AWS Documento técnico

Creación de una infraestructura de VPC AWS redes múltiples escalable y segura

Creación de una infraestructura de VPC AWS redes múltiples escalable y segura: AWS Documento técnico

Table of Contents

Creación de una infraestructura de red multiVPC AWS escalable y segura

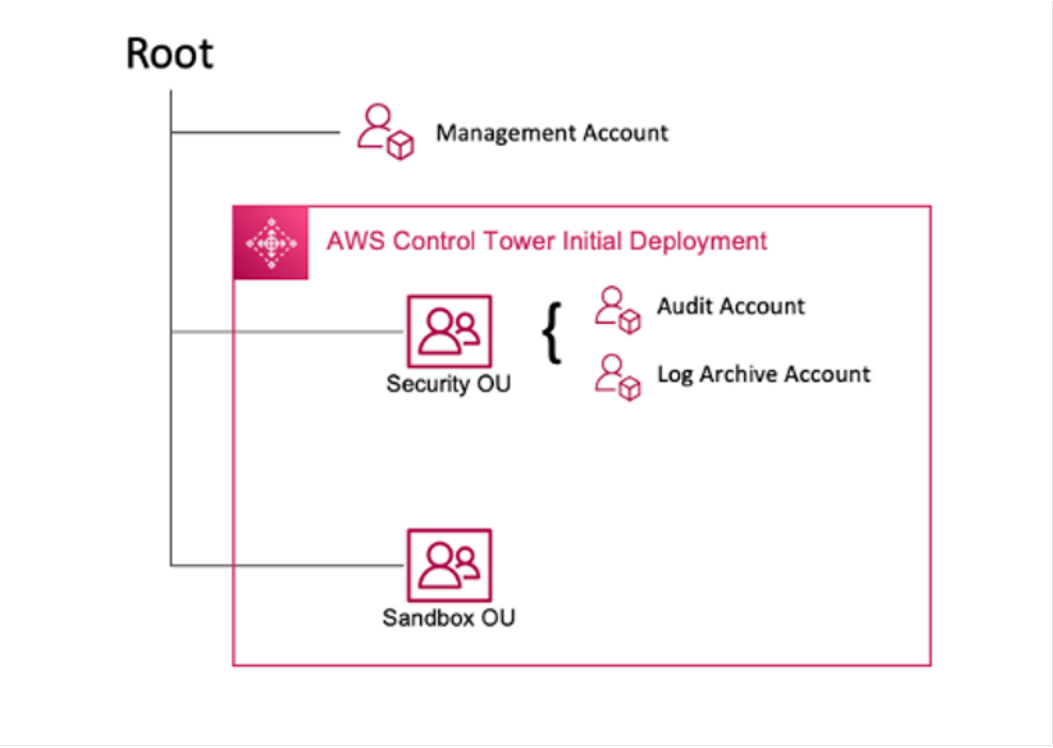
Fecha de publicación: 17 de abril de 2024 () Historial del documento

Los clientes de Amazon Web Services (AWS) suelen confiar en cientos de cuentas y nubes privadas virtuales (VPC) para segmentar sus cargas de trabajo y ampliar su presencia. Este nivel de escala suele plantear desafíos en torno al intercambio de recursos, la conectividad entre VPC y la conectividad entre las instalaciones locales y las VPC.

Este documento técnico describe las prácticas recomendadas para crear arquitecturas de red escalables y seguras en una red grande mediante AWS servicios como Amazon Virtual Private Cloud (Amazon VPC),, AWS Transit Gateway, AWS PrivateLinkGateway AWS Direct ConnectLoad Balancer y Amazon Route 53. AWS Network Firewall Muestra las soluciones para administrar una infraestructura en crecimiento, lo que garantiza la escalabilidad, la alta disponibilidad y la seguridad y, al mismo tiempo, mantiene bajos los costos generales.

Introducción

AWS Los clientes comienzan por acumular recursos en una sola AWS cuenta que representa un límite de administración que segmenta los permisos, los costos y los servicios. Sin embargo, a medida que la organización del cliente crece, se hace necesaria una mayor segmentación de los servicios para monitorear los costos, controlar el acceso y facilitar la administración ambiental. Una solución de cuentas múltiples resuelve estos problemas al proporcionar cuentas específicas para los servicios de TI y los usuarios de una organización. AWS proporciona varias herramientas para administrar y configurar esta infraestructura, entre las que se incluyen AWS Control Tower:



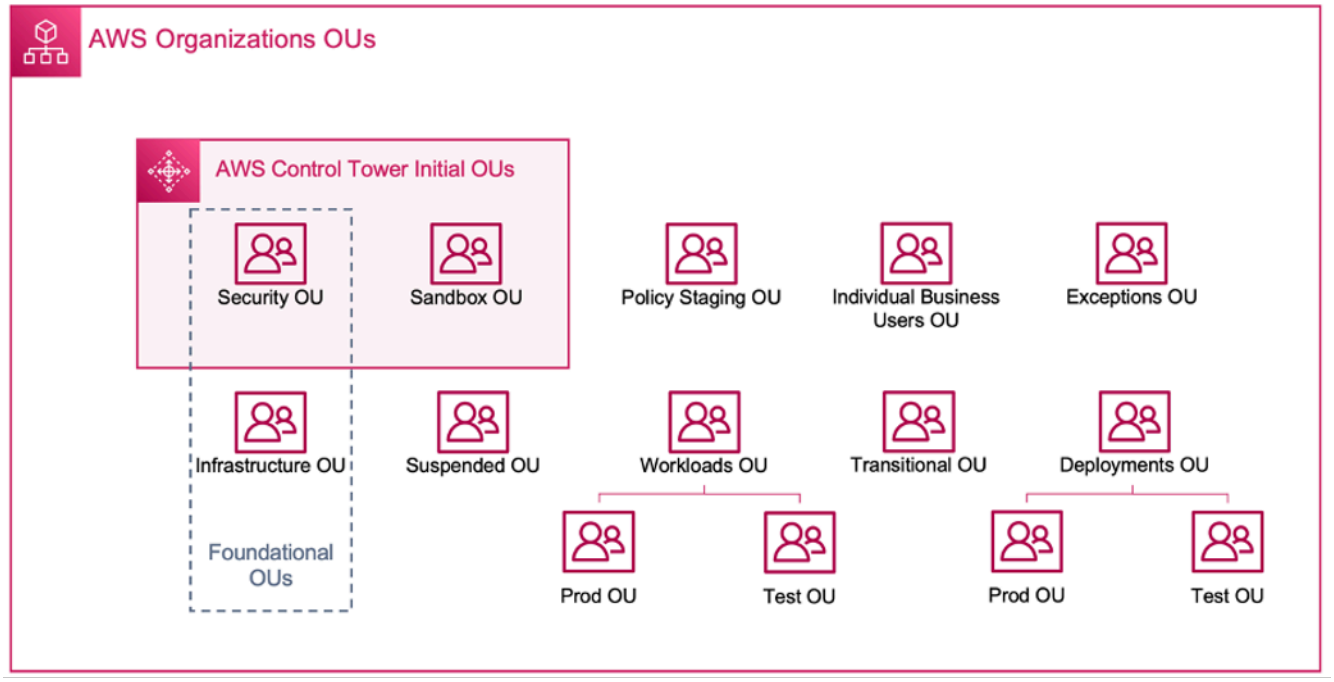
AWS Despliegue inicial de la Torre de Control

Cuando configuras tu entorno de múltiples cuentas mediante AWS Control Tower, se crean dos unidades organizativas (OU):

- OU de seguridad: dentro de esta OU, AWS Control Tower crea dos cuentas:
- Archivo de registros
- Auditoría (esta cuenta corresponde a la cuenta de herramientas de seguridad descrita anteriormente en la guía).
- Unidad organizativa aislada: esta unidad organizativa es el destino predeterminado para las cuentas creadas en ella. AWS Control Tower Contiene cuentas en las que sus creadores pueden explorar y experimentar con AWS los servicios y otras herramientas y servicios, de conformidad con las políticas de uso aceptable de su equipo.

AWS Control Tower le permite crear, registrar y administrar unidades organizativas adicionales para ampliar el entorno inicial e implementar la guía.

El siguiente diagrama muestra las unidades organizativas implementadas inicialmente por AWS Control Tower. Puede ampliar su AWS entorno para implementar cualquiera de las unidades organizativas recomendadas incluidas en el diagrama, a fin de cumplir con sus requisitos.



AWS unidades organizativas

Para obtener más información sobre el uso de un entorno de cuentas múltiples AWS Control Tower, consulte el apéndice E del documento técnico Cómo organizar su AWS entorno con varias cuentas.

> **Note**
>
> En este documento técnico, «Torre de Control» es un término amplio para la configuración escalable, segura y eficiente de múltiples cuentas o múltiples VPC en la que se despliegan las cargas de trabajo. Esta configuración se puede crear con diferentes herramientas. Encontrará más información sobre las prácticas recomendadas, los principios de diseño y las ventajas de la nube multicuenta en el documento técnico Cómo organizar su AWS entorno con varias cuentas.

La mayoría de los clientes comienzan con unas cuantas VPC para implementar su infraestructura. La cantidad de VPC que crea un cliente suele estar relacionada con la cantidad de cuentas, usuarios y entornos preconfigurados (producción, desarrollo, pruebas, etc.). A medida que aumenta el uso de la nube, también aumenta el número de usuarios, unidades de negocio, aplicaciones y regiones con las que interactúa un cliente, lo que lleva a la creación de nuevas VPC.

A medida que aumenta el número de VPC, la administración entre VPC se vuelve esencial para el funcionamiento de la red en la nube del cliente. Este documento técnico describe las mejores prácticas para tres áreas específicas de la conectividad híbrida y entre VPC:

- Conectividad de red: interconexión de VPC y redes locales a escala.
- Seguridad de red: creación de puntos de salida centralizados para acceder a Internet y a puntos finales, como la puerta de enlace de traducción de direcciones de red (NAT), AWS PrivateLinklos puntos finales de VPC y los balanceadores de carga de puerta de enlace. AWS Network Firewall
- Administración de DNS: resolución de DNS dentro de la Torre de Control y DNS híbrido.

Planificación y administración de direcciones IP

Para crear un diseño de red escalable con múltiples cuentas y múltiples VPC, es imprescindible planificar y administrar las direcciones IP. Un buen esquema de direccionamiento IP debe tener en cuenta sus necesidades de red actuales y futuras. Su esquema de direcciones IP debe cubrir sus cargas de trabajo locales y sus cargas de trabajo en la nube, y también debe permitir una expansión futura (por ejemplo, la incorporación de nuevas Regiones de AWS unidades de negocio y las fusiones o adquisiciones). También debería evitar que sus equipos creen, de forma inadvertida, CIDR de IP superpuestos. Si se desea que las CIDR IP se superpongan, por ejemplo, en el caso de cargas de trabajo aisladas o desconectadas, esta decisión debe tomarse de forma consciente y tener en cuenta las implicaciones en el enrutamiento, la seguridad y el costo. Es posible que también deba considerar la posibilidad de crear los procesos de aprobación necesarios para dichas excepciones. Un buen esquema de direcciones IP también ayuda a simplificar el diseño de la red y la configuración del enrutamiento.

Consideraciones clave:

- Planifique su esquema de direcciones IP (tanto IP públicas como privadas) por adelantado y seleccione una herramienta de administración de direcciones IP para asignar, administrar y rastrear el uso de direcciones IP en todas sus cargas de trabajo.
- Utilice esquemas de direcciones IP jerárquicos y resumidos.
- Planifique una asignación de IP coherente en función del entorno Región de AWS, la organización o la unidad de negocio.
- Designe distintos CIDR de IP (tanto IPv4 como IPv6) para las redes locales y en la nube.
- Evite y realice un seguimiento proactivo de los CIDR de IP superpuestos.

