Documento técnico de AWS

Opciones de conectividad de Amazon Virtual Private Cloud

Opciones de conectividad de Amazon Virtual Private Cloud: Documento técnico de AWS

Table of Contents

Opciones de conectividad de Amazon Virtual Private Cloud

Fecha de publicación: 5 de abril de 2023 (Revisiones del documento)

Resumen

Amazon Virtual Private Cloud (Amazon VPC) permite a los clientes aprovisionar una sección privada y aislada de la nube de Amazon Web Services (AWS) donde pueden lanzar los recursos de AWS en una red virtual con rangos de direcciones IP definidos por el cliente. Amazon VPC ofrece a los clientes varias opciones para conectar las redes virtuales de AWS con otras redes remotas. Este documento describe varias opciones comunes de conectividad de red disponibles para nuestros clientes. Estas incluyen opciones de conectividad para integrar redes de clientes remotos con Amazon VPC y conectar varias Amazon VPC a una red virtual contigua.

Este documento técnico está dirigido a arquitectos e ingenieros de redes corporativas o administradores de Amazon VPC que deseen revisar las opciones de conectividad disponibles. Proporciona información general de las distintas opciones para facilitar los análisis sobre la conectividad de red, así como sugerencias sobre documentación y recursos adicionales con información o ejemplos más detallados.

Introducción

Amazon VPC ofrece varias opciones de conectividad de red para su uso, en función de los requisitos y diseños de red actuales. Estas opciones de conectividad incluyen usar la conexión de Internet o una conexión de AWS Direct Connect como núcleo de la red y terminar la conexión en puntos de conexión de red administrada por el usuario o AWS. Además, con AWS, puede elegir cómo se entrega el enrutamiento de red entre Amazon VPC y las redes, aprovechando los servicios de AWS o los equipos y rutas de red administrados por el usuario. En este documento técnico se examinan las siguientes opciones, con una información general y una comparación de alto nivel de cada una de ellas:

- Opciones de conectividad de red a Amazon VPC
  - AWS Site-to-Site VPN: describe el establecimiento de una conexión VPN IPsec administrada desde el equipo de red en una red remota a Amazon VPC.
  - AWS Transit Gateway + AWS Site-to-Site VPN: describe el establecimiento de una conexión VPN IPsec administrada desde el equipo de red en una red remota a un centro de red regional para Amazon VPC, con AWS Transit Gateway.
  - AWS Direct Connect: describe el establecimiento de una conexión lógica y privada desde la red remota a Amazon VPC, con AWS Direct Connect.
  - AWS Direct Connect + AWS Transit Gateway: describe el establecimiento de una conexión lógica y privada desde la red remota a un centro de red regional para las VPC de Amazon, con AWS Direct Connect y AWS Transit Gateway.
  - AWS Direct Connect + AWS Site-to-Site VPN: describe el establecimiento de una conexión privada y cifrada desde la red remota a Amazon VPC, con AWS Direct Connect y AWS Site-to-Site VPN.
  - AWS Direct Connect + AWS Transit Gateway + VPN Site-to-Site de AWS: describe el establecimiento de una conexión cifrada y privada desde la red remota a un centro de red regional para las Amazon VPC, con AWS Direct Connect y AWS Transit Gateway.
  - AWS VPN CloudHub— Describe el establecimiento de un hub-and-spoke modelo para conectar sucursales remotas.
  - VPN de software: describe el establecimiento de una conexión VPN desde el equipo en una red remota a un dispositivo VPN de software administrado por el usuario que se ejecuta dentro de una Amazon VPC.

  - AWS Transit Gateway + Soluciones SD-WAN- Describe la integración de soluciones de red de área amplia (SD-WAN) definidas por software para interconectar varias ubicaciones remotas a un hub de red regional para Amazon VPC, utilizando la red AWS troncal o Internet como red de tránsito.
- Opciones de conectividad de Amazon VPC a Amazon VPC
  - Emparejamiento de VPC: describe la conexión de Amazon VPC dentro de las regiones y entre ellas mediante la característica de emparejamiento de Amazon VPC.
  - AWS Transit Gateway— Describe la conexión de Amazon VPC dentro de las regiones y entre ellas mediante AWS Transit Gateway un hub-and-spoke modelo.
  - AWS PrivateLink: describe la conexión de Amazon VPC con puntos de conexión de interfaz de VPC y servicios de punto de conexión de VPC.
  - VPN de software: describe la conexión de Amazon VPC mediante conexiones VPN establecidas entre dispositivos VPN de software administrado por el usuario que se ejecutan dentro de cada Amazon VPC.
  - VPN de software a AWS Site-to-Site VPN: describe la conexión de Amazon VPC con una conexión VPN establecida entre un dispositivo VPN de software administrado por el usuario en una Amazon VPC y una VPN Site-to-Site AWS conectada a la otra Amazon VPC.
- Opciones de conectividad de acceso remoto de software a Amazon VPC
  - AWS Client VPN: describe la conexión del acceso remoto del software a Amazon VPC mediante el uso de AWS Client VPN.
  - Software Client VPN: describe la conexión del acceso remoto del software a Amazon VPC, aprovechando los dispositivos VPN de software administrado por el usuario.
- VPC de tránsito: describe el establecimiento de una red de tránsito global en AWS mediante una VPN de software junto con una VPN administrada por AWS.
- WAN en la nube de AWS: describe el establecimiento de una red de área extendida (WAN) administrada para crear, administrar y monitorear fácilmente las interconexiones globales entre los recursos de Amazon VPC, los centros de datos y las sucursales remotas.

Opciones de conectividad de red a Amazon VPC

En esta sección, se proporcionan patrones de diseño para conectar redes remotas con el entorno de Amazon VPC. Estas opciones son útiles para integrar los recursos de AWS con los servicios locales existentes (por ejemplo, monitoreo, autenticación, seguridad, datos u otros sistemas) al extender las redes internas a la nube de AWS. Esta extensión de red también permite a los usuarios internos conectarse sin problemas a los recursos alojados en AWS como cualquier otro recurso interno.

La conectividad de VPC a las redes de cliente remotas se logra mejor cuando se utilizan rangos de IP que no se superpongan para cada red que se esté conectando. Por ejemplo, si desea conectar una o más VPC a la red corporativa, asegúrese de que estén configuradas con rangos únicos de enrutamiento entre dominios sin clases (CIDR). Recomendamos que asigne un bloque CIDR único, contiguo y no superpuesto para que lo utilice cada VPC. Para obtener información adicional sobre el enrutamiento y las restricciones de Amazon VPC, consulte las Preguntas frecuentes de Amazon VPC.

Opción	Caso de uso	Ventajas	Limitaciones
AWS Site-to-Site VPN	AWS administró la conexión de AWS de VPN IPsec a través de Internet a una VPC individual	Reutilizar los equipos y procesos de VPN existentes Reutilizar las conexiones de Internet existentes Servicio de VPN de alta disponibilidad administrado por AWS Admite rutas estáticas o interconexión de protocolo de puerta de enlace fronteriza (BGP) dinámica y	La latencia, la variabilidad y la disponibilidad de la red dependen de las condiciones de Internet Es responsable de implementar la redundancia y la conmutación por error (si es necesario) El dispositivo remoto debe admitir el BGP de salto único (si se utiliza el BGP para el enrutamiento dinámico)

Opción	Caso de uso	Ventajas	Limitaciones
		políticas de enrutamiento	
AWS Transit Gateway + AWS Site-to-Site VPN	Conexión VPN IPsec administrada por AWS a través de Internet al enrutador regional para varias VPC	Igual que en la opción anterior AWS administró un centro de red regional de alta disponibilidad y escalabilidad para hasta 5000 archivos adjuntos	Igual que en la opción anterior
AWS Direct Connect	Conexión de red dedicada a través de líneas privadas	Rendimiento de red más predecible Costos de ancho de banda reducidos Admite políticas de enrutamiento y emparejamiento BGP	Puede requerir relaciones adicionales con proveedores de telecomunicaciones y alojamiento o el aprovisionamiento de nuevos circuitos de red
AWS Direct Connect + AWS Transit Gateway	Conexión de red dedicada a través de líneas privadas al enrutador regional para múltiples VPC	Igual que en la opción anterior AWS administró un centro de red regional de alta disponibilidad y escalabilidad para hasta 5000 archivos adjuntos	Igual que en la opción anterior

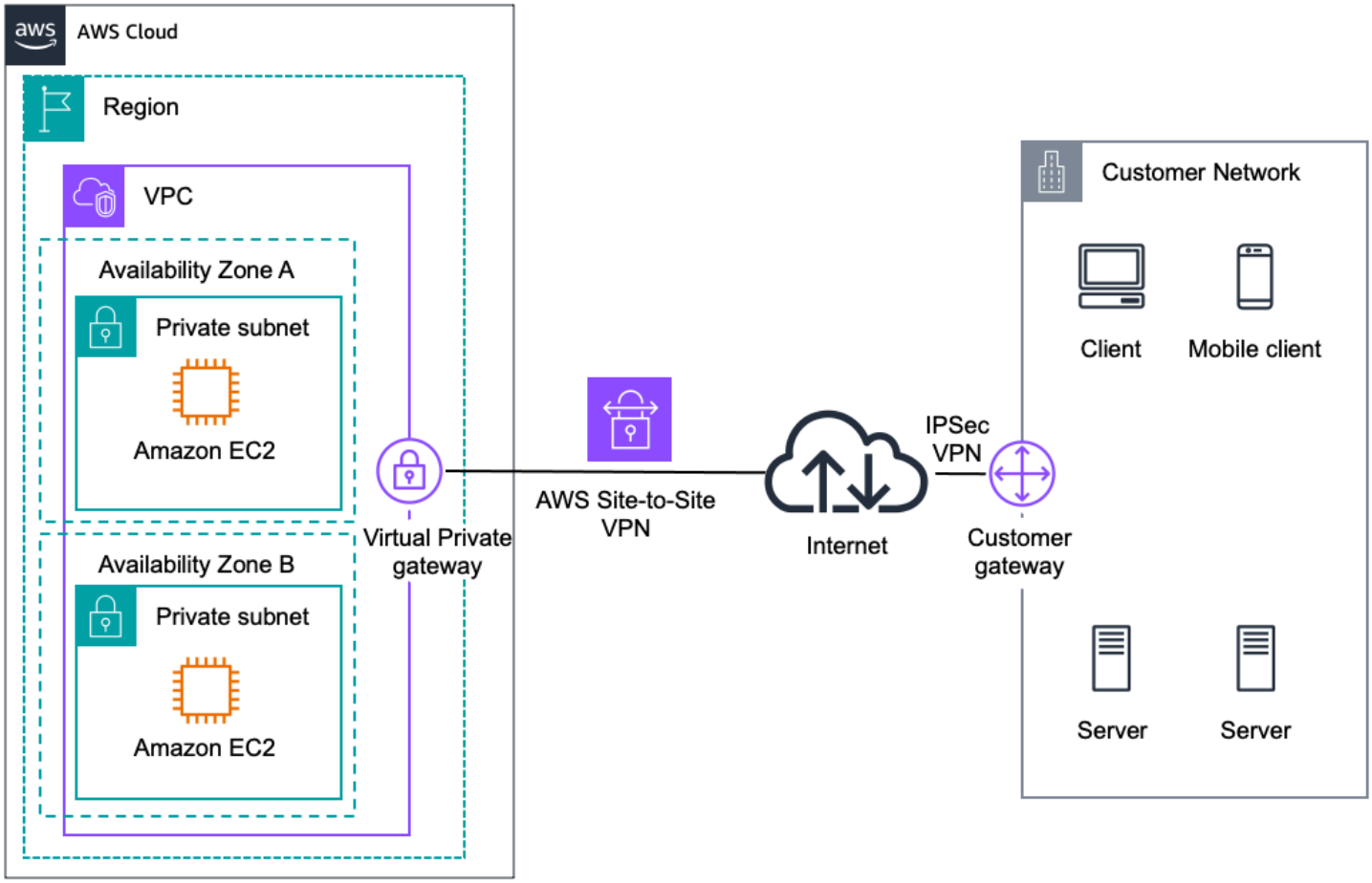
Opción	Caso de uso	Ventajas	Limitaciones
AWS Direct Connect + VPN Site-to-Site de AWS	Conexión VPN IPsec a través de líneas privadas	Rendimiento de red más predecible Costos de ancho de banda reducidos Soporta políticas de enrutamiento y emparejamiento BGP en AWS Direct Connect Reutilizar los equipos y procesos de VPN existentes Servicio de VPN de alta disponibilidad administrado por AWS Admite rutas estáticas o interconexión de protocolo de puerta de enlace fronteriza (BGP) dinámica y políticas de enrutamiento en la conexión de VPN	Puede requerir relaciones adicionales con proveedores de telecomunicaciones y alojamiento o el aprovisionamiento de nuevos circuitos de red Es responsable de implementar la redundancia y la conmutación por error (si es necesario) El dispositivo remoto debe admitir el BGP de salto único (si se utiliza el BGP para el enrutamiento dinámico)

Opción	Caso de uso	Ventajas	Limitaciones
AWS Direct Connect + AWS Transit Gateway + VPN Site-to-Site de AWS	Conexión VPN IPsec de red a través de líneas privadas al enrutador regional para múltiples VPC	Igual que en la opción anterior AWS administró un centro de red regional de alta disponibilidad y escalabilidad para hasta 5000 archivos adjuntos	Igual que en la opción anterior
AWS VPN CloudHub	Connect sucursales remotas en un hub-and-spoke modelo para conectividad principal o de respaldo	Reutilizar las conexiones de Internet existentes y las conexiones de la AWS VPN Servicio de VPN de alta disponibilidad administrado por AWS Admite BGP para intercambiar rutas y prioridades de enrutamiento	La latencia, la variabilidad y la disponibilidad de la red dependen de Internet El usuario ha administrado los puntos de conexión de sucursal y es responsable de implementar la redundancia y la conmutación por error (si es necesario)

Opción	Caso de uso	Ventajas	Limitaciones
AWS Transit Gateway + Soluciones SD-WAN	Conecta sucursales y oficinas remotas con una red de área amplia definida por software utilizando el núcleo de AWS o Internet como una red de tránsito.	Admite una gama más amplia de proveedores, productos y protocolos de SD-WAN Algunas soluciones de proveedores se integran con los servicios nativos de AWS.	Es responsable de implementar la alta disponibilidad (HA) de los dispositivos SD-WAN si están ubicados en una VPC de Amazon.
VPN de software	Conexión de VPN basada en un dispositivo de software a través de Internet	Admite una gama más amplia de proveedores, productos y protocolos de VPN Solución totalmente administrada por el cliente	Es responsable de implementar las soluciones de alta disponibilidad para todos los puntos de conexión de la VPN (si es necesario)

AWS Site-to-Site VPN

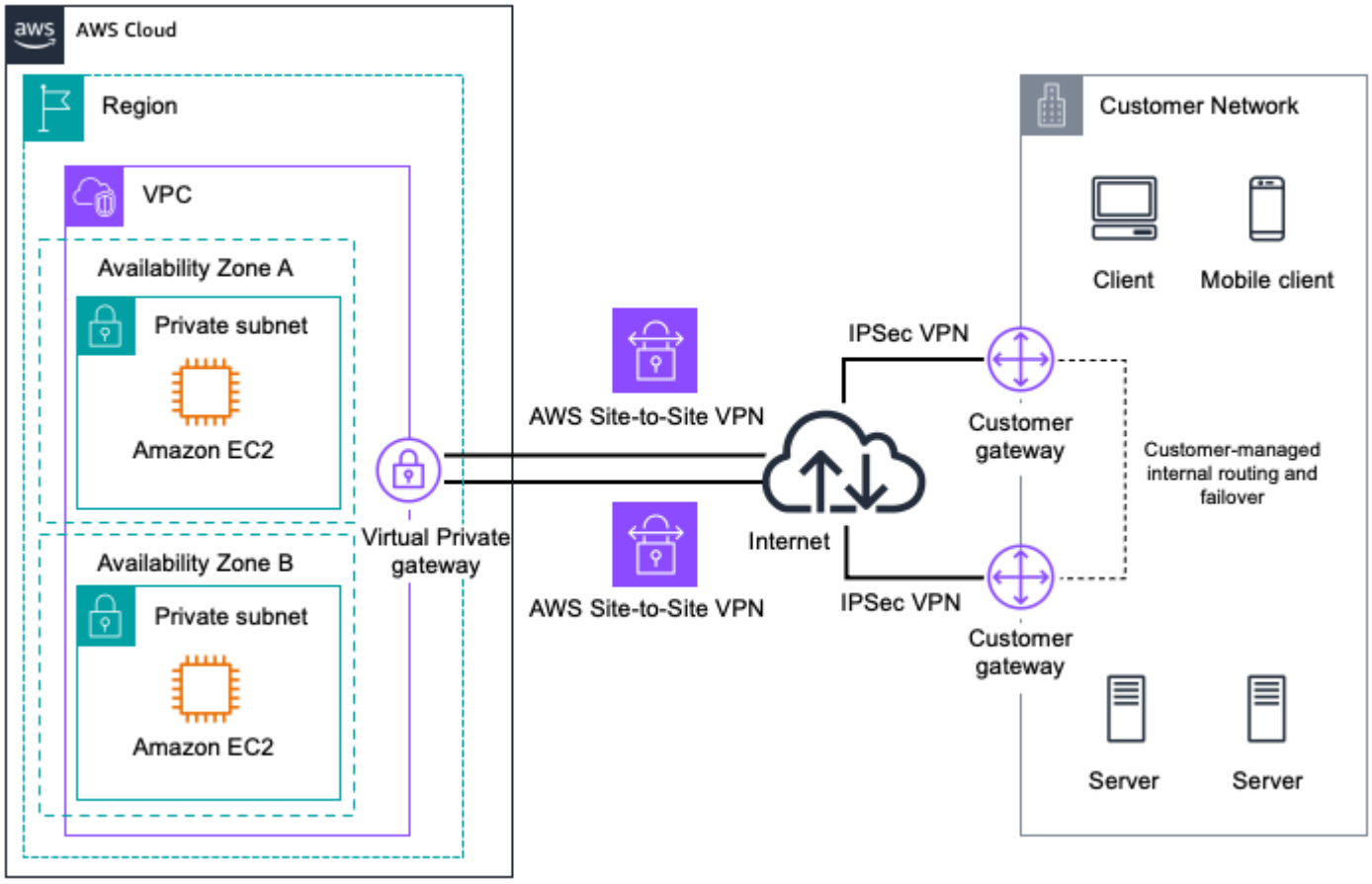
Amazon VPC ofrece la opción de crear una conexión VPN IPsec entre las redes remotas y Amazon VPC a través de Internet, como se muestra en la siguiente imagen.



