cuenta con estado, lo que significa que tiene algún tipo de memoria cuando se trata de a quién permite la entrada o la salida, y la ACL de red no tiene estado, es decir, que no recuerda nada y comprueba cada paquete que cruza su frontera.
- Una buena seguridad de red debe aprovechar tanto las ACL de red como los grupos de seguridad, porque la seguridad detallada es fundamental en las arquitecturas modernas.