- Dimensione sus CIDR IP de manera adecuada para permitir la escalabilidad y el crecimiento futuro.
- Habilite sus cargas de trabajo para que sean compatibles con IPv6 o doble pila para reducir los conflictos de IP y abordar el agotamiento del espacio IPv4.

Puede usar Amazon VPC IP Address Manager (IPAM) para simplificar la planificación, el seguimiento y la supervisión de las direcciones IP públicas y privadas de sus cargas de trabajo. AWS El IPAM le permite organizar, asignar, monitorear y compartir el espacio de direcciones IP en múltiples y. Regiones de AWS Cuentas de AWS También ayuda a asignar automáticamente los CIDR a las VPC mediante reglas empresariales específicas.

Consulte las prácticas recomendadas del administrador de direcciones IP de Amazon VPC, la administración de grupos de IP en las VPC y las regiones mediante el administrador de direcciones IP de Amazon VPC y la administración de direcciones IP para AWS Control Tower obtener información sobre las prácticas recomendadas de direccionamiento IP y cómo usar IPAM para administrar los grupos de IP en las VPC, y. Regiones de AWS AWS Control Tower

¿Tiene Well-Architected?

El marco de AWS Well-Architected le ayuda a entender las ventajas y desventajas de las decisiones que toma al crear sistemas en la nube. Los seis pilares del marco le permitirán aprender las prácticas recomendadas de arquitectura para diseñar y utilizar sistemas fiables, seguros, eficientes, rentables y sostenibles. Mediante AWS Well-Architected Tool, disponible sin costo alguno en la AWS Management Console, puede comparar las cargas de trabajo con estas prácticas recomendadas respondiendo a una serie de preguntas para cada pilar.

Para obtener más orientación experta y prácticas recomendadas para la arquitectura en la nube (implementaciones de arquitectura de referencia, diagramas y documentos técnicos), consulte el Centro de arquitectura de AWS.

Conectividad de VPC a VPC

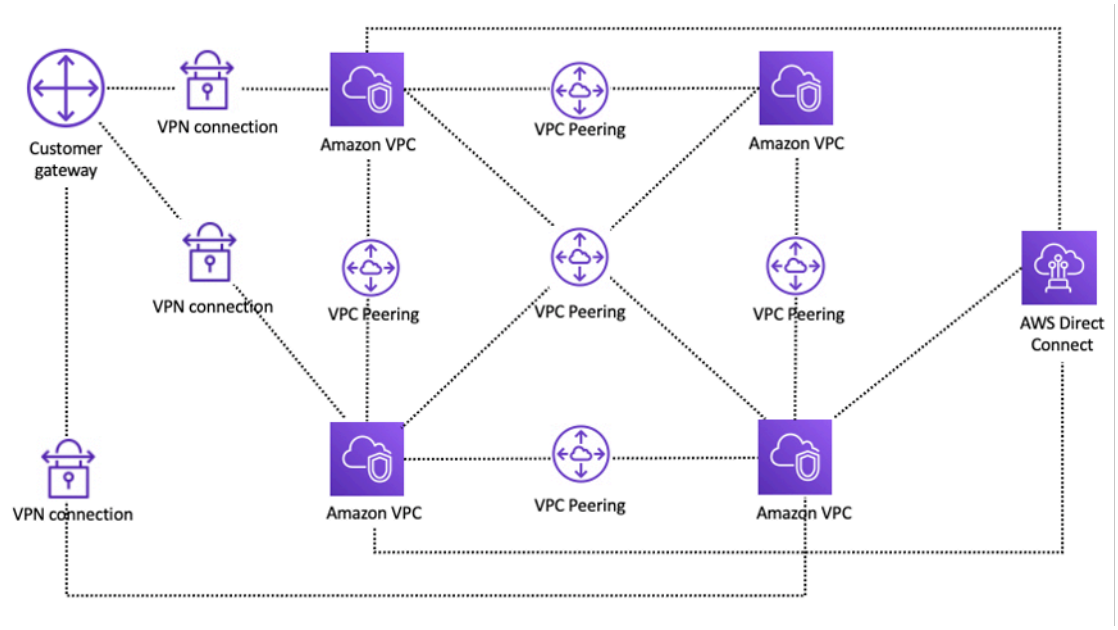
Los clientes pueden usar dos patrones de conectividad de VPC diferentes para configurar entornos de múltiples VPC: de muchas a muchas o de hub and spoke. En many-to-many este enfoque, el tráfico entre cada VPC se administra individualmente entre cada VPC. En el hub-and-spoke modelo, todo el tráfico entre VPC fluye a través de un recurso central, que enruta el tráfico según las reglas establecidas.

Emparejamiento de VPC

La primera forma de conectar dos VPC es mediante el emparejamiento de VPC. En esta configuración, una conexión permite una conectividad bidireccional completa entre las VPC. Esta conexión de emparejamiento se utiliza para enrutar el tráfico entre las VPC. Las VPC de diferentes cuentas y regiones de AWS también se pueden vincular entre sí. Toda la transferencia de datos a través de una conexión de emparejamiento de VPC que permanezca dentro de una zona de disponibilidad es gratuita. Todas las transferencias de datos a través de una conexión de emparejamiento de VPC que atraviese las zonas de disponibilidad se cobran según las tarifas de transferencia de datos estándar de la región. Si las VPC se sincronizan entre regiones, se aplicarán las tarifas estándar de transferencia de datos entre regiones.

El emparejamiento de VPC es point-to-point conectividad y no admite el enrutamiento transitivo. Por ejemplo, si tiene una conexión de emparejamiento de VPC entre la VPC A y la VPC B y entre la VPC A y la VPC C, una instancia de la VPC B no puede transitar por la VPC A para llegar a la VPC C. Para enrutar los paquetes entre la VPC B y la VPC C, debe crear una conexión de emparejamiento de VPC directa.

A gran escala, cuando tiene decenas o cientos de VPC, interconectarlas con el emparejamiento puede generar una malla de cientos o miles de conexiones entre pares. Una gran cantidad de conexiones puede resultar difícil de gestionar y escalar. Por ejemplo, si tiene 100 VPC y desea configurar una interconexión de malla completa entre ellas, se necesitarán 4.950 conexiones de interconexión [`n(n-1)/2`], que `n` es el número total de VPC. Hay un límite máximo de 125 conexiones de emparejamiento activas por VPC.



Configuración de red mediante interconexión de VPC

Si utiliza la interconexión de VPC, se debe establecer una conectividad local (VPN y/o Direct Connect) con cada VPC. Los recursos de una VPC no pueden llegar a las instalaciones locales mediante la conectividad híbrida de una VPC interconectada, como se muestra en la figura anterior.

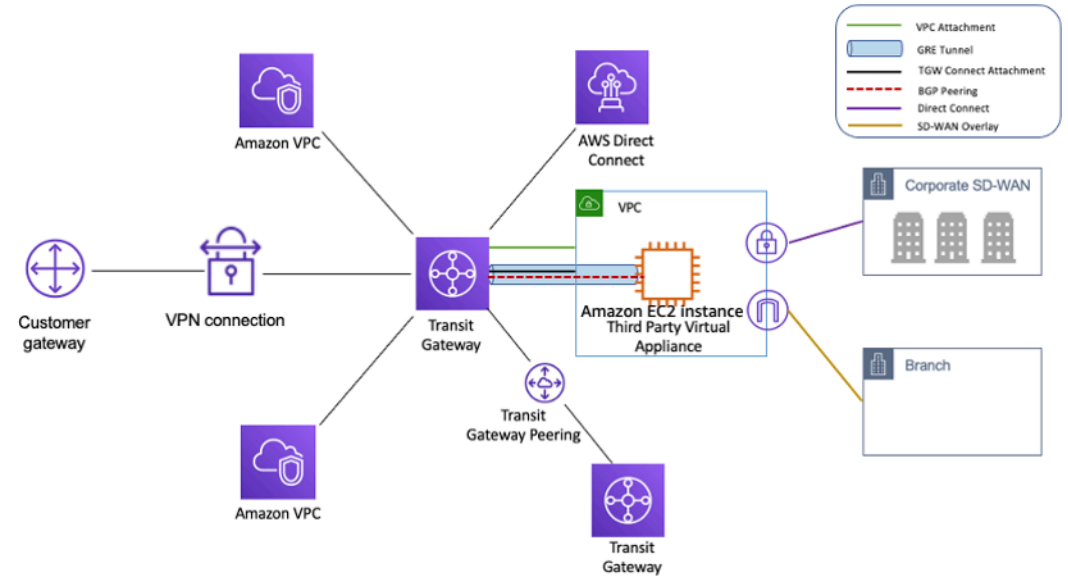
El emparejamiento de VPC se utiliza mejor cuando los recursos de una VPC deben comunicarse con los recursos de otra VPC, el entorno de ambas VPC está controlado y protegido y la cantidad de VPC que se van a conectar es inferior a 10 (para permitir la administración individual de cada conexión). La interconexión de VPC ofrece el costo total más bajo y el rendimiento agregado más alto en comparación con otras opciones de conectividad entre VPC.

AWS Transit Gateway

AWS Transit Gatewayofrece un diseño central y radial para conectar las VPC y las redes locales como un servicio totalmente administrado sin necesidad de aprovisionar dispositivos virtuales de terceros. No se requiere una superposición de VPN y AWS gestiona la alta disponibilidad y escalabilidad.

Transit Gateway permite a los clientes conectar miles de VPC. Puede conectar toda su conectividad híbrida (conexiones VPN y Direct Connect) a una sola puerta de enlace, consolidando y controlando toda la configuración de AWS enrutamiento de su organización en un solo lugar (consulte la siguiente figura). Transit Gateway controla la forma en que se enruta el tráfico entre todas las redes radiales conectadas mediante tablas de enrutamiento. Este hub-and-spoke modelo simplifica la

administración y reduce los costos operativos, ya que las VPC solo se conectan a la instancia de Transit Gateway para acceder a las redes conectadas.



Diseño de eje y radio con AWS Transit Gateway

Transit Gateway es un recurso regional y puede conectar miles de VPC dentro del mismo Región de AWS. Puede conectar varias puertas de enlace a través de una única conexión Direct Connect para una conectividad híbrida. Normalmente, puedes usar una sola instancia de Transit Gateway para conectar todas tus instancias de VPC en una región determinada y usar las tablas de enrutamiento de Transit Gateway para aislarlas donde sea necesario. Tenga en cuenta que no necesita pasarelas de tránsito adicionales para obtener una alta disponibilidad, ya que las pasarelas de tránsito están diseñadas con una alta disponibilidad; para mayor redundancia, utilice una única puerta de enlace en cada región. Sin embargo, hay motivos válidos para crear varias puertas de enlace para limitar los errores de configuración del radio de alcance y segregar las operaciones del plano de control y las administrativas. ease-of-use

Con la interconexión de Transit Gateway, los clientes pueden emparejar sus instancias de Transit Gateway dentro de la misma o de varias regiones y enrutar el tráfico entre ellas. Utiliza la misma infraestructura subyacente que la interconexión de VPC y, por lo tanto, está cifrada. Para obtener más información, consulte Creación de una red global mediante el peering interregional de AWS Transit Gateway y AWS Transit Gateway ahora admite el peering intrarregional.

Coloque la instancia de Transit Gateway de su organización en su cuenta de servicios de red. Esto permite la administración centralizada por parte de los ingenieros de red que administran la cuenta de servicios de red. Utilice AWS Resource Access Manager (RAM) para compartir una instancia de Transit Gateway para conectar VPC entre varias cuentas de su organización de AWS dentro de la

misma región.AWS RAM le permite compartir AWS recursos de forma fácil y segura con cualquier Cuenta de AWS organización de AWS o dentro de ella. Para obtener más información, consulte la sección Automatización de los adjuntos de AWS Transit Gateway a una puerta de enlace de tránsito en una entrada de blog sobre una cuenta central.

