AWS Academy Cloud Foundations (LA)

Module 05 Student Guide

Versión 2.0.19

100-ACCLFO-20-LA-SG

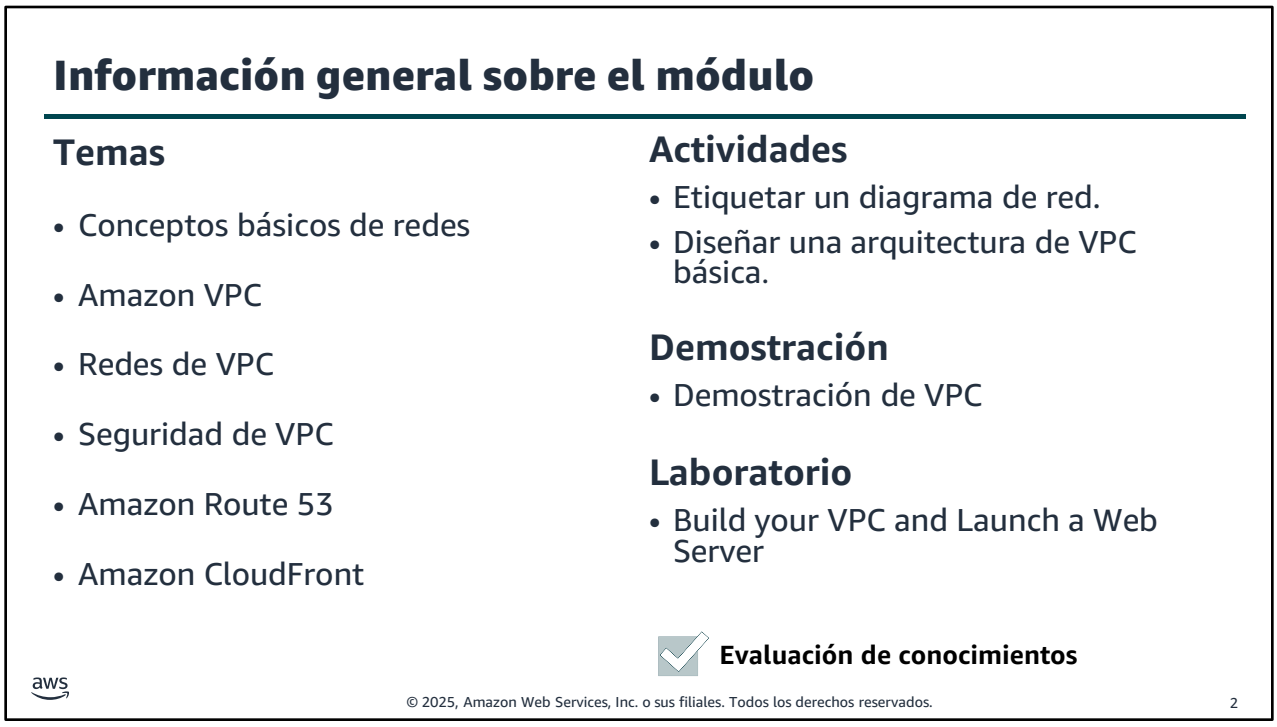
Para correcciones o comentarios relacionados con el curso, contacte con nosotros en https://support.aws.amazon.com/#/contacts/aws-training.

Contenido

Módulo 5: Redes y entrega de contenido 4

Le doy la bienvenida al Módulo 5: Redes y entrega de contenido

Este módulo cubre tres productos de Amazon Web Services (AWS) fundamentales para la creación de redes y la entrega de contenido: Amazon Virtual Private Cloud (Amazon VPC), Amazon Route 53 y Amazon CloudFront.



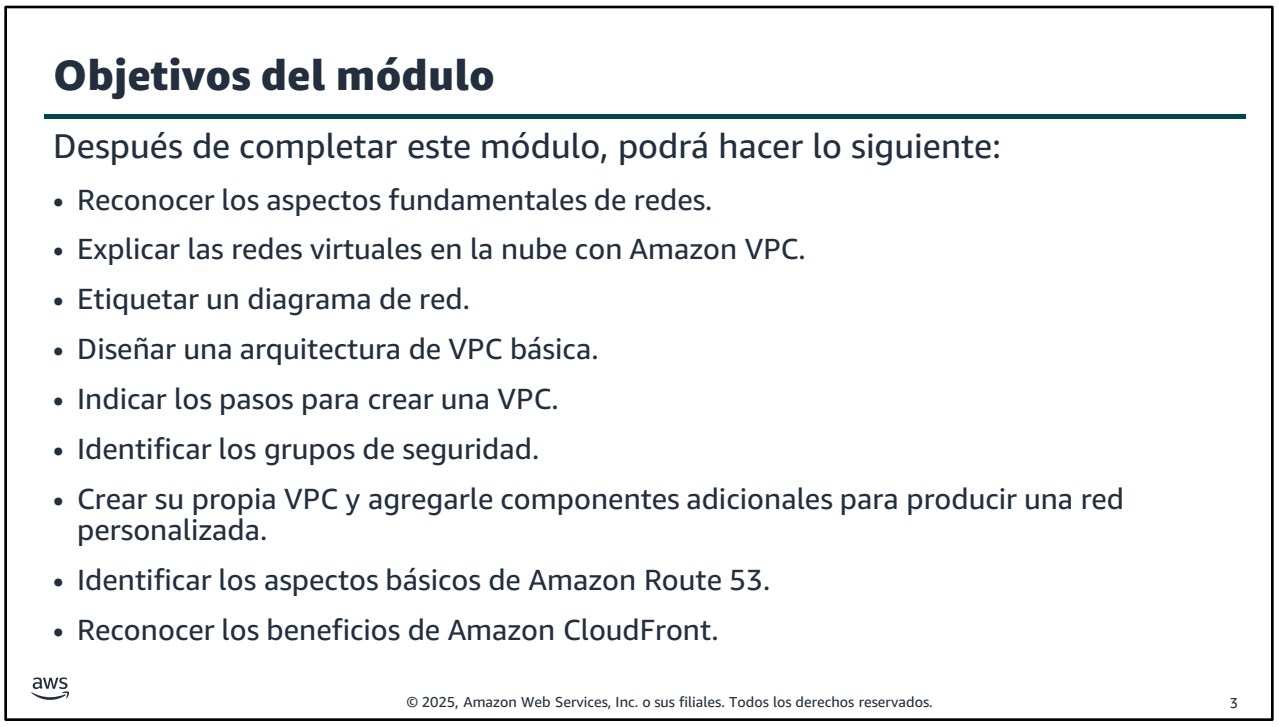
Este módulo aborda los siguientes temas:
- Conceptos básicos de redes
- Amazon Virtual Private Cloud (Amazon VPC)
- Redes de VPC
- Seguridad de VPC
- Amazon Route 53
- Amazon CloudFront

Este módulo incluye algunas actividades que lo desafían a etiquetar un diagrama de red y diseñar una arquitectura VPC básica.

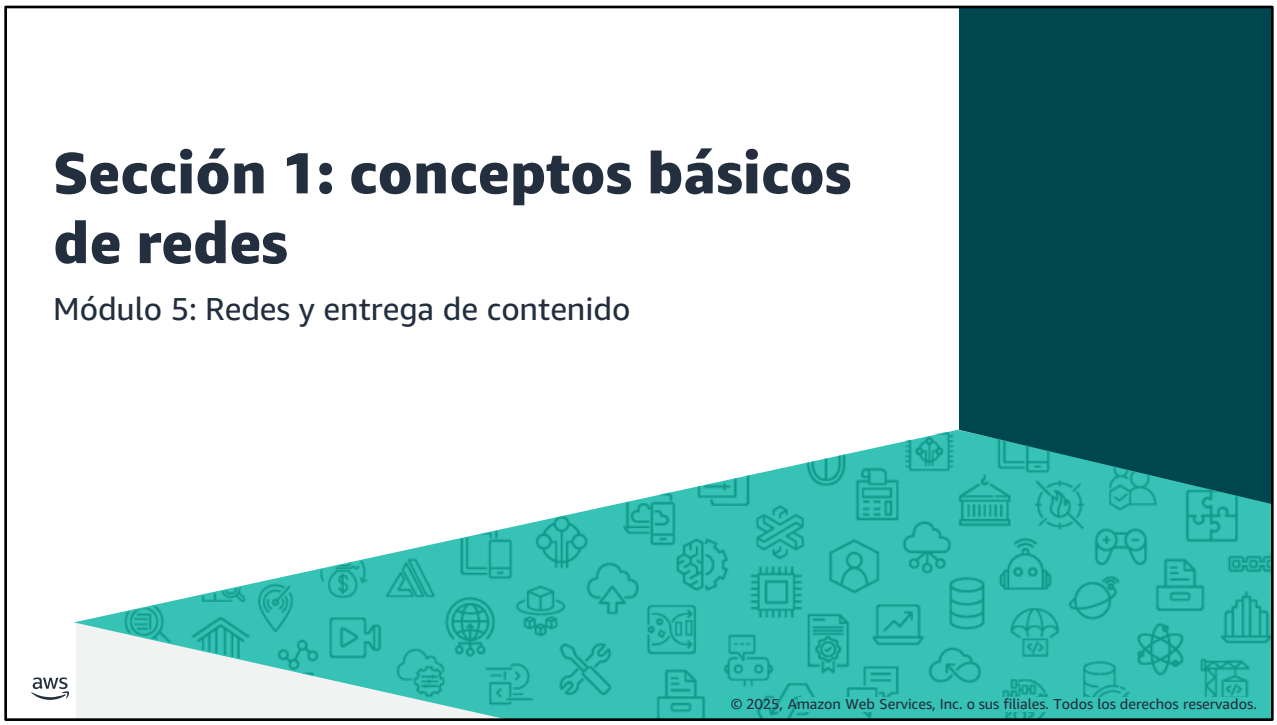
Verá una demostración grabada para aprender a utilizar el VPC Wizard para crear una VPC con subredes públicas y privadas.

Luego tendrá la oportunidad de aplicar lo aprendido en un laboratorio práctico en el que utilizará el VPC Wizard para crear una VPC e iniciar un servidor web.

Finalmente, se le pedirá que complete una evaluación de conocimientos que pondrá a prueba su comprensión de los conceptos clave que se abordan en este módulo.

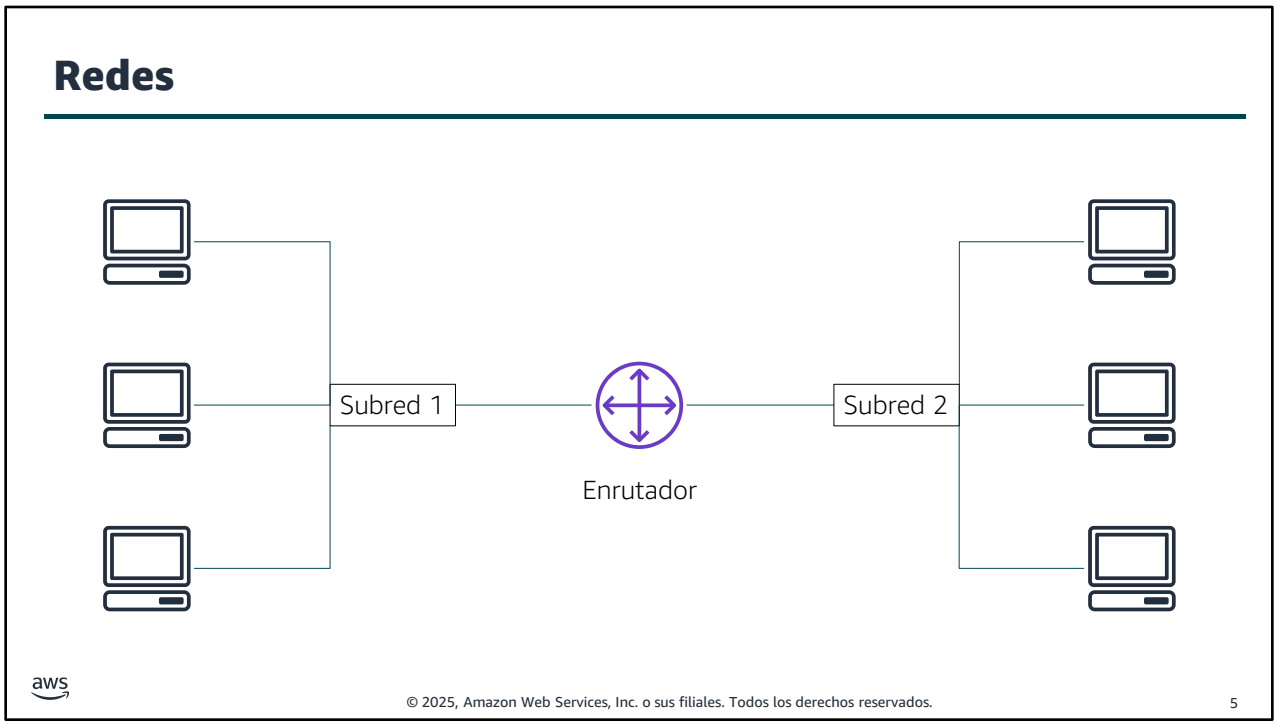


Después de completar este módulo, podrá hacer lo siguiente:
- Reconocer los aspectos fundamentales de redes.
- Explicar las redes virtuales en la nube con Amazon VPC.
- Etiquetar un diagrama de red.
- Diseñar una arquitectura de VPC básica.
- Indicar los pasos para crear una VPC.
- Identificar los grupos de seguridad.
- Crear su propia VPC y agregarle componentes adicionales para producir una red personalizada.
- Identificar los aspectos básicos de Amazon Route 53.
- Reconocer los beneficios de Amazon CloudFront.

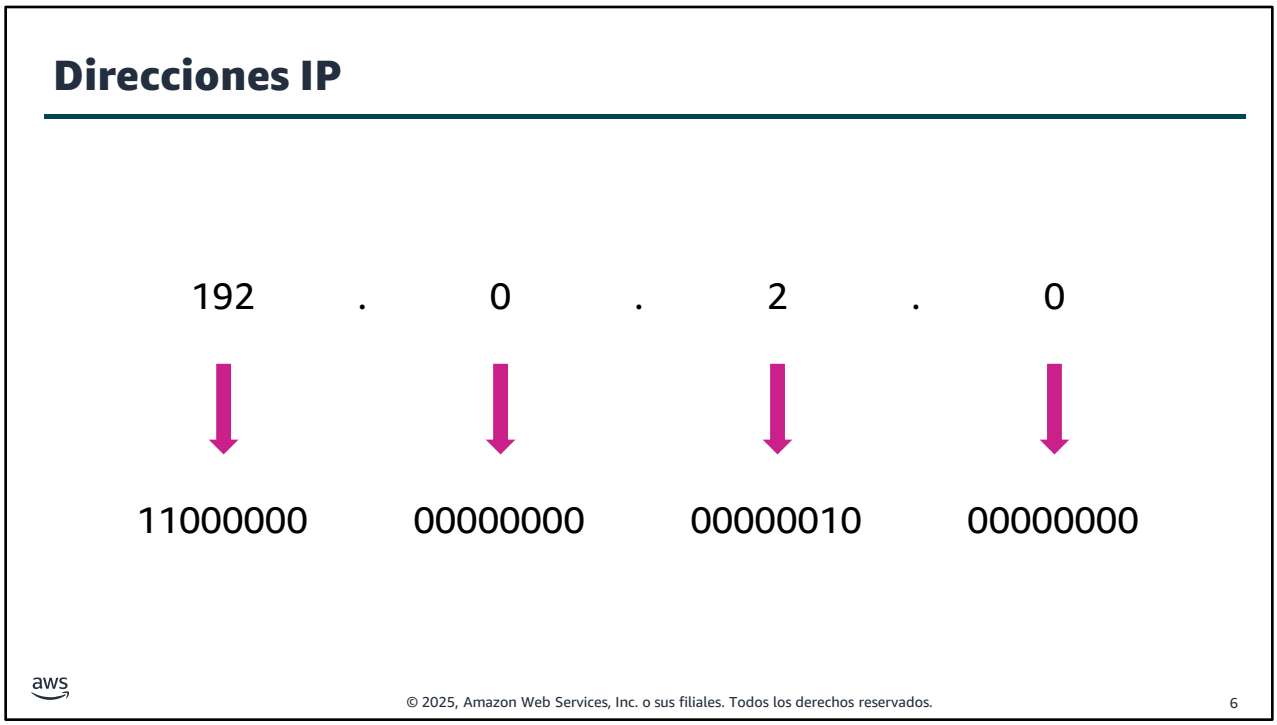


Sección 1: conceptos básicos de redes

En esta sección, revisará algunos conceptos básicos de redes que brindan la base necesaria para comprender el servicio de redes de AWS, Amazon Virtual Private Cloud (Amazon VPC).

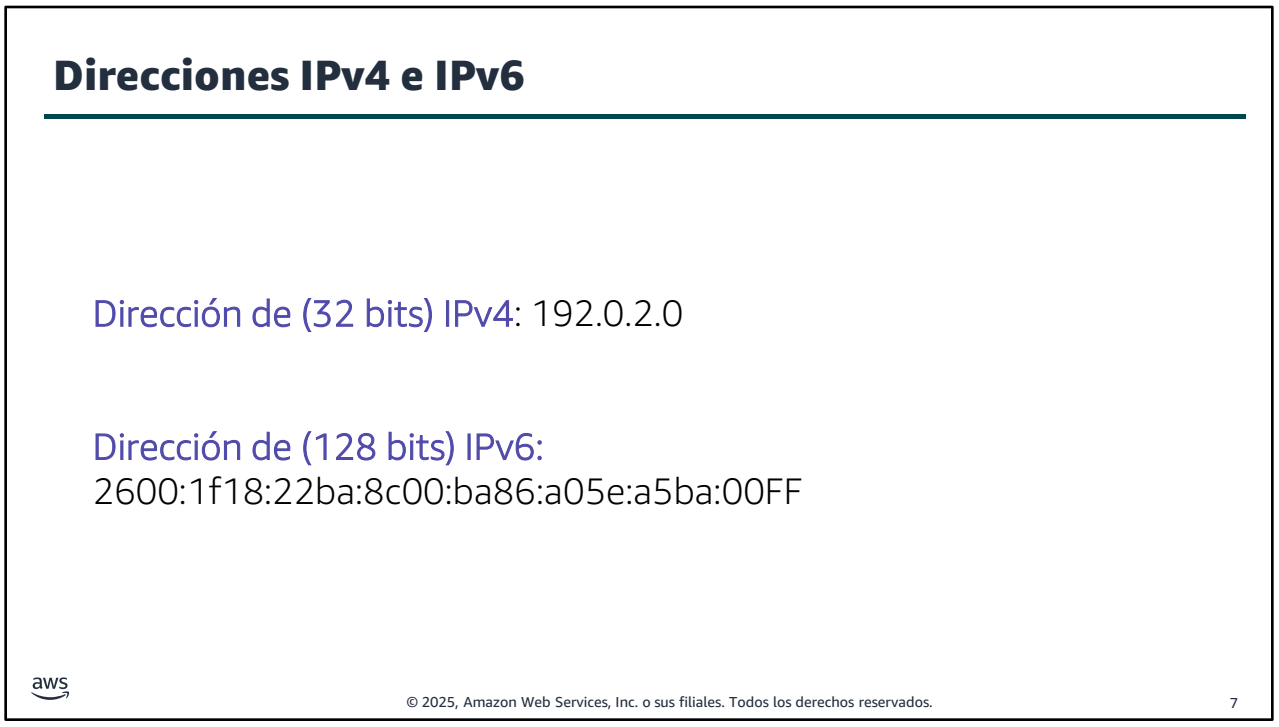


Una *red* informática consiste en dos o más máquinas clientes que están conectadas para compartir recursos. Una red se puede dividir lógicamente en *subredes*. Las redes requieren un dispositivo de red (como un enrutador y un conmutador) para conectar todos los clientes y permitir la comunicación entre ellos.



Cada máquina cliente en una red tiene una dirección de protocolo de internet (IP) única que la identifica. Una dirección IP es una etiqueta numérica en formato decimal. Las máquinas convierten el formato numérico decimal en formato binario.