AWS Managed VPN

Considere la posibilidad de adoptar este enfoque cuando desee aprovechar un punto de conexión de VPN administrado por AWS que incluye redundancia y conmutación por error automatizadas integradas en el lado de AWS de la conexión de VPN.

La puerta de enlace privada virtual también admite y fomenta las conexiones de puerta de enlace de varios usuarios para que pueda implementar la redundancia y la conmutación por error en su lado de la conexión de VPN, como se muestra en la siguiente imagen.



Redundant AWS Site-to-Site VPN Connections

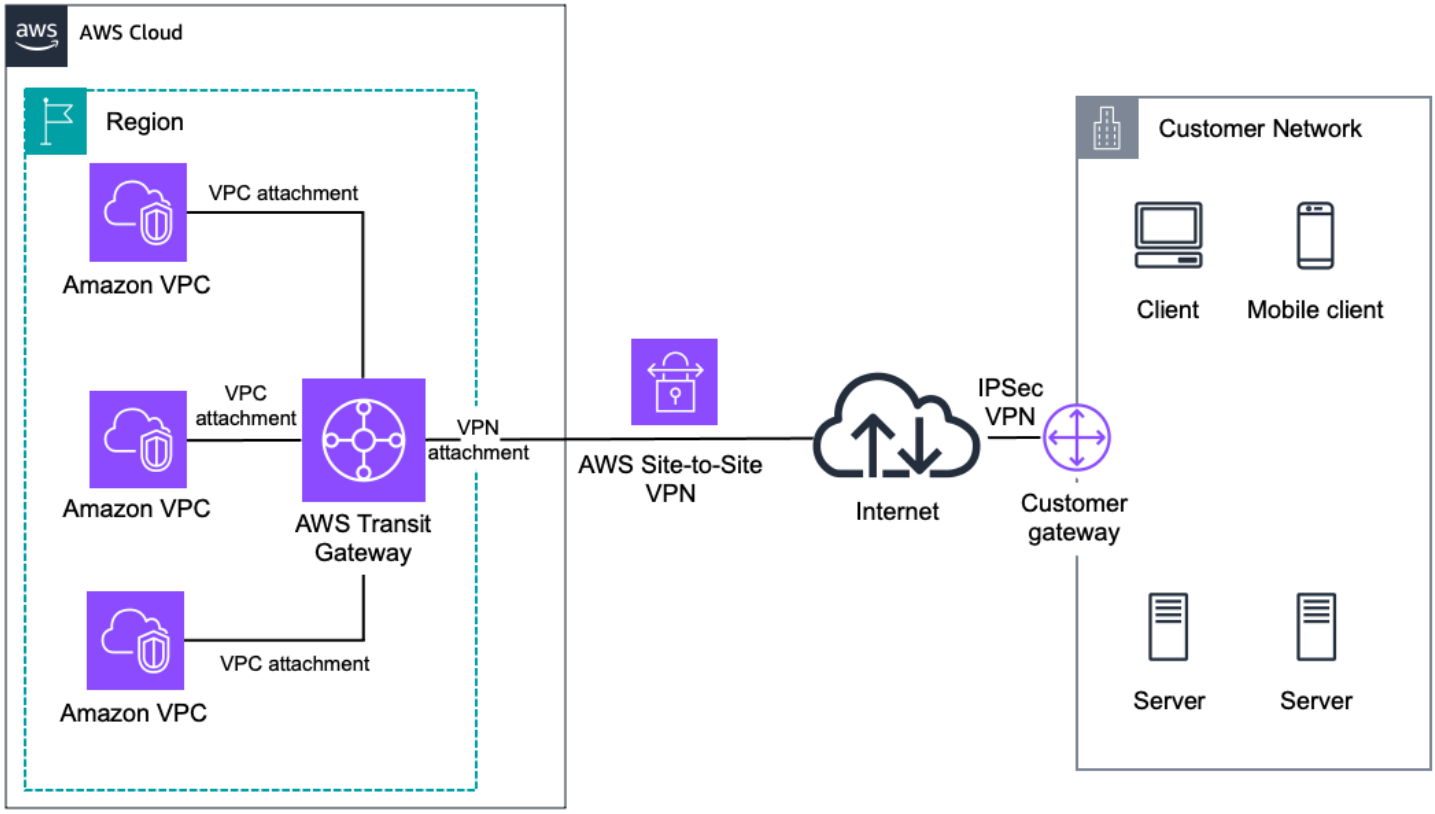
Se proporcionan opciones de enrutamiento dinámico y estático para brindarle flexibilidad en la configuración de enrutamiento. El enrutamiento dinámico utiliza la interconexión de BGP para intercambiar información de enrutamiento entre AWS y estos puntos de conexión remotos. Con el enrutamiento dinámico, también puede especificar las prioridades, políticas y pesos (métricas) de enrutamiento en los anuncios de BGP e influir en la ruta de red entre las redes y AWS. Es importante tener en cuenta que cuando se utiliza BGP, tanto la sesión de IPsec como la de BGP se deben terminar en el mismo dispositivo de puerta de enlace de usuario, por lo que debe ser capaz de terminar las sesiones de IPsec y BGP.

Recursos adicionales de

- Guía del usuario de AWS Site-to-Site VPN
- Requisitos para los dispositivos de puerta de enlace de cliente
- Dispositivos de puerta de enlace de cliente probados con Amazon VPC

AWS Transit Gateway + AWS Site-to-Site VPN

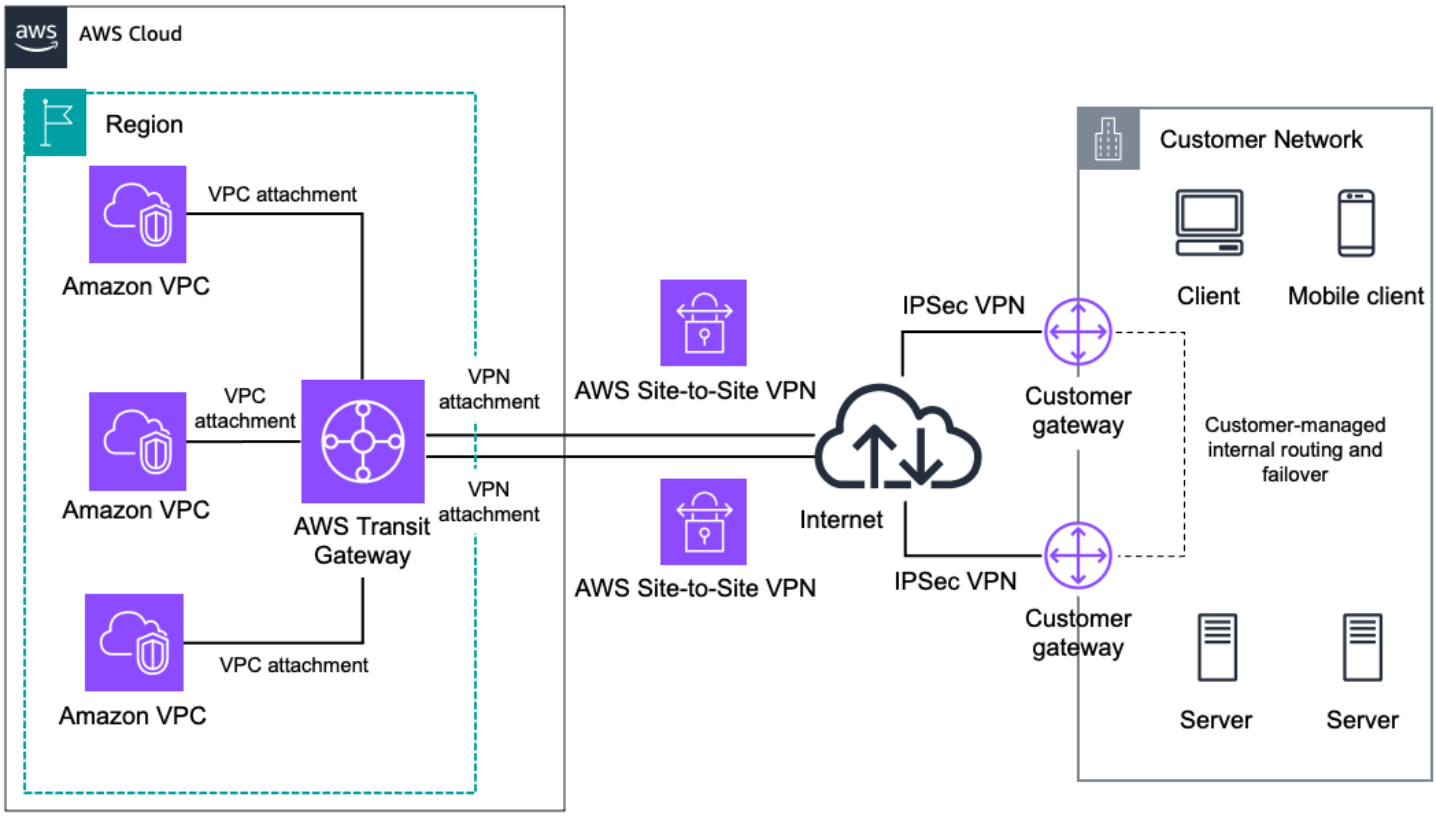
AWS Transit Gateway es un centro de tránsito de red regional de alta disponibilidad y escalabilidad administrado por AWS que se utiliza para interconectar las VPC y las redes de los clientes. AWS Transit Gateway + VPN, con la vinculación de la VPN de puerta de enlace de tránsito, ofrece la opción de crear una conexión VPN IPsec entre la red remota y la puerta de enlace de tránsito a través de Internet, como se muestra en la siguiente imagen.



AWS Transit Gateway and AWS Site-to-Site VPN

Considere la posibilidad de utilizar este enfoque cuando desee aprovechar un punto de conexión de VPN administrado por AWS para conectarse a varias VPC de la misma región sin el costo adicional ni la administración de varias conexiones IPsec VPN a varias VPC de Amazon.

AWS Transit Gateway también admite y fomenta las conexiones de puerta de enlace de varios usuarios para que pueda implementar la redundancia y la conmutación por error en su lado de la conexión de VPN, como se muestra en la siguiente imagen.



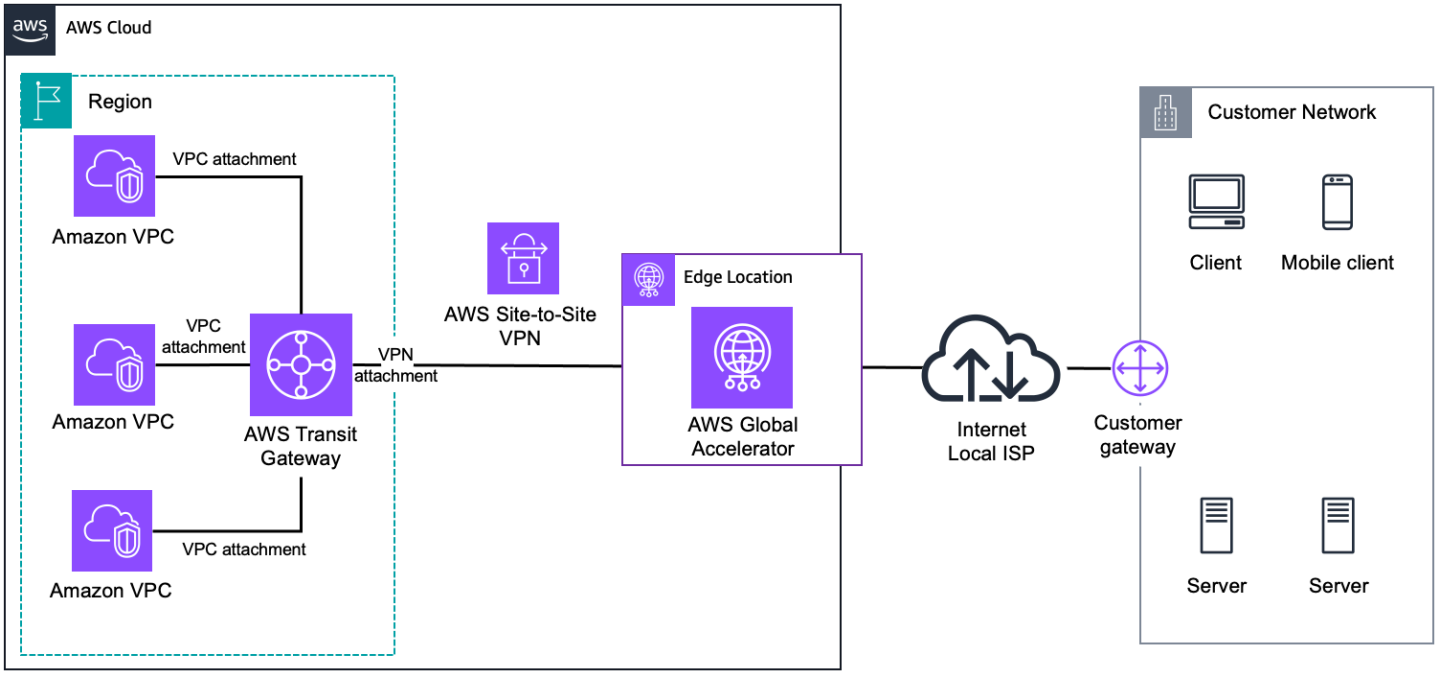
AWS Transit Gateway and Redundant VPN

Se proporcionan opciones de enrutamiento dinámico y estático para brindarle flexibilidad en la configuración de enrutamiento en la vinculación de VPN IPsec de puerta de enlace de tránsito. El enrutamiento dinámico utiliza la interconexión de BGP para intercambiar información de enrutamiento entre AWS y estos puntos de conexión remotos. Con el enrutamiento dinámico, también puede especificar las prioridades, políticas y pesos (métricas) de enrutamiento en los anuncios de BGP e influir en la ruta de red entre las redes y AWS. Es importante tener en cuenta que cuando se utiliza BGP, tanto la sesión de IPsec como la de BGP se deben terminar en el mismo dispositivo de puerta de enlace de usuario, por lo que debe ser capaz de terminar las sesiones de IPsec y BGP.

Por conexión VPN, puede lograr 1.25 Gbps de rendimiento y 140 000 paquetes por segundo. Al finalizar las conexiones de VPN en la puerta de enlace de tránsito, puede utilizar el enrutamiento de rutas múltiples de igual costo (ECMP) para obtener un mayor ancho de banda de VPN agregando varios túneles de VPN. Para usar ECMP, debe configurar el enrutamiento dinámico en las conexiones de VPN; ECMP no es compatible con el enrutamiento estático.

Además, puede habilitar la aceleración en las conexiones de AWS Site-to-Site VPN. Una conexión de VPN acelerada utiliza AWS Global Accelerator para enrutar el tráfico desde la red hasta la ubicación periférica de AWS que está más próxima al dispositivo de puerta de enlace de cliente.

Puede utilizar esta opción para evitar interrupciones de red que es posible que se produzcan cuando el tráfico se enrute a través del Internet público. La aceleración solo se admite en las conexiones de VPN que están asociadas a una puerta de enlace de tránsito, como se muestra en la siguiente imagen:



Accelerated AWS Site-to-Site VPN

Por último, en lo que respecta a las direcciones IP, las conexiones de VPN de sitio a sitio en AWS Transit Gateway admiten el tráfico IPv4 e IPv6. Se aplican las siguientes reglas:

- IPv6 solo es compatible con las direcciones IP internas del túnel de VPN. La dirección IP externa de los AWS puntos finales son direcciones IPv4 públicas. La dirección IP de la puerta de enlace de cliente debe ser una dirección IPv4 pública.
- Las conexiones de Site-to-Site VPN no pueden admitir el tráfico IPv4 e IPv6 a la vez. Si la conectividad híbrida requiere una comunicación de doble pila, debe crear diferentes túneles de VPN para el tráfico IPv4 e IPv6.