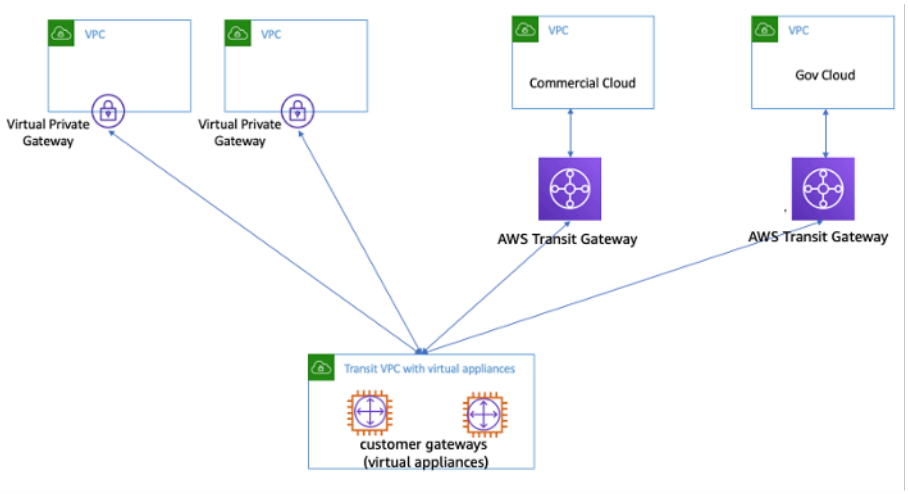
Transit Gateway también le permite establecer la conectividad entre la infraestructura SD-WAN y el AWS uso de Transit Gateway Connect. Utilice un accesorio Transit Gateway Connect con el Border Gateway Protocol (BGP) para el enrutamiento dinámico y el protocolo de túnel Generic Routing Encapsulation (GRE) para obtener un alto rendimiento, con un ancho de banda total de hasta 20 Gbps por cada accesorio Connect (hasta cuatro pares Transit Gateway Connect por cada accesorio Connect). Con Transit Gateway Connect, puede integrar tanto la infraestructura SD-WAN local como los dispositivos SD-WAN que se ejecutan en la nube mediante un adjunto de VPC o AWS Direct Connect un adjunto como capa de transporte subyacente. Consulte Simplifique la conectividad SD-WAN con AWS Transit Gateway Connect para ver las arquitecturas de referencia y la configuración detallada.

Solución Transit VPC

Las VPC de tránsito pueden crear conectividad entre las VPC de una manera diferente a la interconexión de VPC, ya que incorporan un diseño de hub and spoke para la conectividad entre VPC. En una red de VPC de tránsito, una VPC central (la VPC central) se conecta con todas las demás VPC (VPC habladas) a través de una conexión VPN que normalmente aprovecha BGP sobre IPsec. La VPC central contiene instancias de Amazon Elastic Compute Cloud (Amazon EC2) que ejecutan dispositivos de software que enrutan el tráfico entrante a sus destinos mediante la superposición de VPN. La interconexión de VPC de Transit tiene las siguientes ventajas:

- El enrutamiento transitivo se habilita mediante la red VPN superpuesta, lo que permite un diseño de concentrador y radio.
- Cuando se utiliza software de un proveedor externo en la instancia EC2 de la VPC de tránsito central, se puede utilizar la funcionalidad del proveedor en torno a la seguridad avanzada (firewall de capa 7, sistema de prevención de intrusiones (IPS) /sistema de detección de intrusiones (IDS)). Si los clientes utilizan el mismo software en sus instalaciones, se benefician de una experiencia operativa y de supervisión unificada.
- La arquitectura Transit VPC permite la conectividad que puede desearse en algunos casos de uso. Por ejemplo, puede conectar una GovCloud instancia de AWS y una VPC de una región comercial o una instancia de Transit Gateway a una VPC de tránsito y habilitar la conectividad entre las VPC entre las dos regiones. Evalúe sus requisitos de seguridad y conformidad al considerar esta

opción. Para mayor seguridad, puede implementar un modelo de inspección centralizado utilizando los patrones de diseño que se describen más adelante en este documento técnico.



VPC de tránsito con dispositivos virtuales

Transit VPC presenta sus propios desafíos, como los costos más altos de ejecutar dispositivos virtuales de proveedores externos en EC2 en función del tamaño o la familia de las instancias, el rendimiento limitado por conexión VPN (hasta 1,25 Gbps por túnel VPN) y una sobrecarga adicional de configuración, administración y resiliencia (los clientes son responsables de administrar la alta disponibilidad y la redundancia de las instancias de EC2 que ejecutan dispositivos virtuales de proveedores externos).

Emparejamiento de VPC frente a Transit VPC frente a Transit Gateway

Tabla 1: Comparación de conectividad

Criterios	Emparejamiento de VPC	VPC de tránsito	Gateway de tránsito	PrivateLink	WAN en la nube de	VPC Lattice
Ámbito	Regional/ global	Regional	Regional	Regional	Global	Regional
Arquitectura	Malla completa	Basado en VPN hub-and-spoke	Basado en archivos adjuntos	Modelo de proveedor o	Basado en archivos adjuntos,	Conectividad de aplicación

Criterios	Emparejamiento de VPC	VPC de tránsito	Gateway de tránsito	PrivateLink	WAN en la nube de	VPC Lattice
			hub-and-spoke	consumidor	multirregional	a aplicación
Escalado	125 pares activos/VPC	Depende del router virtual/EC2	5000 archivos adjuntos por región	Sin límites	5000 archivos adjuntos por red principal	500 asociaciones de VPC por servicio
Segmentación	Grupos de seguridad	Gestionado por el cliente	Tablas de rutas de Transit Gateway	Sin segmentación	Segmentos	Políticas de servicio y red de servicios
Latencia	Mínima	Además, debido a la sobrecarga de cifrado de la VPN	Tienda adicional de Transit Gateway	El tráfico permanece en la red troncal de AWS, los clientes deberían probarlo	Utiliza el mismo plano de datos que Transit Gateway	El tráfico permanece en la red troncal de AWS, los clientes deberían probarlo
Límite de ancho de banda	Límites por instancia, sin límite agregado	Sujeto a los límites de ancho de banda de las instancias EC2 según el tamaño o la familia	Hasta 100 Gbps (ráfaga) por archivo adjunto	10 Gbps por zona de disponibilidad, se amplía automáticamente hasta 100 Gbps	Hasta 100 Gbps (ráfaga) por archivo adjunto	10 Gbps por zona de disponibilidad

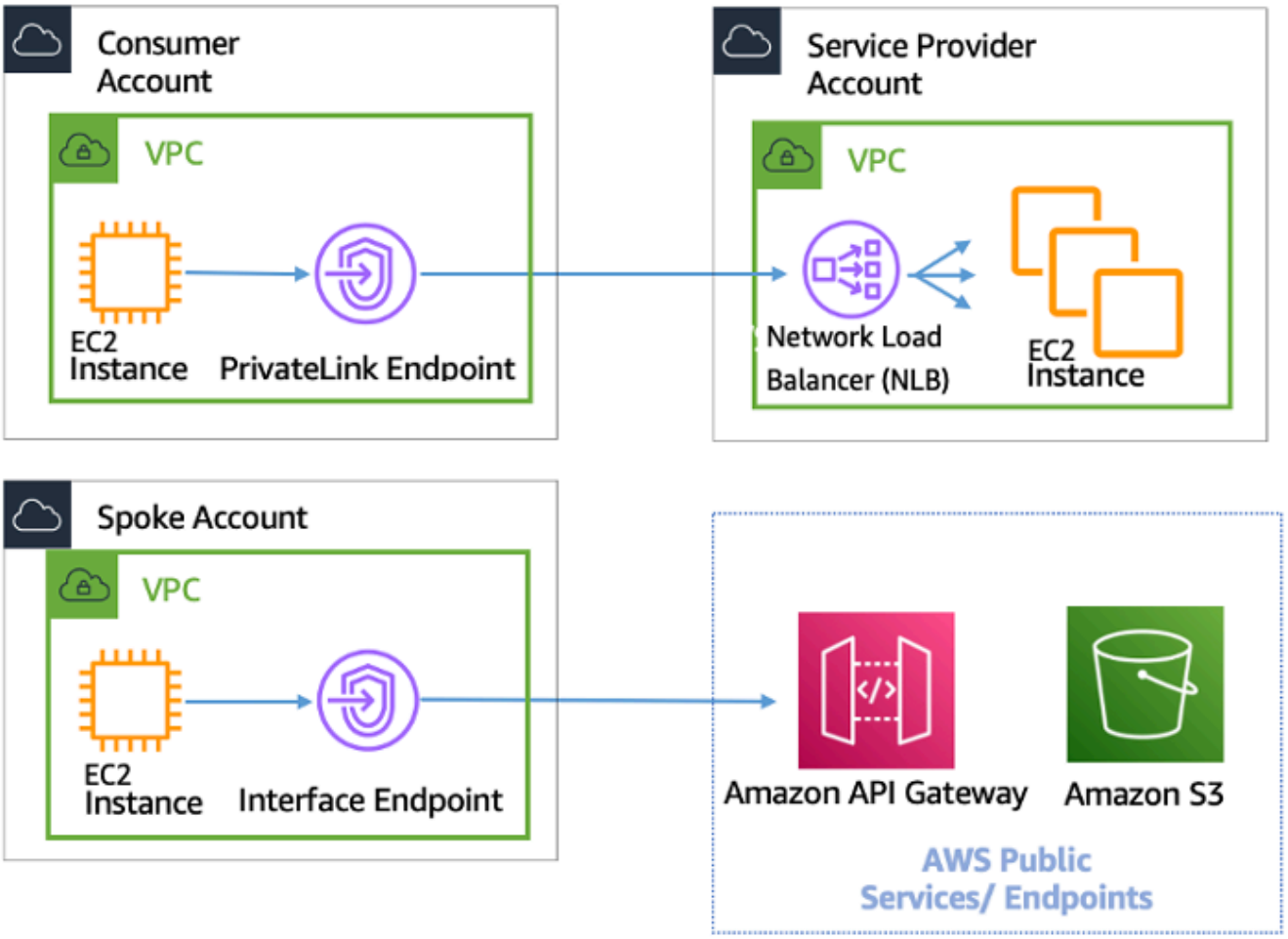
Criterios	Emparejamiento de VPC	VPC de tránsito	Gateway de tránsito	PrivateLink	WAN en la nube de	VPC Lattice
Visibility	Logs de flujo de VPC	Registros y métricas de flujo de VPC CloudWatch	Transit Gateway Network Manager, registros de flujo de VPC, métricas CloudWatch	CloudWatch Métricas	Administrador de red, registros de flujo de VPC, métricas CloudWatch	CloudWatch Registros de acceso
Grupo de seguridad referencias cruzadas	Compatible	No admitido	No admitido	No admitido	No admitido	No aplicable
Compatibilidad con IPv6	Compatible	Depende del dispositivo virtual	Soportado	Soportado	Soportado	Soportado

AWS PrivateLink

AWS PrivateLinkproporciona conectividad privada entre las VPC, los servicios de AWS y las redes locales sin exponer el tráfico a la Internet pública. Los puntos finales de interfaz de VPC, con tecnología AWS PrivateLink, facilitan la conexión AWS y otros servicios entre diferentes cuentas y VPC, lo que simplifica considerablemente la arquitectura de red. Esto permite a los clientes que deseen exponer de forma privada un servicio o una aplicación que reside en una VPC (proveedor de servicios) a otras VPC (de consumo) de forma que solo las VPC de consumo Región de AWS inicien conexiones con la VPC del proveedor de servicios. Un ejemplo de ello es la posibilidad de que sus aplicaciones privadas accedan a las API de los proveedores de servicios.