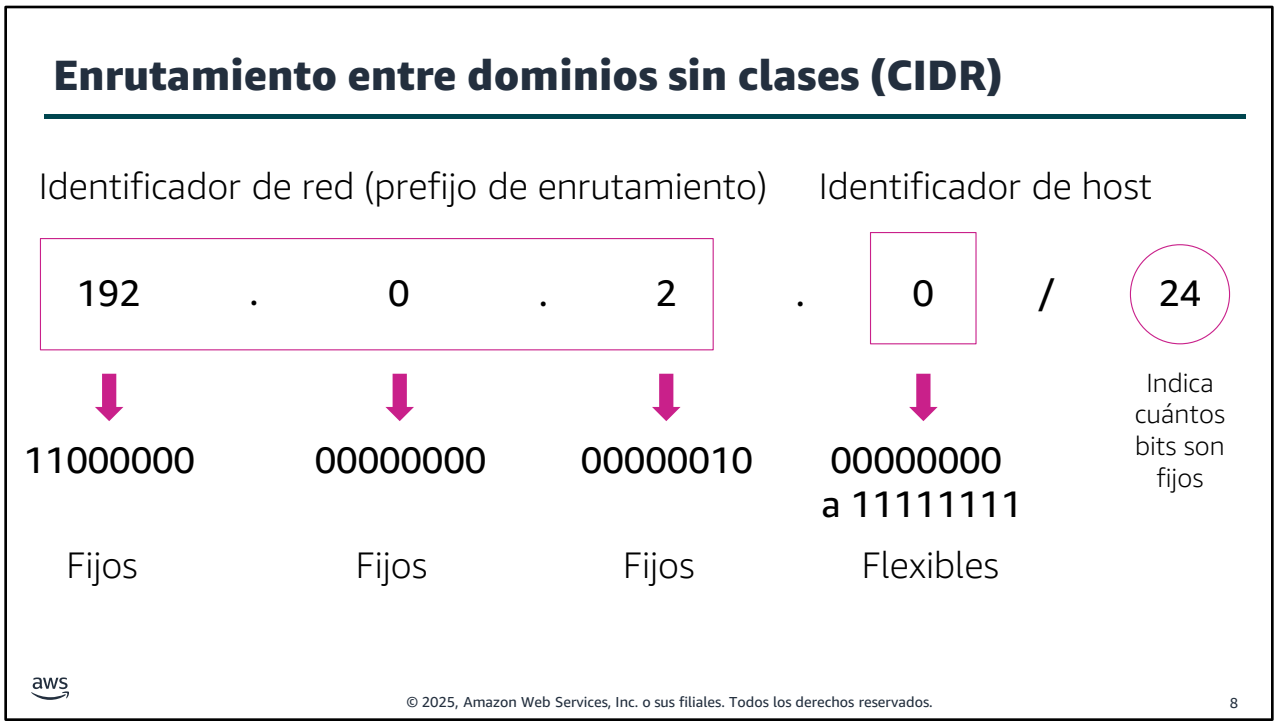
En este ejemplo, la dirección de IP es 192.0.2.0. Cada uno de los cuatro números separados por puntos (.) de la dirección IP representa 8 bits en formato de número octal. Eso significa que cada uno de los cuatro números puede ser del 0 al 255. El total combinado de los cuatro números de una dirección IP es de 32 bits en formato binario.



Una dirección IP de 32 bits se denomina dirección IPv4.

También están disponibles las direcciones IPv6, que son de 128 bits. Las direcciones IPv6 pueden acomodar más dispositivos de usuario.

Las direcciones IPv6 están compuestas de ocho grupos de cuatro letras y números separados por dos puntos (:). En este ejemplo, la dirección IPv6 es: 2600:1f18:22ba:8c00:ba86:a05e:a5ba:00FF Cada uno de los ocho grupos separados por dos puntos de la dirección IPv6 representa 16 bits en formato numérico hexadecimal. Eso significa que cada uno de los ocho grupos puede ser del 0 al FFFF. El total combinado de los ocho grupos de una dirección IP IPv6 es de 128 bits en formato binario.



Un método común para describir redes es el Enrutamiento entre dominios sin clases (CIDR). La dirección del CIDR se expresa de la siguiente manera:

- Un dirección IP (que es la primera dirección de la red).
- A continuación, un carácter de barra (/).
- Finalmente, un número indica cuántos bits del prefijo de enrutamiento deben fijarse o asignarse para el identificador de la red.

Los bits que no están fijos pueden cambiar. CIDR es una forma de expresar un grupo de direcciones IP consecutivas entre sí.

En este ejemplo, el CIDR es 192.0.2.0/24. El último número (24) le informa que los primeros 24 bits no se pueden cambiar. Los últimos 8 bits son flexibles, lo que significa que hay 2^8 (o 256) direcciones IP disponibles para la red, que van desde 192.0.2.0 a 192.0.2.255. Se permite que el cuarto dígito decimal cambie de 0 a 255.

Si el CIDR era 192.0.2.0/16, el último número (16) le informa que los primeros 16 bits no se pueden cambiar. Los últimos 16 bits son flexibles, lo que significa que hay 2^{16} (o 65.536) direcciones IP disponibles para la red, que van desde 192.0.0.0 a 192.0.255.255. El tercer y cuarto dígito decimal pueden cambiar de 0 a 255.

Hay dos casos especiales:

- Las direcciones IP fijas, en las que todos los bits son fijos, representan una única dirección IP (por ejemplo, *192.0.2.0/32)*. Es tipo de dirección es útil cuando quiere configurar una regla de firewall y dar acceso a un host específico.
- Internet, donde todos los bits son flexibles, se representa como 0.0.0.0/0

Modelo de interconexión de sistemas abiertos (OSI)

Capa	Número	Función	Protocolo/Dirección
Aplicación	7	Medios para que una aplicación acceda a una red informática.	HTTP(S), FTP, DHCP, LDAP
Presentación	6	• Garantiza que la capa de aplicación pueda leer los datos. • Cifrado.	ASCII, ICA
Sesión	5	Permite el intercambio ordenado de datos.	NetBIOS, RPC
Transporte	4	Proporciona protocolos para respaldar la comunicación de host a host.	TCP y UDP
Red	3	Enrutamiento y reenvío de paquetes (enrutadores).	IP
Enlace de datos	2	Transfiere datos en la misma red LAN (puentes y conmutadores).	MAC
Física	1	Transmisión y recepción de flujos de bits sin procesar a través de un medio físico (concentradores).	Señales (1 y 0)

aws

 9

El modelo de interconexión de sistemas abiertos (OSI) es un modelo conceptual que se utiliza para explicar cómo viajan los datos a través de una red. Consta de siete capas y muestra los protocolos y direcciones comunes que se utilizan para enviar datos en cada capa. Por ejemplo, los concentradores y conmutadores funcionan en la capa 2 (la capa de enlace de datos). Los enrutadores funcionan en la capa 3 (la capa de red). El modelo de interconexión de sistemas abiertos (OSI) también se puede utilizar para comprender cómo se produce la comunicación en una nube virtual privada (VPC), algo que aprenderá en la siguiente sección.

ICA es una arquitectura de computación independiente, desarrollada por Citrix Systems para facilitar la transferencia de datos eficiente entre un servidor y un cliente.

Sección 2: Amazon VPC

Muchos de los conceptos de una red local se aplican a una red basada en la nube, pero gran parte de la complejidad de configurar una red se ha abstraído sin sacrificar el control, la seguridad y la usabilidad. En esta sección, aprenderá sobre Amazon VPC y los componentes fundamentales de una VPC.

Amazon VPC

Amazon VPC

- Le permite aprovisionar una sección aislada de forma lógica de la nube de AWS, donde puede iniciar recursos de AWS en una red virtual que usted defina.
- Le permite controlar sus recursos de redes virtuales, entre ellos:
  - Selección de un rango de direcciones IP
  - Creación de subredes
  - Configuración de tablas de enrutamiento y puertas de enlace de red
- Le permite personalizar la configuración de red de su VPC.
- Le permite utilizar varias capas de seguridad.

aws

 11

Amazon Virtual Private Cloud (Amazon VPC) es un servicio que permite aprovisionar una sección aislada de forma lógica de la nube de AWS (llamada nube virtual privada o VPC) en la que puede iniciar recursos de AWS.

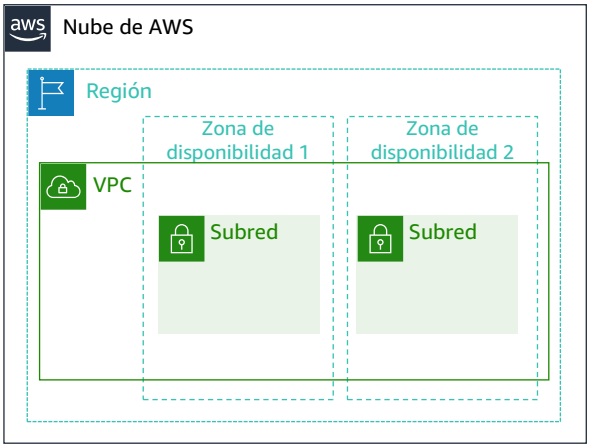
Amazon VPC le brinda control de todos los recursos de red virtual, incluida la selección de su propio intervalo de direcciones IP, la creación de subredes y la configuración de tablas de enrutamiento y puertas de enlace de red. Puede usar IPv4 e IPv6 en su VPC para un acceso seguro a los recursos y las aplicaciones.

También puede personalizar la configuración de red de su VPC. Por ejemplo, puede crear una subred pública para sus servidores web que puedan acceder a la internet pública. Puede colocar sus sistemas de backend (como bases de datos o servidores de aplicaciones) en una subred privada sin acceso público a internet.

Finalmente, puede utilizar varias capas de seguridad, incluidos los grupos de seguridad y las listas de control de acceso (ACL de redes) para ayudar a controlar el acceso a las instancias de Amazon Elastic Compute Cloud (Amazon EC2) en cada subred.

VPC y subredes

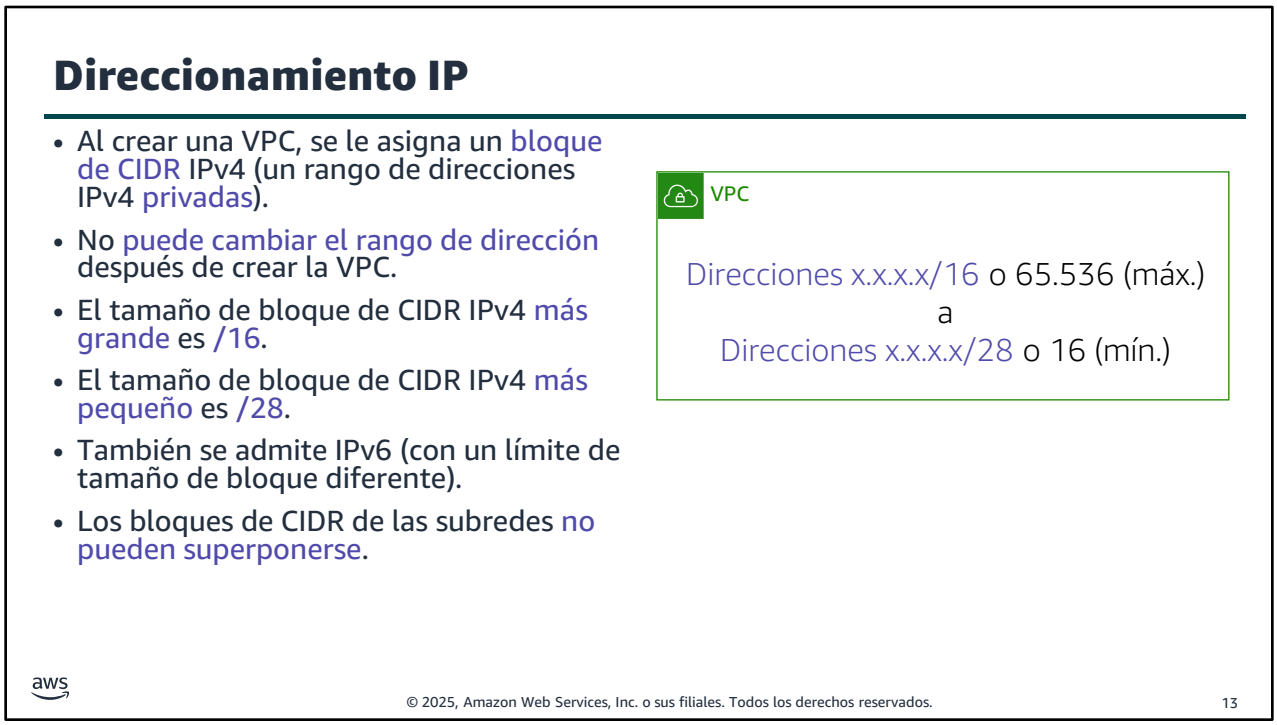
- VPC:
  - Se encuentra aislada de forma lógica de otras VPC
  - Dedicada a su cuenta de AWS
  - Pertenece a una única región de AWS y puede abarcar varias zonas de disponibilidad
- Subredes:
  - Intervalo de direcciones IP que divide una VPC
  - Pertenece a una única zona de disponibilidad
  - Se clasifica como pública o privada



 12

Amazon VPC le permite aprovisionar nubes virtuales privadas (VPC). Una *VPC* es una red virtual que está aislada de forma lógica de otras redes virtuales en la nube de AWS. Una VPC está dedicada a su cuenta. Las VPC pertenecen a una única región de AWS y puede abarcar varias zonas de disponibilidad.

Después de crear una VPC, puede dividirla en una o más subredes. Una *subred* es un intervalo de direcciones IP en una VPC. Las subredes pertenecen a una única zona de disponibilidad. Puede crear subredes en diferentes zonas de disponibilidad. Las subredes suelen clasificarse como públicas o privadas. Las *subredes públicas* tienen acceso directo a internet, pero las *subredes privadas* no.



Las direcciones IP habilitan los recursos de su VPC para comunicarse entre sí y con los recursos de internet. Al crear una VPC, se le asigna un bloque de CIDR IPv4 (un rango de direcciones IPv4 *privadas*). Después de crear una VPC, no se puede cambiar el rango de direcciones, por lo que es importante elegirlo con cuidado. El bloque de CIDR IPv4 puede ser tan grande como /16 (que son 2^{16}, o 65.536 direcciones) o tan pequeño como /28 (que son 2^4, o 16 direcciones).

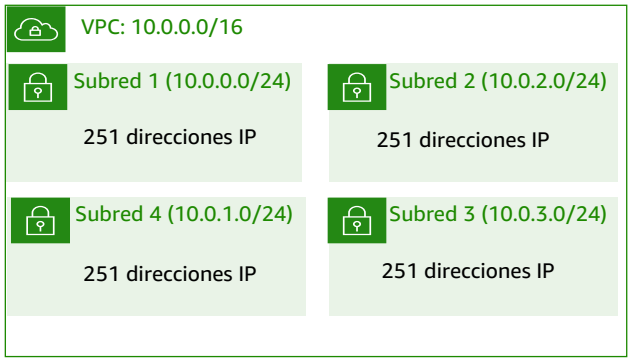
Opcionalmente, puede asociar un bloque de CIDR IPv6 con su VPC y subredes, y asignar direcciones IPv6 de ese bloque a los recursos en su VPC. Los bloques de CIDR IPv6 tienen un límite de tamaño de bloque diferente.

El bloque de CIDR de una subred puede ser el mismo que el bloque de CIDR para la VPC. En este caso, la VPC y la subred tienen el mismo tamaño (la VPC tiene una única subred). Además, el bloque de CIDR de una subred puede ser un subconjunto del bloque de CIDR para la VPC. Esta estructura permite la definición de múltiples subredes. Si crea más de una subred en una VPC, los bloques de CIDR de las subredes no pueden superponerse. No puede tener direcciones IP duplicadas en la misma VPC.

Para obtener más información sobre direccionamiento IP en una VPC, consulte la Documentación de AWS en https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html.

Direcciones IP reservadas

Ejemplo: una VPC con un bloque de CIDR IPv4 de 10.0.0.0/16 tiene 65.536 direcciones IP en total. La VPC tiene cuatro subredes del mismo tamaño. Solamente hay 251 direcciones IP disponibles para su uso en cada subred.



Direcciones IP para el bloque de CIDR 10.0.0.0/24	Reservado para
10.0.0.0	Direcciones de red
10.0.0.1	Comunicaciones internas
10.0.0.2	Resolución del sistema de nombres de dominio (DNS)
10.0.0.3	Uso futuro
10.0.0.255	Dirección de difusión de red

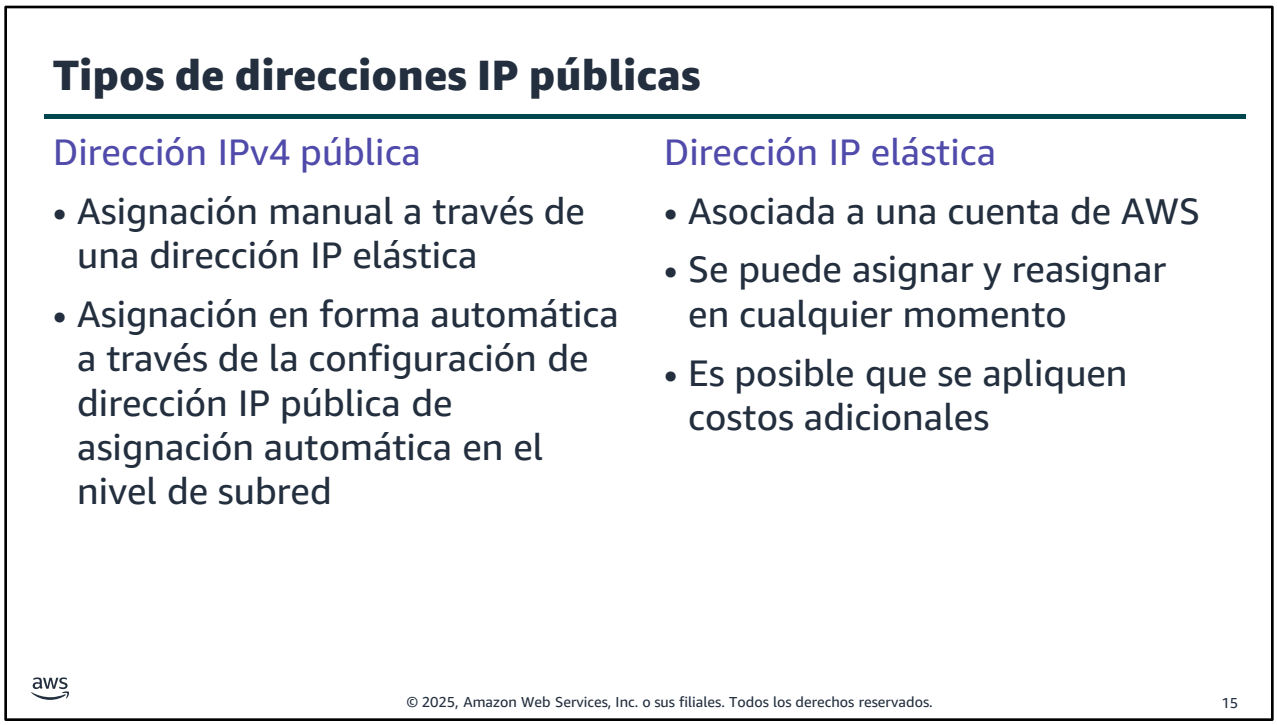
aws

 14

Al crear una subred, esta necesita su propio bloque de CIDR. Para cada bloque de CIDR que especifique, AWS reserva cinco direcciones IP dentro de ese bloque y esas direcciones no están disponibles para usarse. AWS se reserva cinco direcciones IP para:

- Direcciones de red
- Enrutador local de la VPC (comunicaciones internas)
- Resolución del sistema de nombres de dominio (DNS)
- Uso futuro
- Dirección de difusión de red

Por ejemplo, supongamos que se crea una subred con un bloque de CIDR IPv4 de 10.0.0.0/24 (que tiene 256 direcciones IP en total). La subred tiene 256 direcciones IP, pero solo 251 están disponibles porque 5 están reservadas.



Cuando crea una VPC, cada instancia de esa VPC obtiene automáticamente una dirección IP privada. También puede solicitar que se asigne una dirección IP pública cuando crea la instancia al modificar las propiedades de asignación automática de dirección IP pública de la subred.

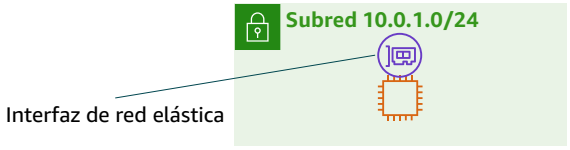
Una *dirección IP elástica* es una dirección de IPv4 estática y pública que está diseñada para el cómputo en la nube dinámico. Puede asociar una dirección IP elástica a cualquier instancia o interfaz de red de cualquier VPC de su cuenta. Con una dirección IP elástica, puede reasignar rápidamente la dirección a otra instancia de su VPC para enmascarar los errores de una instancia. Asociar la dirección IP elástica con la interfaz de red tiene una ventaja sobre asociarla directamente con la instancia. Puede mover todos los atributos de la interfaz de red de una instancia a otra en un solo paso.