Recursos adicionales de

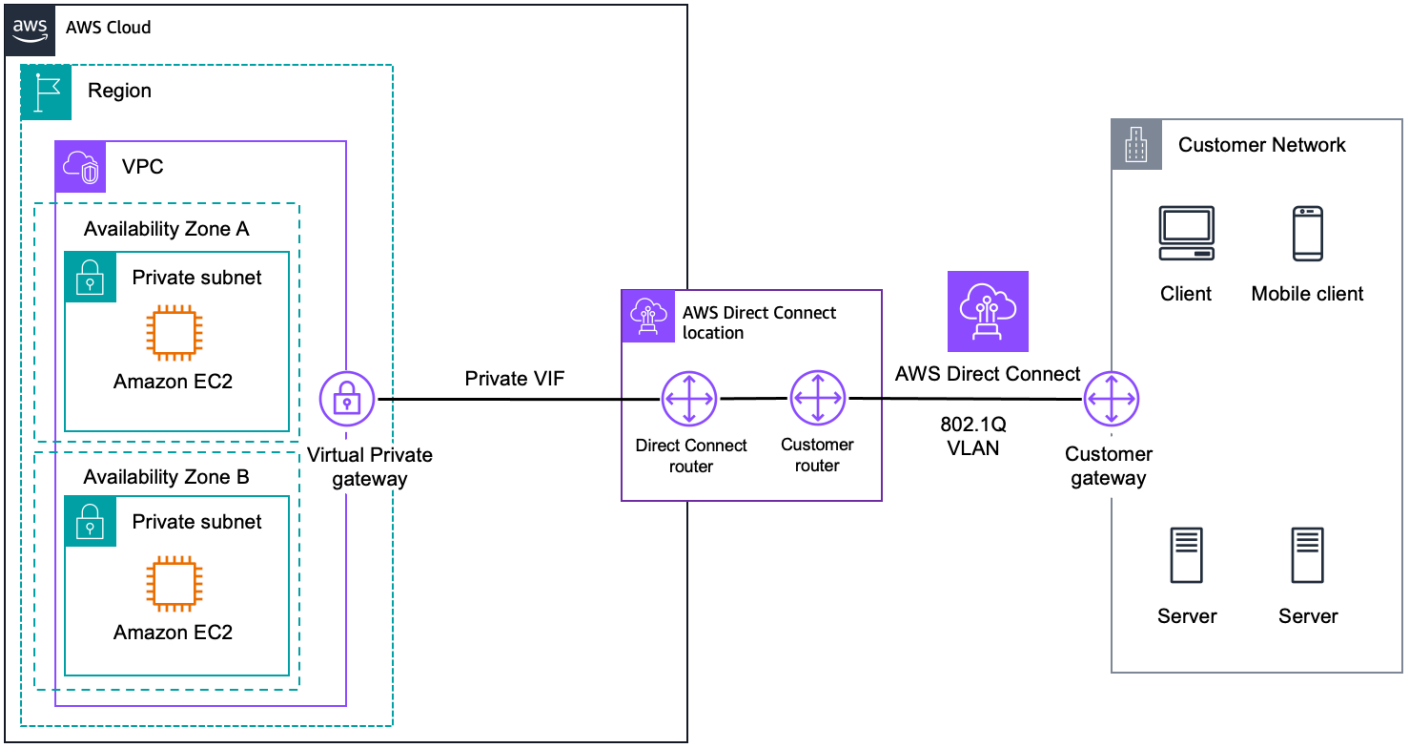
- Vinculaciones de VPN de la puerta de enlace de tránsito
- Puerta de enlace de cliente
- Uso de Site-to-Site VPN

- Conexiones de Site-to-Site VPN aceleradas

AWS Direct Connect

AWS Direct Connectfacilita el establecimiento de una conexión dedicada desde una red local a una o más VPC. AWS Direct Connect puede reducir los costes de la red, aumentar el rendimiento del ancho de banda y proporcionar una experiencia de red más coherente que las conexiones basadas en Internet. Utiliza las VLAN 802.1Q estándar del sector para conectarse a Amazon VPC mediante direcciones IP privadas. Las VLAN se configuran mediante interfaces virtuales (VIF) y puede configurar tres tipos diferentes de VIF:

- Interfaz virtual pública: establezca la conectividad entre los puntos finales AWS públicos y su centro de datos, oficina o entorno de colocación.
- Interfaz virtual de tránsito: establezca una conectividad privada entre AWS Transit Gateway su centro de datos, oficina o entorno de colocación. Esta opción de conectividad está cubierta en la sección ???.
- Interfaz virtual privada: establezca una conectividad privada entre los recursos de Amazon VPC y el centro de datos, la oficina o el entorno de coubicación. En la siguiente ilustración se muestra el uso de VIF privadas.



AWS Direct Connect

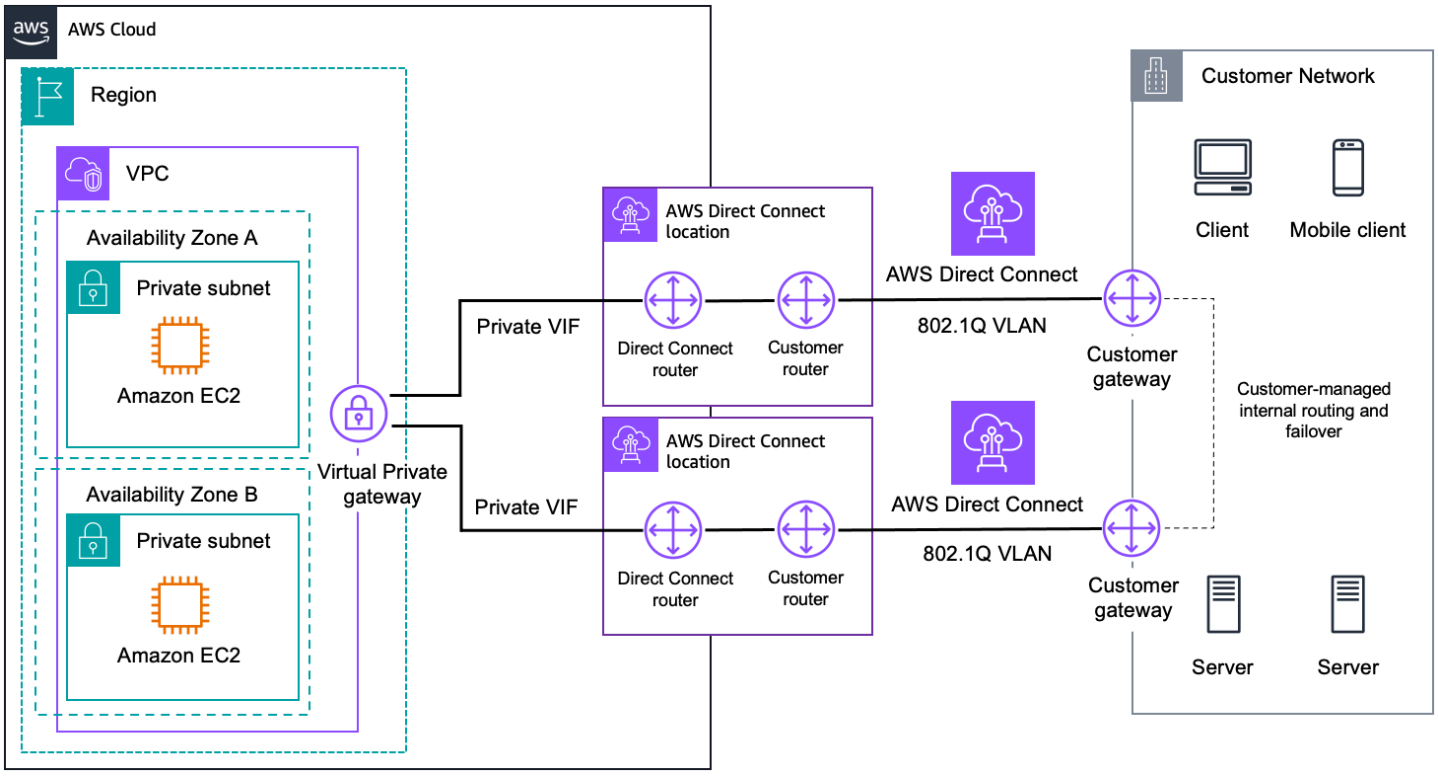
Puede establecer la conectividad con la AWS red troncal AWS Direct Connect mediante el establecimiento de una conexión cruzada con los AWS dispositivos en una ubicación de Direct Connect. Puede acceder a cualquier AWS región desde cualquiera de nuestras ubicaciones de Direct Connect (excepto China). Si no tiene equipos en una ubicación, puede elegir entre un ecosistema de proveedores de servicios de WAN para integrar su AWS Direct Connect terminal en una AWS Direct Connect ubicación con sus redes remotas.

Con AWS Direct Connect, tiene dos tipos de conexión:

- Conexiones dedicadas, son conexiones Ethernet físicas asociadas a un único cliente. Puede solicitar velocidades de puerto de 1, 10 o 100 Gbps. Es posible que necesite trabajar con un AWS Direct Connect socio del Programa de Socios para que le ayude a establecer circuitos de red entre una AWS Direct Connect conexión y su centro de datos, oficina o entorno de colocación.
- Conexiones alojadas, en las que un AWS Direct Connect socio proporciona una conexión Ethernet física y la comparte contigo. Puede solicitar velocidades de puerto de entre 50 Mbps y 10 Gbps. Usted trabaja con el socio tanto en la AWS Direct Connect conexión que estableció como en los circuitos de red entre una AWS Direct Connect conexión y su centro de datos, oficina o entorno de colocación.

En el caso de las conexiones dedicadas, también puede utilizar un grupo de agregación de enlaces (LAG) para agregar varias conexiones en un único AWS Direct Connect punto final. Las trata como una única conexión administrada. Puede agregar hasta cuatro conexiones de 1 o 10 Gbps y hasta dos conexiones de 100 Gbps.

Cuando hablemos de la alta disponibilidad en AWS Direct Connect, recomendamos utilizar AWS Direct Connect conexiones adicionales. El kit de herramientas de AWS Direct Connect resiliencia ofrece orientación para crear conexiones de red altamente AWS resilientes entre su centro de datos, oficina o entorno de colocación. La siguiente figura muestra un ejemplo de una opción de conectividad de alta resiliencia, con dos AWS Direct Connect conexiones que terminan en dos ubicaciones diferentes. AWS Direct Connect

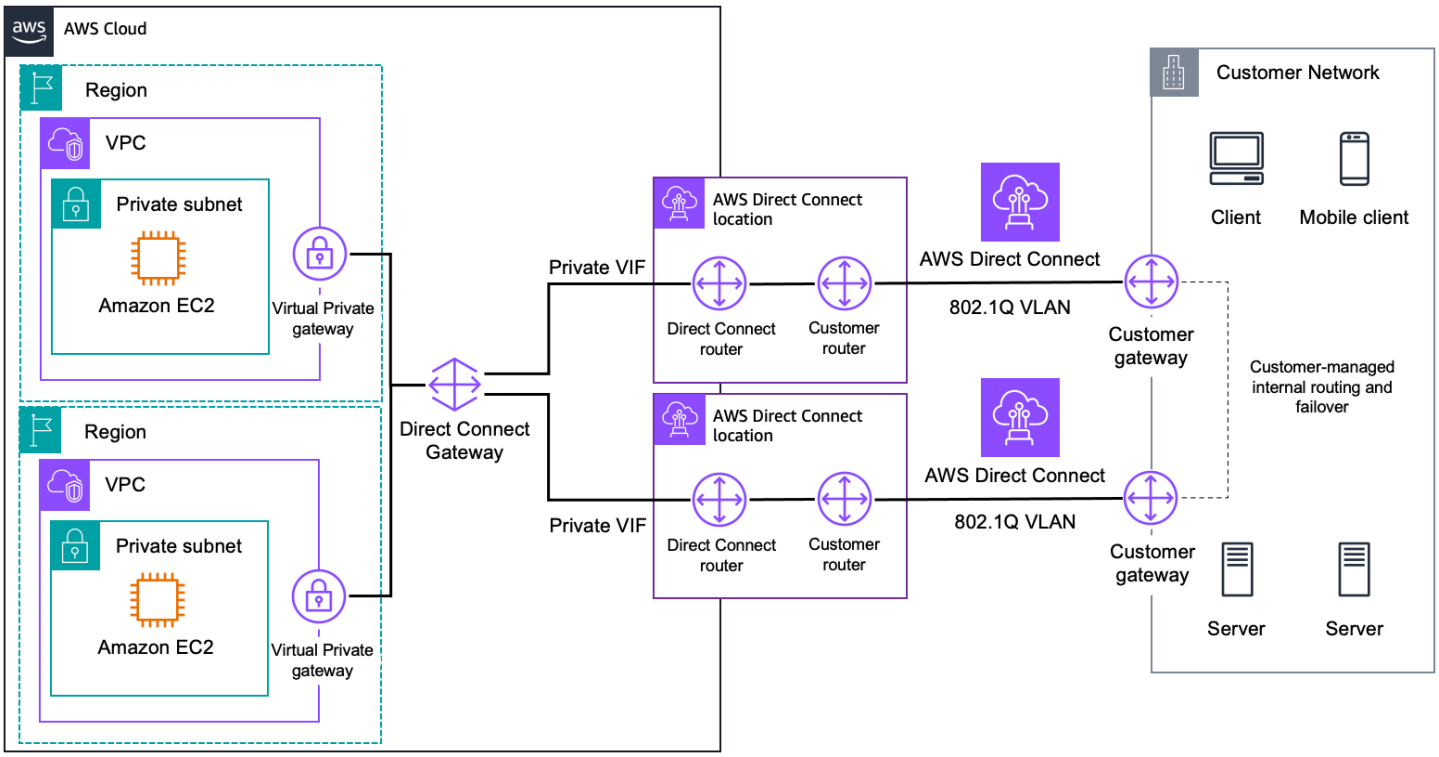


Redundante AWS Direct Connect

AWS Direct Connect no está cifrado de forma predeterminada. Para conexiones dedicadas de 10 o 100 Gbps, puede utilizar la seguridad de MAC (MACsec) como una opción de cifrado. Para conexiones de 1 Gbps o menos, puede crear túneles VPN sobre la conexión; esta opción está cubierta en las secciones AWS Direct Connect + VPN Site-to-Site de AWS y AWS Direct Connect + AWS Transit Gateway + VPN Site-to-Site de AWS.

Un recurso importante AWS Direct Connect es la puerta de enlace Direct Connect, que es un recurso disponible en todo el mundo para permitir conexiones a múltiples Amazon VPC o Transit Gateways

en diferentes regiones o AWS cuentas. Este recurso también le permite conectarse a cualquier VPC o puerta de enlace de tránsito participante desde una VIF privada o una VIF de tránsito, lo que reduce la administración de AWS Direct Connect , como se muestra en la siguiente imagen.



AWS Direct Connect Gateway

En cuanto al direccionamiento IP, las interfaces AWS Direct Connect virtuales admiten sesiones BGP de IPv4 e IPv6 para un funcionamiento de doble pila.

- La configuración de IPv4 de las VIF privadas y de tránsito utiliza direcciones IPv4 generadas por AWS o direcciones configuradas por usted. Para el intercambio de tráfico BGP para IPv4 de VIF públicas, debe especificar un CIDR IPv4 /31 público único de su propiedad (o enviar una solicitud para que se le asigne un bloque de CIDR).
- Para todos los tipos de intercambio de tráfico BGP para IPv6 de VIF, AWS asigna un CIDR /125, que no es configurable.

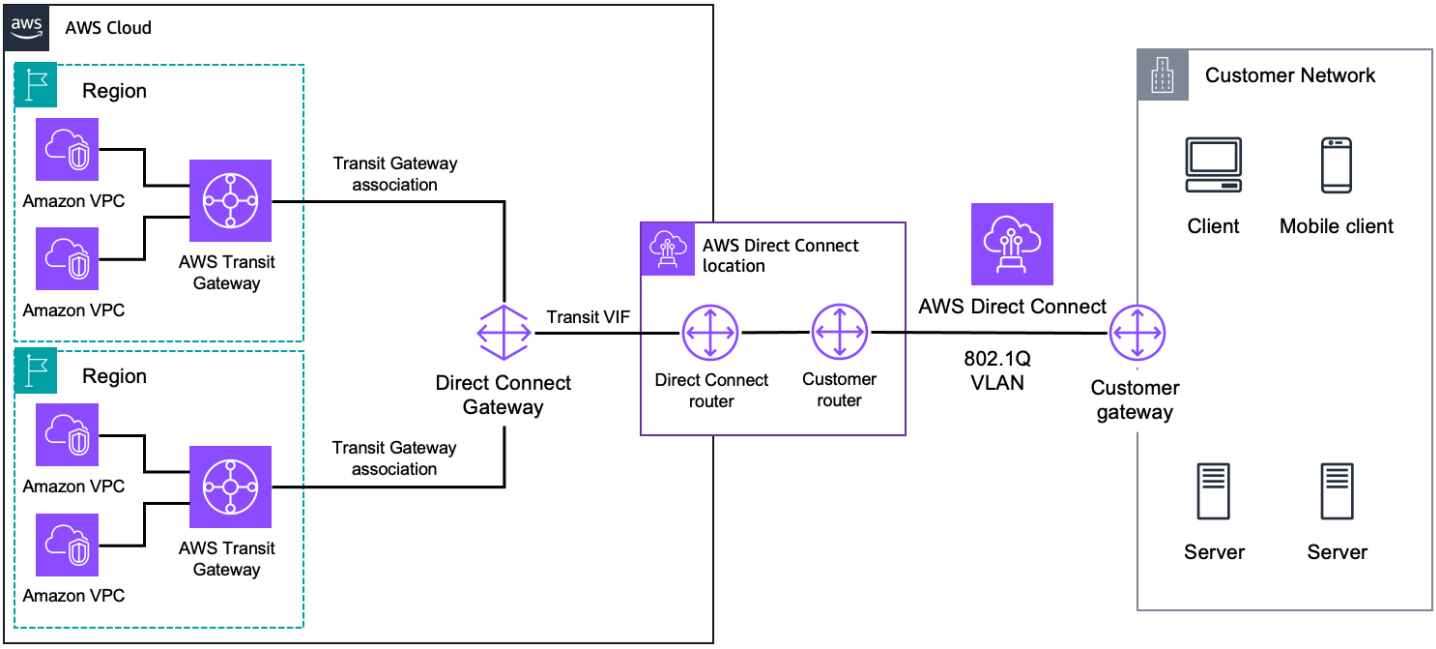
Recursos adicionales de

- AWS Direct Connect Guía del usuario
- AWS Direct Connect interfaces virtuales
- AWS Direct Connect puertas de enlace

- AWS Direct Connect Kit de herramientas de resiliencia
- AWS Direct Connect Seguridad MAC
- AWS Direct Connect ubicaciones
- AWS Direct Connect Socios de entrega

AWS Direct Connect + AWS Transit Gateway

AWS Direct Connect+ AWS Transit Gateway, que utiliza la conexión VIF de tránsito a la puerta de enlace Direct Connect, permite que su red conecte varios enrutadores centralizados regionales a través de una conexión dedicada privada. El siguiente diagrama muestra la conexión a dos enrutadores.