Para usarlo AWS PrivateLink, cree un Network Load Balancer para su aplicación en su VPC y cree una configuración de servicio de punto final de VPC que apunte a ese balanceador de carga. A continuación, un consumidor de servicios crea un punto final de interfaz para tu servicio. Esto crea una interface de red elástica (ENI) en la subred del consumidor con una dirección IP privada que sirve como punto de entrada para el tráfico destinado al servicio. No es necesario que el consumidor y el servicio estén en la misma VPC. Si la VPC es diferente, las VPC del consumidor y del proveedor de servicios pueden tener intervalos de direcciones IP superpuestos. Además de crear el punto de enlace de la VPC de la interfaz para acceder a los servicios de otras VPC, puede crear puntos de enlace de la VPC de la interfaz para acceder de forma privada a los servicios de AWS compatibles AWS PrivateLink, como se muestra en la siguiente figura.

Con Application Load Balancer (ALB) como objetivo de NLB, ahora puede combinar las capacidades de enrutamiento avanzado de ALB con. AWS PrivateLink Consulte Grupo objetivo tipo Application Load Balancer para Network Load Balancer para ver las arquitecturas de referencia y la configuración detallada.



AWS PrivateLink para la conectividad con otras VPC y servicios de AWS

La elección entre Transit Gateway o VPC peering depende de la AWS PrivateLink conectividad.

- AWS PrivateLink— Úselo AWS PrivateLink cuando tenga un cliente/servidor configurado en el que desee permitir el acceso unidireccional de una o más VPC de consumo a un servicio o conjunto de instancias específicos en la VPC del proveedor de servicios o a determinados servicios. AWS Solo los clientes con acceso a la VPC de consumo pueden iniciar una conexión al servicio en la VPC o servicio del proveedor de servicios. AWS Esta también es una buena opción cuando el cliente y los servidores de las dos VPC tienen direcciones IP superpuestas, ya que AWS PrivateLink utiliza ENI dentro de la VPC del cliente de una manera que garantiza que no haya conflictos de IP con el proveedor de servicios. Puede acceder a AWS PrivateLink los puntos de conexión a través de interconexiones de VPC, VPN, Transit Gateway, Cloud WAN y. AWS Direct Connect
- Emparejamiento de VPC y Transit Gateway: utilice el emparejamiento de VPC y Transit Gateway cuando desee habilitar la conectividad IP de capa 3 entre las VPC.

  Su arquitectura contendrá una combinación de estas tecnologías para adaptarse a diferentes casos de uso. Todos estos servicios se pueden combinar y operar entre sí. Por ejemplo, AWS PrivateLink gestionar la conectividad cliente-servidor al estilo de una API, la interconexión de VPC para gestionar los requisitos de conectividad directa cuando aún se necesiten grupos de ubicación dentro de la región o la conectividad interregional, y Transit Gateway para simplificar la conectividad de las VPC a escala, así como la consolidación perimetral para la conectividad híbrida.

Uso compartido de VPC

Compartir las VPC resulta útil cuando el propietario de la VPC no tiene que gestionar estrictamente el aislamiento de la red entre equipos, sino los usuarios y los permisos a nivel de cuenta. Con la VPC compartida, varias cuentas de AWS crean sus recursos de aplicaciones (como las instancias de Amazon EC2) en VPC de Amazon compartidas y administradas de forma centralizada. En este modelo, la cuenta propietaria de la VPC (propietario) comparte una o más subredes con otras cuentas (participantes). Después de compartir una subred, los participantes pueden ver, crear, modificar y eliminar los recursos de su aplicación en las subredes compartidas con ellos. Los participantes no pueden ver, modificar ni eliminar recursos que pertenezcan a otros participantes o al propietario de la VPC. La seguridad entre los recursos de las VPC compartidas se administra mediante grupos de seguridad, listas de control de acceso a la red (NACL) o mediante un firewall entre las subredes.

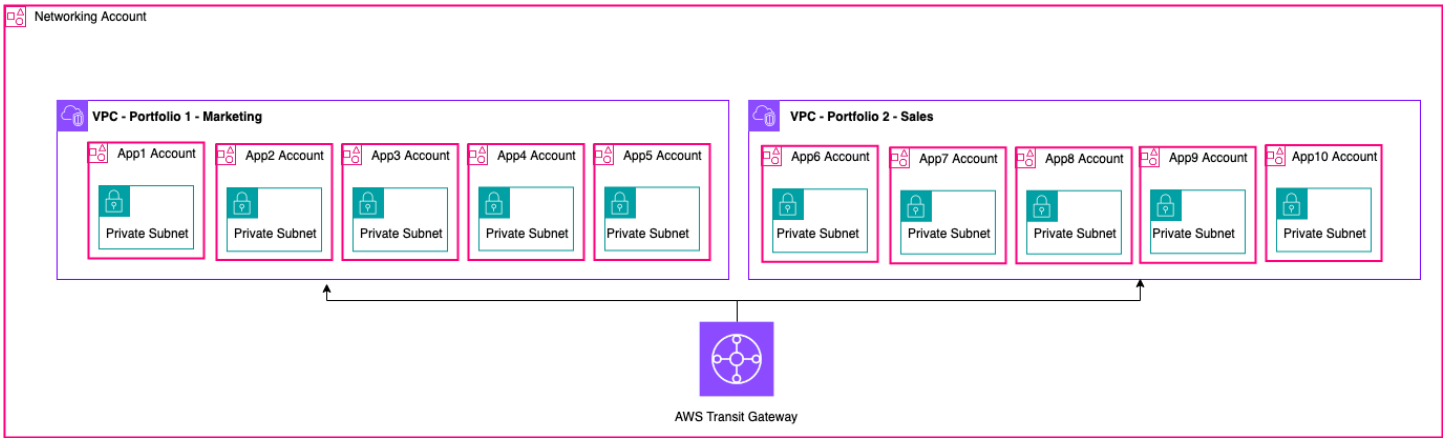
Ventajas del uso compartido de VPC:

- Diseño simplificado: sin complejidad en torno a la conectividad entre VPC
- Menos VPC gestionadas
- Separación de funciones entre los equipos de red y los propietarios de las aplicaciones
- Mejor utilización de las direcciones IPv4
- Costos más bajos: sin cargos por transferencia de datos entre instancias que pertenezcan a cuentas diferentes dentro de la misma zona de disponibilidad

> **Note**
>
> Cuando compartes una subred con varias cuentas, tus participantes deberían tener cierto nivel de cooperación, ya que comparten espacio IP y recursos de red. Si es necesario, puede optar por compartir una subred diferente para cada cuenta de participante. Una subred por participante permite que la ACL de red proporcione aislamiento de red además de los grupos de seguridad.

La mayoría de las arquitecturas de los clientes contendrán varias VPC, muchas de las cuales se compartirán con dos o más cuentas. Se pueden usar Transit Gateway y el emparejamiento de VPC para conectar las VPC compartidas. Por ejemplo, supongamos que tiene 10 aplicaciones. Cada aplicación requiere su propia cuenta de AWS. Las aplicaciones se pueden clasificar en dos carteras de aplicaciones (las aplicaciones de la misma cartera tienen requisitos de red similares: las aplicaciones de 1 a 5 en «Marketing» y las aplicaciones de 6 a 10 en «Ventas»).

Puede tener una VPC por cartera de aplicaciones (dos VPC en total) y la VPC se comparte con las distintas cuentas de propietarios de aplicaciones de esa cartera. Los propietarios de aplicaciones implementan aplicaciones en sus respectivas VPC compartidas (en este caso, en las diferentes subredes para segmentar y aislar las rutas de la red mediante NACL). Las dos VPC compartidas se conectan a través de Transit Gateway. Con esta configuración, podría pasar de tener que conectar 10 VPC a solo dos, como se muestra en la siguiente figura.

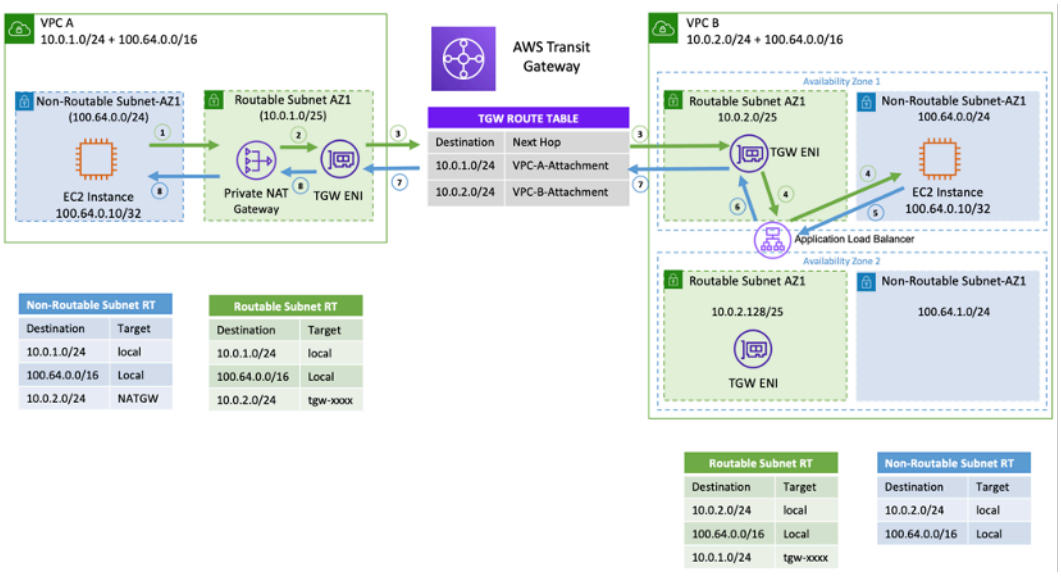


Ejemplo de configuración: VPC compartida

> **Note**
>
> Los participantes que comparten VPC no pueden crear todos los recursos de AWS en una subred compartida. Para obtener más información, consulte la sección Limitaciones de la documentación sobre el uso compartido de VPC.
> Para obtener más información sobre las consideraciones clave y las mejores prácticas para el uso compartido de VPC, consulte la entrada del blog Uso compartido de VPC: consideraciones clave y mejores prácticas.

Puerta de enlace NAT privada

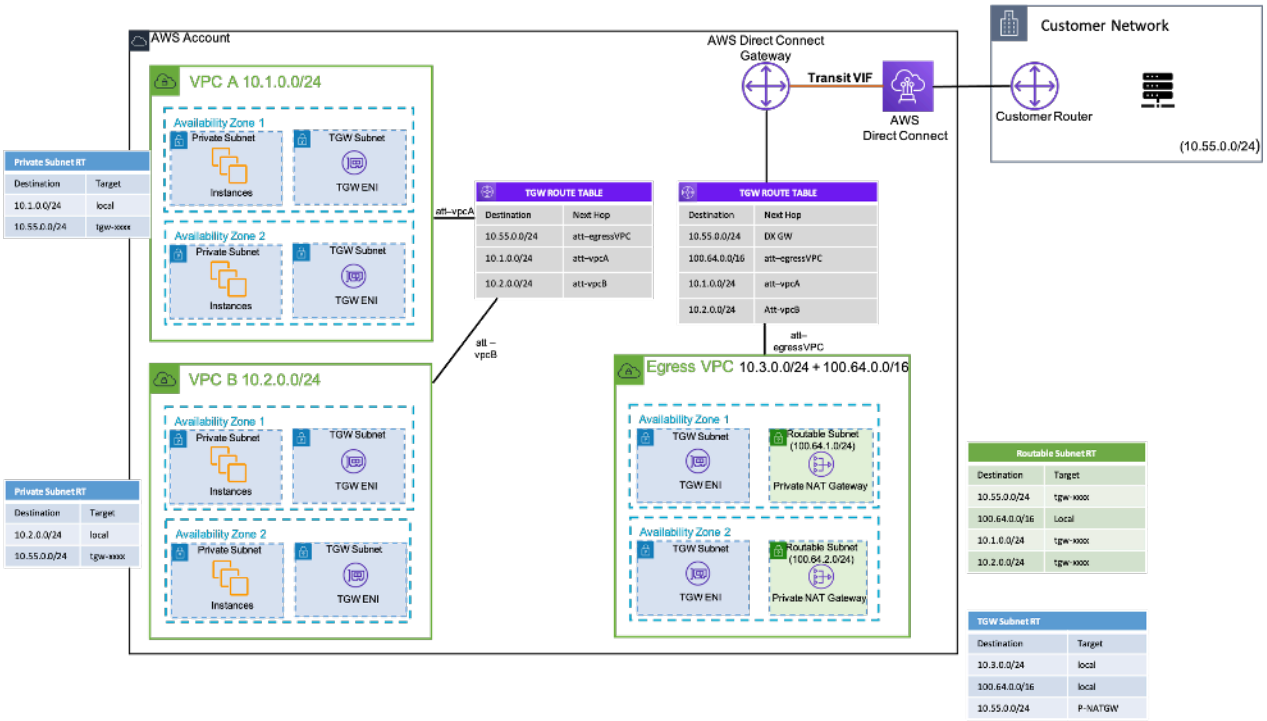
Los equipos suelen trabajar de forma independiente y pueden crear una nueva VPC para un proyecto, que puede tener bloques de enrutamiento entre dominios (CIDR) superpuestos. Para la integración, es posible que deseen habilitar la comunicación entre redes con CIDR superpuestos, lo que no se puede lograr con funciones como la interconexión de VPC y Transit Gateway. Una puerta de enlace NAT privada puede ayudar con este caso de uso. La puerta de enlace NAT privada utiliza una dirección IP privada única para realizar la NAT de origen para la dirección IP de origen superpuesta, y el ELB realiza la NAT de destino para la dirección IP de destino superpuesta. Puede enrutar el tráfico desde su puerta de enlace NAT privada a otras VPC o redes locales mediante Transit Gateway o una puerta de enlace privada virtual.