Es posible que se apliquen costos adicionales cuando utilice direcciones IP elásticas, por lo que es importante liberarlas cuando ya no las necesite.

Para obtener más información sobre las direcciones IP elásticas, consulte Direcciones IP elásticas en la Documentación de AWS en https://docs.aws.amazon.com/vpc/latest/userguide/vpc-eips.html.

Interfaz de red elástica

- Una interfaz de red elástica es una interfaz de red virtual que puede:
  - Adjuntar a una instancia.
  - Desconectar de la instancia y conectarla a otra instancia para redirigir el tráfico de red.
- Sus atributos siguen cuando se reasigna a una nueva instancia.
- Cada instancia de su VPC tiene una interfaz de red predeterminada a la que se asigna una dirección IPv4 privada del intervalo de direcciones IPv4 de la VPC.



16

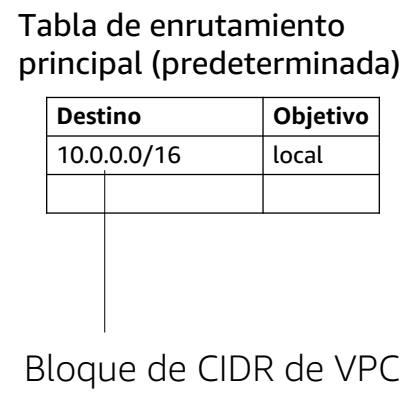
Una *interfaz de red elástica* es una interfaz de red virtual que se puede conectar o desconectar de una instancia en una VPC. Los atributos de una interfaz de red la siguen cuando se vuelve a conectar a otra instancia. Cuando mueve una interfaz de red de una instancia a otra, el tráfico de la red se redirige a la nueva instancia.

Cada instancia de su VPC tiene una interfaz de red predeterminada (la interfaz de red principal) a la que se puede asignar una dirección IPv4 privada del intervalo de su VPC. No se puede desconectar una interfaz de red principal de una instancia. Puede crear y adjuntar una interfaz de red adicional a cualquier instancia de su VPC. El número de interfaces de red que se pueden conectar varía según el tipo de instancia.

Para obtener más información sobre las Interfaces de red elásticas, consulte la Documentación de AWS en https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html.

Tablas de enrutamiento y rutas

- Una tabla de enrutamiento contiene un conjunto de reglas (o rutas) que puede configurar para dirigir el tráfico de red de su subred.
- Cada ruta especifica un destino y un objetivo.
- De forma predeterminada, cada tabla de enrutamiento contiene una ruta local para la comunicación dentro de la VPC.
- Cada subred de su VPC debe estar asociada a una tabla de enrutamiento (cómo máximo una).



17

Una *tabla de enrutamiento* contiene una serie de reglas (llamadas *rutas*) que determinan hacia dónde se dirige el tráfico de red de su subred. Cada ruta especifica un *destino* y un *objetivo*. El *destino* es el bloque de CIDR de destino, a donde desea que vaya el tráfico de su subred. El *objetivo* es el objetivo a través del cual se envía el tráfico de destino. De forma predeterminada, cada tabla de enrutamiento que crea contiene una *ruta local* para la comunicación dentro de la VPC. Puede personalizar las tablas de enrutamiento al agregar rutas. No puede eliminar la entrada de ruta local, que se utiliza para las comunicaciones internas.

Cada subred en su VPC se debe asociar a una tabla de enrutamiento. La *tabla de enrutamiento principal* es la tabla de enrutamiento que se asigna automáticamente a su VPC. Esta controla el enrutamiento de todas las subredes que no estén asociadas de forma explícita a ninguna otra tabla de enrutamiento. Una subred puede asociarse solamente a una tabla de enrutamiento por vez, pero pueden asociarse varias subredes a la misma tabla de enrutamiento.

Para obtener más información sobre las tablas de enrutamiento, consulte la Documentación de AWS en https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Route_Tables.html.

Sección 2: conclusiones importantes

- Una VPC es una sección aislada de forma lógica de la nube de AWS.
- Una VPC pertenece a una región y requiere un bloque de CIDR.
- Una VPC se subdivide en subredes.
- Una subred pertenece a una zona de disponibilidad y requiere un bloque de CIDR.
- Tablas de enrutamiento para controlar el flujo de tráfico para una subred.
- Las tablas de enrutamiento tienen una ruta local integrada.
- Tiene rutas adicionales para la tabla.
- La ruta local no se puede eliminar.

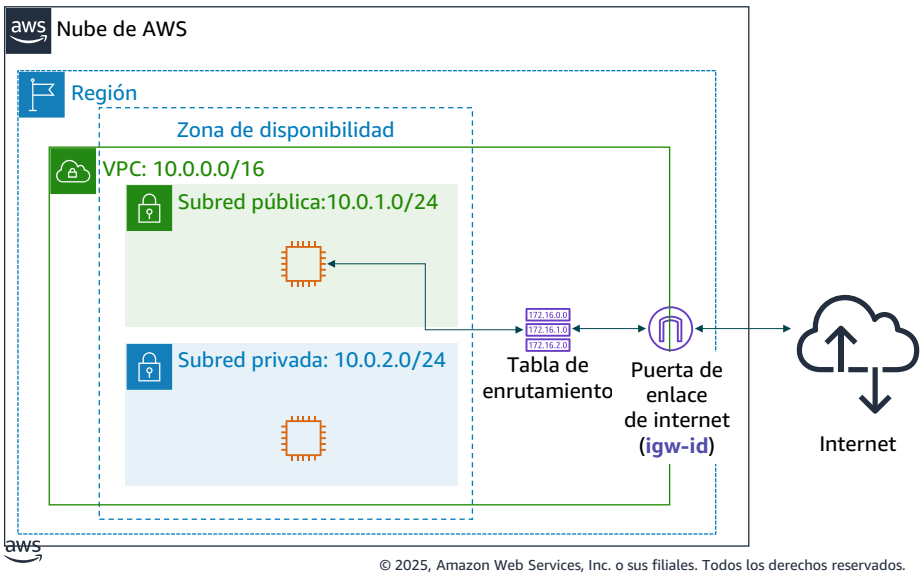
 18

Estas son algunas conclusiones clave de esta sección del módulo:
- Una VPC es una sección aislada de forma lógica de la nube de AWS.
- Una VPC pertenece a una región y requiere un bloque de CIDR.
- Una VPC se subdivide en subredes.
- Una subred pertenece a una zona de disponibilidad y requiere un bloque de CIDR.
- Tablas de enrutamiento para controlar el flujo de tráfico para una subred.
- Las tablas de enrutamiento tienen una ruta local integrada.
- Tiene rutas adicionales para la tabla.
- La ruta local no se puede eliminar.

Sección 3: redes de VPC

Ahora que ha aprendido acerca de los componentes básicos de una VPC, puede comenzar a enrutar el tráfico de maneras interesantes. En esta sección, aprenderá sobre diferentes opciones de redes.

Puerta de enlace de internet

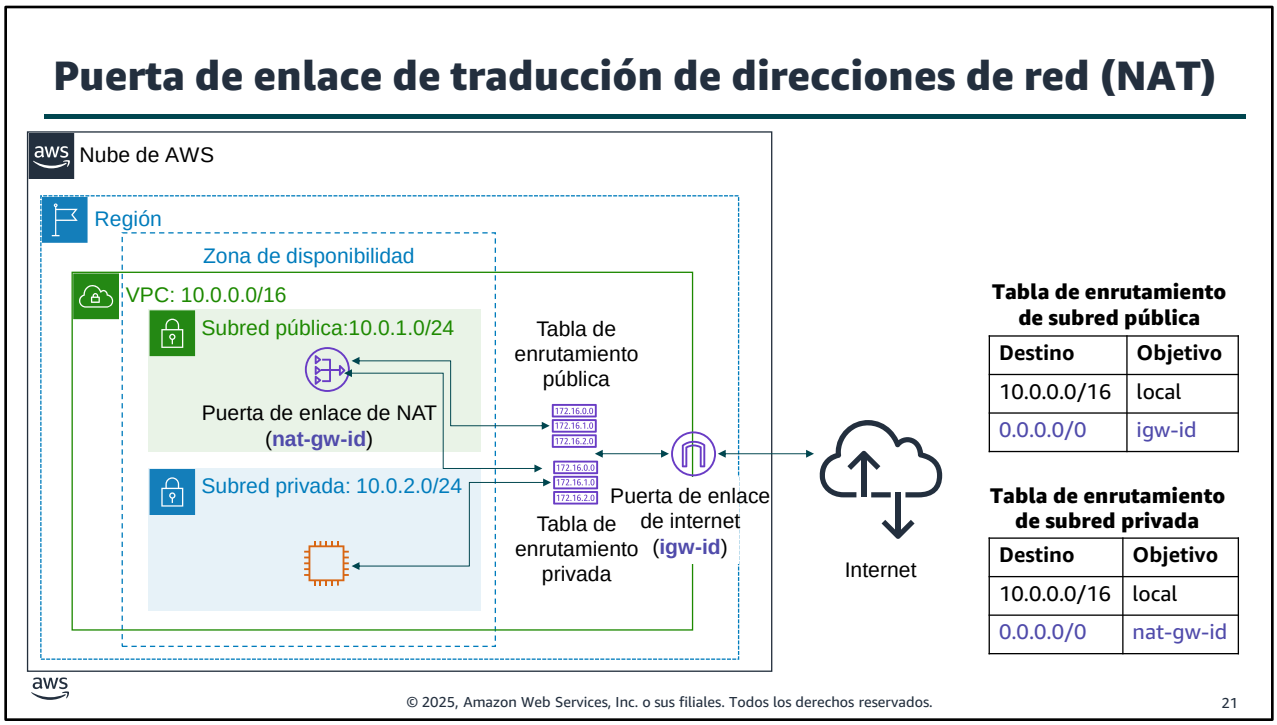


 20

Una *puerta de enlace de internet* es un componente de la VPC de alta disponibilidad, redundante y escalable que permite la comunicación entre las instancias en la VPC e internet. Una puerta de enlace de internet tiene dos funciones: proporcionar un objetivo en las tablas de enrutamiento de VPC para el tráfico que se puede enrutar a través de internet y traducir direcciones de red para instancias a las cuales se les asignaron direcciones IPv4 públicas..

Para que una subred sea *pública*, puede adjuntar una *puerta de enlace de internet* a su VPC y agregar una ruta a la tabla de enrutamiento para enviar tráfico no local a través de la puerta de enlace de internet a internet (0.0.0.0/0).

Para obtener más información sobre las puertas de enlace de internet, consulte Puertas de enlace de internet, en la Documentación de AWS en https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Internet_Gateway.html.

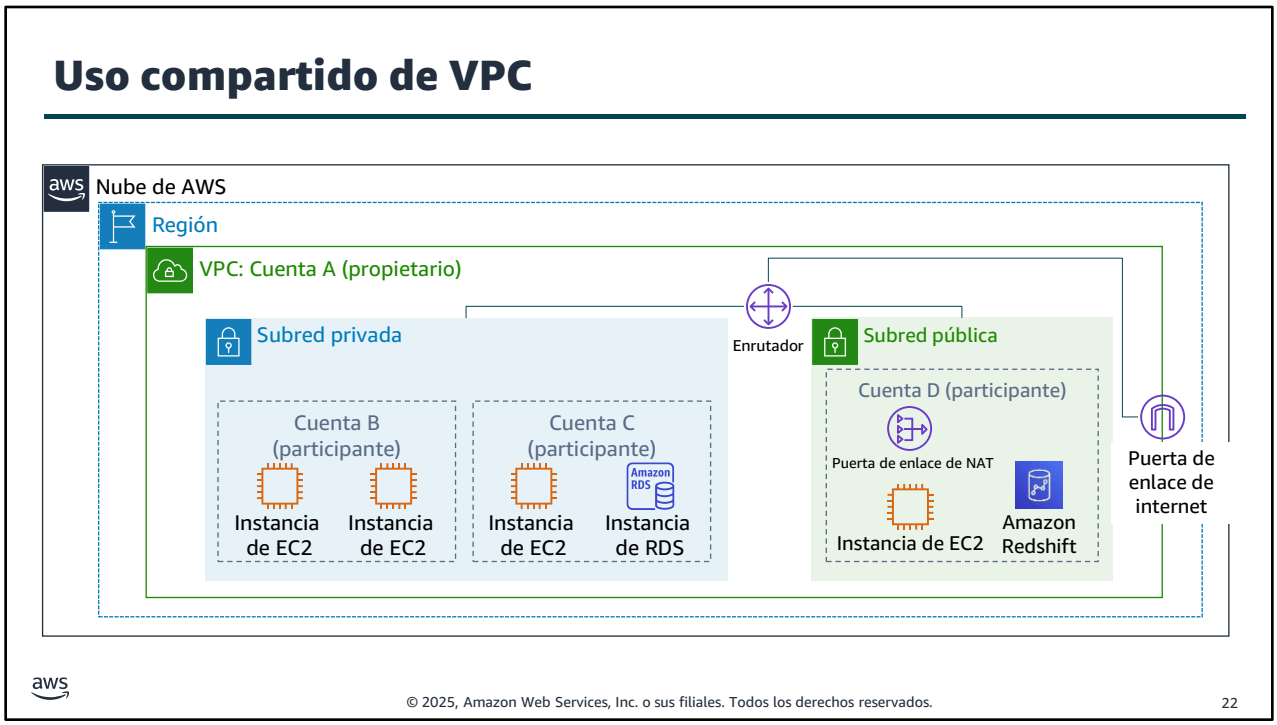


Una *puerta de enlace de traducción de direcciones de red (NAT)* habilita las instancias de una subred privada para conectarse a internet o a otros servicios de AWS, pero impide que internet inicie una conexión con esas instancias.

Para crear una puerta de enlace de NAT, debe especificar la subred pública en la que se debe ubicar la puerta de enlace de NAT. También debe especificar una dirección IP elástica para asociar a la puerta de enlace de NAT cuando la cree. Después de crear una puerta de enlace de NAT, debe actualizar la tabla de enrutamiento que está asociada a una o más de las subredes privadas para dirigir el tráfico de internet a la puerta de enlace de NAT. De esa manera, las instancias de sus subredes privadas se pueden comunicar con internet.

También puede utilizar una instancia de NAT en una subred pública de su VPC en lugar de una puerta de enlace de NAT. Sin embargo, una puerta de enlace de NAT es un servicio NAT administrado que ofrece mayor disponibilidad, mayor ancho de banda y menos esfuerzo administrativo. Para los casos de uso habituales, AWS recomienda utilizar una puerta de enlace de NAT en lugar de una instancia de NAT.

Consulte la documentación de AWS para obtener más información sobre:
- Puertas de enlace de NAT en https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html.
- Instancias de NAT en https://docs.aws.amazon.com/vpc/latest/userguide/VPC_NAT_Instance.html.
- Diferencias entre puertas de enlace de NAT e instancias de NAT en https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-comparison.html.



El uso compartido de VPC permite a los clientes compartir subredes con otras cuentas de AWS en la misma organización en AWS Organizations. El uso compartido de VPC permite que varias cuentas de AWS creen sus recursos de aplicaciones, como instancias de Amazon EC2, bases de datos de Amazon Relational Database Service (Amazon RDS), clústeres de Amazon Redshift y funciones de Lambda en VPC administradas compartidas. En este modelo, la cuenta propietaria de la VPC (propietario) comparte una o más subredes con otras cuentas (participantes) que pertenecen a la misma organización en AWS Organizations. Después de compartir una subred, los participantes pueden ver, crear, modificar y eliminar los recursos de su aplicación en las subredes que se comparten con ellos. Los participantes no pueden ver, modificar ni eliminar recursos que pertenezcan a otros participantes o al propietario de la VPC.

El uso compartido de VPC ofrece varios beneficios:

- Separación de funciones: estructura de VPC, enrutamiento y asignación de direcciones IP controlados centralmente.
- Propiedad: los propietarios de aplicaciones siguen siendo propietarios de recursos, cuentas y grupos de seguridad.
- Grupos de seguridad: los participantes que comparten VPC pueden hacer referencia a los ID de grupo de seguridad de cada uno.
- Eficiencias: mayor densidad en subredes, uso eficiente de VPN y AWS Direct Connect
- Sin límites estrictos: se pueden evitar los límites estrictos; por ejemplo, 50 interfaces virtuales por conexión de AWS Direct Connect a través de una arquitectura de red simplificada.
- Costos optimizados: los costos se pueden optimizar mediante la reutilización de puertas de enlace de NAT, puntos de conexión de interfaz de VPC y tráfico dentro de la zona de disponibilidad.

El uso compartido de VPC le permite desacoplar cuentas y redes. Tiene menos VPC, más grandes y administradas de forma centralizada. Las aplicaciones altamente interconectadas se benefician automáticamente de este enfoque.

Interconexión de VPC

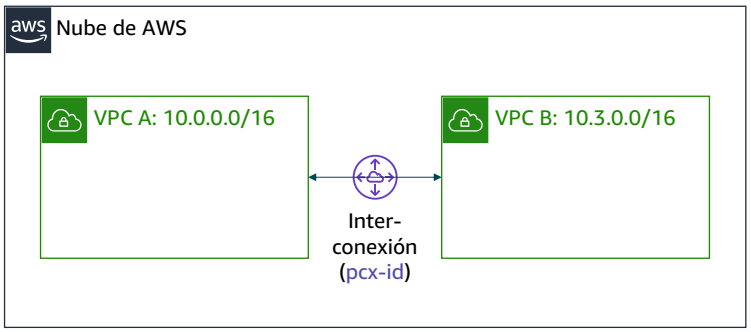


Tabla de enrutamiento para la VPC A

Destino	Objetivo
10.0.0.0/16	local
10.3.0.0/16	pcx-id

Tabla de enrutamiento para la VPC B

Destino	Objetivo
10.3.0.0/16	local
10.0.0.0/16	pcx-id

Puede conectar VPC en su propia cuenta de AWS, entre cuentas de AWS o entre regiones de AWS.

Restricciones:
- Los espacios IP no se pueden superponer.
- La interconexión transitiva no está admitida.
- Puede tener solo un recurso de interconexión entre dos VPC.

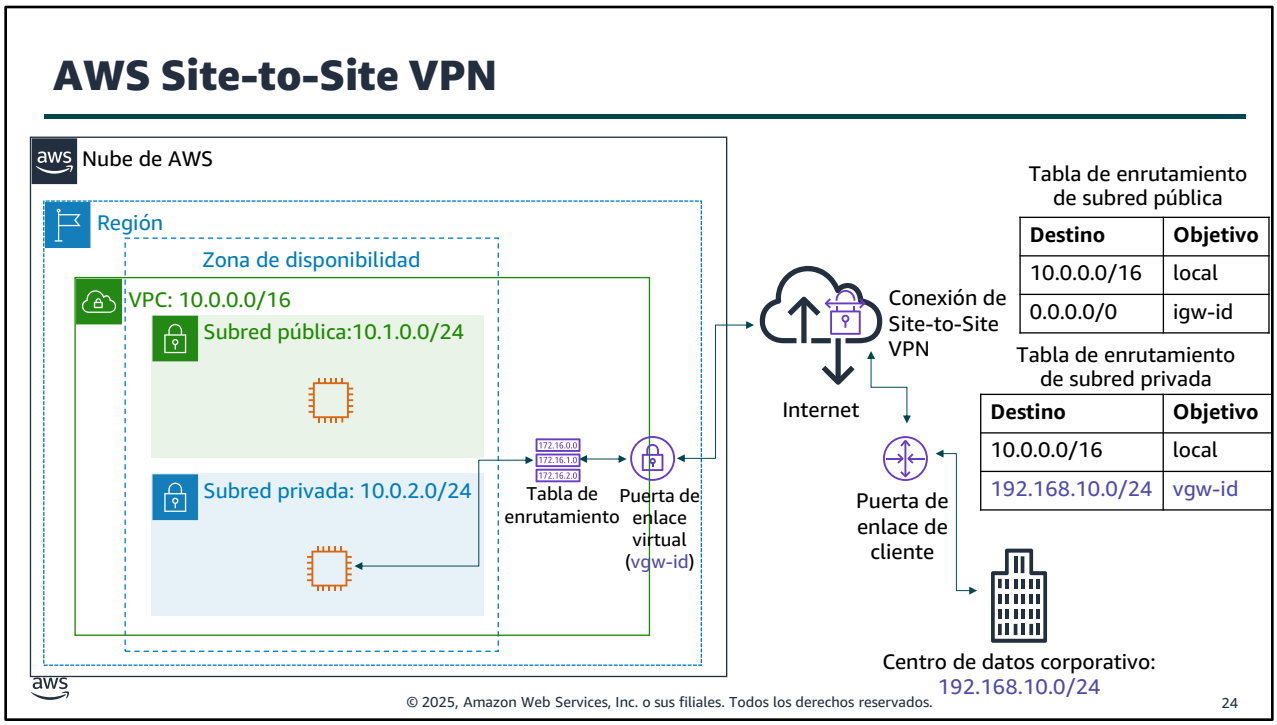
 23

Una *interconexión de VPC* es una conexión de redes entre dos VPC que le permite dirigir el tráfico entre ellas de forma privada. Las instancias en cualquiera de las VPC se pueden comunicar entre sí como si estuvieran en la misma red. Puede crear una interconexión de VPC entre sus propias VPC, con una VPC en otra cuenta de AWS o con una VPC en una región de AWS diferente.