AWS Direct Connect and AWS Transit Gateway

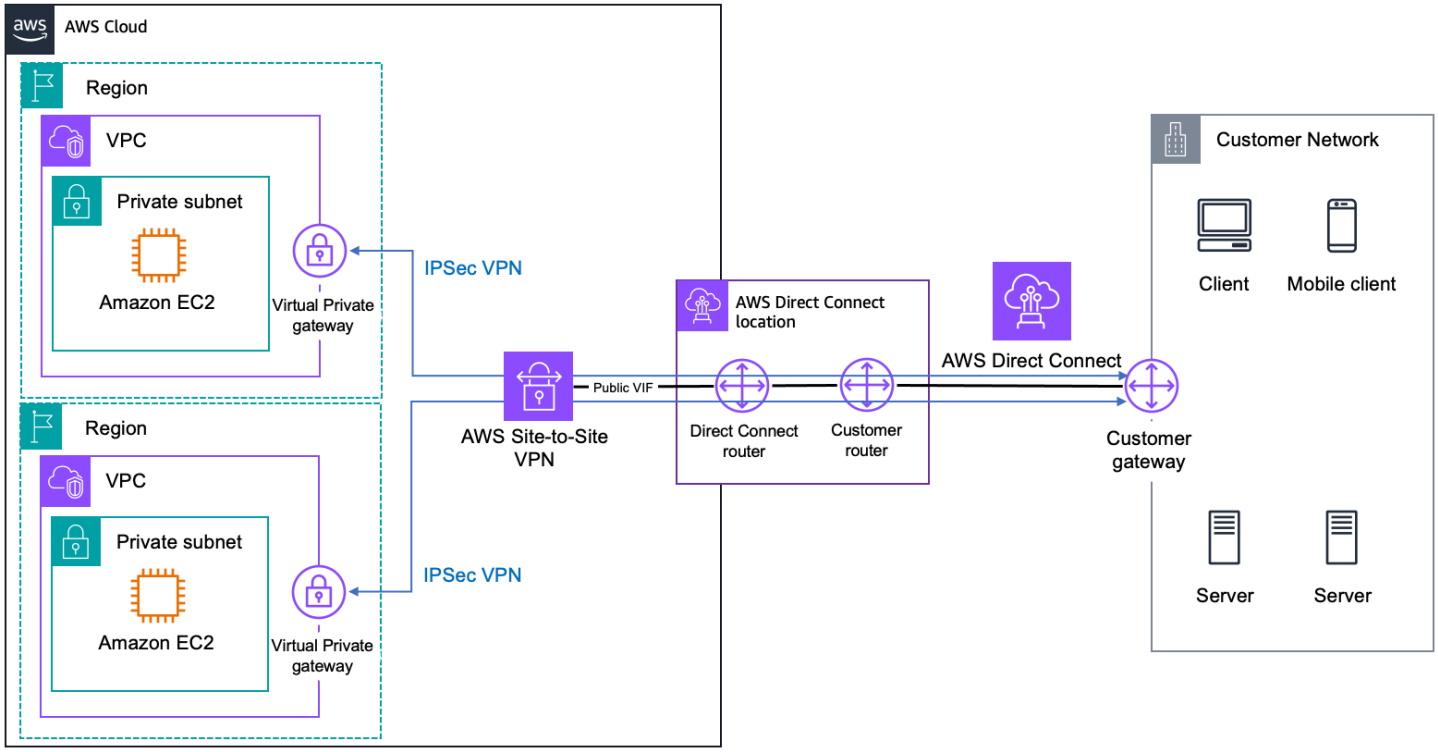
Cada uno AWS Transit Gateway es un centro de tránsito de red para interconectar las VPC en la misma región, lo que consolida la configuración de enrutamiento de Amazon VPC en un solo lugar. Esta solución simplifica la administración de las conexiones entre una Amazon VPC y las redes a través de una conexión privada, lo que puede reducir los costos de la red, aumentar el rendimiento del ancho de banda y proporcionar una experiencia de red más coherente que las conexiones basadas en Internet.

Recursos adicionales de

- Guía del usuario de AWS Direct Connect
- Enlaza grupos de agregación en AWS Direct Connect
- Publicación en blog: IIntegrating sub-1 Gbps hosted connections with AWS Transit Gateway

AWS Direct Connect + VPN Site-to-Site de AWS

Con AWS Direct Connect+ AWS Site-to-Site VPN, puede combinar AWS Direct Connect conexiones con una solución de VPN administrada por AWS. AWS Direct Connect Las VIF públicas establecen una conexión de red dedicada entre su red y los recursos públicos de AWS, como un punto de conexión VPN Site-to-Site de AWS. Una vez establecida la conexión con el servicio, puede crear conexiones IPsec a las correspondientes puertas de enlace privadas virtuales de Amazon VPC. La siguiente imagen ilustra esta opción.



AWS Direct Connect and AWS Site-to-Site VPN

Esta solución combina las ventajas de una conexión IPsec end-to-end segura con una baja latencia y un mayor ancho de banda AWS Direct Connect para ofrecer una experiencia de red más uniforme que las conexiones VPN basadas en Internet. Se establece una sesión de conexión BGP entre el

router AWS Direct Connect y el VIF público. Se establecerá otra sesión de BGP o una ruta estática entre la puerta de enlace privada virtual y el enrutador en los túneles VPN de IPsec.

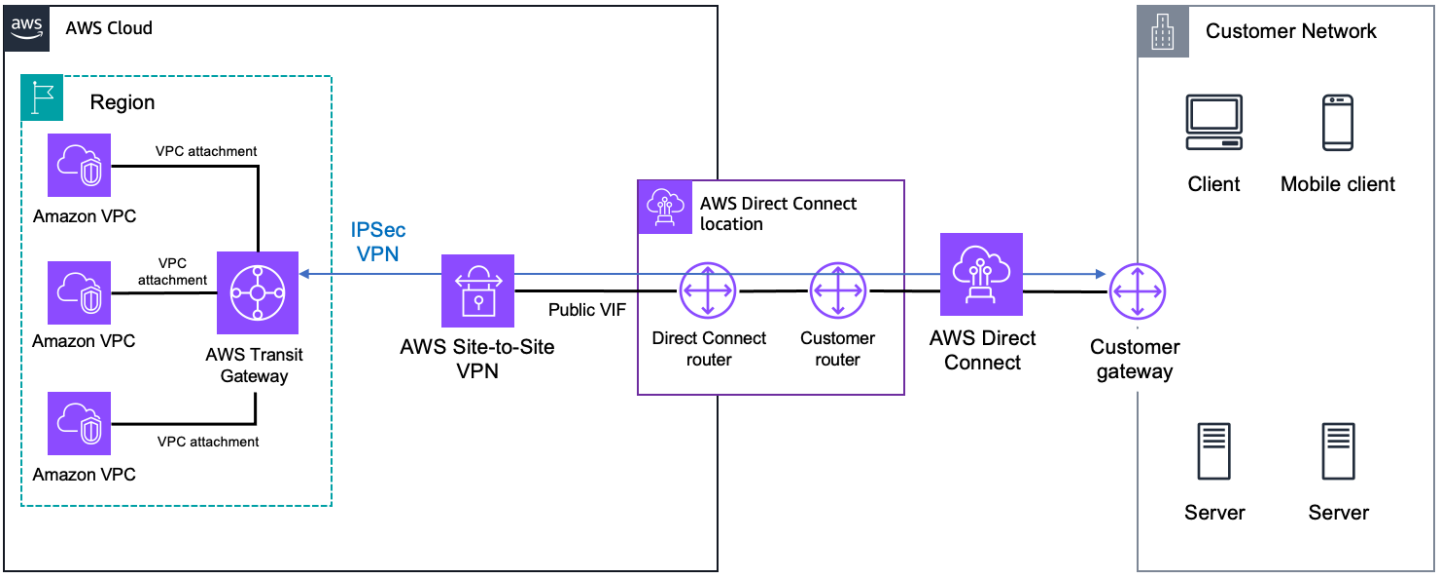
Recursos adicionales de

- AWS Direct Connect
- AWS Direct Connect interfaces virtuales
- Guía del usuario de AWS Site-to-Site VPN

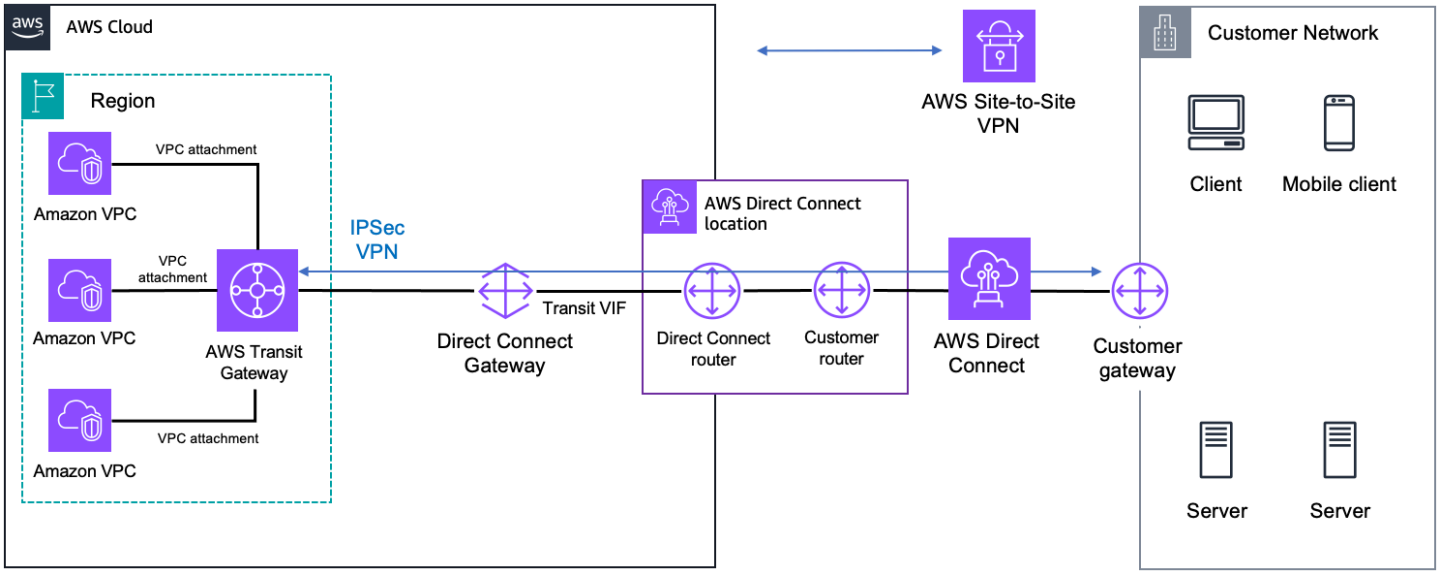
AWS Direct Connect + AWS Transit Gateway + VPN Site-to-Site de AWS

Con AWS Direct Connect+ AWS Transit Gateway+ AWS Site-to-Site VPN, puede habilitar conexiones end-to-end cifradas con IPSec entre sus redes y un router centralizado regional para Amazon VPC a través de una conexión privada dedicada.

Puede utilizar las VIF AWS Direct Connect públicas para establecer primero una conexión de red dedicada entre su red y los recursos públicos de AWS, como los puntos de enlace de VPN Site-to-Site de AWS. Una vez establecida esta conexión, puede crear una conexión IPsec a. AWS Transit Gateway La siguiente imagen ilustra esta opción.



AWS Direct Connect, AWS Transit Gateway, and AWS Site-to-Site VPN (public VIF)



AWS Direct Connect, AWS Transit Gateway, and AWS Site-to-Site VPN (transit VIF)

Considere la posibilidad de adoptar este enfoque cuando desee simplificar la administración y minimizar el costo de las conexiones de VPN de IPsec a varias Amazon VPC en la misma región, con los beneficios de una experiencia de red coherente y de baja latencia de una conexión dedicada privada sobre una VPN basada en Internet. Se establece una sesión de BGP entre el router AWS Direct Connect y el VIF mediante el VIF público o el de tránsito. Se establecerá otra sesión de BGP o una ruta estática entre el router AWS Transit Gateway y el túnel VPN de IPSec.

Recursos adicionales de

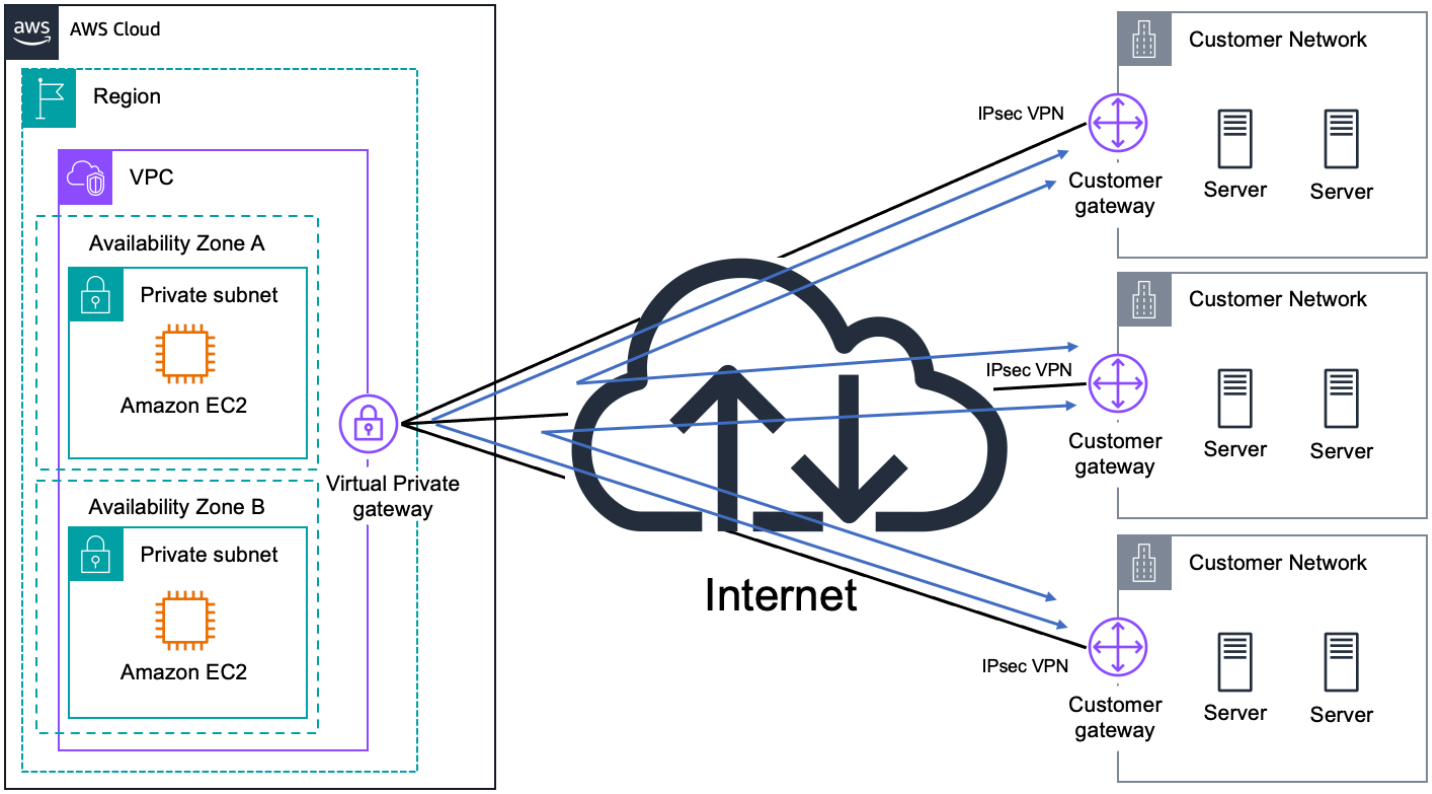
- Interfaces virtuales de AWS Direct Connect
- Vinculaciones de VPN de la puerta de enlace de tránsito
- Requisitos para los dispositivos de puerta de enlace de cliente
- Dispositivos de puerta de enlace de cliente probados con Amazon VPC
- AWS Site-to-Site VPN: VPN con IP privada con AWS Direct Connect

AWS VPN CloudHub

Basándose en las opciones de VPN administradas por AWS descritas anteriormente, puede comunicarse de forma segura de un sitio a otro mediante el AWS VPN CloudHub. AWS VPN CloudHub Funciona con un hub-and-spoke modelo sencillo que se puede utilizar con o sin una VPC. Utilice este enfoque si tiene varias sucursales y conexiones a Internet existentes y desea

implementar un hub-and-spoke modelo práctico y potencialmente económico para la conectividad principal o de respaldo entre estas oficinas remotas.

En la siguiente figura se muestra la AWS VPN CloudHub arquitectura, con líneas que indican el tráfico de red entre sitios remotos que se enruta a través de sus AWS VPN conexiones.



AWS VPN CloudHub

AWS VPN CloudHub utiliza una puerta de enlace privada virtual de Amazon VPC con varias puertas de enlace de cliente, cada una de las cuales utiliza números de sistema autónomos (ASN) de BGP únicos. Los sitios remotos no pueden tener rangos de IP solapados. Las puertas de enlace anuncian las rutas adecuadas (prefijos de BGP) a través de las conexiones de VPN. Estos anuncios de enrutamiento se reciben y se vuelven a anunciar a cada parte de BGP, lo que permite que cada sitio pueda enviar y recibir datos de otros sitios.

Recursos adicionales de

- Proporciona una comunicación segura entre sitios mediante una VPN CloudHub
- Guía del usuario de AWS Site-to-Site VPN
- Requisitos para los dispositivos de puerta de enlace de cliente

- Dispositivos de puerta de enlace de cliente probados con Amazon VPC

AWS Transit Gateway + Soluciones SD-WAN

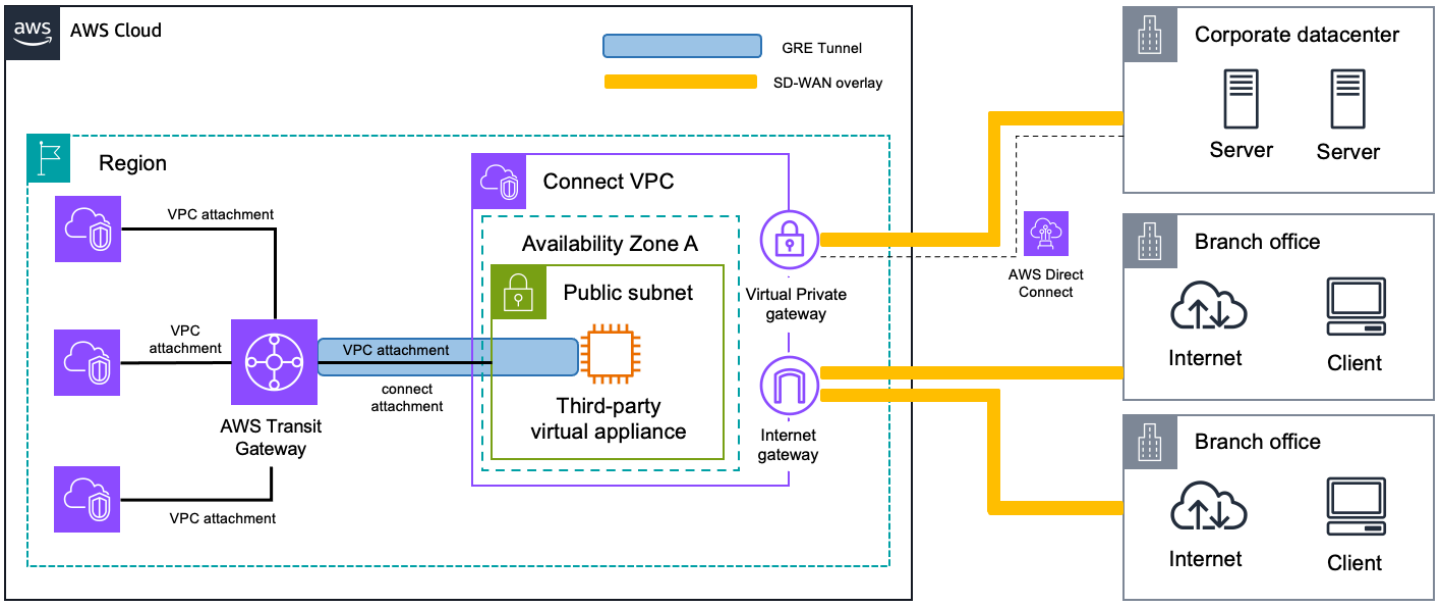
Las redes de área amplia definidas por software (SD-WAN) se utilizan para conectar sus centros de datos, oficinas o entornos de colocación a través de diferentes redes de tránsito (como Internet pública, redes MPLS o la red troncal de AWS AWS Direct Connect), gestionando el tráfico de forma automática y dinámica a través de la ruta más adecuada y eficiente en función de las condiciones de la red, el tipo de aplicación o los requisitos de calidad de servicio (QoS).