Ejemplo de configuración: puerta de enlace NAT privada

La figura anterior muestra dos `100.64.0.0/16` subredes no enrutables (CIDR superpuestas) en la VPC A y B. Para establecer una conexión entre ellas, puede agregar CIDR secundarios que no se superponen o se pueden enrutar (subredes enrutables) a la VPC A y B, respectivamente. `10.0.1.0/24` `10.0.2.0/24` El equipo de administración de red responsable de la asignación de IP debe asignar los CIDR enrutables. Se agrega una puerta de enlace NAT privada a la subred enrutable de la VPC A con una dirección IP de. `10.0.1.125` La puerta de enlace NAT privada realiza la traducción de direcciones de red de origen en las solicitudes de instancias de la subred no enrutable de la VPC A (`100.64.0.10`) como `10.0.1.125` el ENI de la puerta de enlace NAT privada. Ahora el tráfico se puede dirigir a una dirección IP enrutable asignada al Application Load Balancer (ALB) de la VPC B `10.0.2.10` (), cuyo objetivo es. `100.64.0.10` El tráfico se enruta a través de Transit Gateway. La puerta de enlace NAT privada procesa el tráfico de retorno y lo devuelve a la instancia Amazon EC2 original que solicitó la conexión.

La puerta de enlace NAT privada también se puede utilizar cuando la red local restringe el acceso a las IP aprobadas. Las redes locales de unos pocos clientes están obligadas a comunicarse únicamente con redes privadas (sin IGW) únicamente a través de un bloque contiguo limitado de direcciones IP aprobadas propiedad del cliente. En lugar de asignar a cada instancia una IP independiente del bloque, puede ejecutar grandes cargas de trabajo en AWS VPC detrás de cada IP de la lista de permitidos mediante una puerta de enlace NAT privada. Para obtener más información, consulte la entrada del blog Cómo solucionar el agotamiento de la IP privada con una solución de NAT privada.



Ejemplo de configuración: cómo utilizar la puerta de enlace NAT privada para proporcionar direcciones IP aprobadas para la red local

AWS WAN en la nube

La WAN en la nube de AWS es una nueva forma de conectar redes que antes podíamos hacer con Transit Gateways, VPC Peering y túneles VPN IPSEC. Antes, configuraba una o más VPC, las conectaba mediante uno de los métodos anteriores y utilizaba una VPN IPSEC o AWS Direct Connect se conectaba a redes locales. Tendría definidas las estructuras de red y seguridad en un lugar y las redes en otro. La WAN en la nube le permite centralizar todas estas estructuras en un solo lugar. Por política, puede segmentar sus redes para determinar quién puede hablar con quién y aislar el tráfico de producción a través de estos segmentos de las cargas de trabajo de desarrollo o prueba, o de sus redes locales.

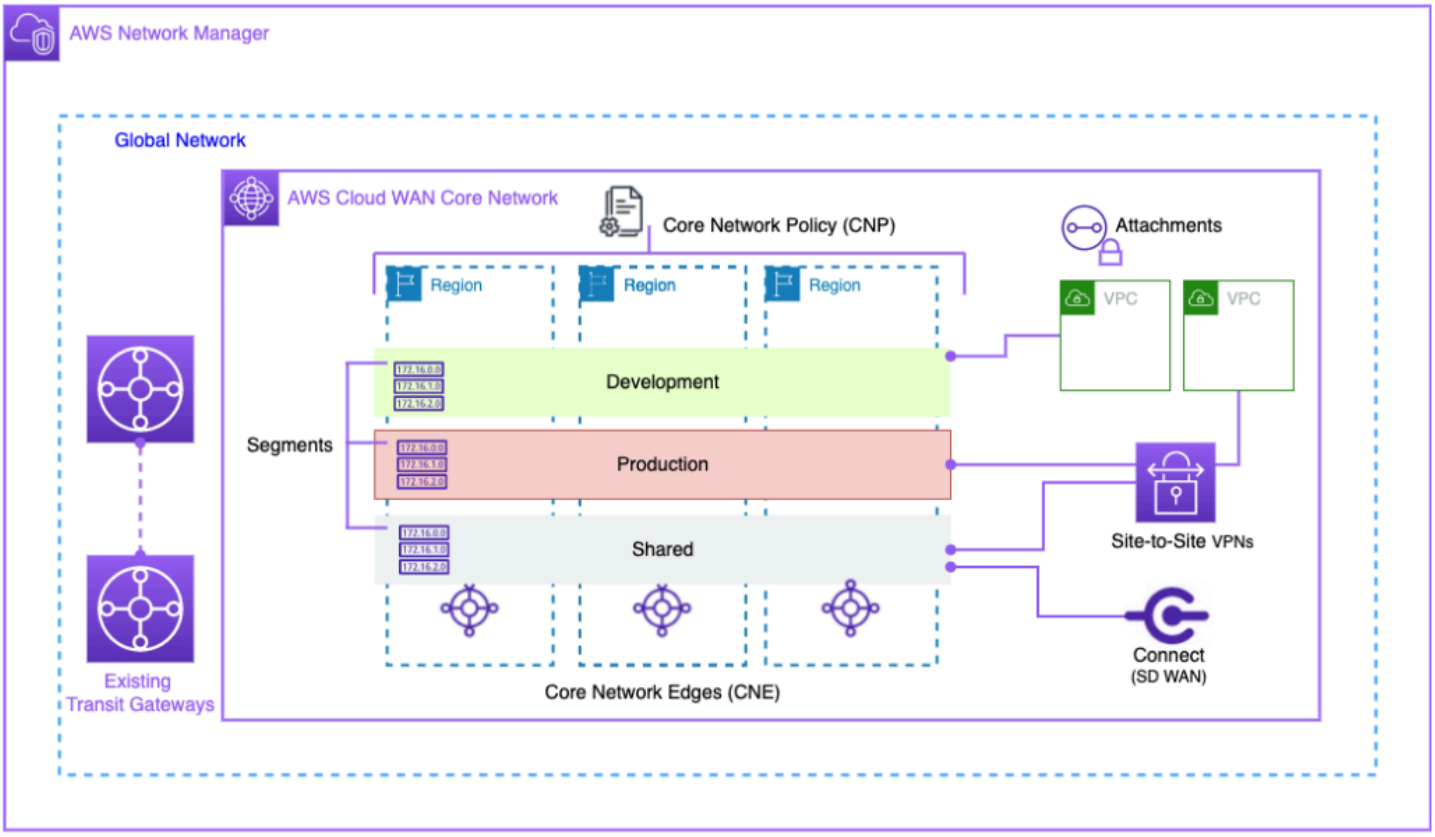


Diagrama de bloques de WAN en la nube

Administre su red global a través de la interfaz de usuario y las API de AWS Network Manager. La red global es el contenedor a nivel raíz de todos los objetos de la red; la red principal es la parte de la red global administrada por AWS. Una política de red principal (CNP) es un documento de política con una sola versión que define todos los aspectos de su red principal. Los adjuntos son cualquier conexión o recurso que desee añadir a su red principal. Un perímetro de red central (CNE) es un punto de conexión local para los archivos adjuntos que cumplen con la política. Los segmentos de red son dominios de enrutamiento que, de forma predeterminada, permiten la comunicación solo dentro de un segmento.

Para usar CloudWAN:

1. En AWS Network Manager, cree una red global y una red principal asociada.
2. Cree un CNP que defina los segmentos, el rango de ASN Regiones de AWS y las etiquetas que se utilizarán para adjuntarlos a los segmentos.
3. Aplique la política de red.
4. Comparta la red principal con sus usuarios, cuentas u organizaciones mediante el administrador de acceso a los recursos.

5. Cree y etiquete archivos adjuntos.
6. Actualice las rutas de las VPC conectadas para incluir la red principal.

Cloud WAN se diseñó para simplificar el proceso de conexión de su infraestructura de AWS a nivel mundial. Le permite segmentar el tráfico con una política de permisos centralizada y utilizar la infraestructura existente en las ubicaciones de su empresa. La WAN en la nube también conecta las VPC, las SD-WAN, las VPN de clientes, los firewalls, las VPN y los recursos del centro de datos para conectarse a la WAN en la nube. Para obtener más información, consulte las publicaciones del blog AWS Cloud WAN.

La WAN en la nube de AWS permite una red unificada que conecta los entornos locales y en la nube. Las organizaciones utilizan firewalls de última generación (NGFW) y sistemas de prevención de intrusiones (IPS) para garantizar la seguridad. La entrada del blog sobre los patrones de migración e interoperabilidad de AWS Cloud WAN y Transit Gateway describe los patrones arquitectónicos para administrar e inspeccionar de forma centralizada el tráfico de red saliente en una red WAN en la nube, incluidas las redes de una o varias regiones, y configura las tablas de rutas. Estas arquitecturas garantizan que los datos y las aplicaciones permanezcan seguros y, al mismo tiempo, mantienen un entorno de nube seguro.

Para obtener más información sobre la WAN en la nube, consulte la entrada del blog AWS Cloud WAN sobre la arquitectura de inspección saliente centralizada.

Amazon VPC Lattice

Amazon VPC Lattice es un servicio de redes de aplicaciones totalmente gestionado que se utiliza para conectar, supervisar y proteger los servicios de varias cuentas y nubes privadas virtuales. VPC Lattice ayuda a interconectar los servicios dentro de un límite lógico, de modo que pueda gestionarlos y detectarlos de forma eficaz.