Cuando configura la interconexión, crea reglas en su tabla de enrutamiento que permiten que las VPC se comuniquen entre sí a través del recurso de interconexión. Por ejemplo, suponga que tiene dos VPC. En la tabla de enrutamiento para la VPC A, establece que el destino sea la dirección IP de la VPC B y que el objetivo sea el ID del recurso de interconexión. En la tabla de enrutamiento para la VPC B, establece que el destino sea la dirección IP de la VPC A y que el objetivo sea el ID del recurso de interconexión.

La interconexión de VPC tiene algunas restricciones:
- Los intervalos de direcciones IP no pueden superponerse.
- La interconexión transitiva no está admitida. Por ejemplo, suponga que tiene tres VPC: A, B y C. La VPC A está conectada a la VPC B y la VPC A está conectada a la VPC C. Sin embargo, la VPC B *no* está conectada a la VPC C implícitamente. Para conectar la VPC B a la VPC C, debe establecer explícitamente esa conectividad.
- Puede tener solo un recurso de interconexión entre dos VPC.

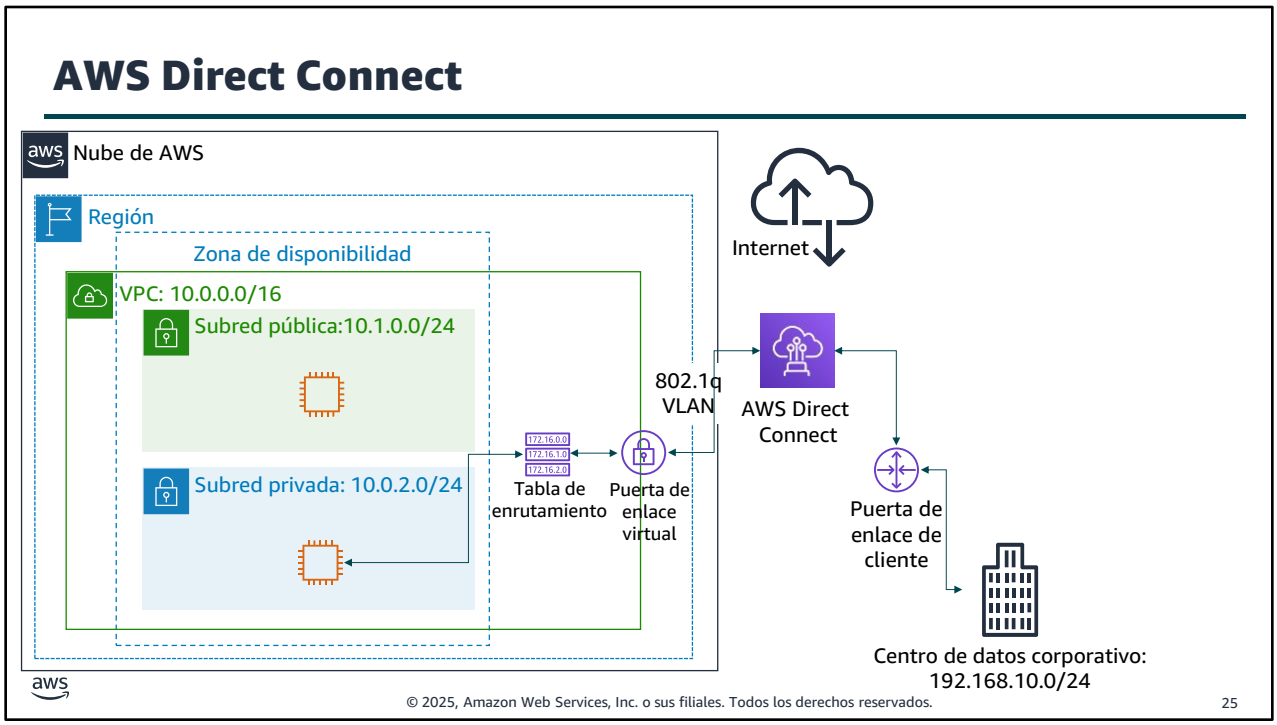
Para obtener más información acerca de la interconexión de VPC, consulte Interconexiones de VPC en la Documentación de AWS en https://docs.aws.amazon.com/vpc/latest/userguide/vpc-peering.html.



De manera predeterminada, las instancias que usted lanza en una VPC no pueden comunicarse con una red remota. Para conectar su VPC a su red remota (que significa, crear una red privada virtual o conexión VPN), usted debe:

1. Crear un nuevo dispositivo de puerta de enlace (llamado una *puerta de enlace de red privada virtual (VPN)*) y adjuntar a su VPC.
2. Definir la configuración del dispositivo VPN o la *puerta de enlace del cliente.* La puerta de enlace de cliente no es un dispositivo sino un recurso de AWS que brinda información sobre su dispositivo VPN a AWS.
3. Crear una tabla de enrutamiento personalizada para dirigir el tráfico del centro de datos corporativo a la puerta de enlace VPN. También debe actualizar las reglas del grupo de seguridad. (Aprenderá sobre los grupos de seguridad en la siguiente sección).
4. Establecer una *conexión de AWS Site-to-Site VPN* (Site-to-Site VPN) para enlazar los dos sistemas.
5. Configure el enrutamiento para pasar el tráfico a través de la conexión.

Para obtener más información sobre AWS Site-to-Site VPN y otras opciones de conectividad VPN, consulte Conexiones de VPN en la Documentación de AWS en https://docs.aws.amazon.com/vpc/latest/userguide/vpn-connections.html.



Uno de los desafíos de la comunicación de red es el rendimiento de la red. El rendimiento se puede ver afectado de forma negativa si su centro de datos está ubicado lejos de su región de AWS. Para este tipo de situaciones, AWS ofrece AWS Direct Connect o DX. *AWS Direct Connect* le permite establecer una conexión de red dedicada y privada entre su red y una de las ubicaciones de DX. Esta conexión privada puede reducir los costos de red, mejorar el rendimiento del ancho de banda y proporcionar una experiencia de red más uniforme que las conexiones basadas en internet. DX utiliza redes de área local virtual (VLAN) 802.1q de estándar abierto.

Para obtener más información sobre DX, consulte la página de productos de AWS Direct Connect en https://aws.amazon.com/directconnect/.

Puntos de conexión de VPC

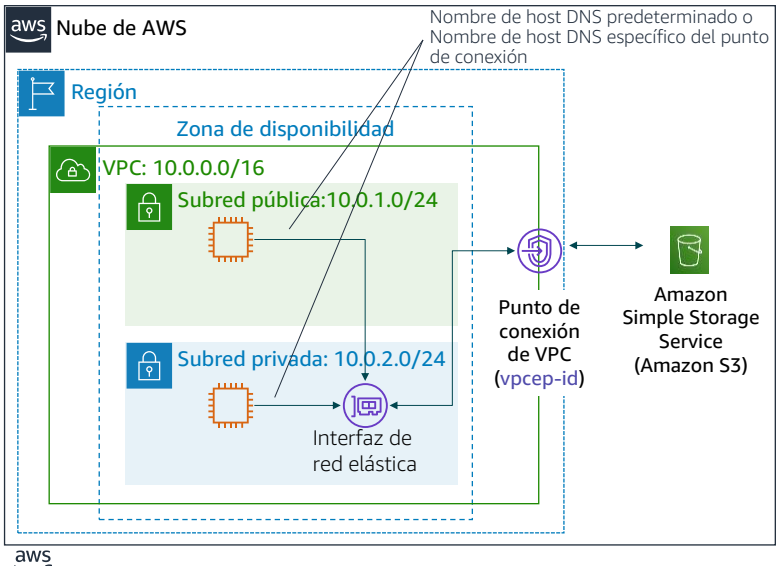


Tabla de enrutamiento de subred pública

Destino	Objetivo
10.0.0.0/16	local
ID de Amazon S3	vpcep-id

Dos tipos de puntos de conexión:

- Puntos de conexión de **interfaz** (con tecnología de AWS PrivateLink)
- Puntos de conexión de **puertas de enlace** (Amazon S3 y Amazon DynamoDB)

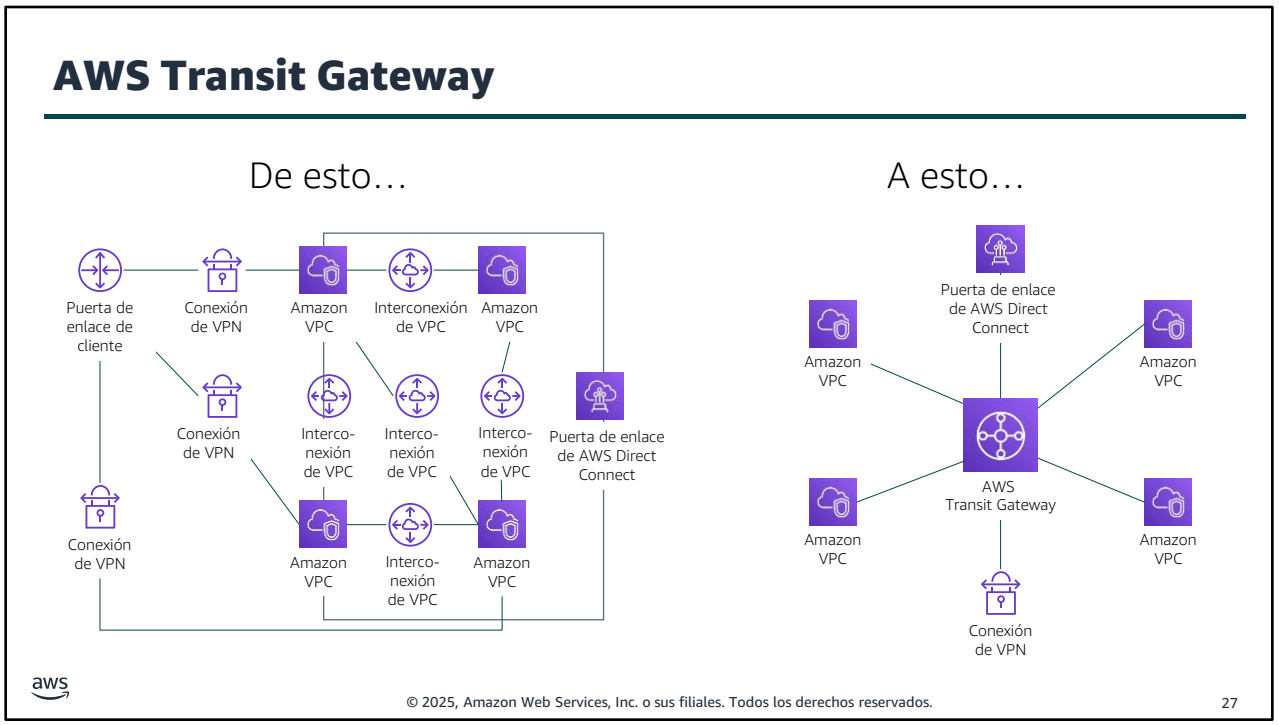
 26

Un *punto de conexión de VPC* es un dispositivo virtual que le permite conectar de forma privada su VPC a los servicios de AWS compatibles y a los servicios de punto de conexión de VPC con tecnología de AWS PrivateLink. La conexión a estos servicios no requiere puerta de enlace de internet, dispositivo NAT, conexión VPN ni conexión AWS Direct Connect. Las instancias de la VPC no requieren direcciones IP públicas para comunicarse con los recursos en el servicio. El tráfico entre la VPC y el otro servicio no sale de la red de Amazon.

Hay dos tipos de puntos de conexión de la VPC:

- Un *punto de conexión de VPC* (punto de conexión de interfaz), le permite conectarse a servicios con tecnología de AWS PrivateLink. Estos servicios incluyen algunos servicios de AWS, servicios alojados por otros clientes y socios de AWS y red de socios de AWS (APN) en sus propias VPC (denominados *servicios de punto de conexión*) y servicios de socios de AWS Marketplace y APN compatibles. El propietario del servicio es el *proveedor del servicio* y usted, como entidad principal que crea el punto de conexión de la interfaz, son el *consumidor del servicio*. Se le cobra por crear y usar un punto de conexión de interfaz en un servicio. Se aplican tarifas de uso por hora y tarifas de procesamiento de datos. Consulte la Documentación de AWS para obtener una lista de puntos de conexión de interfaz compatibles y obtener más información sobre el ejemplo que se muestra aquí en https://docs.aws.amazon.com/vpc/latest/privatelink/create-interface-endpoint.html.
- Puntos de conexión de puerta de enlace: el uso de puntos de conexión de puerta de enlace no genera ningún cargo adicional. Se aplicará la tarifa estándar por la transferencia de datos y por el uso de recursos.

Para obtener más información acerca de los puntos de conexión de VPC, consulte Puntos de conexión de VPC en la Documentación de AWS en https://docs.aws.amazon.com/vpc/latest/privatelink/concepts.html.



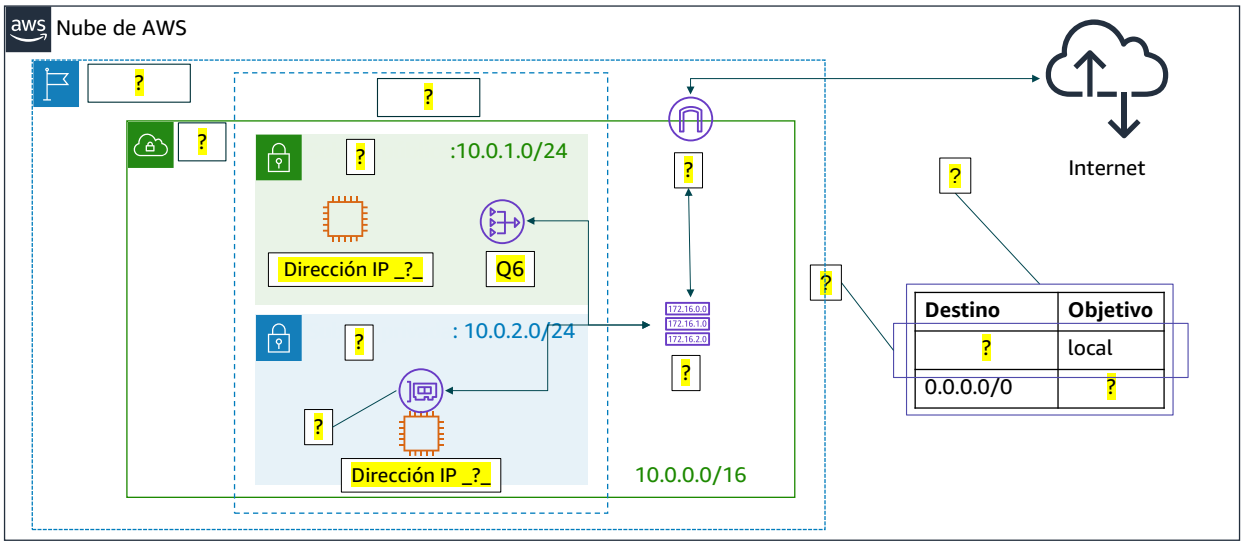
Puede configurar sus VPC de varias maneras y aprovechar numerosas opciones de conectividad y puertas de enlace. Estas opciones y puertas de enlace incluyen AWS Direct Connect (a través de puertas de enlace DX), puertas de enlace NAT, puertas de enlace de internet, interconexión de VPC, etc. No es raro encontrar clientes de AWS con cientos de VPC distribuidas en cuentas y regiones de AWS para atender múltiples líneas de negocios, equipos, proyectos, etc. Las cosas se vuelven más complejas cuando los clientes comienzan a configurar la conectividad entre sus VPC. Todas las opciones de conectividad son estrictamente punto a punto, por lo que la cantidad de conexiones de VPC a VPC puede crecer rápidamente. A medida que aumenta la cantidad de cargas de trabajo que se ejecutan en AWS, debe poder escalar sus redes en múltiples cuentas y VPC para mantenerse al día con el crecimiento.

Si bien puede utilizar interconexión de VPC para conectar pares de VPC, la administración de la conectividad punto a punto en muchas VPC, sin la capacidad para centralizar la administración de las políticas de conectividad, puede ser costosa en términos operativos y difícil. Para conectividad en las instalaciones, debe asociar el VPN a cada VPC individual. Esta solución puede ser de lenta creación y difícil administración cuando hay cientos de VPC.

Para resolver este problema, puede usar AWS Transit Gateway para simplificar su modelo de redes. Con AWS Transit Gateway, solo debe crear y administrar una única conexión desde la puerta de enlace central a cada VPC, centro de datos en las instalaciones u oficina remota en su red. Una puerta de enlace de tránsito actúa como un centro que controla la manera en la que el tráfico se enruta a todas las redes conectadas, que funcionan como radios. Este sistema radial simplifica de manera significativa la administración y reduce los costos operativos porque cada red solo debe conectarse a la gateway de tránsito y a ninguna otra red. cualquier VPC nueva se

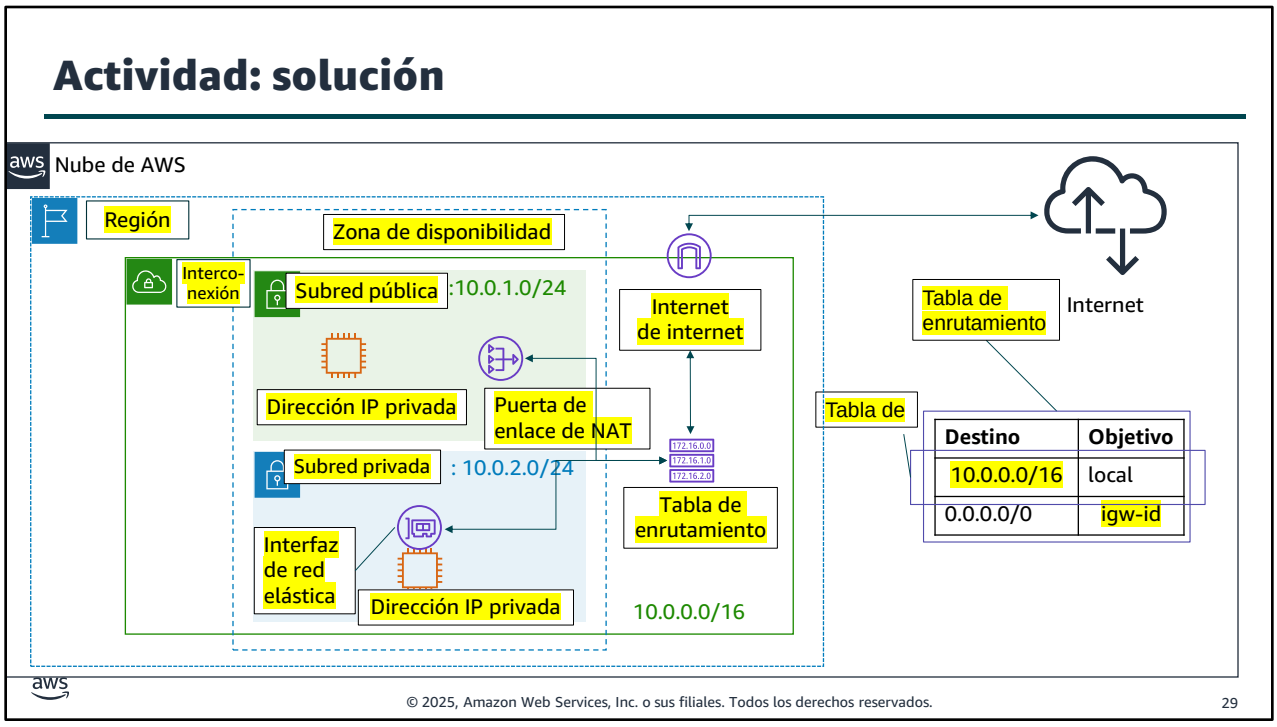
conecta a la puerta de enlace de tránsito y queda disponible automáticamente para cualquier otra red que esté conectada a la puerta de enlace de tránsito. Esta facilidad de conectividad simplifica la capacidad de escalar su red a medida que crece.