Utilice este enfoque si tiene una topología de red compleja, con varios centros de datos, oficinas o entornos de coubicación que necesitan comunicarse entre sí y con AWS. Las soluciones SD-WAN pueden ayudarlo a administrar este tipo de red de manera eficiente.

Cuando se habla de la conexión de una red SD-WAN a AWS, AWS Transit Gateway proporciona un centro de tránsito de red regional escalable y de alta disponibilidad gestionado para interconectar las VPC y su red SD-WAN. Las conexiones de Connect de puerta de enlace de tránsito proporcionan una forma nativa de conectar la infraestructura y los dispositivos de SD-WAN con AWS. Esto facilita la ampliación de SD-WAN a AWS sin tener que configurar las VPN de IPsec.

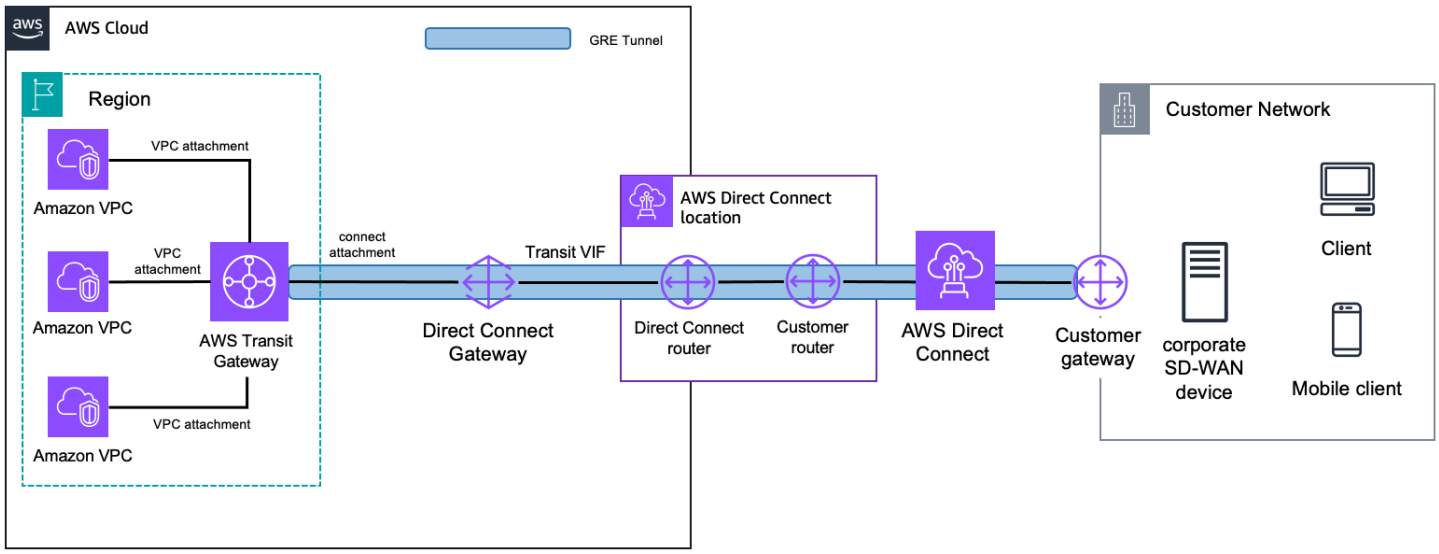
Las conexiones de Connect de puerta de enlace de tránsito admiten la encapsulación de enrutamiento genérico (GRE) para obtener un mayor rendimiento de ancho de banda en comparación con una conexión VPN. Admite el protocolo de puerta de enlace fronteriza (BGP) para enrutamiento dinámico y elimina la necesidad de configurar rutas estáticas. Esto simplifica el diseño de la red y reduce los costos operativos asociados. Además, su integración con el administrador de red de la puerta de enlace de tránsito proporciona una visibilidad avanzada a través de la topología de la red global, las métricas de rendimiento del nivel de conexión y los datos de telemetría.

Al integrar la red SD-WAN en la puerta de enlace de tránsito mediante vinculaciones de Connect, tiene dos patrones comunes. El primero consiste en colocar los dispositivos virtuales de la red SD-WAN en una VPC dentro de AWS. A continuación, se utiliza una conexión de VPC como transporte subyacente para la conexión de Connect de la puerta de enlace de tránsito entre los dispositivos virtuales y la puerta de enlace de tránsito, como se muestra en la siguiente imagen.



SD-WAN connectivity with AWS Transit Gateway (virtual appliance in AWS)

Como alternativa, puede ampliar y segmentar el tráfico de SD-WAN a AWS sin agregar infraestructura adicional. Puede crear adjuntos de conexión de Transit Gateway utilizando una AWS Direct Connect conexión como transporte subyacente, como se muestra en la siguiente figura.



SD-WAN connectivity with AWS Transit Gateway (Direct Connect as transport)

Hay algunas consideraciones que se deben tener en cuenta al utilizar las conexiones de Connect de la puerta de enlace de tránsito:

- Puede crear conexiones de Connect en las puertas de enlace de tránsito existentes.

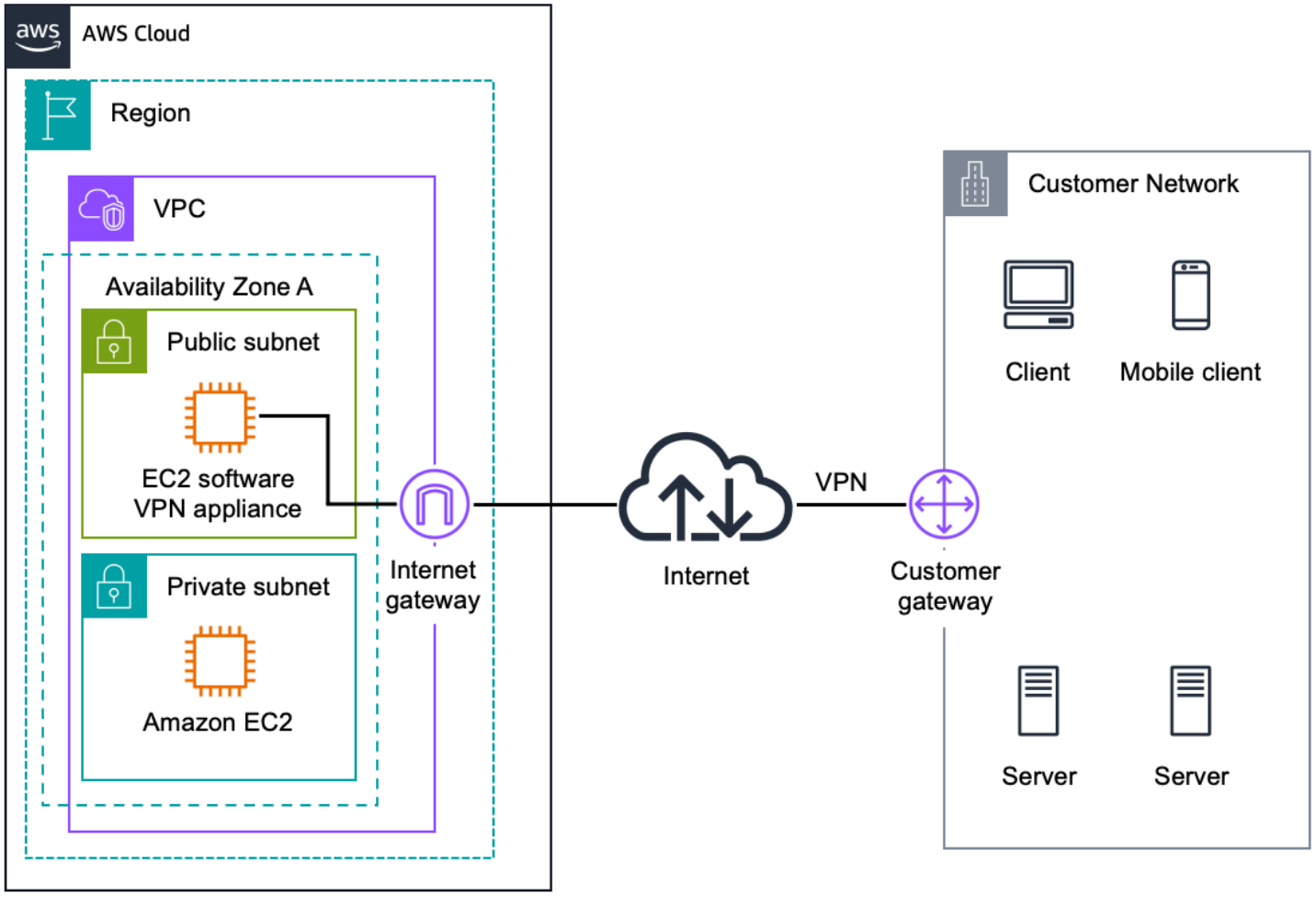
- Los dispositivos de terceros deben configurarse con un túnel de GRE para enviar y recibir tráfico desde la puerta de enlace de tránsito mediante las conexiones de Connect. El dispositivo debe estar configurado con BGP para actualizaciones de rutas dinámicas y comprobaciones de estado.
- Las conexiones de Connect no admiten rutas estáticas.
- Las conexiones de Connect de puerta de enlace de tránsito admiten un ancho de banda máximo de cinco Gbps por túnel de GRE. Se puede lograr un ancho de banda superior a cinco Gbps anunciando los mismos prefijos en varios pares de Connect (túneles de GRE) para la misma conexión de Connect.
- Se admite un máximo de cuatro pares de conexión para cada conexión de Connect.
- Las conexiones de Connect de puerta de enlace de tránsito admiten IPv6 y anuncios de rutas dinámicas mediante extensiones multiprotocolo para BGP (MBGP o MP-BGP).

Recursos adicionales de

- Vinculaciones de interconexiones de puerta de enlace de tránsito
- Requisitos y consideraciones
- Simplify SD-WAN connectivity with AWS Transit Gateway Connect

VPN de software

Amazon VPC le ofrece la flexibilidad de administrar completamente ambos lados de la conectividad de Amazon VPC mediante la creación de una conexión VPN entre la red remota y un dispositivo VPN de software que se ejecuta en la red de Amazon VPC. Esta opción se recomienda si debe administrar ambos extremos de la conexión VPN, ya sea por motivos de cumplimiento o para aprovechar dispositivos de puerta de enlace que actualmente no son compatibles con la solución de VPN de Amazon VPC. En la siguiente imagen se muestra esta opción.



Software Site-to-Site VPN

Puede elegir entre un ecosistema de varios socios y comunidades de código abierto que han creado dispositivos VPN de software que se ejecutan en Amazon EC2. Junto con esta elección viene la responsabilidad de administrar el dispositivo de software, incluida la configuración, los parches y las actualizaciones.

Tenga en cuenta que este diseño presenta un posible punto único de error en el diseño de la red porque el dispositivo de la VPN de software se ejecuta en una única instancia de Amazon EC2. Para obtener información adicional, consulte arquitectura para instancias de VPN de software Apéndice A: Arquitectura de alta disponibilidad de alto nivel para instancias de VPN de software.

Recursos adicionales de

- Los dispositivos VPN están disponibles en AWS Marketplace
- Tech Brief - Connecting Cisco ASA to VPC EC2 Instance (IPsec)

- Tech Brief - Connecting Multiple VPCs with EC2 Instances (IPsec)
- Tech Brief - Connecting Multiple VPCs with EC2 Instances (SSL)

Opciones de conectividad de Amazon VPC a Amazon VPC

Utilice estos patrones de diseño cuando desee integrar varias Amazon VPC en una red virtual más grande. Esto resulta útil si necesita varias VPC por motivos de seguridad, facturación, presencia en varias regiones o requisitos internos de devolución de cargos, para integrar más fácilmente los recursos de AWS entre las VPC de Amazon. También puede combinar estos patrones con las opciones de conectividad red a Amazon VPC para crear una red corporativa que abarque redes remotas y múltiples VPC.

La conectividad de VPC entre las VPC se logra mejor cuando se utilizan rangos de IP que no se superpongan para cada VPC que se esté conectando. Por ejemplo, si desea conectar varias VPC, asegúrese de que cada VPC esté configurada con rangos únicos de enrutamiento entre dominios sin clases (CIDR). Por lo tanto, le recomendamos que asigne un bloque CIDR único, contiguo y no superpuesto para que lo utilice cada VPC. Para obtener información adicional sobre el enrutamiento y las restricciones de Amazon VPC, consulte las preguntas frecuentes sobre Amazon VPC.

Opción	Caso de uso	Ventajas	Limitaciones
Emparejamiento de VPC	Conectividad de red proporcionada por AWS entre dos VPC.	Aprovecha la infraestructura de redes escalable administrada por AWS	La interconexión de VPC no admite relaciones de interconexión transitivas Difícil de administrar a escala
AWS Transit Gateway	Conectividad de enrutador regional proporcionada por AWS para las VPC	Servicio de alta disponibilidad y escalabilidad administrado de AWS Centro de red regional para hasta 5000 vinculaciones	La interconexión de la puerta de enlace de tránsito solo admite rutas estáticas
AWS PrivateLink	Conectividad de red proporcionada	Aprovecha la infraestructura de redes	Los servicios de punto de conexión de VPC

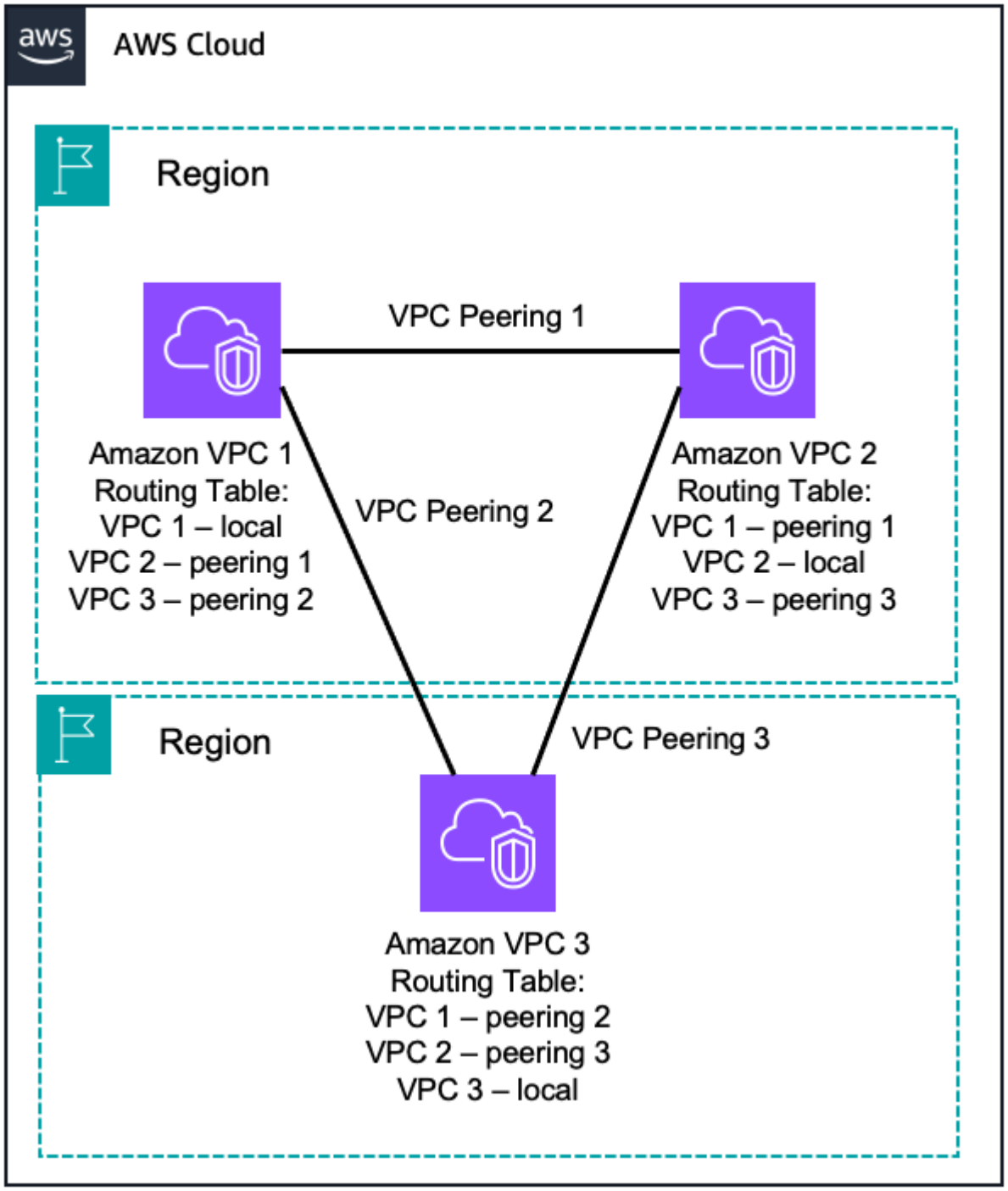
Opción	Caso de uso	Ventajas	Limitaciones
	por AWS entre dos VPC con puntos de conexión de interfaz	escalable administr ada por AWS	solo están disponibl es en la región de AWS en la que se han creado
VPN de software	Conexiones VPN entre VPC basadas en dispositivos de software	Admite una gama amplia de proveedor es, productos y protocolos de VPN Administrado en su totalidad por usted	Es responsable de implementar las soluciones de alta disponibilidad para todos los puntos de conexión de la VPN (si es necesario) Las instancias de VPN podrían convertir se en un cuello de botella de red

Opción	Caso de uso	Ventajas	Limitaciones
VPN de software a AWS Site-to-Site VPN	Dispositivo de software a conexión de VPN entre VPC	Conexión VPN de VPC de alta disponibilidad administrada por AWS Admite una gama amplia de proveedores y productos de VPN administrados por usted Admite rutas estáticas y políticas dinámicas de enrutamiento y emparejamiento de BGP	Es responsable de implementar las soluciones de alta disponibilidad para todos los puntos de conexión de la VPN de dispositivo de software (si es necesario) Las instancias de VPN podrían convertirse en un cuello de botella de red Protocolo VPN IPsec solo para VPN administrada por AWS

Emparejamiento de VPC

La interconexión de VPC es una conexión en red entre dos VPC que permite direccionar a través de las direcciones IP privadas de cada VPC, como si estuviesen en la misma red. Las conexiones de emparejamiento de VPC se pueden crear entre sus propias VPC o con una VPC de otra cuenta de AWS. La interconexión con VPC también admite la interconexión entre regiones.