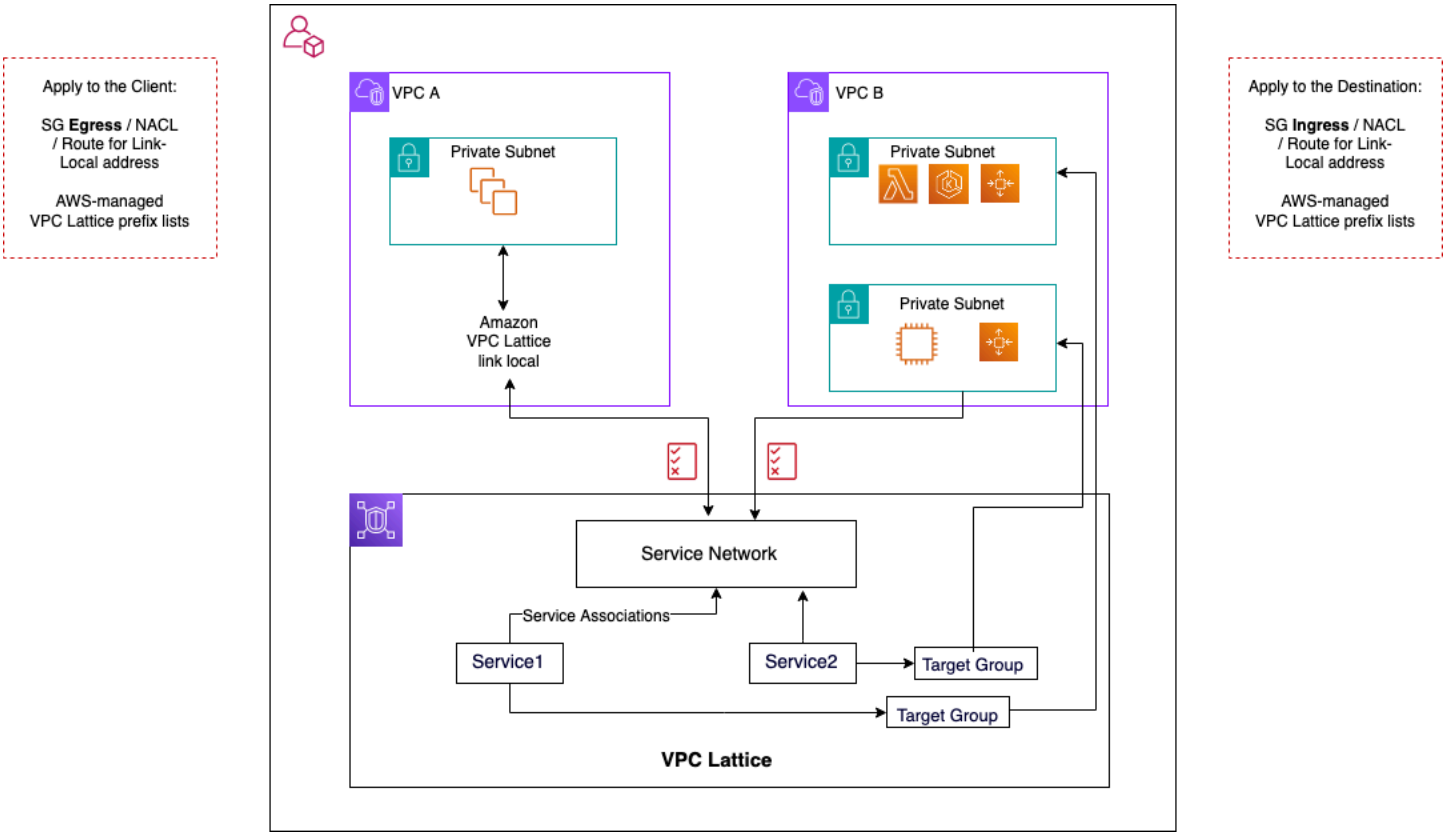
Los componentes de VPC Lattice constan de:

- Servicio: es una unidad de aplicación que se ejecuta en una instancia, un contenedor o una función Lambda y consta de oyentes, reglas y grupos objetivo.
- Red de servicios: este es el límite lógico que se utiliza para implementar automáticamente la detección y la conectividad de los servicios y aplicar políticas comunes de acceso y observabilidad a un conjunto de servicios.

- Políticas de autenticación: políticas de recursos de IAM que se pueden asociar a una red de servicios o a servicios individuales para respaldar la autenticación a nivel de solicitud y la autorización específica del contexto.
- Directorio de servicios: una vista centralizada de los servicios que posee o que se han compartido con usted a través de AWS Resource Access Manager.

Pasos de uso de VPC Lattice:

1. Cree la red de servicio. La red de servicio normalmente reside en una cuenta de red a la que un administrador de red tiene acceso total. La red de servicios se puede compartir entre varias cuentas de una organización. El uso compartido se puede realizar en servicios individuales o en toda la cuenta de servicio.
2. Adjunte las VPC a la red de servicios para habilitar la red de aplicaciones para cada VPC, de modo que los distintos servicios puedan empezar a consumir otros servicios que estén registrados en la red. Los grupos de seguridad se aplican para controlar el tráfico.
3. Los desarrolladores definen los servicios, que se rellenan en el directorio de servicios y se registran en la red de servicios. VPC Lattice contiene la libreta de direcciones de todos los servicios configurados. Los desarrolladores también pueden definir políticas de enrutamiento para utilizar despliegues azules o verdes. La seguridad se gestiona a nivel de la red de servicio, donde se definen las políticas de autenticación y autorización, y a nivel de servicio, donde se implementan las políticas de acceso con IAM.



Flujos de comunicación de VPC Lattice

Encontrará más información en la guía del usuario de VPC Lattice.

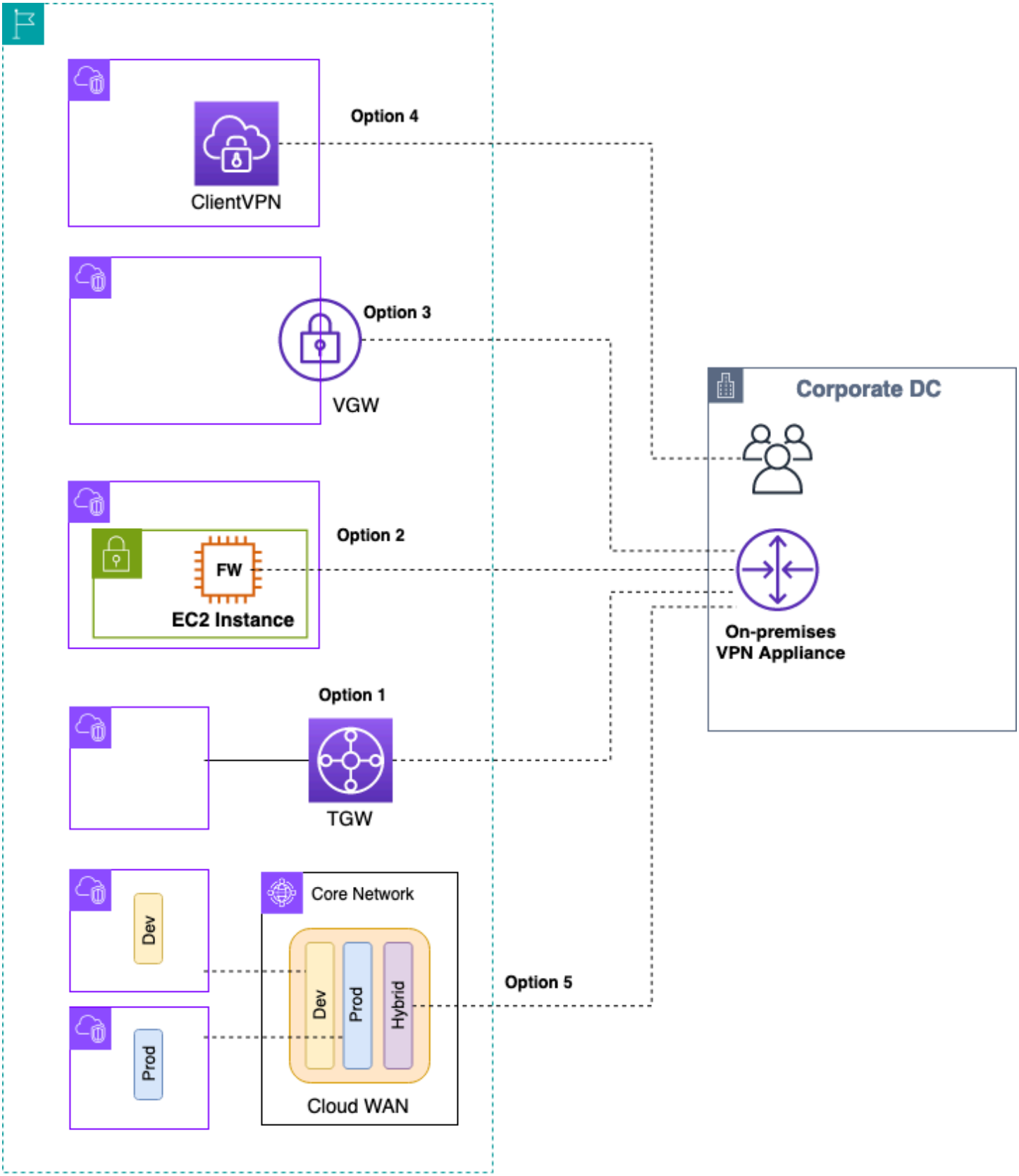
Conectividad híbrida

Esta sección se centra en conectar de forma segura los recursos de la nube con los centros de datos locales. Existen tres enfoques para habilitar la conectividad híbrida:

- ne-to-one Conectividad O: en esta configuración, se crea una conexión VPN o una VIF privada de Direct Connect para cada VPC. Esto se logra mediante la puerta de enlace privada virtual (VGW). Esta opción es ideal para pequeñas cantidades de VPC, pero a medida que un cliente escala sus VPC, la administración de la conectividad híbrida por VPC puede resultar difícil.
- Consolidación perimetral: en esta configuración, los clientes consolidan la conectividad de TI híbrida para varias VPC en un único punto final. Todas las VPC comparten estas conexiones híbridas. Esto se logra mediante el uso AWS Transit Gateway de la AWS Direct Connect puerta de enlace.
- Consolidación híbrida de malla completa: en esta configuración, los clientes consolidan la conectividad de varias VPC en un único punto final mediante CloudWAN, integrada. AWS Transit Gateway Se trata de un enfoque totalmente basado en políticas para la creación de redes en una o más cuentas de AWS, representadas en código. En este momento, el uso AWS Direct Connect para la conectividad perimetral requiere conectar Transit Gateway a CloudWAN.

VPN

Hay varias formas de configurar la VPN en AWS:



AWS VPN opciones

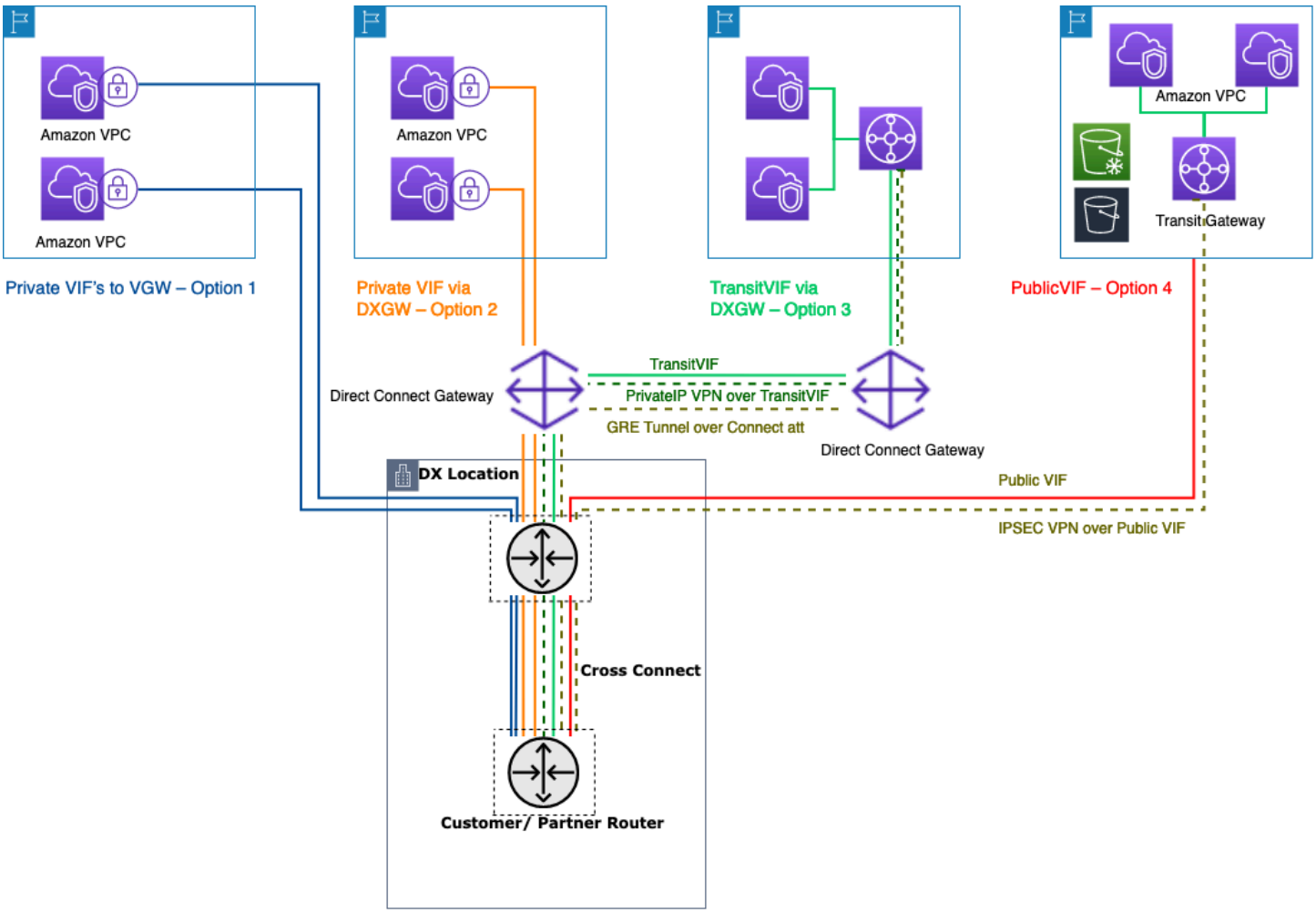
- Opción 1: consolidar la conectividad VPN en Transit Gateway: esta opción aprovecha el adjunto VPN de Transit Gateway en Transit Gateway. Transit Gateway admite la terminación de IPsec para la site-to-site VPN. Los clientes pueden crear túneles VPN hacia la Transit Gateway y acceder a las VPC conectadas a ella. Transit Gateway admite conexiones VPN dinámicas basadas en BGP y estáticas. Transit Gateway también admite rutas múltiples de igual costo (ECMP) en los archivos adjuntos de VPN. Cada conexión VPN tiene un rendimiento máximo de 1,25 Gbps por túnel. Al habilitar el ECMP, puede agregar el rendimiento entre las conexiones VPN, lo que le permite escalar más allá del límite máximo predeterminado de 1,25 Gbps. En esta opción, pagas tanto el precio como AWS VPN el precio de Transit Gateway. AWS recomienda usar esta opción para la conectividad VPN. Para obtener más información, consulte la entrada del blog Cómo escalar el rendimiento de la VPN con AWS Transit Gateway.
- Opción 2: cancelar la VPN en una instancia de Amazon EC2: los clientes aprovechan esta opción en casos extremos cuando desean un conjunto de funciones de software de un proveedor en particular (como Cisco DMVPN o Generic Routing Encapsulation (GRE)) o desean coherencia operativa en las distintas implementaciones de VPN. Puede usar el diseño de la VPC de tránsito para la consolidación perimetral, pero es importante recordar que todas las consideraciones clave de la Conectividad de VPC a VPC sección sobre la VPC de tránsito se aplican a la conectividad de la VPN híbrida. Usted es responsable de gestionar la alta disponibilidad y paga por la instancia EC2, así como los costes de soporte y licencias de software de cualquier proveedor.
- Opción 3: Terminar la VPN en una puerta de enlace privada virtual (VGW): esta opción del servicio AWS Site-to-Site VPN one-to-one permite un diseño de conectividad en el que se crea una conexión VPN (compuesta por un par de túneles VPN redundantes) por VPC. Esta es una forma estupenda de empezar a utilizar la conectividad VPN en AWS, pero a medida que se amplía el número de VPC, administrar un número cada vez mayor de conexiones VPN puede convertirse en un desafío. Por lo tanto, el diseño de consolidación perimetral que aproveche Transit Gateway acabará siendo una mejor opción. El rendimiento de una VPN a una VGW está limitado a 1,25 Gbps por túnel y no se admite el balanceo de carga mediante ECMP. Desde el punto de vista de los precios, solo paga los precios de las VPN de AWS y no se aplica ningún cargo por ejecutar una VGW. Para obtener más información, consulte los AWS VPN precios y AWS VPN la pasarela privada virtual.
- Opción 4: finalizar la conexión VPN en el punto final de la VPN del cliente: AWS Client VPN es un servicio de VPN gestionado y basado en el cliente que le permite acceder de forma segura a los recursos de AWS y a los recursos de su red local. Con Client VPN, puede acceder a sus recursos desde cualquier ubicación mediante un cliente VPN de OpenVPN o proporcionado por AWS. Al configurar un punto final Client VPN, los clientes y los usuarios pueden conectarse para establecer

una conexión VPN de Transport Layer Security (TLS). Para obtener más información, consulte la documentación de AWS Client VPN.

- Opción 5: consolidar la conexión VPN en la nube WAN de AWS: esta opción es similar a la primera opción de esta lista, pero utiliza la estructura CloudWAN para configurar las conexiones VPN mediante programación a través del documento de política de red.

AWS Direct Connect

Si bien la VPN a través de Internet es una excelente opción para empezar, es posible que la conectividad a Internet no sea fiable para el tráfico de producción. Debido a esta falta de fiabilidad, muchos clientes se AWS Direct Connectdecantan por ello. AWS Direct Connect es un servicio de red que ofrece una alternativa al uso de Internet para conectarse a AWS. Por AWS Direct Connect lo tanto, los datos que anteriormente se habrían transportado a través de Internet se entregan a través de una conexión de red privada entre sus instalaciones y AWS. En muchos casos, las conexiones de red privada pueden reducir los costos, aumentar el ancho de banda y proporcionar una experiencia de red más uniforme que las conexiones basadas en Internet. Existen varias formas de conectarse AWS Direct Connect a las VPC:



Formas de conectar sus centros de datos locales mediante AWS Direct Connect

- Opción 1: Crear una interfaz virtual privada (VIF) para una VGW conectada a una VPC: puede crear 50 VIF por conexión Direct Connect, lo que le permite conectarse a un máximo de 50 VPC (una VIF proporciona conectividad a una VPC). Hay un emparejamiento de BGP por VPC. La conectividad en esta configuración está restringida a la región de AWS a la que se encuentra la ubicación de Direct Connect. La one-to-one asignación de VIF a VPC (y la falta de acceso global) hacen que esta sea la forma menos preferida de acceder a las VPC en la zona de aterrizaje.
- Opción 2: Crear un VIF privado en una puerta de enlace de Direct Connect asociada a varias VGW (cada VGW está conectada a una VPC): una puerta de enlace de Direct Connect es un recurso disponible en todo el mundo. Puede crear la puerta de enlace Direct Connect en cualquier región y acceder a ella desde todas las demás regiones, incluida GovCloud (excepto China). Una puerta de enlace Direct Connect puede conectarse a hasta 20 VPC (mediante VGWs) de todo el mundo en cualquier cuenta de AWS a través de un único VIF privado. Esta es una excelente opción si

una zona de destino consta de un número reducido de VPC (diez o menos VPC) o si necesita acceso global. Hay una sesión de emparejamiento BGP por puerta de enlace de Direct Connect por conexión de Direct Connect. La puerta de enlace Direct Connect es solo para el flujo de tráfico norte/sur y no permite la conectividad de VPC a VPC. Consulte la sección sobre las asociaciones de pasarelas privadas virtuales en la documentación para obtener más información. AWS Direct Connect Con esta opción, la conectividad no se limita a la región de AWS en la que se encuentra la ubicación de Direct Connect. AWS Direct Connect la puerta de enlace es solo para el flujo de tráfico norte/sur y no permite la conectividad de VPC a VPC. Una excepción a esta regla es cuando se anuncia una superred en dos o más VPC que tienen sus VGW conectadas asociadas a la misma puerta de enlace y en la misma interfaz virtual. AWS Direct Connect En este caso, las VPC pueden comunicarse entre sí a través del punto final. AWS Direct Connect Consulte la documentación de AWS Direct Connect las pasarelas para obtener más información.

- Opción 3: Crear un VIF de tránsito a una puerta de enlace de Direct Connect asociada a Transit Gateway: puede asociar una instancia de Transit Gateway a una puerta de enlace de Direct Connect mediante un VIF de tránsito. AWS Direct Connect ahora admite conexiones a Transit Gateway para todas las velocidades de puerto, lo que ofrece una opción más rentable para los usuarios de Transit Gateway cuando no se requieren conexiones de alta velocidad (superiores a 1 Gbps). Esto le permite usar Direct Connect a velocidades de 50, 100, 200, 300, 400 y 500 Mbps para conectarse a Transit Gateway. Transit VIF le permite conectar su centro de datos local a un máximo de seis instancias de Transit Gateway por AWS Direct Connect puerta de enlace (que se pueden conectar a miles de VPC) en diferentes regiones de AWS y cuentas de AWS mediante un único peering VIF de tránsito y BGP. Esta es la configuración más sencilla entre las opciones para conectar varias VPC a escala, pero debes tener en cuenta las cuotas de Transit Gateway. Un límite clave a tener en cuenta es que solo puedes anunciar 200 prefijos desde un Transit Gateway a un router local a través del VIF de tránsito. Con las opciones anteriores, usted paga los precios de Direct Connect. Con esta opción, también paga los cargos por procesamiento de datos y adjuntos de Transit Gateway. Para obtener más información, consulte la documentación de Transit Gateway Associations on Direct Connect.
- Opción 4: Cree una conexión VPN a Transit Gateway a través de una VIF pública de Direct Connect: una VIF pública le permite acceder a todos los servicios públicos y puntos de conexión de AWS mediante las direcciones IP públicas. Cuando crea un adjunto de VPN en una Transit Gateway, obtiene dos direcciones IP públicas para los puntos de conexión de la VPN en AWS. Se puede acceder a estas IP públicas a través de la VIF pública. Puede crear tantas conexiones VPN a tantas instancias de Transit Gateway como desee a través de Public VIF. Cuando crea un emparejamiento de BGP a través del VIF público, AWS anuncia todo el rango de IP públicas de AWS en su router. Para asegurarse de que solo permite cierto tráfico (por ejemplo, permitir el