Actividad: Etiquetar este diagrama

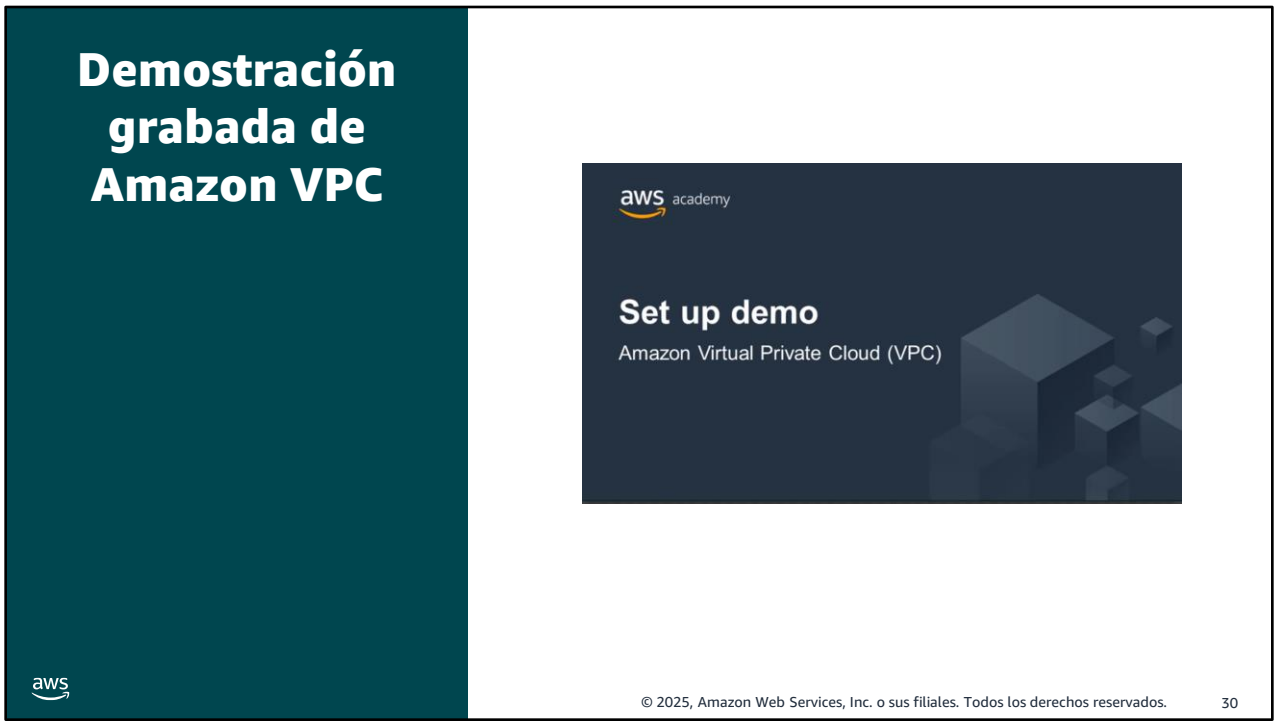


28

Vea si puede reconocer los diferentes componentes de red de VPC que conoció al etiquetar este diagrama de red.



Ahora, mire lo bien que lo hizo.



Ahora que sabe cómo diseñar una VPC, mire la demostración en https://aws-tc-largeobjects.s3-us-west-2.amazonaws.com/ILT-TF-100-ACFNDS-20-EN/Module_5_VPC_Wizard+v2.0.mp4 para aprender a utilizar el asistente de VPC para configurar una VPC con subredes públicas y privadas.

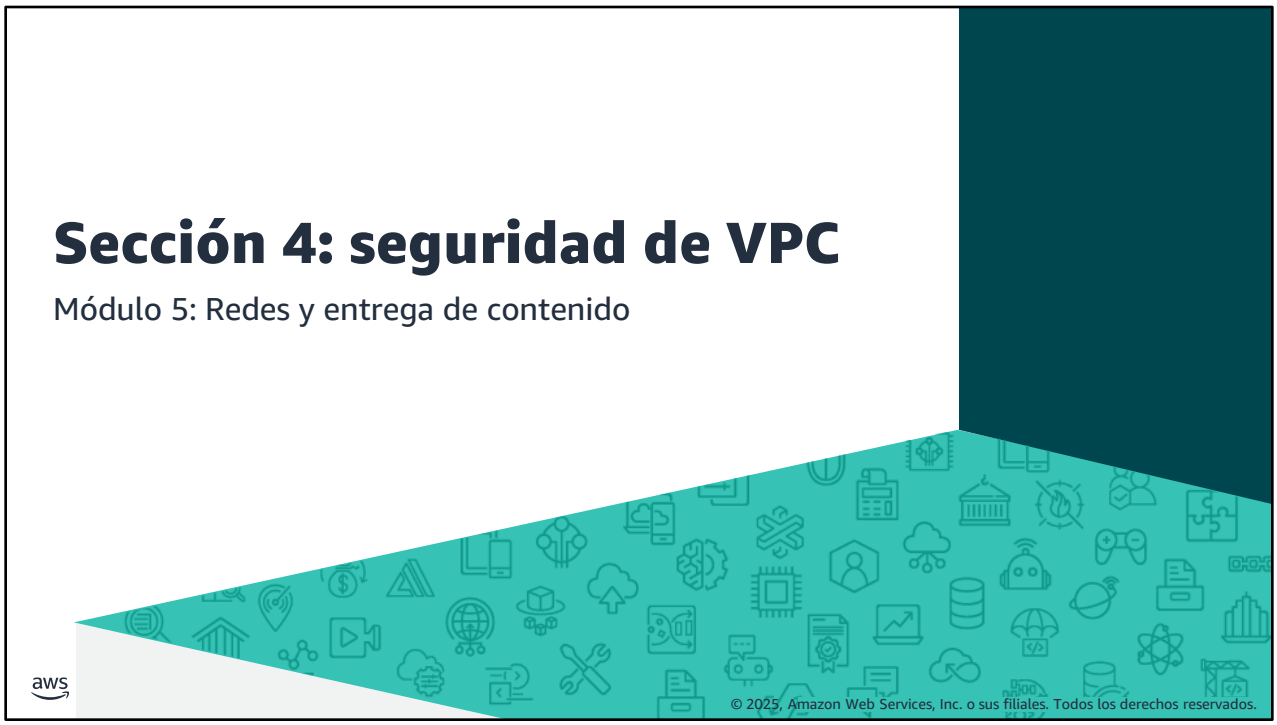
Sección 3: conclusiones importantes

- Hay varias opciones de redes de VPC, que incluyen:
  - Puerta de enlace de internet
  - Puerta de enlace de NAT
  - Punto de conexión de VPC
  - Interconexión de VPC
  - Uso compartido de VPC
  - AWS Site-to-Site VPN
  - AWS Direct Connect
  - AWS Transit Gateway
- Puede utilizar el asistente de VPC para implementar su diseño.

 31

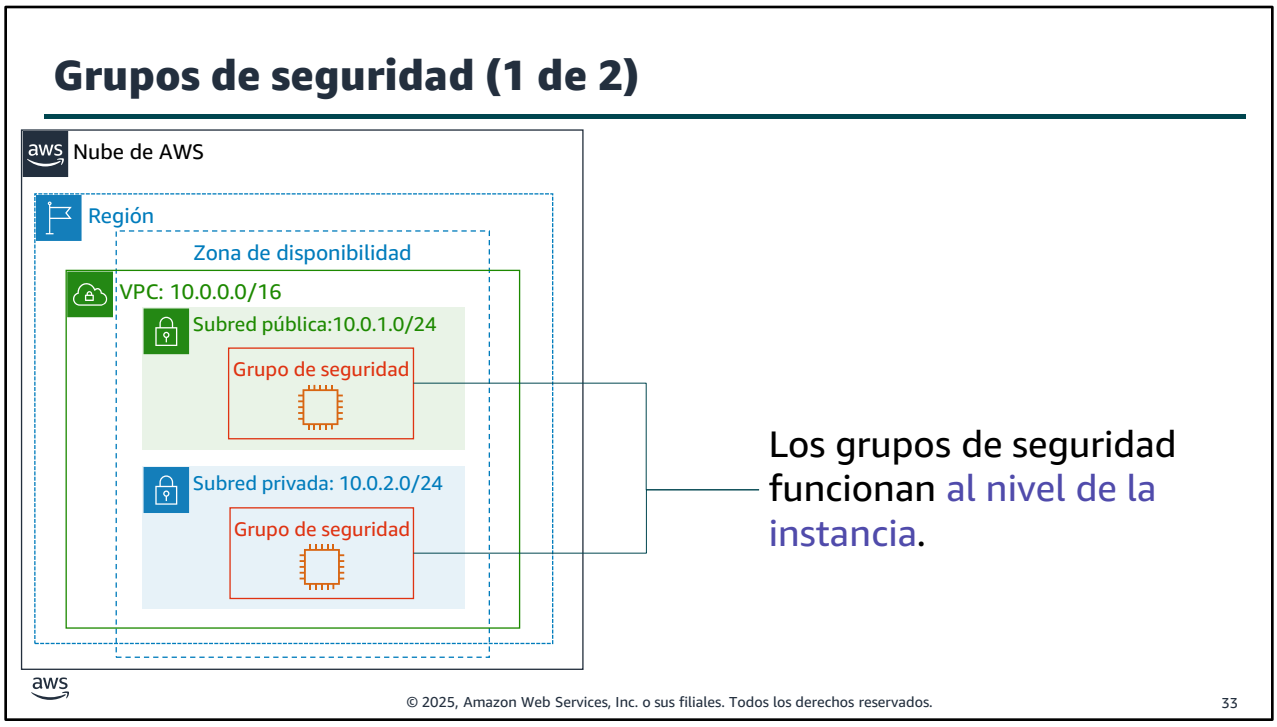
Estas son algunas conclusiones clave de esta sección del módulo:

- Hay varias opciones de redes de VPC, que incluyen:
  - Puerta de enlace de internet: conecta su VPC a internet
  - Puerta de enlace de NAT: habilita instancias en una subred privada para conectarse a internet
  - Punto de conexión de VPC: conecta de forma privada su VPC a los servicios de AWS compatibles
  - Interconexión de VPC: conecta su VPC a otras VPC
  - Uso compartido de VPC: permite que varias cuentas de AWS creen sus recursos de aplicaciones en Amazon VPC compartidas y administradas de forma centralizada.
  - AWS Site-to-Site VPN: conecta su VPC a redes remotas
  - AWS Direct Connect: conecta su VPC a una red remota mediante una conexión de red dedicada
  - AWS Transit Gateway: una alternativa de conexión central y periférica a la interconexión de VPC
- Puede utilizar el asistente de VPC para implementar su diseño.



Sección 4: seguridad de VPC

Puede incorporar seguridad en su arquitectura de VPC de varias maneras para tener control total sobre el tráfico entrante y saliente. En esta sección, conocerá dos opciones de firewall de Amazon VPC que puede utilizar para proteger su VPC: grupos de seguridad y listas de control de acceso a la red (ACL de red).



Un *grupo de seguridad* actúa como un firewall virtual para una instancia y controla el tráfico de entrada y salida. 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.
- Los grupos de seguridad son grupos 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.

aws

34

Los grupos de seguridad tienen *reglas* que controlan el tráfico de entrada y de salida. Cuando crea un grupo de seguridad, no tiene reglas de entrada. Por lo tanto, *no se permite el tráfico de entrada que se origina en otro host a su instancia* 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*. Es posible quitar esta regla y agregar reglas salientes que permitan solo el tráfico saliente específico. Si un grupo de seguridad no tiene reglas de salida, no se permite el tráfico saliente que se origina en la instancia.

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.

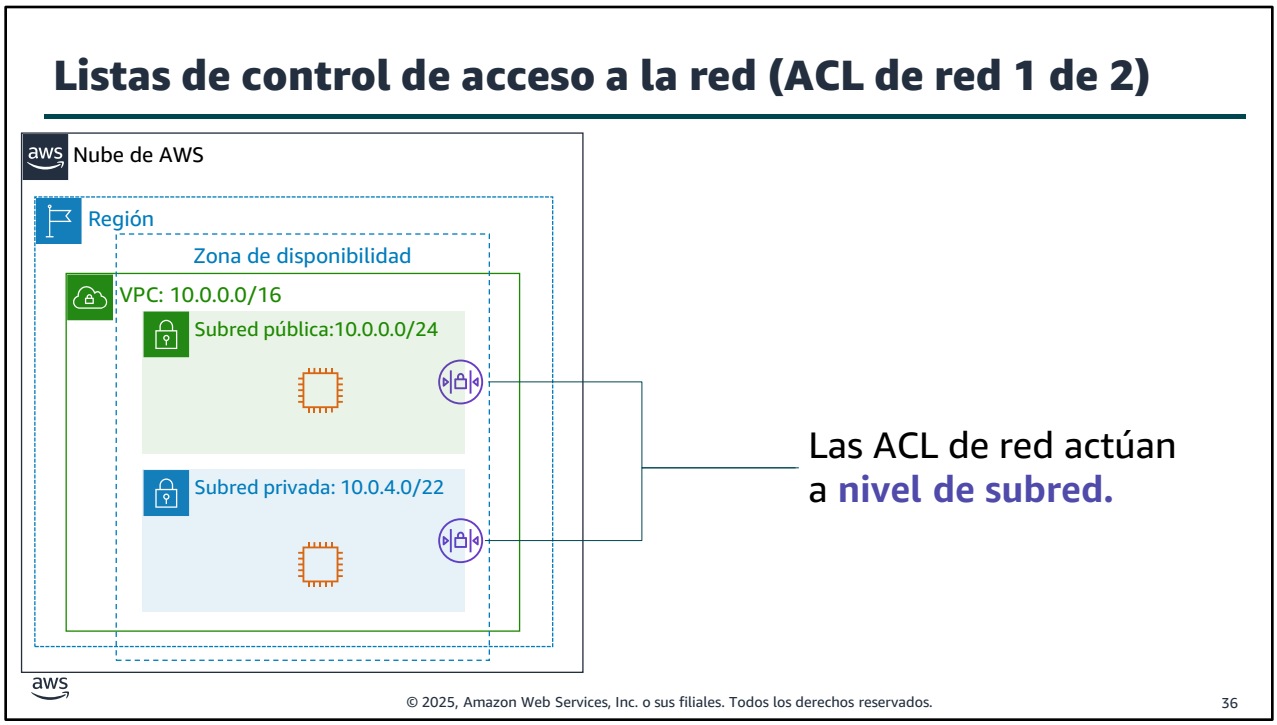
Reglas personalizadas del grupo de seguridad

- Puede especificar reglas de permiso, pero no reglas de denegación.
- Se evalúan todas las reglas antes de decidir permitir tráfico.

Entrada			
Origen	**Protocolo**	**Intervalo de puertos**	**Descripción**
0.0.0.0/0	TCP	80	Permiten el acceso HTTP entrante desde todas las direcciones IPv4
0.0.0.0/0	TCP	443	Permiten el acceso HTTPS entrante desde todas las direcciones IPv4
Intervalo de direcciones IPv4 públicas de la red	TCP	22	Permiten el acceso SSH entrante a las instancias de Linux desde direcciones IP IPv4 de su red (a través de la puerta de enlace de internet).

Salida			
Destino	Protocolo	Intervalo de puertos	Descripción
El ID del grupo de seguridad para sus servidores de bases de datos de Microsoft SQL Server.	TCP	1433	Permiten el acceso saliente de Microsoft SQL Server a las instancias del grupo de seguridad especificado

Cuando crea un grupo de seguridad personalizado, puede especificar reglas de permiso, pero no reglas de denegación. Se evalúan todas las reglas antes de decidir permitir tráfico.



Una *lista de control de acceso a la red (ACL de red)* es una capa opcional de seguridad para su VPC de Amazon. 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 solo a una ACL de red por vez. Cuando se asocia una ACL de red a una subred, se elimina la asociación anterior.

Listas de control de acceso a la red (ACL de red 2 de 2)

- Una ACL de red tiene reglas de entrada y salida independientes y cada regla puede permitir o rechazar tráfico.
- Las ACL de red predeterminadas permiten todo el tráfico entrante y saliente de la IPv4.
- Las ACL de red son ACL sin estado.

Entrada					
Regla	**Tipo**	**Protocolo**	**Intervalo de puertos**	**Origen**	**Permitir/Denegar**
100	Todo el tráfico IPv4	Todos	Todos	0.0.0.0/0	PERMITIR
*	Todo el tráfico IPv4	Todos	Todos	0.0.0.0/0	DENEGAR

Salida					
Regla	**Tipo**	**Protocolo**	**Intervalo de puertos**	**Destino**	**Permitir/Denegar**
100	Todo el tráfico IPv4	Todos	Todos	0.0.0.0/0	PERMITIR
*	Todo el tráfico IPv4	Todos	Todos	0.0.0.0/0	DENEGAR

aws

37

Una ACL de red tiene reglas de entrada y salida independientes y cada regla puede permitir o rechazar tráfico. Su VPC incluye automáticamente una ACL de red predeterminada y modificable. De forma predeterminada, permite todo el tráfico IPv4 entrante y saliente y, si corresponde, el tráfico IPv6. La tabla muestra una ACL de red predeterminada.

Las ACL de red son *sin estado*, lo que significa que no se mantiene ninguna información sobre una solicitud después de procesarla.

Ejemplos de ACL de red personalizadas

- Las ACL de red personalizadas niegan todo el tráfico entrante y saliente hasta que se agregan las reglas.
- Puede especificar ambas reglas permitir y negar
- Las reglas se evalúan en orden, comenzando con la regla con el número más bajo.

Entrada					
Regla	**Tipo**	**Protocolo**	**Intervalo de puertos**	**Origen**	**Permitir/Denegar**
100	HTTPS	TCP	443	0.0.0.0/0	PERMITIR
120	SSH	TCP	22	192.0.2.0/24	PERMITIR
*	Todo el tráfico IPv4	Todos	Todos	0.0.0.0/0	DENEGAR

Salida					
Regla	**Tipo**	**Protocolo**	**Intervalo de puertos**	**Destino**	**Permitir/Denegar**
100	HTTPS	TCP	443	0.0.0.0/0	PERMITIR
120	SSH	TCP	22	192.0.2.0/24	PERMITIR
*	Todo el tráfico IPv4	Todos	Todos	0.0.0.0/0	DENEGAR

 38

Puede crear una ACL de red personalizada y asociarla a una subred. De forma predeterminada, cada ACL de red personalizada deniega todo el tráfico de entrada y de salida hasta que se agregan las reglas.

Una ACL de red contiene una lista numerada de reglas que se evalúan en orden, comenzando por la regla con el número más bajo. El propósito es determinar si el tráfico está permitido dentro o fuera de cualquier subred que esté asociada a la ACL de red. El número más alto que puede utilizar para una regla es 32.766. AWS recomienda que cree reglas en incrementos (por ejemplo, incrementos de 10 o 100) para que pueda insertar reglas nuevas donde las necesite más tarde.

Para obtener más información acerca de las ACL de red, consulte see ACL de red en la Documentación de AWS en https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html.

Comparación de los grupos de seguridad y las ACL de red

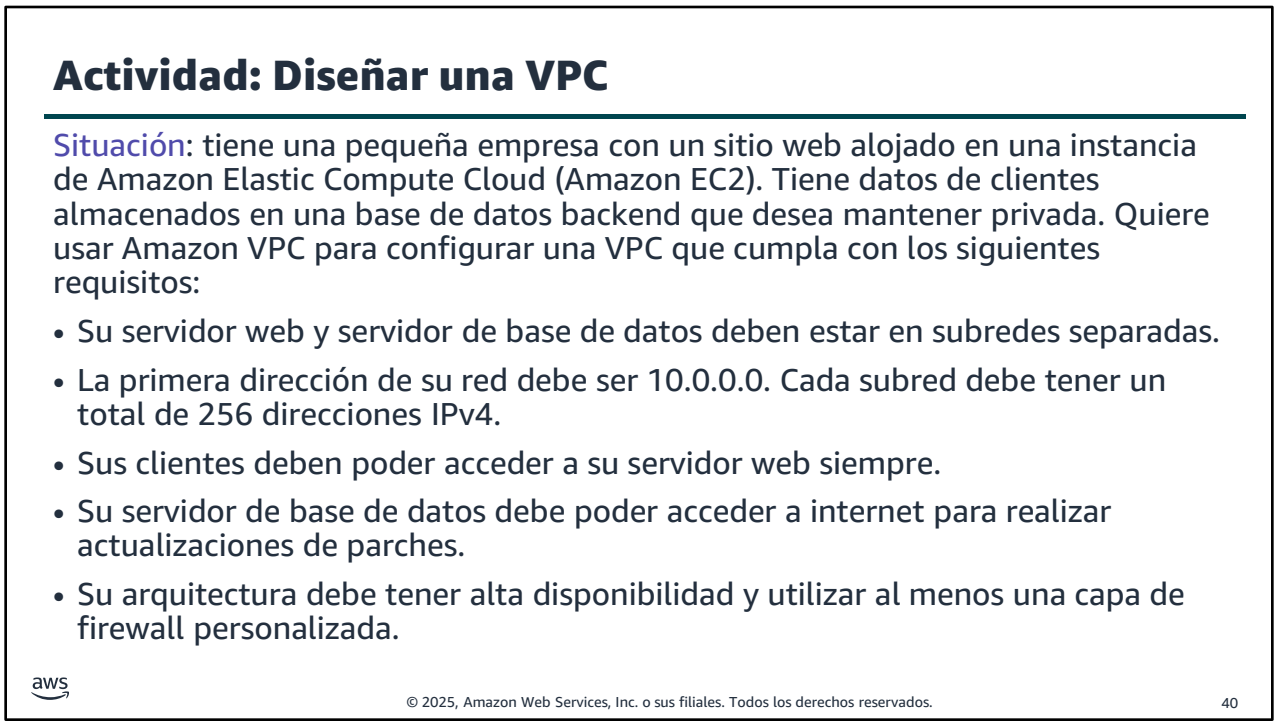
Atributo	Grupos de seguridad	ACL de red
Alcance	Nivel de instancia	Nivel de subred
Reglas admitidas	Solo reglas de permiso	Reglas de permiso y de denegación
Estado	Con estado (el tráfico de retorno se permite automáticamente, independientemente de las reglas)	Sin estado (el tráfico de retorno debe estar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

aws

39

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, 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.