El tráfico con interconexión con VPC entre regiones siempre permanece en el núcleo de AWS global y nunca pasa por la red pública de Internet, lo que reduce los vectores de amenazas, como las vulnerabilidades comunes y los ataques DDoS.



VPC-to-VPC Peering

AWS utiliza la infraestructura existente de una VPC para crear conexiones de emparejamiento de VPC y no depende de una pieza independiente de hardware físico. Por lo tanto, no presentan un posible punto único de error ni un cuello de botella en el ancho de banda de la red entre las VPC. Además, las tablas de enrutamiento de VPC, los grupos de seguridad y las listas de control de

acceso a la red se pueden aprovechar para controlar qué subredes o instancias pueden utilizar la conexión de emparejamiento de VPC.

Las VPC de Amazon no admiten la interconexión transitiva, lo que significa que no puede comunicar dos VPC que no estén conectadas directamente mediante una tercera VPC como tránsito. Si desea que todas las VPC se comuniquen entre sí mediante el emparejamiento de VPC, tendrá que crear conexiones de emparejamiento de VPC 1:1 entre cada una de ellas. Como alternativa, puede utilizar AWS Transit Gateway o WAN en la nube de AWS para que actúe como un centro de tránsito de red.

Las conexiones de emparejamiento de VPC admiten tráfico IPv4 e IPv6. Sin embargo, no se pueden emparejar dos VPC si el bloque CIDR de IPv4 principal se superpone, independientemente de los bloques CIDR de IPv4 o IPv6 secundarios que se utilicen. Tenga esto en cuenta al asignar el bloque CIDR principal a las VPC si planea utilizar el emparejamiento de VPC entre ellas.

Recursos adicionales de

- Interconexión de Amazon VPC
- ¿Qué es una interconexión de VPC?

AWS Transit Gateway

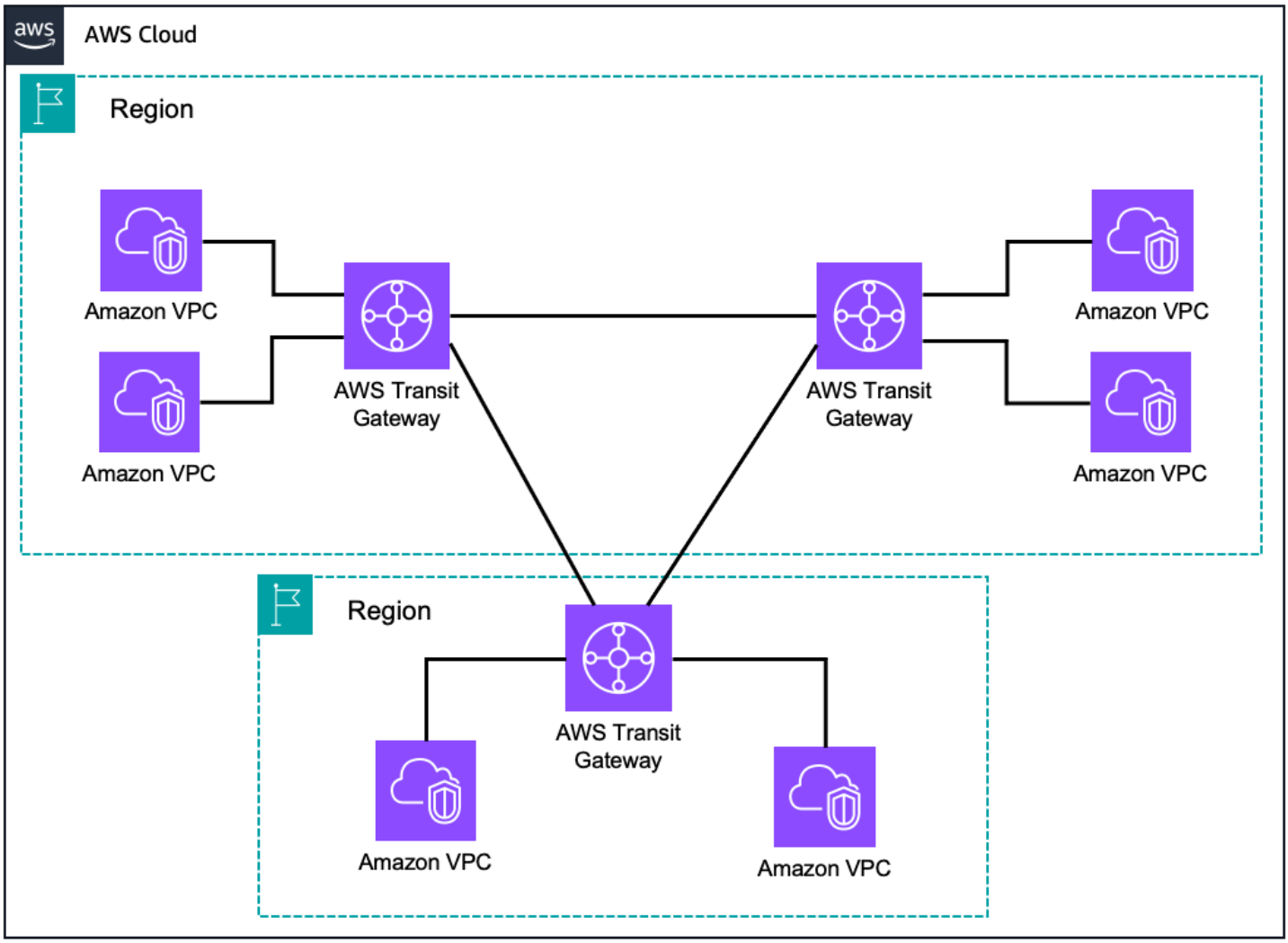
AWS Transit Gatewayes un servicio escalable y de alta disponibilidad para consolidar la configuración de enrutamiento de VPC de AWS para una región con una hub-and-spoke arquitectura. Cada VPC radial solo necesita conectarse a la puerta de enlace de tránsito para acceder a otras VPC conectadas. El tráfico IPv4 e IPv6 se admite en AWS Transit Gateway.

Puede aprovechar varias tablas de enrutamiento, asociaciones y propagaciones de la puerta de enlace de tránsito para segmentar el tráfico dentro de la misma puerta de enlace de tránsito. Podrá administrar diferentes dominios de enrutamiento (por ejemplo, el tráfico de producción y el de no producción) desde un único punto de administración, lo que garantizará que estos dominios de enrutamiento no puedan comunicarse entre sí.

También puede aprovechar la hub-and-spoke arquitectura creada por Transit Gateway para centralizar el acceso a los servicios compartidos, como la inspección del tráfico, el acceso a los puntos finales de la interfaz de la VPC o el tráfico de salida a través de una puerta de enlace NAT o instancias de NAT. Esta centralización simplifica la complejidad de administrar estos recursos en varias VPC y permite un mejor control a medida que amplía su presencia en AWS.

Las puertas de enlace de tránsito se pueden interconectar con las demás dentro de la misma región de AWS o entre diferentes regiones de AWS. El tráfico de AWS Transit Gateway siempre permanece en el núcleo de AWS global y nunca pasa por la red pública de Internet, lo que reduce los vectores de amenazas, como las vulnerabilidades comunes y los ataques DDoS.

Con una gran cantidad de VPC, la puerta de enlace de tránsito proporciona una administración de comunicación de VPC a VPC más sencilla a través de la interconexión de VPC, como se muestra en la siguiente imagen.



AWS Transit Gateway

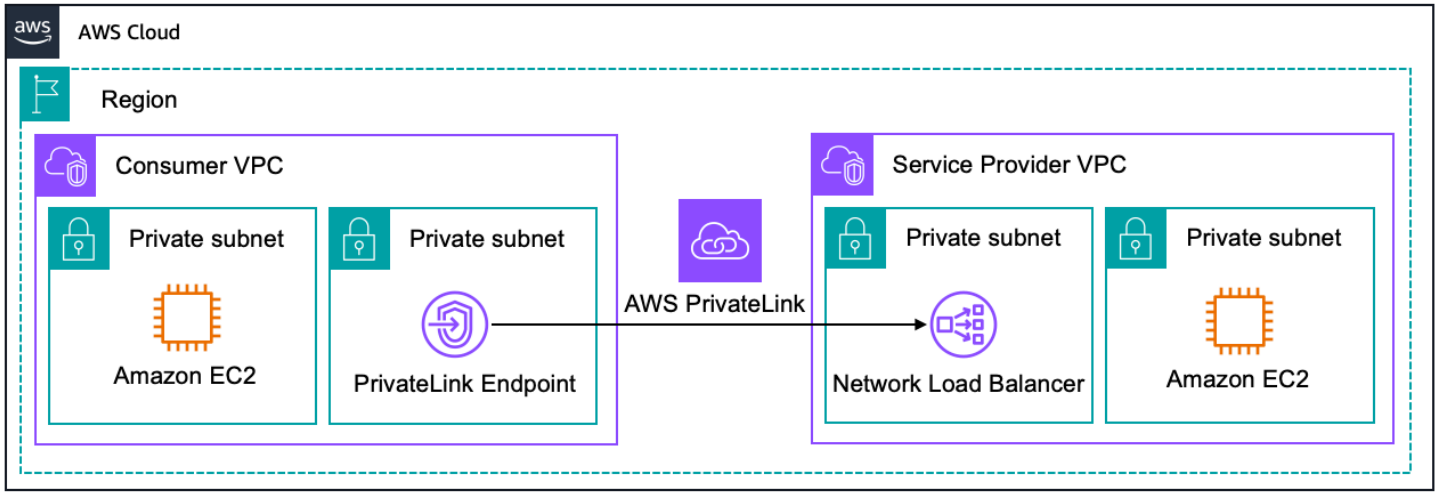
Para obtener una visibilidad centralizada del tráfico IP que entra y sale de sus Transit Gateways, puede publicar los registros de flujo de Transit Gateway en Amazon CloudWatch Logs y Amazon S3. Los datos de registro de flujo se recopilan fuera de la ruta del tráfico de red y, por lo tanto, no afectan al rendimiento ni a la latencia de la red.

Recursos adicionales de

- Puerta de enlace de tránsito de Amazon VPC
- Vinculaciones de interconexiones de puerta de enlace de tránsito
- Utilizar puerta de enlaces de tránsito
- Registro del tráfico de red mediante registros de flujo de puerta de enlace de tránsito

AWS PrivateLink

AWS PrivateLink le permite conectarse a algunos servicios de AWS, servicios alojados por otras cuentas de AWS (denominados servicios de punto de conexión) y servicios de socios de AWS Marketplace admitidos, a través de las direcciones IP privadas en la VPC. Los puntos de conexión de la interfaz se crean directamente dentro de la VPC, mediante interfaces de red elásticas y direcciones IP en las subredes de la VPC. Esto significa que los grupos de seguridad de la VPC se pueden usar para administrar el acceso a los puntos de conexión.



AWS PrivateLink

Recomendamos este enfoque si desea utilizar los servicios ofrecidos por otra VPC de forma segura dentro de una red de AWS, mediante direcciones IP privadas. Como alternativa, AWS PrivateLink es una buena solución cuando las VPC tienen direcciones IP superpuestas.

AWS PrivateLink es totalmente compatible con IPv6, pero las VPC de destino, las subredes de VPC, el equilibrador de carga de red y los nombres de DNS deben estar habilitados o modificados para utilizar la doble pila. Una vez que se cumplan estos requisitos previos, se puede habilitar IPv6 en la configuración del servicio del punto de conexión.

Controles de acceso a AWS PrivateLink

Los puntos de conexión de la interfaz se crean directamente dentro de la VPC al usar interfaces de red elásticas y direcciones IP en las subredes de la VPC. Esto significa que los grupos de seguridad de la VPC se pueden usar para administrar el acceso de red a los puntos de conexión.

Cuando crea un punto de conexión de interfaz o un punto de conexión de puerta de enlace, puede también adjuntar una política de punto de conexión. La política de punto de conexión controla qué entidades principales de AWS (cuentas de AWS, usuarios y roles de IAM) pueden utilizar el punto de conexión de VPC para acceder al servicio de punto de conexión.

No puede asociar más de una política a un punto de enlace. Sin embargo, puede modificar una política de punto de conexión en cualquier momento.

Una política de punto de conexión no invalida ni reemplaza las políticas de usuario de IAM ni las políticas específicas de servicios (como las políticas de bucket de Amazon S3). Si utiliza un punto de conexión de interfaz para conectarse a Amazon S3, también puede utilizar las políticas de bucket de Amazon S3 para controlar el acceso a los buckets desde puntos de conexión específicos o VPC específicas.

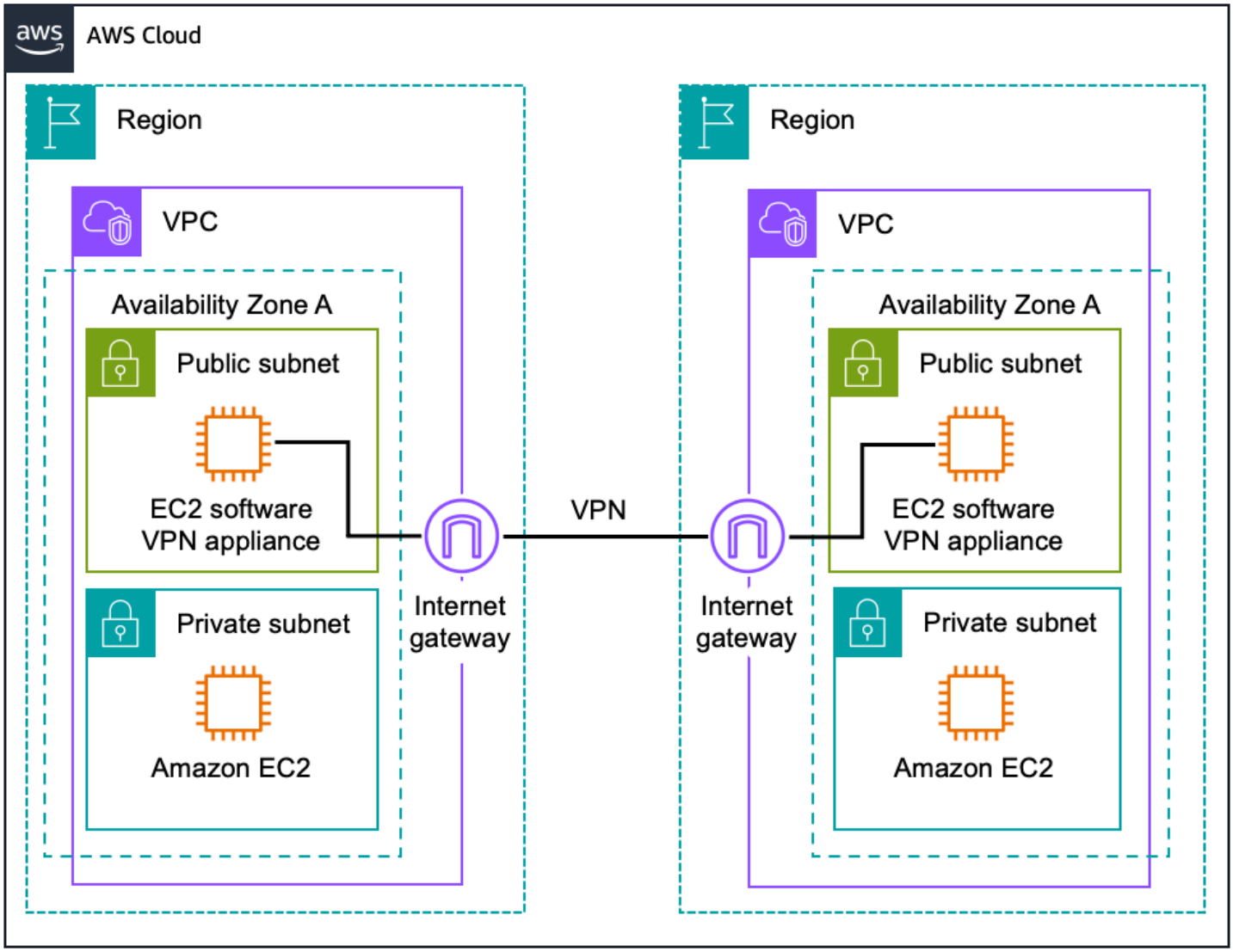
Recursos adicionales de

- Puntos de conexión de VPC de interfaz (AWS PrivateLink)
- Servicios de punto de conexión de VPC (AWS PrivateLink)
- Publicación de blog: Acelere su adopción de IPv6 con PrivateLink servicios y puntos de enlace
- Publicación en el blog: Connecting Networks with Overlapping IP Ranges
- Socios de AWS PrivateLink

VPN de software

Amazon VPC ofrece flexibilidad de enrutamiento de red. Esto incluye la capacidad de crear túneles de la VPN seguros entre dos o más dispositivos de VPN de software para conectar varias VPC a una red privada virtual más grande, de modo que las instancias de cada VPC puedan conectarse entre sí sin problemas mediante direcciones IP privadas. Esta opción se recomienda si desea administrar ambos extremos de la conexión VPN con el proveedor de software de VPN preferido. Esta opción

utiliza una puerta de enlace de Internet conectada a cada VPC para facilitar la comunicación entre los dispositivos de VPN de software.