Ahora es su turno. En esta situación, tiene una pequeña empresa con un sitio web alojado en una instancia de Amazon Elastic Compute Cloud (Amazon EC2). Tiene datos de clientes almacenados en una base de datos backend que desea mantener privada.

Vea si puede diseñar una VPC que cumpla con los siguientes requisitos:
- Su servidor web y servidor de base de datos deben estar en subredes separadas.
- La primera dirección de su red debe ser 10.0.0.0. Cada subred debe tener 256 direcciones IPv4.
- Sus clientes deben poder acceder a su servidor web siempre.
- Su servidor de base de datos debe poder acceder a internet para realizar actualizaciones de parches.
- Su arquitectura debe tener alta disponibilidad y utilizar al menos una capa de firewall personalizada.

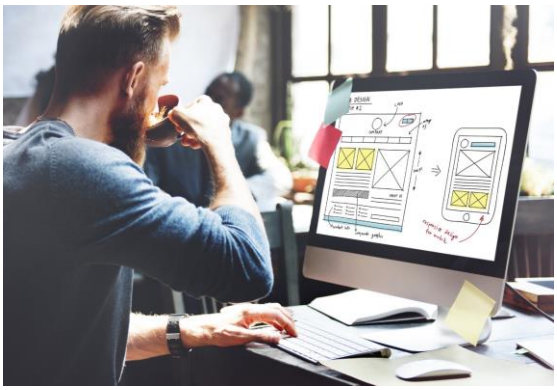
Sección 4: conclusiones importantes

- Integre la seguridad en su arquitectura de VPC:
  - Aísle las subredes si es posible.
  - Elija el dispositivo de puerta de enlace o la conexión de VPN adecuada para sus necesidades.
  - Utilice firewalls.
- Los grupos de seguridad y las ACL de red son opciones de firewall que puede utilizar para proteger su VPC.

 41

Los puntos clave de esta sección del módulo son:
- Integre la seguridad en su arquitectura de VPC.
- Los grupos de seguridad y las ACL de red son opciones de firewall que puede utilizar para proteger su VPC.

Laboratorio 2: Build Your VPC and Launch a Web Server



 42

Ahora usted trabajará en el Laboratorio 2: Build Your VPC and Launch a Web Server.

Laboratorio 2: situación

En este laboratorio, deberá utilizar VPC de Amazon para crear su propia VPC y agregar componentes adicionales con el fin de producir una red personalizada. Creará un grupo de seguridad para la VPC. También puede crear una instancia de EC2 y configurarla para ejecutar un servidor web y utilizar el grupo de seguridad. Luego inicie la instancia de EC2 en la VPC.

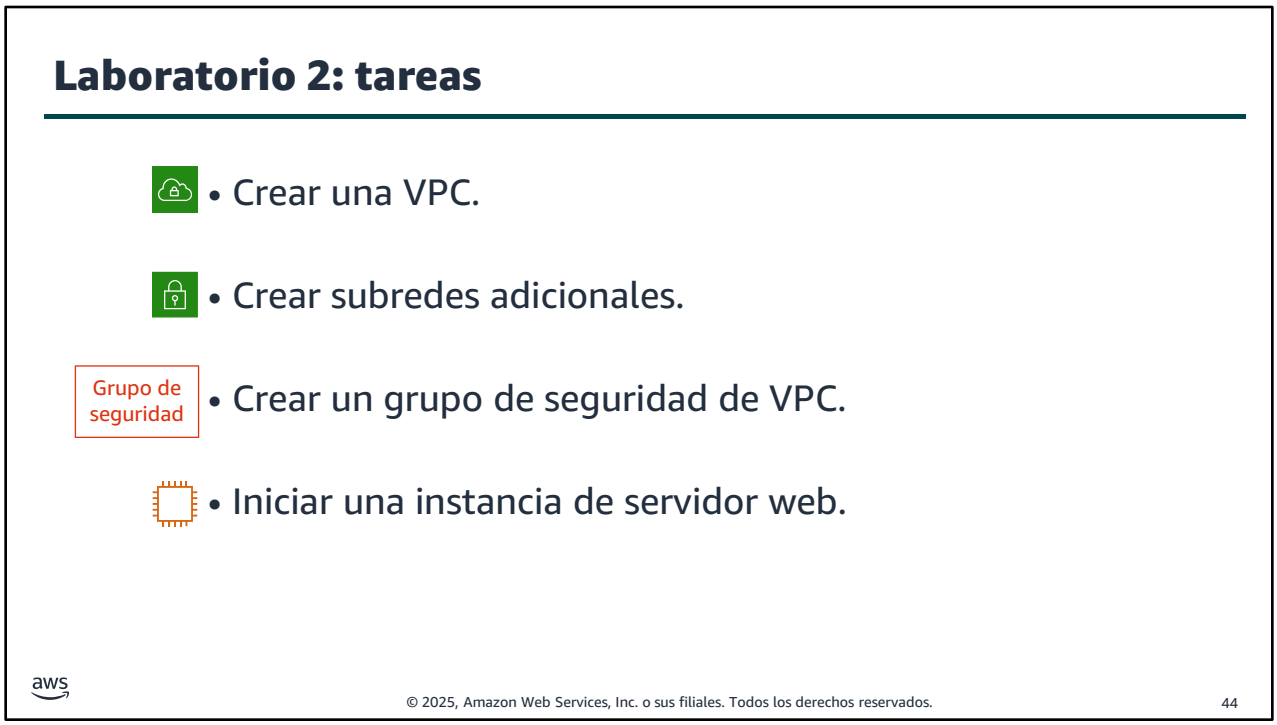

Amazon VPC


Amazon EC2

aws

 43

En este laboratorio, deberá utilizar VPC de Amazon para crear su propia VPC y agregar componentes adicionales con el fin de producir una red personalizada. También puede crear un grupo de seguridad para su VPC y luego, una instancia de EC2 y configurarla para ejecutar un servidor web y utilizar el grupo de seguridad. Luego inicie la instancia de EC2 en la VPC.



En esta práctica de laboratorio, completará estas tareas:

- Crear una VPC.
- Crear subredes adicionales.
- Crear un grupo de seguridad de VPC.
- Iniciar una instancia de servidor web.

Laboratorio 2: producto final

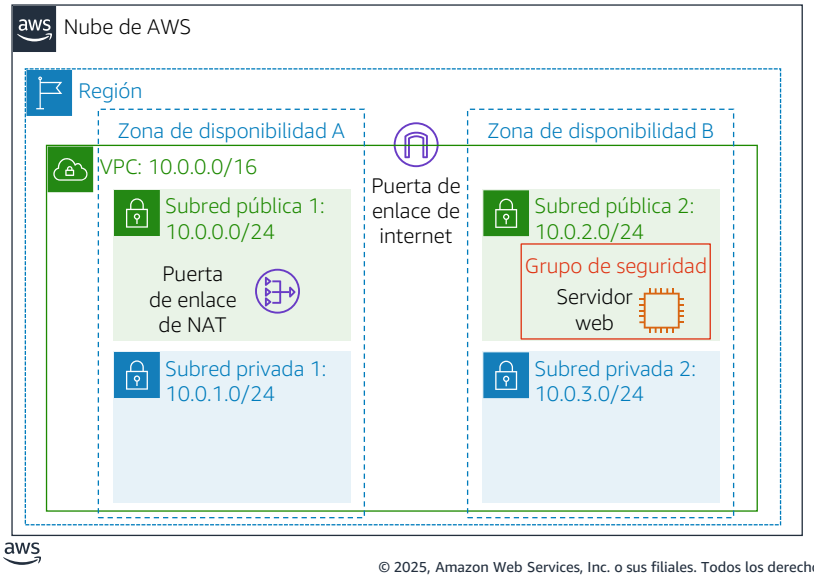


Tabla de enrutamiento pública

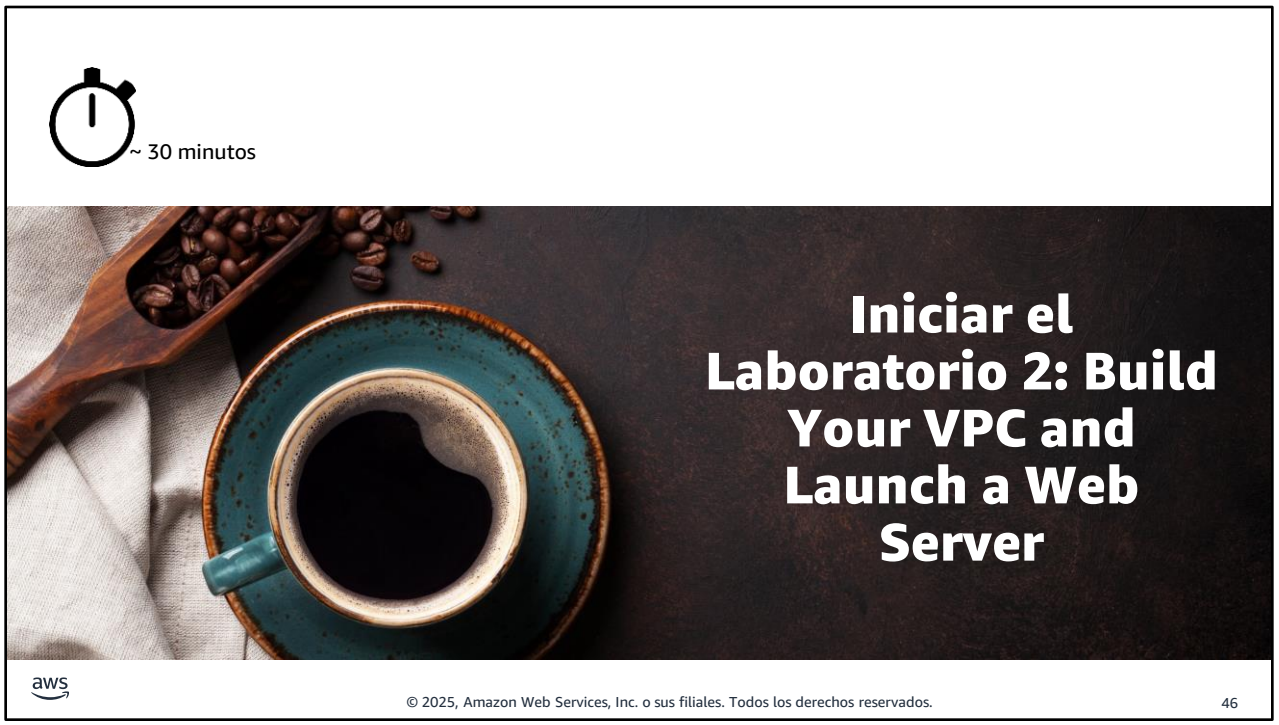
Destino	Objetivo
10.0.0.0/16	Local
0.0.0.0/0	Puerta de enlace de internet

Tabla de enrutamiento privada

Destino	Objetivo
10.0.0.0/16	Local
0.0.0.0/0	Puerta de enlace de NAT

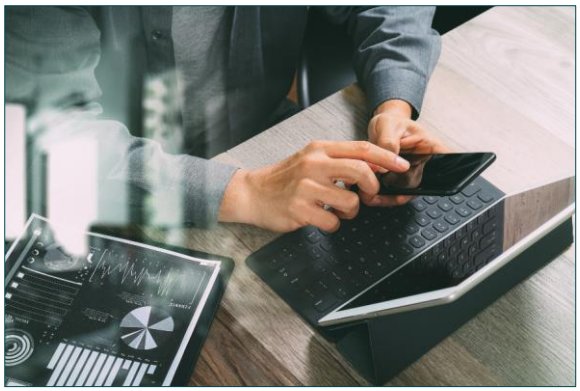
 45

Este diagrama de arquitectura representa lo que creó en el laboratorio.



Es momento de comenzar con el laboratorio. El tiempo estimado para completar este laboratorio es de 30 minutos.

Análisis posterior al laboratorio: aprendizajes clave



 47

En este laboratorio, hizo lo siguiente:

- Creó una Amazon VPC.
- Creó subredes adicionales.
- Creó un grupo de seguridad de Amazon VPC.
- Lanzó una instancia de servidor web en Amazon EC2.

Sección 5: Amazon Route 53

Amazon Route 53

Amazon Route 53

- Es un servicio web de sistema de nombres de dominio (DNS) escalable y de alta disponibilidad.
- Se utiliza para redirigir a los usuarios finales a las aplicaciones de internet mediante la traducción de nombres (como *www.example.com*) en direcciones IP numéricas (como *192.0.2.1)* que las computadoras utilizan para conectarse entre ellas.
- Es totalmente compatible con IPv4 e IPv6.
- Conecta de manera efectiva las solicitudes de los usuarios con la infraestructura que se ejecuta en AWS y también fuera de AWS.
- Se utiliza para comprobar el estado de sus recursos.
- Cuenta con flujo de tráfico.
- Le permite registrar nombres de dominio.

 49

Amazon Route 53 es un servicio web del sistema de nombres de dominio (DNS) escalable y de alta disponibilidad en la nube. Está diseñado para ofrecer a los desarrolladores y a las empresas una forma fiable y rentable de dirigir a los usuarios finales hacia las aplicaciones de internet, mediante la conversión de nombres (como *www.example.com*) en direcciones IP numéricas (como *192.0.2.1)* que los equipos utilizan para conectarse entre ellos. Además, Amazon Route 53 cumple con IPv6. Consulte más información sobre el sistema de nombres de dominio en https://aws.amazon.com/route53/what-is-dns/.

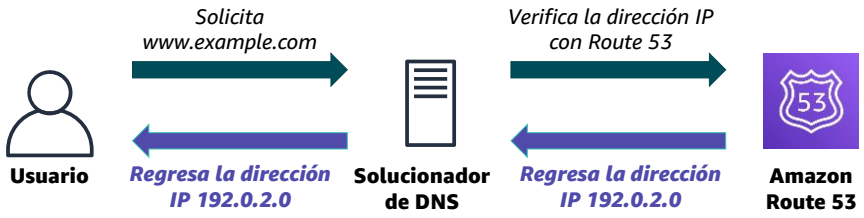
Amazon Route 53 conecta de forma efectiva las solicitudes del usuario con la infraestructura en ejecución en AWS (como instancias de Amazon EC2, equilibradores de carga de Elastic Load Balancing o buckets de Amazon S3) y también puede utilizarse para dirigir a los usuarios a infraestructuras externas a AWS.

Puede utilizar Amazon Route 53 para configurar verificaciones de estado de DNS con el fin de dirigir el tráfico a puntos de conexión en buen estado o supervisar de manera independiente el estado de la aplicación y los puntos de conexión.

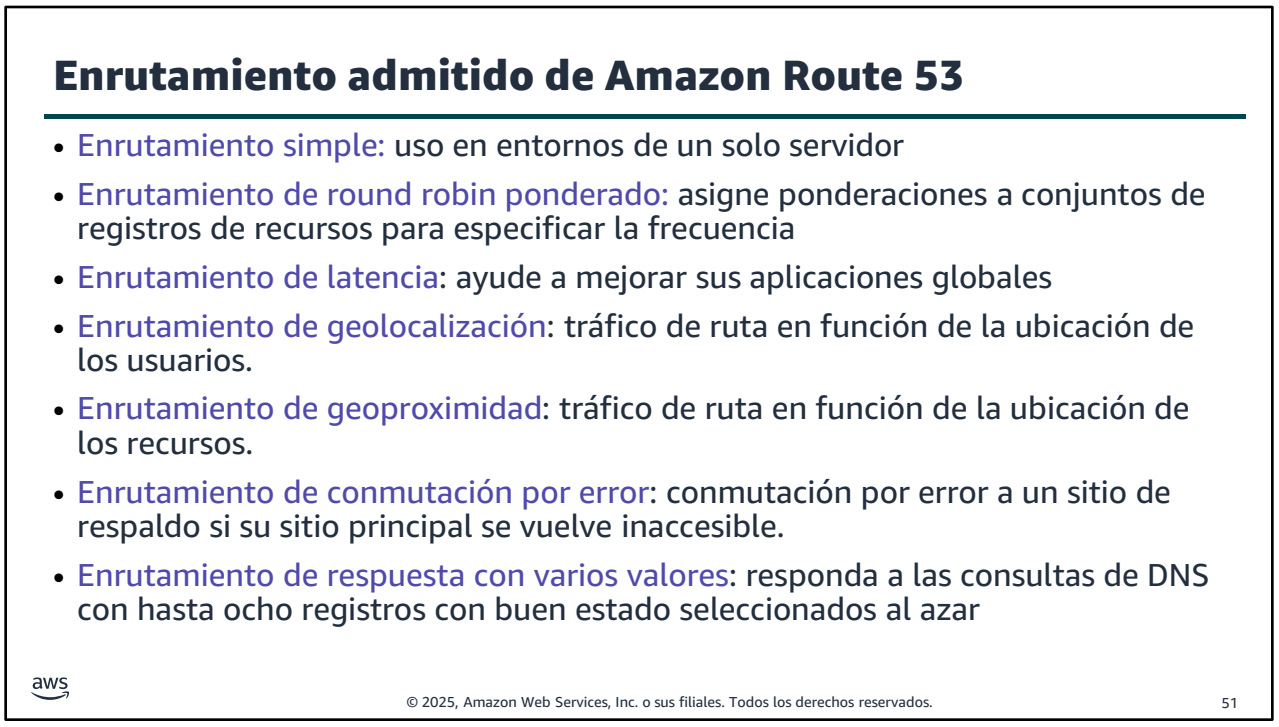
El flujo de tráfico de Amazon Route 53 lo ayuda a administrar el tráfico globalmente a través de varios tipos de enrutamiento, que se pueden combinar con la conmutación por error de DNS para habilitar varias arquitecturas de baja latencia y tolerancia a fallas. Puede utilizar el sencillo editor visual del flujo de tráfico de Amazon Route 53 para administrar el modo de redirigir a los usuarios hacia los puntos de conexión de la aplicación, ya sea en una sola región de AWS o en todo el mundo.

Amazon Route 53 también ofrece el registro del nombre de dominio. Puede adquirir y administrar nombres de dominio (como *example.com*) y Amazon Route 53 configurará de forma automática los ajustes de DNS para sus dominios.

Resolución DNS de Amazon Route 53



Este es el patrón básico que sigue Amazon Route 53 cuando un usuario inicia una solicitud de DNS. El solucionador de DNS verifica con su dominio en Route 53, obtiene la dirección IP y se la devuelve al usuario.