Software Site-to-Site VPN VPC-to-VPC Routing

Puede elegir entre un ecosistema de varios socios y comunidades de código abierto que han producido dispositivos de VPN por software que se ejecutan en Amazon EC2. Junto con esta elección, tiene la responsabilidad de administrar el dispositivo de software, incluida la configuración, los parches y las actualizaciones.

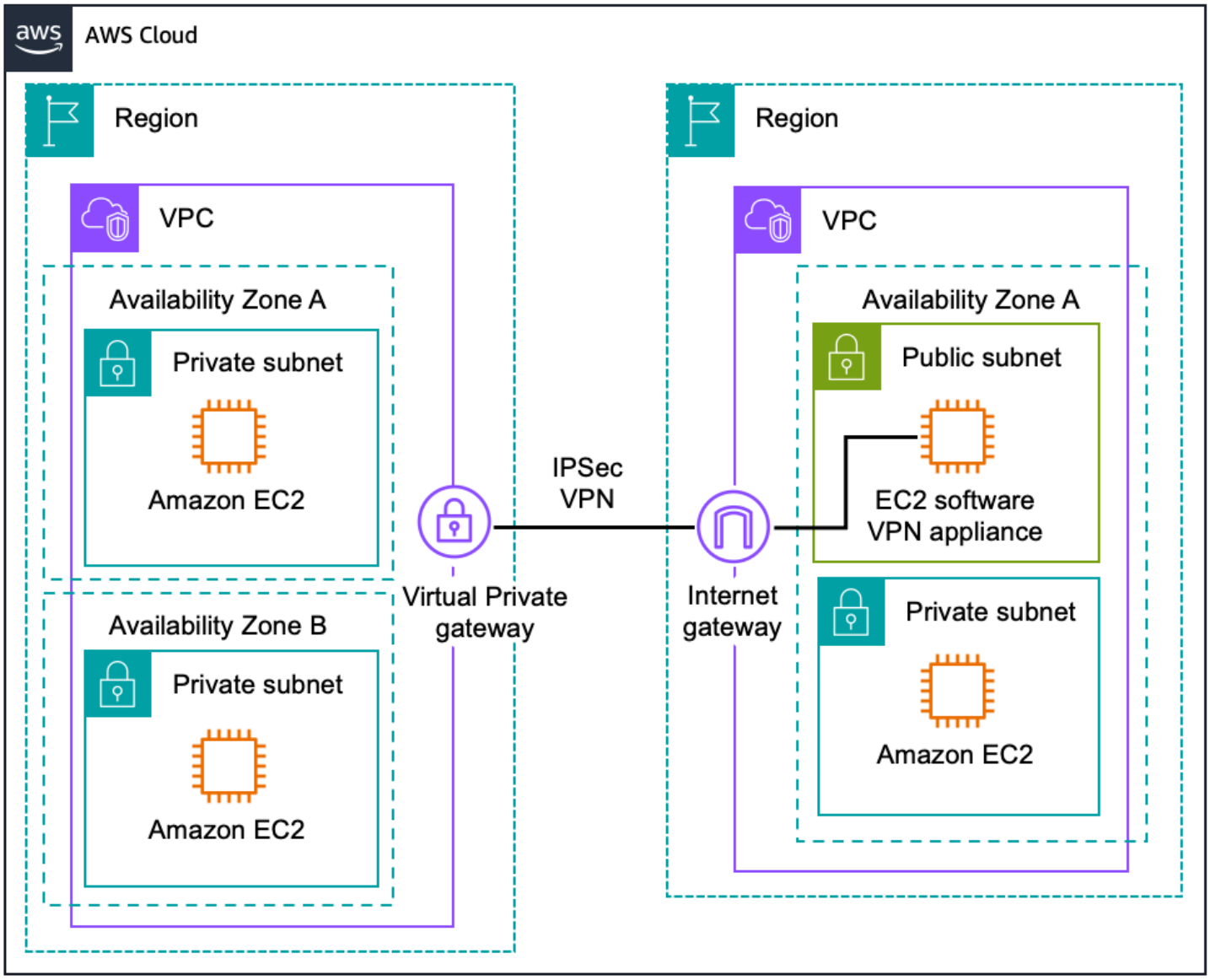
Tenga en cuenta que este diseño presenta un posible punto único de error en el diseño de la red, ya que el dispositivo de la VPN de software se ejecuta en una única instancia de Amazon EC2. Para obtener información adicional, consulte Apéndice A: Arquitectura de alta disponibilidad de alto nivel para instancias de VPN de software.

Recursos adicionales de

- Los dispositivos de VPN están disponibles en AWS Marketplace
- Tech Brief - Connecting Multiple VPCs with EC2 Instances (IPsec)
- Tech Brief - Connecting Multiple VPCs with EC2 Instances (SSL)

VPN de software a AWS Site-to-Site VPN

Amazon VPC ofrece la flexibilidad de combinar las opciones de la VPN administrada por AWS y la VPN de software para conectar varias VPC. Con este diseño, puede crear túneles de la VPN seguros entre un dispositivo de VPN de software y una puerta de enlace privada virtual, lo que permite que las instancias de cada VPC se conecten entre sí sin problemas mediante direcciones IP privadas. Esta opción utiliza una puerta de enlace privada virtual en una Amazon VPC y una combinación de una puerta de enlace de Internet y un dispositivo VPN de software en otra Amazon VPC, como se muestra en la siguiente imagen.



Software VPN to AWS Site-to-Site VPN VPC-to-VPC Routing

Tenga en cuenta que este diseño presenta un posible punto único de error en el diseño de la red. Para obtener información adicional, consulte Apéndice A: Arquitectura de alta disponibilidad de alto nivel para instancias de VPN de software.

Recursos adicionales de

- Los dispositivos de VPN están disponibles en AWS Marketplace
- Guía del usuario de AWS Site-to-Site VPN
- Requisitos para los dispositivos de puerta de enlace de cliente

Opciones de conectividad de acceso remoto de software a Amazon VPC

Con la VPN de acceso remoto de software, puede aprovechar los servicios seguros, elásticos y de bajo costo para implementar soluciones de acceso remoto y, al mismo tiempo, ofrecer una experiencia fluida de conexión a los recursos alojados en AWS. Por lo general, esta opción la prefieren las empresas más pequeñas con redes remotas menos extensas o que aún no han creado e implementado soluciones de acceso remoto para los empleados.

Puede combinar estos patrones con las opciones de conectividad Opciones de conectividad de red a Amazon VPC y Opciones de conectividad de Amazon VPC a Amazon VPC para crear una red que abarque redes remotas y múltiples VPC.

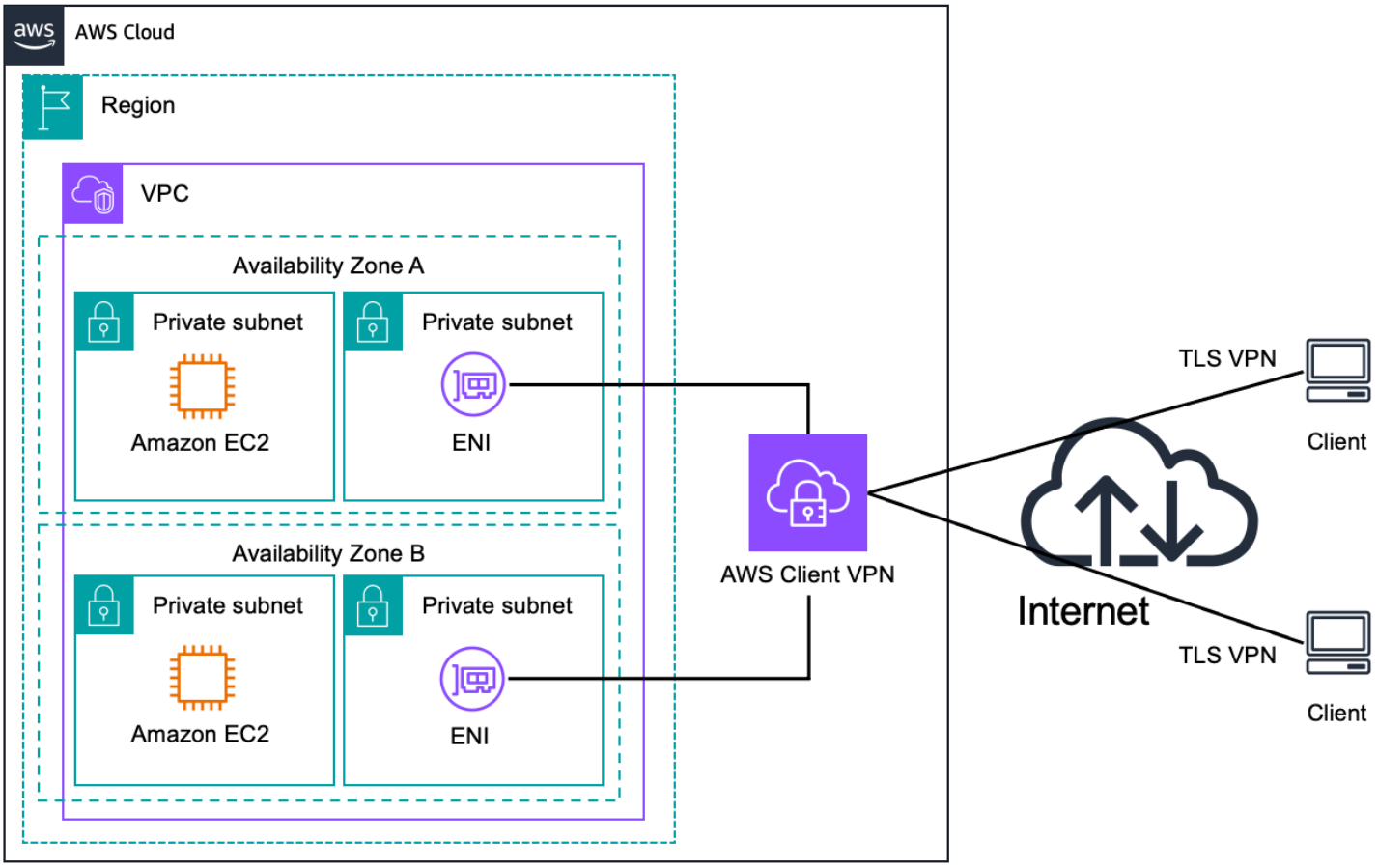
En la siguiente tabla se exponen las ventajas y limitaciones de estas opciones.

Opción	Caso de uso	Ventajas	Limitaciones
AWS Client VPN	Solución de acceso remoto administrado por AWS a Amazon VPC o redes internas	Servicio de alta disponibilidad y escalabilidad administrado de AWS	Solo para clientes de OpenVPN
Software Client VPN	Solución de acceso remoto de dispositivo de VPN de software a Amazon VPC o redes internas	Admite una gama más amplia de proveedores, productos y protocolos de VPN Solución totalmente administrada por el cliente	Es responsable de implementar las soluciones de alta disponibilidad

AWS Client VPN

AWS Client VPN es un servicio de alta disponibilidad y escalabilidad administrado por AWS que permite el acceso remoto seguro al software. Ofrece la opción de crear una conexión TLS segura

entre los clientes remotos y las VPC de Amazon para acceder de forma segura a los recursos de AWS y en las instalaciones a través de Internet, como se muestra en la siguiente imagen.



AWS Client VPN Remote Access

Los clientes remotos pueden ser AWS Client VPN para Desktop o clientes de VPN de OpenVPN de terceros, con autenticación mediante Active Directory o mediante autenticación con certificado mutuo.

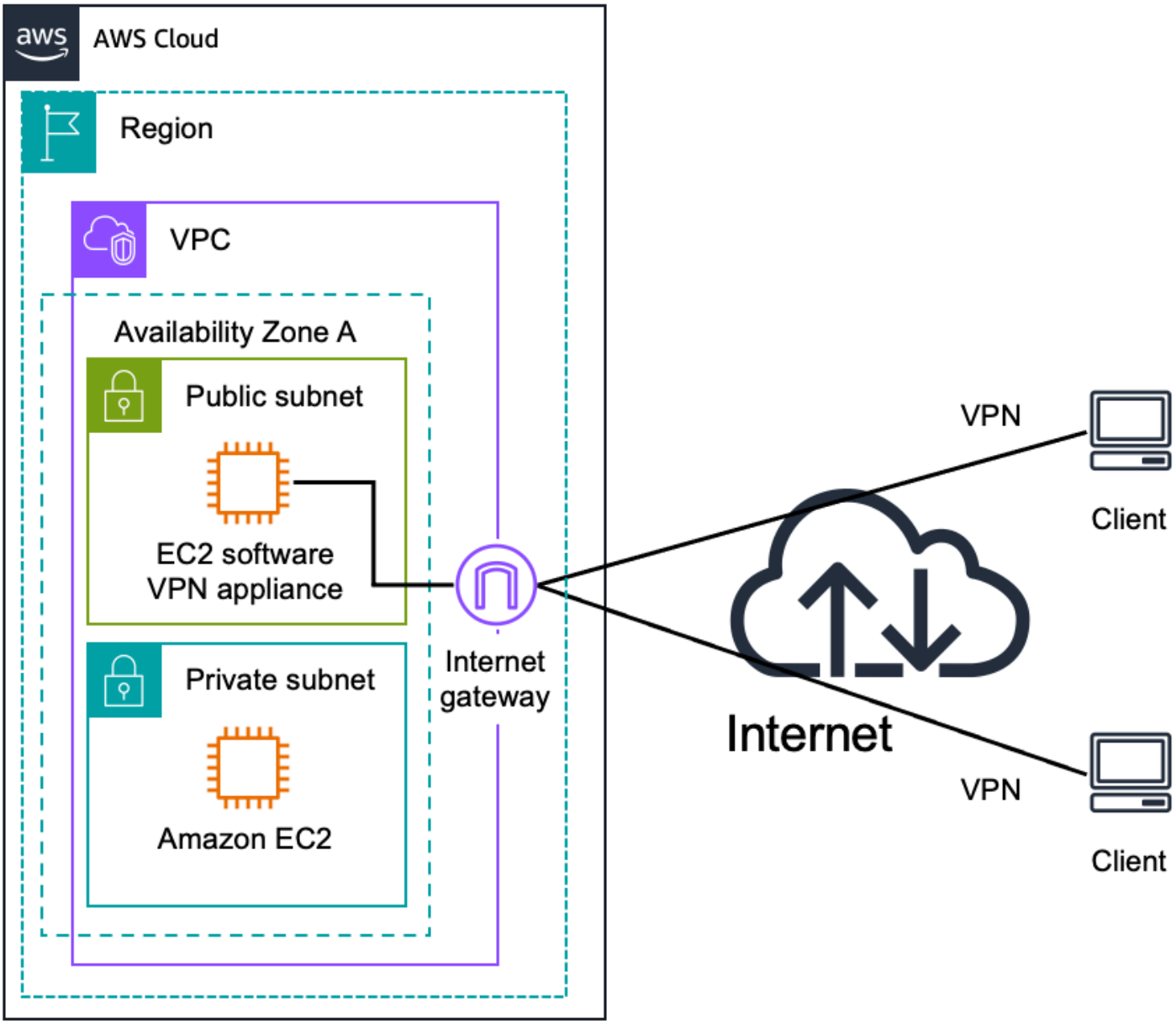
Recursos adicionales de

- Guía del administrador de AWS Client VPN

Software Client VPN

Puede elegir entre un ecosistema de varios socios y comunidades de código abierto que han creado soluciones de acceso remoto que se ejecutan en Amazon EC2. Estas soluciones ofrecen una gran flexibilidad en el uso del protocolo de seguridad para el acceso remoto a las VPC de Amazon, para

acceder de forma segura a los recursos de AWS y en las instalaciones a través de Internet, como se muestra en la siguiente imagen.



Software Client VPN Remote Access

Las soluciones de acceso remoto varían en complejidad, admiten múltiples opciones de autenticación de clientes (incluida la autenticación multifactorial) y se pueden integrar con Amazon VPC o con soluciones de administración de identidad y acceso alojadas de forma remota (aprovechando una de las opciones de red a Amazon VPC), como Microsoft Active Directory u otras soluciones de autenticación LDAP/multifactor.