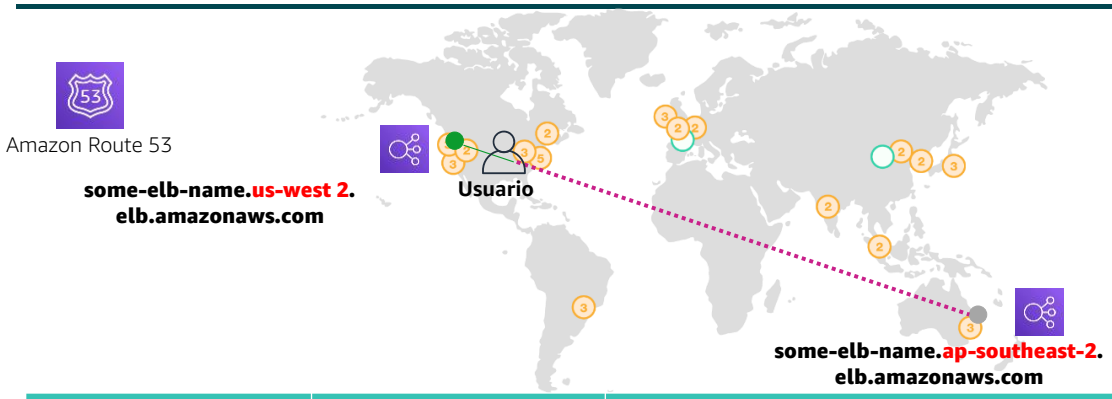
Amazon Route 53 admite varios tipos de políticas de enrutamiento, que determinan cómo Amazon Route 53 responde a las consultas:

- *Enrutamiento simple (round robin)*: se utiliza para un único recurso que realiza una función determinada para su dominio (por ejemplo, un servidor web que ofrece contenido para el sitio web example.com).
- *Enrutamiento de round robin ponderado*: se utiliza para dirigir el tráfico a varios recursos en las proporciones que especifique. Le permite asignar ponderaciones a un conjunto de registros de recursos para especificar la frecuencia con la que se ofrecen diferentes respuestas. Es posible que desee utilizar esta capacidad para realizar pruebas A/B, que es cuando envía una pequeña parte del tráfico a un servidor donde realizó un cambio de software. Por ejemplo, supongamos que tiene dos conjuntos de registros asociados con un nombre DNS: uno con peso 3 y otro con peso 1. En este caso, el 75 por ciento de las veces, Amazon Route 53 devolverá el registro establecido con peso 3, y el 25 por ciento de las veces, Amazon Route 53 devolverá el registro establecido con peso 1. Los pesos pueden ser cualquier número entre 0 y 255.
- *Enrutamiento de latencia (LBR)*: se utiliza si tiene recursos en varias regiones de AWS y quiere redirigir el tráfico a la región que proporciona la latencia más baja. El enrutamiento de latencia funciona al enrutar a sus clientes al punto de conexión de AWS (por ejemplo, instancias de Amazon EC2, direcciones IP elásticas), o equilibradores de carga) que proporcionan la experiencia más rápida basada en mediciones de rendimiento reales de las diferentes regiones de AWS donde se ejecuta

su aplicación.

- *Enrutamiento de geolocalización:* se utiliza si desea dirigir el tráfico en función de la ubicación de los usuarios. Cuando utiliza el enrutamiento de geolocalización, puede localizar su contenido y presentar parte o la totalidad de su sitio web en el idioma de sus usuarios. También puede utilizar el enrutamiento de geolocalización para restringir la distribución de contenido solo a las ubicaciones donde tiene derechos de distribución. Otro uso posible es equilibrar la carga entre los puntos de conexión de una manera predecible y fácil de administrar, de modo que la ubicación de cada usuario se enrute consistentemente al mismo punto de conexión.
- *Enrutamiento de geoproximidad*: se utiliza cuando quiere dirigir el tráfico en función de la ubicación de los recursos y, de manera opcional, desviar el tráfico de los recursos de una ubicación a los de otra.
- *Enrutamiento de conmutación por error (conmutación por error de DNS)*: se utiliza si desea configurar la conmutación por error activa-pasiva. Amazon Route 53 puede ayudar a detectar una interrupción de su sitio web y redirigir a sus usuarios a ubicaciones alternativas donde su aplicación esté funcionando correctamente. Cuando habilita esta característica, los agentes de verificación de estado de Amazon Route 53 supervisarán cada ubicación o punto de conexión de su aplicación para determinar su disponibilidad. Puede aprovechar esta característica para aumentar la disponibilidad de su aplicación de cara al cliente.
- *Enrutamiento de respuesta con varios valores*: se utiliza si desea que Route 53 responda a consultas de DNS con hasta ocho registros en buen estado seleccionados al azar. Puede configurar Route 53 para que muestre varios valores, como direcciones IP a los servidores web, en respuesta a las consultas de DNS. Puede especificar varios valores para casi cualquier registro, pero el enrutamiento de respuestas con varios valores también le permite verificar el estado de cada recurso para que Route 53 solo devuelva valores para recursos en buen estado. No es un reemplazo para un equilibrados de carga, pero la capacidad de mostrar varias direcciones IP cuyo estado sea comprobable constituye una forma de utilizar el DNS para mejorar
la disponibilidad y el equilibrio de carga.

Caso práctico: implementación en varias regiones



Nombre	Tipo	Valor
example.com	ALIAS	some-elb-name.us-west-2.elb.amazonaws.com
example.com	ALIAS	some-elb-name.ap-southeast-2.elb.amazonaws.com

 52

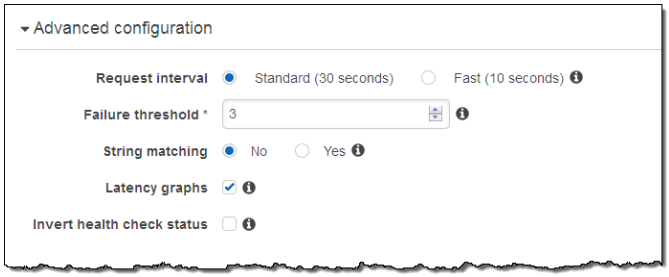
La implementación multirregional es un caso de uso de ejemplo para Amazon Route 53. Con Amazon Route 53, se dirige automáticamente al usuario al equilibrador de carga de Elastic Load Balancing más cercano al usuario.

Los beneficios de la implementación multirregional de Route 53 incluyen:
- Enrutamiento basado en la latencia para la región
- Enrutamiento de balanceo de carga para zona de disponibilidad

Conmutación por error de DNS de Amazon Route 53

Mejore la disponibilidad de sus aplicaciones que se ejecutan en AWS:

- Con la configuración de escenarios de respaldo y conmutación por error para sus propias aplicaciones
- Con la habilitación de arquitecturas multirregionales de alta disponibilidad en AWS
- Con la creación de comprobaciones de estado

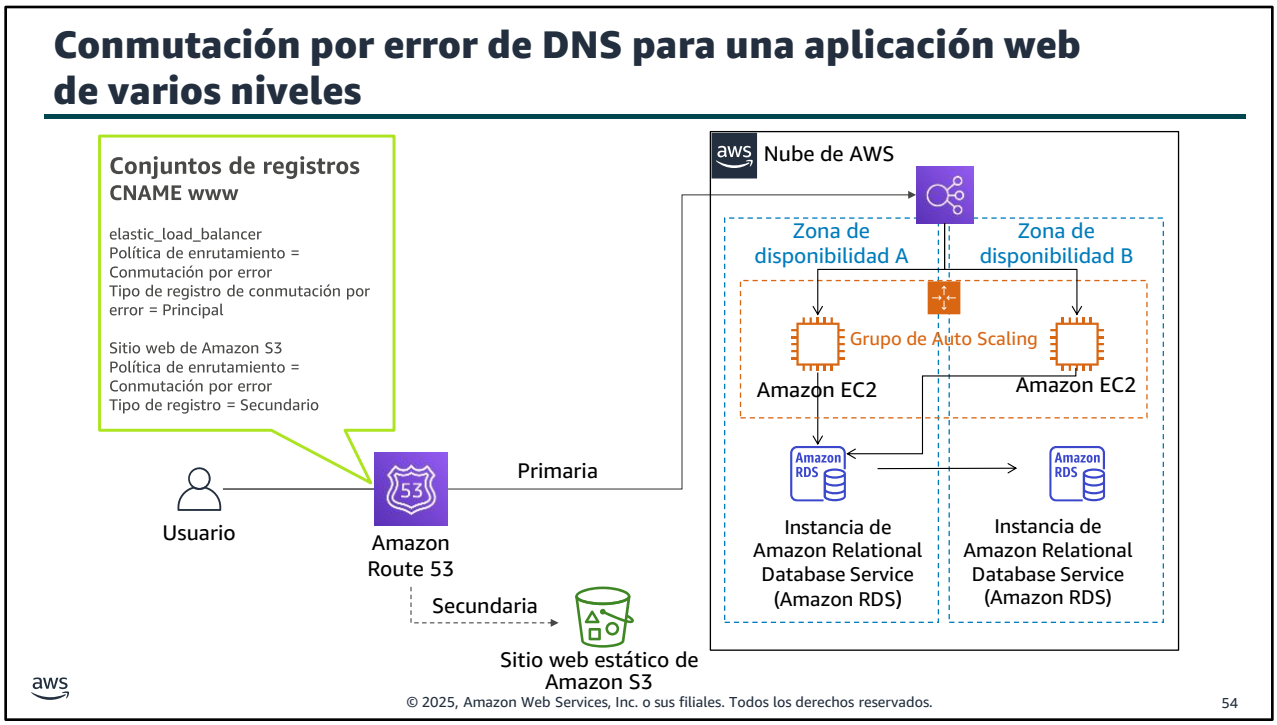


aws

 53

Amazon Route 53 le permite mejorar la disponibilidad de sus aplicaciones que se ejecutan en AWS:

- Con la configuración de escenarios de respaldo y conmutación por error para sus propias aplicaciones.
- Con la habilitación de arquitecturas multirregionales de alta disponibilidad en AWS.
- Con la creación de comprobaciones de estado para supervisar el estado y el rendimiento de su aplicación web, servidores web y otros recursos. Cada comprobación de estado que cree puede supervisar uno de los siguientes: el estado de un recurso específico, como un servidor web; el estado de otras comprobaciones de estado; y el estado de una alarma de Amazon CloudWatch.



Este diagrama indica cómo funciona la conmutación por error de DNS en una arquitectura típica para una aplicación web de varios niveles. Route 53 pasa el tráfico a un equilibrador de carga, que luego distribuye el tráfico a una flota de instancias de EC2.

Puede realizar las siguientes tareas con Route 53 para garantizar una alta disponibilidad:

1. Crear dos registros de DNS para el Registro de nombre canónico (CNAME) *www* con una política de enrutamiento de *Conmutación por error.* El primer registro es la política de ruta principal, que apunta al equilibrador de carga de su aplicación web. El segundo registro es la política de ruta secundaria, que apunta a su sitio web estático de Amazon S3.
2. Utilice las comprobaciones de estado de Route 53 para asegurarse de que el sistema principal esté funcionando. Si es así, todo el tráfico se dirige de forma predeterminada a su pila de aplicaciones web. La conmutación por error al sitio de respaldo estático se activaría si el servidor web falla (o deja de responder) o si la instancia de la base de datos falla.

Sección 5: conclusiones importantes

- Amazon Route 53 es un servicio web DNS en la nube escalable y de alta disponibilidad que traduce nombres de dominio en direcciones IP numéricas.
- Amazon Route 53 admite varios tipos de políticas de enrutamiento.
- La implementación multirregional mejora el rendimiento de su aplicación para una audiencia global.
- Puede utilizar la conmutación por error de Amazon Route 53 para mejorar la disponibilidad de sus aplicaciones.

 55

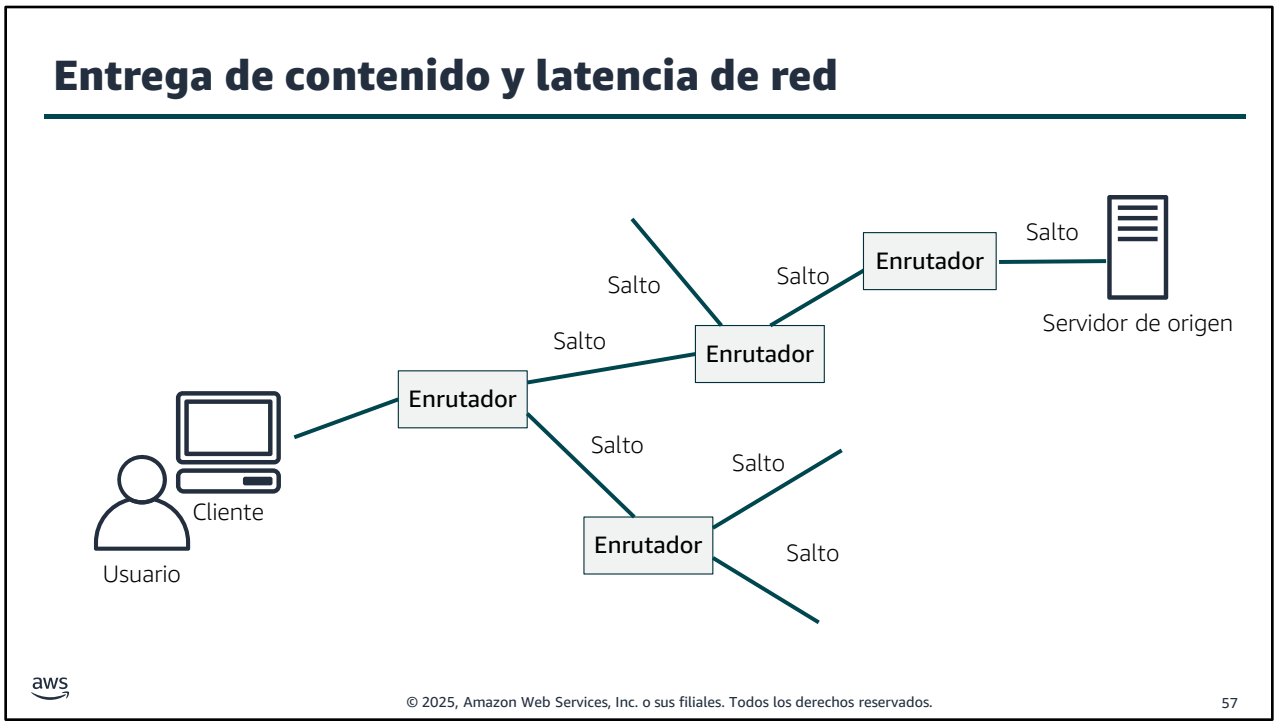
Estas son algunas conclusiones clave de esta sección del módulo:

- Amazon Route 53 es un servicio web DNS en la nube escalable y de alta disponibilidad que traduce nombres de dominio en direcciones IP numéricas.
- Amazon Route 53 admite varios tipos de políticas de enrutamiento.
- La implementación multirregional mejora el rendimiento de su aplicación para una audiencia global.
- Puede utilizar la conmutación por error de Amazon Route 53 para mejorar la disponibilidad de sus aplicaciones.

Sección 6: Amazon CloudFront

El propósito de la creación de redes es compartir información entre recursos conectados. Hasta ahora, en este módulo, ha aprendido sobre las redes de VPC con Amazon VPC Aprendió sobre las diferentes opciones para conectar su VPC a internet, a redes remotas, a otras VPC y a servicios de AWS.

La entrega de contenido también ocurre a través de redes; por ejemplo, cuando transmite una película desde su servicio de transmisión favorito. En esta sección final, aprenderá sobre Amazon CloudFront, que es unservicio de red de entrega de contenido (CDN).



Como se explicó anteriormente en este módulo cuando estaba aprendiendo sobre AWS Direct Connect, uno de los desafíos de la comunicación de red es el rendimiento de la red. Cuando navega por un sitio web o transmite un video, su solicitud se enruta a través de muchas redes diferentes para llegar a un servidor de origen. El servidor de origen (u origen) almacena las versiones originales y definitivas de los objetos (páginas web, imágenes y archivos multimedia). La cantidad de saltos de red y la distancia que debe recorrer la solicitud afectan significativamente el rendimiento y la capacidad de respuesta del sitio web. Además, la latencia de la red es diferente en distintas ubicaciones geográficas. Por estos motivos, una red de distribución de contenidos podría ser la solución.

Red de entrega de contenido (CDN)

- Es un sistema distribuido globalmente de servidores de caché.
- Copias en caché de archivos solicitados comúnmente (contenido estático).
- Entrega una copia local del contenido solicitado desde una periferia de caché cercana o un punto de presencia.
- Acelera la entrega de contenido dinámico o estático.
- Mejora el rendimiento y el escalado de las aplicaciones.

aws

 58

Una red de entrega de contenido, CDN es un sistema distribuido globalmente de servidores de almacenamiento en caché que acelera la entrega de contenido Una CDN almacena en caché copias de archivos solicitados comúnmente (contenido estático, como lenguaje de marcado de hipertexto o HTML; Cascading Style Sheets o CSS; JavaScript y archivos de imagen) que están alojados en el servidor de origen de la aplicación. La CDN entrega una copia local del contenido solicitado desde una periferia de caché o punto de presencia que proporciona la entrega más rápida al solicitante.

Las CDN también ofrecen contenido dinámico que es exclusivo del solicitante y no se puede almacenar en caché. Tener una CDN que entregue contenido dinámico mejora el rendimiento y el escalado de las aplicaciones. La CDN establece y mantiene conexiones seguras más cercanas al solicitante. Si la CDN está en la misma red que el origen, se acelera el enrutamiento de regreso al origen para recuperar contenido dinámico. Además, el contenido como datos de formularios, imágenes y texto se puede ingerir y enviar de vuelta al origen, aprovechando así las conexiones de baja latencia y el comportamiento de proxy del PoP.

Amazon CloudFront

Amazon CloudFront

- Servicio CDN rápido, global y seguro
- Ubicaciones periféricas de la red global y cachés periféricas regionales
- Modelo de autoservicio
- Precios de pago por uso

59

Amazon CloudFront es un servicio rápido de CDN que suministra datos, videos, aplicaciones e interfaces de programación de aplicaciones (API) de manera segura a clientes de todo el mundo, con baja latencia y altas velocidades de transferencia. También proporciona un entorno amigable para los desarrolladores. Amazon CloudFront entrega archivos a los usuarios a través de una red global de ubicaciones periféricas y cachés periféricas regionales. Amazon CloudFront se diferencia de las soluciones tradicionales de entrega de contenido porque le permite obtener rápidamente los beneficios de la entrega de contenido de alto rendimiento sin contratos negociados, precios altos o tarifas mínimas. Al igual que otros servicios de AWS, Amazon CloudFront es una oferta de autoservicio con precios de pago por uso.

Infraestructura de Amazon CloudFront

Amazon CloudFront entrega contenido a través de una red mundial de centros de datos denominados ubicaciones periféricas. Cuando un usuario solicita contenido que usted proporciona mediante CloudFront, el usuario se dirige a la ubicación periférica que presente la menor latencia (o retardo) para entregar el contenido con el mejor rendimiento posible. Las ubicaciones periféricas de CloudFront están diseñadas para entregar contenido popular a sus visores rápidamente.

A medida que los objetos pierden popularidad, las ubicaciones periféricas pueden eliminarlos para dejar espacio para el contenido más popular. Para el contenido menos popular, CloudFront tiene *Cachés periféricas regionales.* Las cachés periféricas regionales son ubicaciones de CloudFront que se implementan globalmente, cerca de sus visores. Están ubicados entre su servidor de origen y ubicaciones periféricas globales que brindan contenido directamente a los visores. Una memoria caché periférica regional tiene una memoria caché más grande que una ubicación periférica individual, por lo que los objetos permanecen en la memoria caché periférica regional más cercana. La mayor parte de su contenido permanece más cerca de sus visores, lo que reduce la necesidad de que CloudFront vuelva a su servidor de origen y mejora el rendimiento general para los visores.

Para obtener más información sobre cómo funciona Amazon CloudFront, consulte "Cómo CloudFront entrega contenido" en la Documentación de AWS en https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/HowCloudFrontWorks.html#HowCloudFrontWorksContentDelivery.