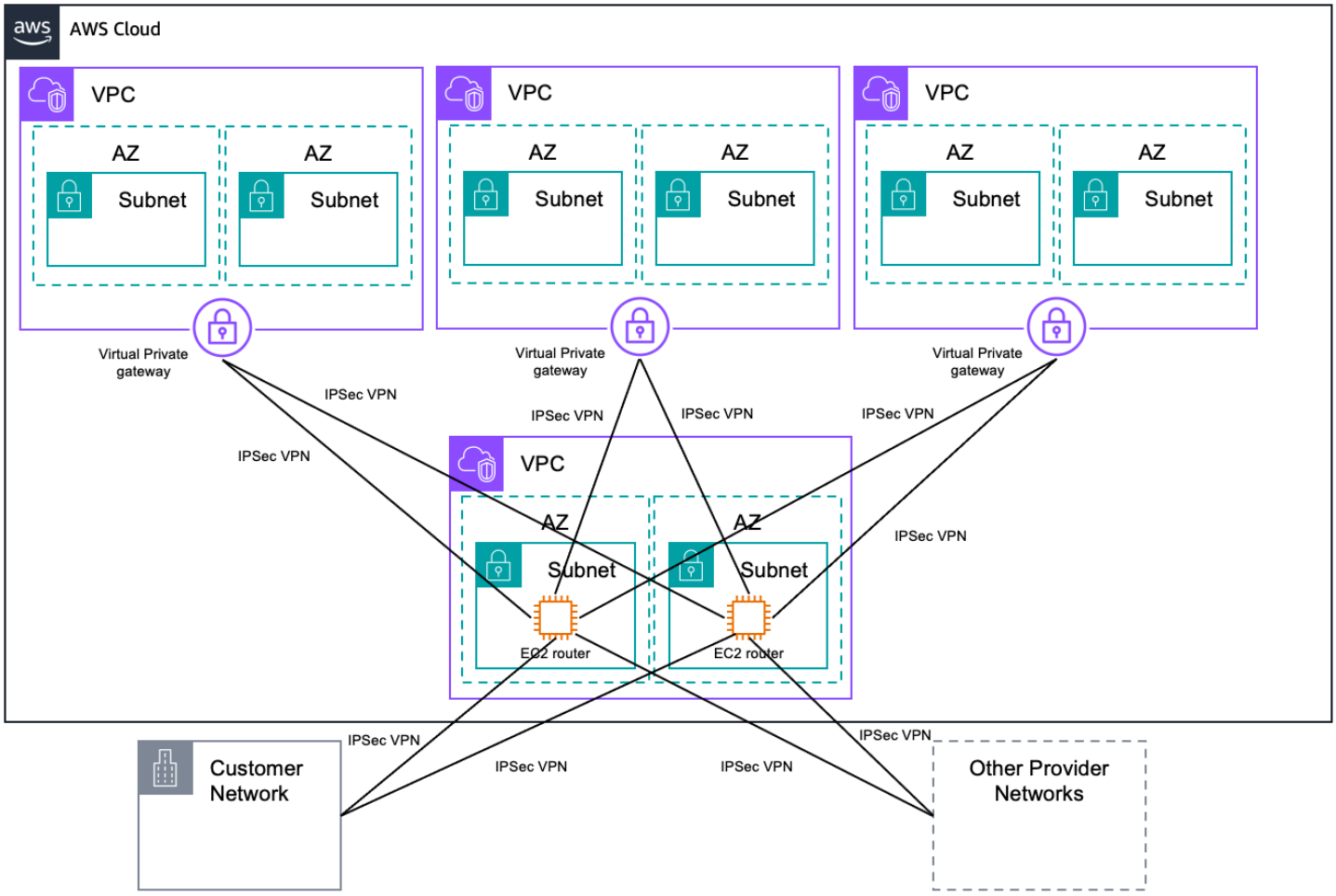
Es responsable de administrar el software de acceso remoto, incluida la administración de usuarios, la configuración, los parches y las actualizaciones. Este diseño presenta un posible punto único de error en el diseño de la red, ya que el servidor de acceso remoto se ejecuta en una única instancia de Amazon EC2. Para obtener información adicional, consulte Apéndice A: Arquitectura de alta disponibilidad de alto nivel para instancias de VPN de software.

Recursos adicionales de

- Dispositivos VPN disponibles en AWS Marketplace
- Guía de inicio rápido del servidor de acceso OpenVPN

VPC de tránsito

En función de los diseños de VPN por software mencionados anteriormente, puede crear una red de tránsito global en AWS. Una VPC de tránsito es una estrategia común para la conexión de varias VPC y redes remotas dispersas geográficamente para crear un centro de tránsito de red global. Una VPC de tránsito simplifica la administración de la red y minimiza el número de conexiones necesarias para conectar varias VPC y redes remotas. La siguiente imagen ilustra este diseño.



Transit VPC

Además de proporcionar un enrutamiento de red directo entre las VPC y las redes en las instalaciones, este diseño también permite a la VPC de tránsito implementar reglas de enrutamiento más complejas, como la traducción de direcciones de red entre rangos de redes superpuestas o agregar filtros o inspecciones de paquetes adicionales en el nivel de red. El diseño de la VPC de tránsito se puede utilizar para respaldar casos de uso importantes, como las redes privadas, la conectividad compartida y el uso entre cuentas de AWS.

Recursos adicionales de

- AWS Transit Gateway
- Cisco Catalyst 8000V para SD-WAN y enrutamiento AWS Marketplace

WAN en la nube de AWS

WAN en la nube de AWS es una red de área extendida (WAN) administrada basada en la intención que se describe mediante una política que usted define que unifica el centro de datos, la rama y las redes de AWS. Aunque puede crear su propia red global mediante la interconexión de varias puertas de enlace de tránsito entre regiones, WAN en la nube ofrece características integradas de automatización, segmentación y administración de la configuración diseñadas específicamente para crear y operar redes globales, en función de la política de red principal. WAN en la nube ha agregado características como los adjuntos de VPC automatizados, el monitoreo integrado del rendimiento y la configuración centralizada.

La política de red principal está redactada en un lenguaje declarativo que define los segmentos, el enrutamiento de región de AWS y la forma en que los archivos adjuntos se deben asignar a los segmentos. Con una política de red principal, puede describir su intención de controlar el acceso y enrutar el tráfico, mientras que WAN en la nube de AWS se encarga de los detalles de la configuración de la red.

WAN en la nube se administra dentro de AWS Network Manager, que le permite administrar de forma centralizada y visualizar la red central de WAN en la nube y las redes de puerta de enlace de tránsito en cuentas, regiones y ubicaciones en las instalaciones de AWS. Network Manager le proporciona varias visualizaciones de paneles para ayudarlo a ver y monitorear todos los aspectos de la red global. Algunos de los paneles incluyen:

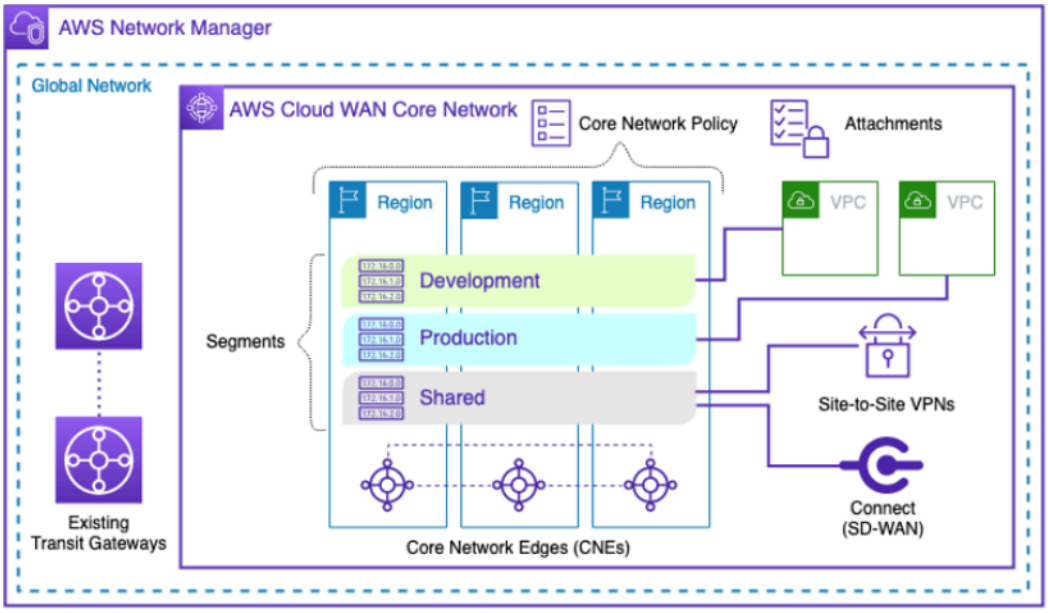
- Mapas mundiales que indican dónde se encuentran los recursos de la red, como las ubicaciones periféricas, los dispositivos y los archivos adjuntos.
- Supervisión que utiliza CloudWatch Events para realizar un seguimiento de las estadísticas de 15 meses, lo que le brinda una mejor perspectiva del rendimiento de sus redes.
- Seguimiento de eventos que transmite los eventos en tiempo real a un panel de eventos.
- Diagramas topológicos y lógicos de las redes de puertas de enlace de tránsito y puertas de enlace de tránsito.

La puerta de enlace de tránsito y WAN en la nube permiten la conectividad centralizada entre las VPC y las ubicaciones en las instalaciones. La puerta de enlace de tránsito es un centro de conectividad de redes regional y es ideal para los clientes que operan en algunas regiones de AWS, que desean administrar su propia configuración de enrutamiento e interconexión o que prefieren usar su propia automatización. WAN en la nube es óptima para los clientes que desean definir la red

global mediante una política y hacer que el servicio implemente los componentes subyacentes de forma automática.

Cosas que debe saber

- El CNE (Core Network Edge) hereda muchas características de Transit Gateway, como el rendimiento por adjunto de VPC.
- WAN en la nube admite IPv4 e IPv6.
- Actualmente, WAN en la nube no admite archivos adjuntos de forma nativa de AWS Direct Connect. Para usarlo AWS Direct Connect con Cloud WAN, necesitas una Transit Gateway conectada a una puerta de AWS Direct Connect enlace y, a continuación, la Transit Gateway conectada a Cloud WAN.
- En el caso de redes grandes con muchos cambios, considere la posibilidad de crear una red global independiente de desarrollo y pruebas en la que pueda validar los cambios.



AWS Cloud WAN

Recursos adicionales de

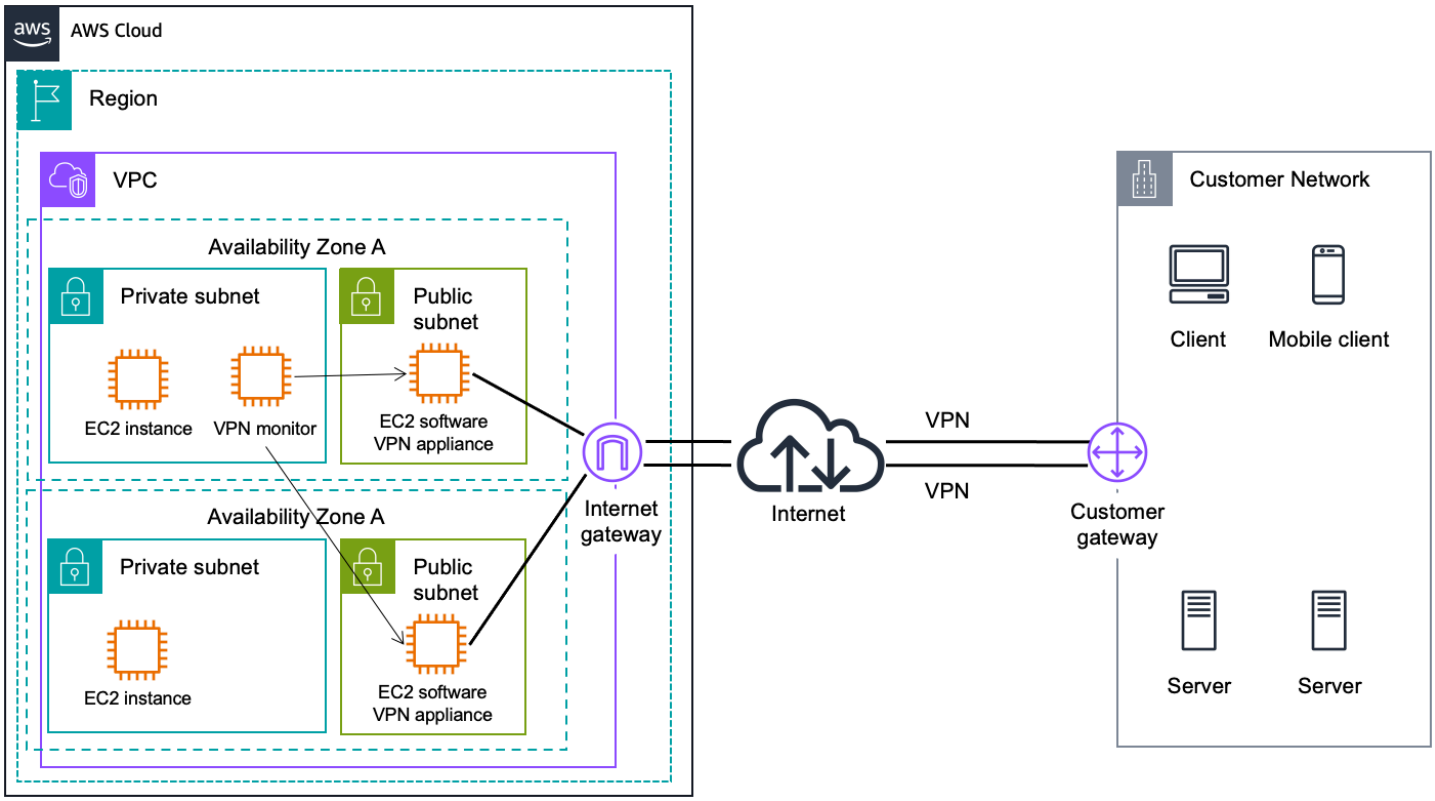
- Documentación sobre WAN en la nube de AWS
- Publicación en el blog: AWS Cloud WAN and AWS Transit Gateway migration and interoperability patterns

Conclusión

AWS ofrece una serie de opciones de conectividad eficaces y seguras para ayudarle a sacar el máximo partido de AWS a la hora de integrar las redes remotas con Amazon VPC. Las opciones que se proporcionan en este documento técnico destacan varias de las opciones y patrones de conectividad que los clientes han utilizado para integrar correctamente las redes remotas o varias redes de Amazon VPC. Puede utilizar la información que se proporciona aquí para determinar el mecanismo más adecuado para conectar la infraestructura necesaria para el funcionamiento de la empresa, independientemente de dónde esté ubicada o alojada físicamente.

Apéndice A: Arquitectura de alta disponibilidad de alto nivel para instancias de VPN de software

La creación de una conexión de VPC totalmente resiliente para las instancias de VPN de software requiere la instalación y configuración de varias instancias de VPN y una instancia de monitoreo para supervisar el estado de las conexiones de VPN.



Alta disponibilidad de VPN de software de alto nivel

Recomendamos configurar las tablas de enrutamiento de la VPC para aprovechar todas las instancias de VPN de forma simultánea y dirigir el tráfico de todas las subredes de una zona de disponibilidad a través de sus respectivas instancias de VPN en la misma zona de disponibilidad. A continuación, cada instancia de VPN proporciona conectividad de VPN a las instancias que comparten la misma zona de disponibilidad.

Monitoreo de VPN

Para monitorear un dispositivo de VPN basado en software, puede crear un monitor de VPN. El monitor de VPN es una instancia personalizada que necesitará para ejecutar los scripts de

monitoreo de VPN. Esta instancia está diseñada para ejecutar y monitorear el estado de la conexión VPN y las instancias de VPN. Si una instancia o conexión de VPN deja de funcionar, el monitor debe detener, finalizar o reiniciar la instancia de VPN y, al mismo tiempo, redirigir el tráfico de las subredes afectadas a la instancia de VPN en funcionamiento hasta que ambas conexiones vuelvan a funcionar. Dado que los requisitos de los clientes varían, AWS no proporciona actualmente una guía prescriptiva para configurar esta instancia de monitoreo. Sin embargo, se podría utilizar un script de ejemplo para habilitar la alta disponibilidad entre las instancias de NAT como punto de partida para crear una solución de alta disponibilidad para las instancias de VPN de software. Le recomendamos que analice la lógica empresarial necesaria para notificar o intentar reparar automáticamente la conectividad de la red en caso de que se produzca un error en la conexión de la VPN.

Además, puede supervisar los túneles de VPN gestionados por AWS mediante CloudWatch las métricas de Amazon, que recopilan puntos de datos del servicio de VPN en métricas legibles prácticamente en tiempo real. Cada conexión VPN recopila y publica una variedad de métricas de túneles en Amazon CloudWatch. Estas métricas le permiten monitorear el estado y la actividad de los túneles y crear acciones automatizadas.

Colaboradores

Los colaboradores de este documento son:

- Daniel Yu, mánager técnico sénior de cuentas de AWS Enterprise Support
- Garvit Singh, creador de soluciones, AWS Solution Architecture
- Steve Morad, mánager sénior de desarrolladores de soluciones, AWS Solution Architecture
- Sohaib Tahir, arquitecto de soluciones, AWS Solution Architecture
- Fiona Armada, arquitecta principal de soluciones, arquitectura de soluciones de AWS
- Pablo Sánchez Carmona, arquitecto de soluciones especializado en redes, AWS Solution Architecture
- Tony Hawke, mánager técnico de cuentas especialista sénior, AWS Enterprise Support

Revisiones del documento

Para recibir notificaciones sobre las actualizaciones de este documento técnico, suscríbase a la fuente RSS.

Cambio	Descripción	Fecha
Documento técnico actualizado	Se han agregado opciones de adjuntos de conexión de WAN en la nube de AWS y puerta de enlace de tránsito, diagramas actualizados e información en todas partes.	5 de abril de 2023
Documento técnico actualizado	Se han agregado opciones de AWS Transit Gateway y AWS Client VPN, se han actualizado diagramas e información en todas partes.	6 de junio de 2020
Actualización menor	Cambio menor para corregir la referencia al dispositivo de VPN de software.	20 de mayo de 2020
Documento técnico actualizado	Información actualizada en todo momento. Concéntrese en los siguientes diseños o características: VPC de tránsito, puerta de enlace de Direct Connect y AWS PrivateLink.	1 de enero de 2018
Publicación inicial	Opciones de conectividad de Amazon Virtual Private Cloud publicadas.	1 de julio de 2014

Avisos

Es responsabilidad de los clientes realizar su propia evaluación independiente de la información que contiene este documento. Este documento: (a) tiene solo fines informativos, (b) representa las ofertas y prácticas actuales de los productos de AWS, que están sujetas a cambios sin previo aviso y (c) no supone ningún compromiso ni garantía por parte de AWS y sus filiales, proveedores o licenciantes. Los productos o servicios de AWS se proporcionan “tal cual” sin garantías, declaraciones ni condiciones de ningún tipo, ya sean expresas o implícitas. Las responsabilidades y obligaciones de AWS con respecto a sus clientes se controlan mediante los acuerdos de AWS y este documento no forma parte ni modifica ningún acuerdo entre AWS y sus clientes.

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.