Beneficio de Amazon CloudFront

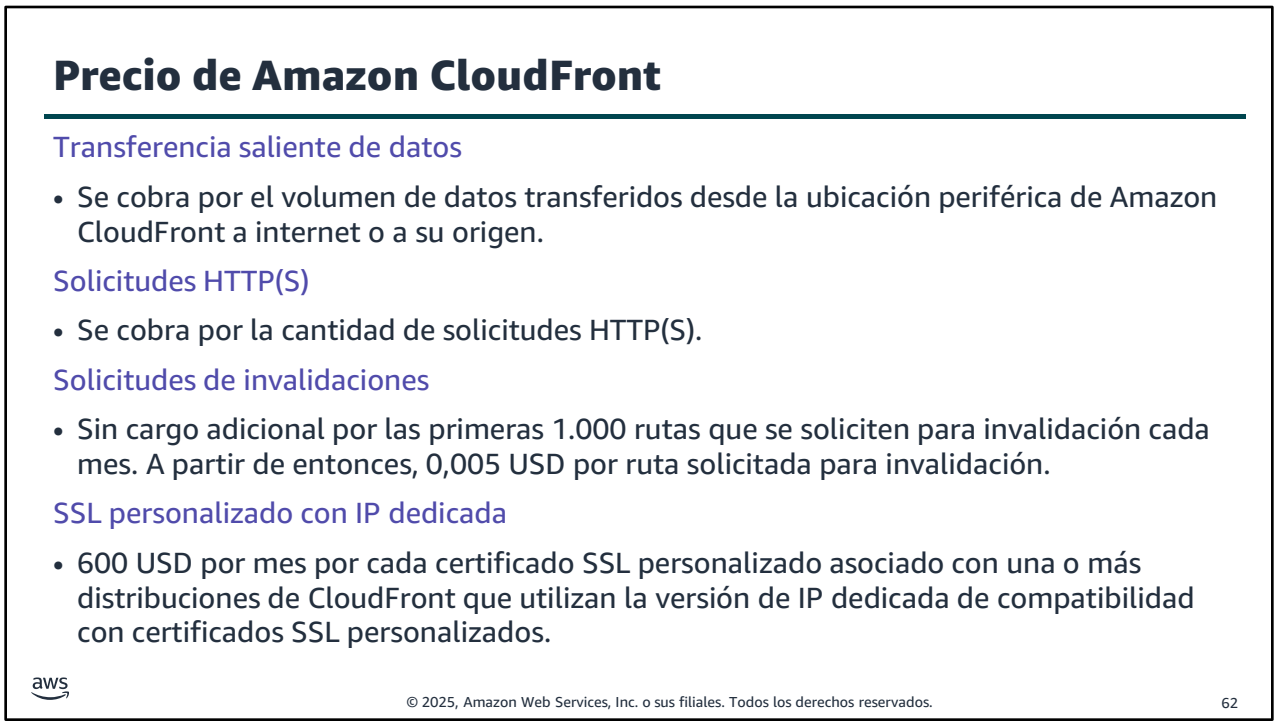
- Rapidez y alcance mundial
- Seguridad en la periferia
- Alta capacidad de programación
- Integración profunda con AWS
- Rentable

 61

Amazon CloudFront proporciona los siguientes beneficios:

- *Rapidez y alcance mundial*: Amazon CloudFront es masivamente escalado y distribuido a nivel global. Para entregar contenido a los usuarios finales con baja latencia, Amazon CloudFront utiliza una red global que consta de ubicaciones periféricas y cachés regionales.
- *Seguridad en la periferia*: Amazon CloudFront proporciona protección a nivel de red y de aplicación. Su tráfico y sus aplicaciones se benefician a través de varias protecciones integradas, como AWS Shield Estándar, sin costo adicional. También puede utilizar características configurables, como AWS Certificate Manager (ACM), para crear y administrar certificados de Secure Sockets Layer (SSL) personalizados sin costos adicionales.
- *Alta capacidad de programación* : las funciones de Amazon CloudFront se pueden personalizar para requisitos de aplicación específicos. Se integra con Lambda@Edge para que pueda ejecutar código personalizado en ubicaciones de AWS en todo el mundo, lo que le permite acercar la lógica de aplicaciones complejas a los usuarios para mejorar la capacidad de respuesta. La CDN también admite integraciones con otras herramientas e interfaces de automatización para DevOps. Ofrece entornos de integración y entrega continuas (CI/CD).
- *Integración profunda con AWS*: Amazon CloudFront está integrado con AWS mediante ubicaciones físicas conectadas directamente con la infraestructura global de AWS y otros servicios de AWS. Puede utilizar API o Consola de administración de AWS para configurar todas las funciones de manera programática en la CDN.

- *Rentable*: Amazon CloudFront es rentable porque no tiene compromisos mínimos y le cobra solo por lo que usa. En comparación con el autoalojamiento, Amazon CloudFront evita gastos y la complejidad de operar una red de servidores de caché en varios sitios de internet. Elimina la necesidad de sobreaprovisionar capacidad para atender posibles picos de tráfico. Amazon CloudFront también utiliza técnicas como contraer solicitudes simultáneas de espectadores en una ubicación periférica para el mismo archivo en una única solicitud a su servidor de origen. El resultado es una carga reducida en sus servidores de origen y una menor necesidad de escalar su infraestructura de origen, lo que puede resultar en mayores ahorros de costos. Si utiliza servicios de origen de AWS, como Amazon Simple Storage Service (Amazon S3) o Elastic Load Balancing, paga solo por los costos de almacenamiento y no por los datos transferidos entre estos servicios y CloudFront.



Los cargos de Amazon CloudFront se basan en el uso real del servicio en cuatro áreas:

- *Transferencia de datos:* se le cobra por el volumen de datos que se transfiere desde las ubicaciones periféricas de Amazon CloudFront, medido en GB, a internet o a su origen (tanto orígenes de AWS como otros servidores de origen). El uso de transferencia de datos se totaliza por separado para regiones geográficas específicas y luego el costo se calcula en función de los niveles de precios para cada área. Si utiliza otros servicios de AWS como origen de sus archivos, se le cobrará por separado el uso de esos servicios, incluido el almacenamiento y las horas del cómputo.
- *Solicitudes HTTP(S):* se le cobra por la cantidad de solicitudes HTTP(S) que se realizan a Amazon CloudFront para su contenido.
- *Solicitudes de invalidaciones:* se le cobra por ruta en su solicitud de invalidación. Una ruta que aparece en su solicitud de invalidación representa la URL (o varias URL si la ruta contiene un carácter comodín) del objeto que desea invalidar de la caché de CloudFront. Puede solicitar hasta 1000 rutas cada mes desde Amazon CloudFront sin cargo adicional. Más allá de las primeras 1000 rutas, se le cobrará por la ruta que figura en sus solicitudes de invalidación.
- *IP dedicada Secure Sockets Layer (SSL):* usted paga 600 USD por mes por cada certificado SSL personalizado asociado con una o más distribuciones de CloudFront que utilizan la versión de IP dedicada de soporte de certificado SSL personalizado. Esta tarifa mensual se prorratea por hora. Por ejemplo, si su certificado SSL personalizado estuvo asociado con al menos una distribución de CloudFront durante solo 24 horas (es decir, 1 día) en el mes de junio, su cargo total por usar la función de certificado SSL personalizado en junio es (1 día/30 días) * 600 USD = 20 USD.

Para obtener la información más reciente sobre precios, consulte la página de precios de Amazon CloudFront en https://aws.amazon.com/cloudfront/pricing/.

Sección 6: conclusiones importantes

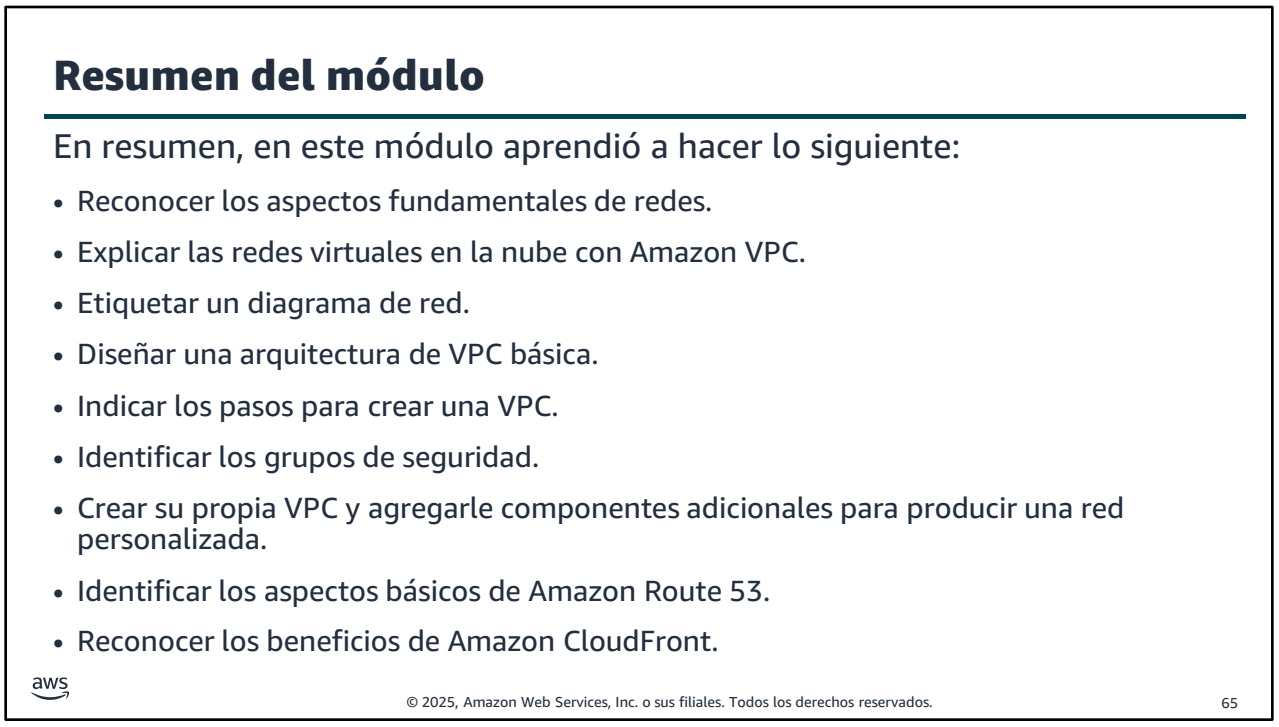
- Una CDN es un sistema distribuido globalmente de servidores de almacenamiento en caché que acelera la entrega de contenido
- Amazon CloudFront es un servicio de CDN que ofrece entregas de datos, videos, aplicaciones y API de forma segura en una infraestructura global con baja latencia y altas velocidades de transferencia.
- Amazon CloudFront ofrece muchos beneficios.

 63

Estas son algunas conclusiones clave de esta sección del módulo:

- Una CDN es un sistema distribuido globalmente de servidores de almacenamiento en caché que acelera la entrega de contenido.
- Amazon CloudFront es un servicio de CDN que ofrece entregas de datos, videos, aplicaciones y API de forma segura en una infraestructura global con baja latencia y altas velocidades de transferencia.
- Amazon CloudFront ofrece muchos beneficios que incluyen:
    - Rapidez y alcance mundial
    - Seguridad en la periferia
    - Alta capacidad de programación
    - Integración profunda con AWS
    - Rentable

Ahora es el momento de revisar el módulo y concluir con una evaluación de conocimientos y una discusión sobre una pregunta del examen de certificación de práctica.



En resumen, en este módulo aprendió a hacer lo siguiente:
- Reconocer los aspectos fundamentales de redes.
- Explicar las redes virtuales en la nube con Amazon VPC.
- Etiquetar un diagrama de red.
- Diseñar una arquitectura de VPC básica.
- Indicar los pasos para crear una VPC.
- Identificar los grupos de seguridad.
- Crear su propia VPC y agregarle componentes adicionales para producir una red personalizada.
- Identificar los aspectos básicos de Amazon Route 53.
- Reconocer los beneficios de Amazon CloudFront.

Completar la evaluación de conocimientos

Ahora, complete la evaluación de conocimientos.

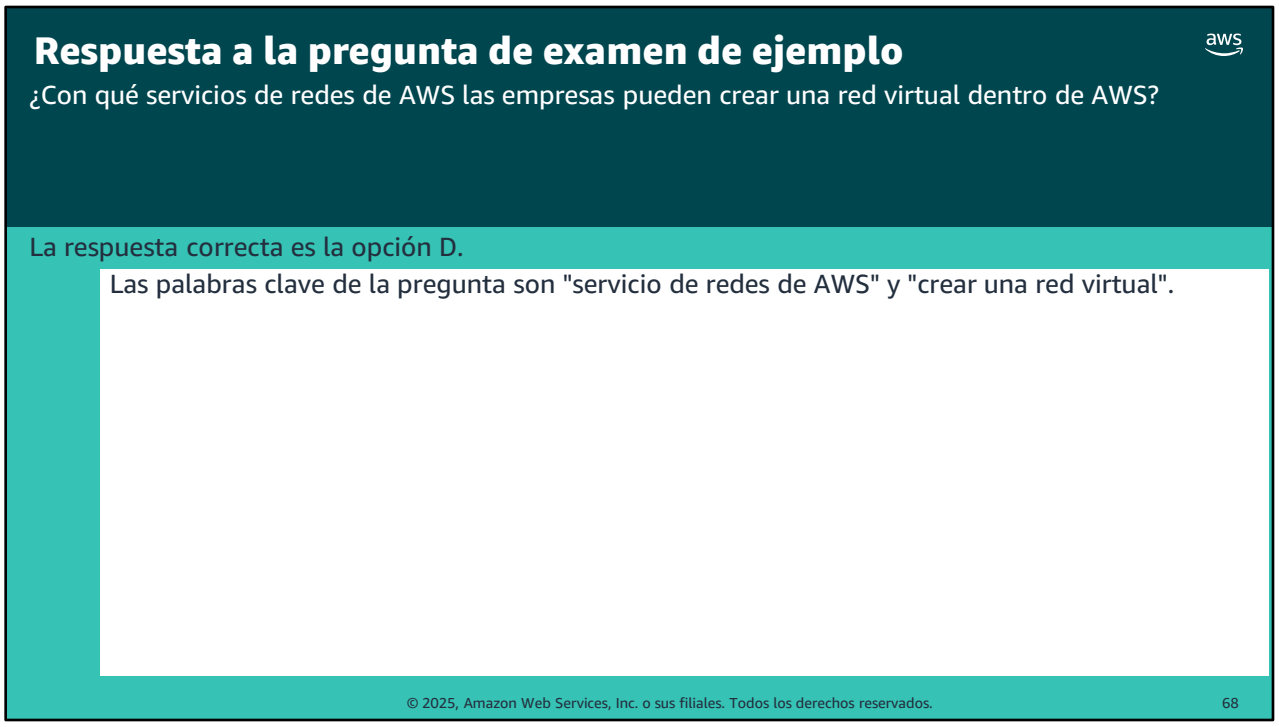
Pregunta de examen de ejemplo

¿Con qué servicios de redes de AWS las empresas pueden crear una red virtual dentro de AWS?

Opción	Respuesta
A	AWS Config
B	Amazon Route 53
C	AWS Direct Connect
D	Amazon VPC

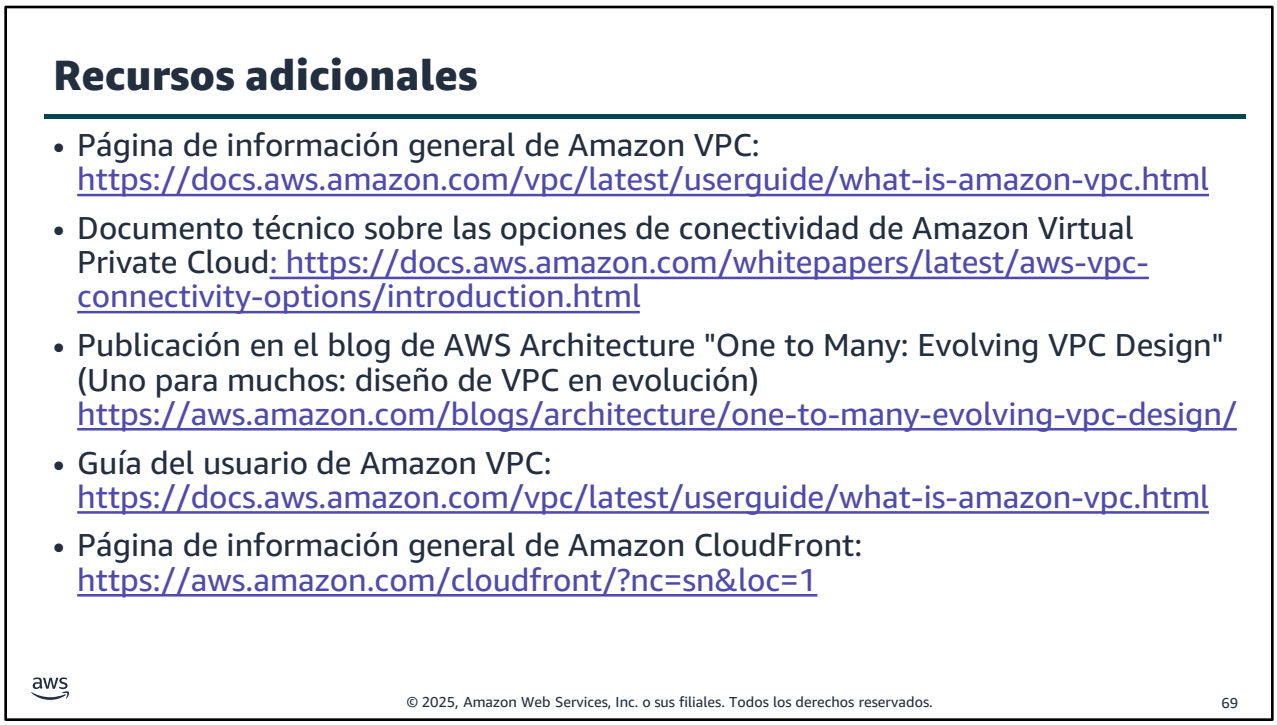
 67

Mire las opciones de respuesta y descártelas según las palabras clave.



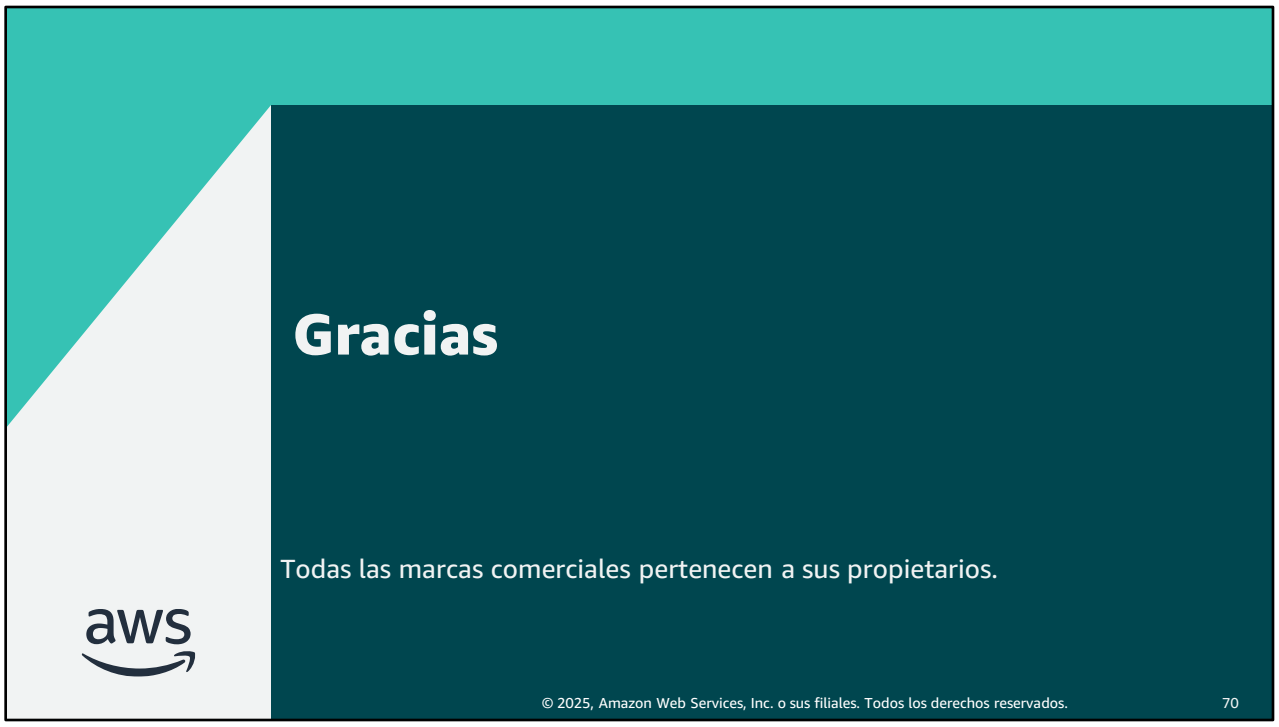
Las siguientes son las palabras clave a reconocer: **“Servicio de redes de AWS” y “crear una red virtual”.**

La respuesta correcta es la opción D.



Si desea obtener más información sobre los temas tratados en este módulo, es posible que le resulten útiles los siguientes recursos adicionales:

- Página de información general de Amazon VPC: https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html
- Documento técnico sobre las opciones de conectividad de Amazon Virtual Private Cloud: https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/introduction.html
- Publicación en el blog de AWS Architecture "One to Many: Evolving VPC Design" (Uno para muchos: diseño de VPC en evolución) https://aws.amazon.com/blogs/architecture/one-to-many-evolving-vpc-design/
- Guía del usuario de Amazon VPC: https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html
- Página de información general de Amazon CloudFront: https://aws.amazon.com/cloudfront/?nc=sn&loc=1



Gracias por completar este módulo.