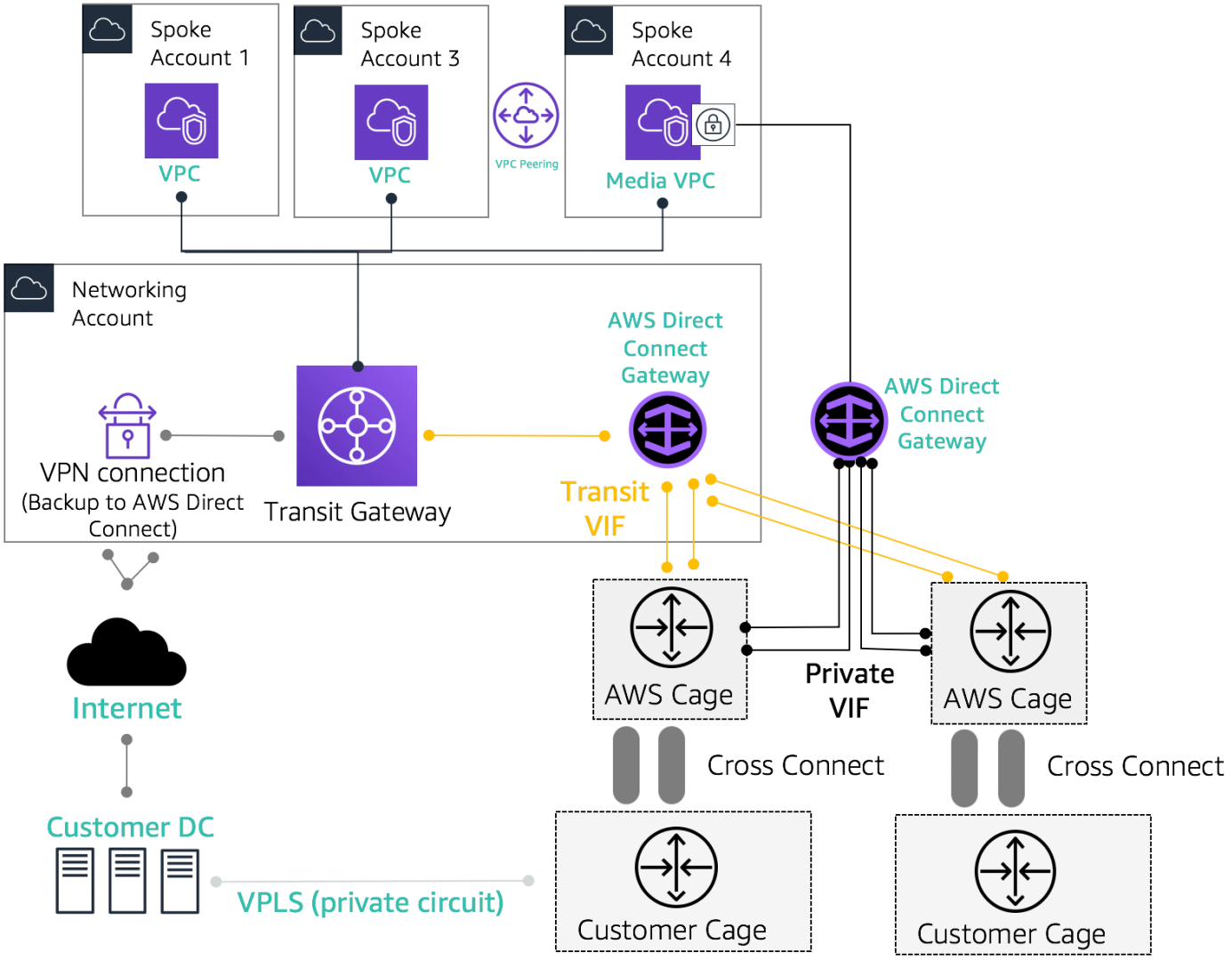
tráfico únicamente a los puntos de conexión de la VPN), le recomendamos que utilice un firewall local. Esta opción se puede utilizar para cifrar Direct Connect en la capa de red.

- Opción 5: Cree una conexión VPN a Transit Gateway AWS Direct Connect mediante una VPN con IP privada: la VPN con IP privada es una función que ofrece a los clientes la posibilidad de implementar conexiones de VPN Site-to-Site de AWS a través de Direct Connect mediante direcciones IP privadas. Con esta función, puede cifrar el tráfico entre sus redes locales y AWS a través de conexiones Direct Connect sin necesidad de direcciones IP públicas, lo que mejora la seguridad y la privacidad de la red al mismo tiempo. La VPN con IP privada se implementa sobre los VIF de Transit, por lo que le permite usar Transit Gateway para la administración centralizada de las VPC y las conexiones de los clientes a las redes locales de una manera más segura, privada y escalable.
- Opción 6: Cree túneles GRE hacia Transit Gateway a través de un VIF de tránsito: el tipo de accesorio Transit Gateway Connect admite GRE. Con Transit Gateway Connect, la infraestructura SD-WAN se puede conectar de forma nativa a AWS sin tener que configurar VPN IPsec entre los dispositivos virtuales de la red SD-WAN y Transit Gateway. Los túneles GRE se pueden establecer a través de un VIF de tránsito, con Transit Gateway Connect como tipo de conexión, lo que proporciona un mayor rendimiento de ancho de banda en comparación con una conexión VPN. Para obtener más información, consulte la entrada del blog Simplifique la conectividad SD-WAN AWS Transit Gateway con Connect.

La opción «VIF de tránsito a la puerta de enlace Direct Connect» puede parecer la mejor opción, ya que le permite consolidar toda la conectividad local de un solo punto (Transit Gateway) mediante una sola sesión de BGP por conexión de Direct Connect; sin embargo, algunos de los límites y consideraciones en torno a esta opción pueden llevarlo a utilizar VIF privados y de tránsito junto con los requisitos de conectividad de su zona de aterrizaje. Región de AWS

La siguiente figura ilustra un ejemplo de configuración en el que se usa Transit VIF como método predeterminado para conectarse a las VPC y se usa un VIF privado para un caso de uso perimetral en el que se deben transferir cantidades de datos excepcionalmente grandes de un centro de datos local a la VPC multimedia. El VIF privado se utiliza para evitar los cargos por procesamiento de datos de Transit Gateway. Como práctica recomendada, debe tener al menos dos conexiones en dos ubicaciones diferentes de Direct Connect para obtener la máxima redundancia (un total de cuatro conexiones). Cree un VIF por conexión para un total de cuatro VIF privados y cuatro VIF de tránsito. También puede crear una VPN como conectividad de respaldo a las conexiones. AWS Direct Connect

Con la opción «Crear túneles GRE a Transit Gateway a través de un VIF de tránsito», tiene la capacidad de conectar de forma nativa su infraestructura de SD-WAN con AWS. Elimina la necesidad de configurar VPN IPsec entre los dispositivos virtuales de la red SD-WAN y Transit Gateway.



Ejemplo de arquitectura de referencia para conectividad híbrida

Utilice la cuenta de servicios de red para crear recursos de Direct Connect que permitan la demarcación de los límites administrativos de la red. Las conexiones Direct Connect, las puertas de enlace Direct Connect y las pasarelas de tránsito pueden residir en una cuenta de servicios de red. Para compartir la AWS Direct Connect conectividad con tu zona de aterrizaje, simplemente comparte la Transit Gateway AWS RAM con otras cuentas.

Seguridad MACsec en las conexiones Direct Connect

Los clientes pueden usar el cifrado MAC Security Standard (MACsec) (IEEE 802.1AE) con sus conexiones Direct Connect para conexiones dedicadas de 10 Gbps y 100 Gbps en ubicaciones seleccionadas. Con esta capacidad, los clientes pueden proteger sus datos en el nivel 2 y Direct Connect proporciona point-to-point cifrado. Para habilitar la función MACsec de Direct Connect, asegúrese de que se cumplan los requisitos previos de MACsec. Dado que MACSec protege los enlaces de hop-by-hop forma específica, su dispositivo debe tener una adyacencia directa de capa 2 con nuestro dispositivo Direct Connect. Tu proveedor de última milla puede ayudarte a comprobar que tu conexión funciona con MACSec. Para obtener más información, consulte Añadir la seguridad MACsec a las conexiones de AWS Direct Connect.

AWS Direct Connect recomendaciones de resiliencia

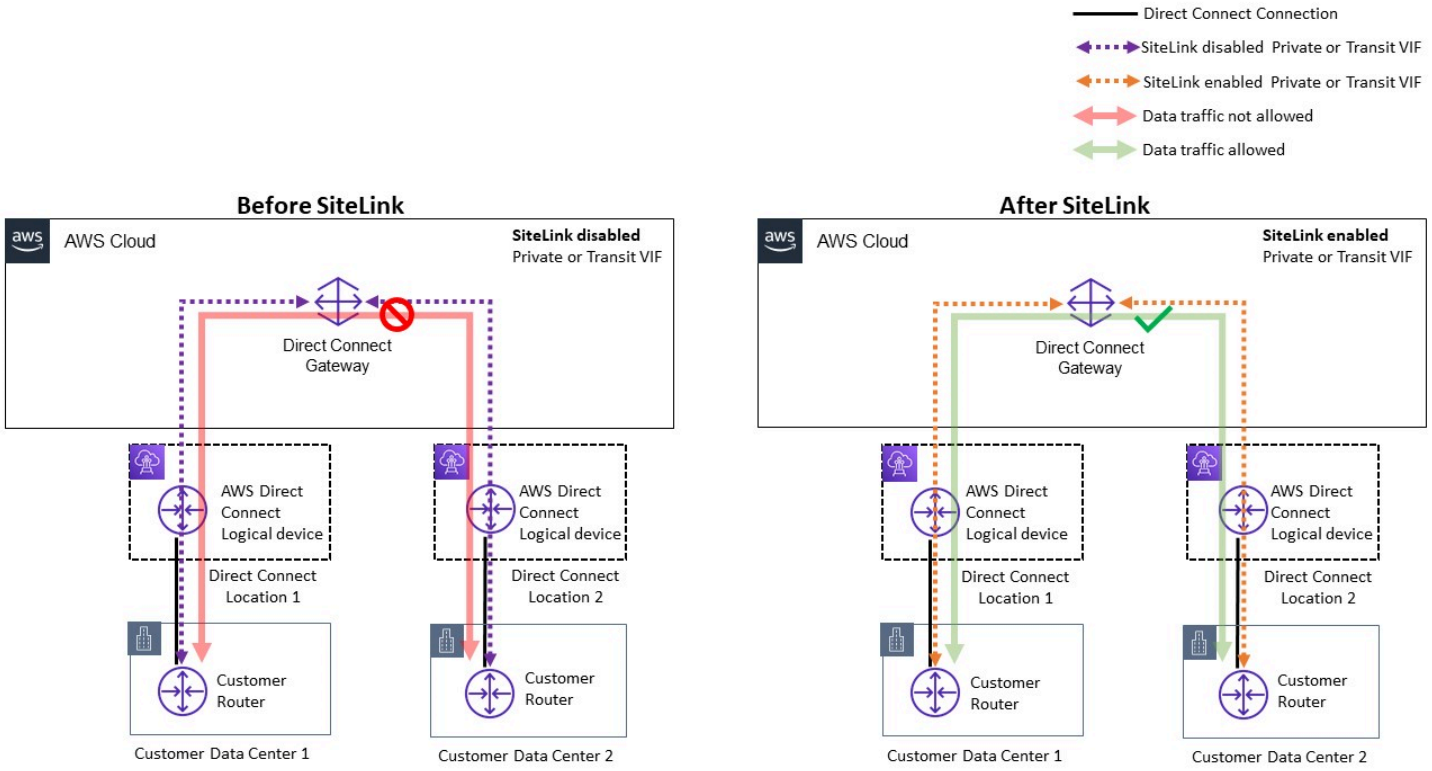
Con ello AWS Direct Connect, los clientes pueden lograr una conectividad altamente resiliente con sus VPC de Amazon y los recursos de AWS desde sus redes locales. La mejor práctica es que los clientes se conecten desde varios centros de datos para eliminar cualquier fallo en la ubicación física en un solo punto. También se recomienda que, según el tipo de cargas de trabajo, los clientes utilicen más de una conexión Direct Connect para obtener redundancia.

AWS también ofrece el kit de herramientas de AWS Direct Connect resiliencia, que proporciona a los clientes un asistente de conexión con varios modelos de redundancia para ayudarlos a determinar qué modelo funciona mejor para sus requisitos de acuerdo de nivel de servicio (SLA) y a diseñar su conectividad híbrida mediante conexiones Direct Connect en consecuencia. Para obtener más información, consulte las recomendaciones de resiliencia.AWS Direct Connect

AWS Direct Connect SiteLink

Anteriormente, la configuración de site-to-site los enlaces para las redes locales solo era posible mediante la generación directa de circuitos a través de fibra oscura u otras tecnologías, mediante VPN IPSEC o mediante el uso de proveedores de circuitos de terceros con tecnologías como MPLS o circuitos T1 antiguos. MetroEthernet Con la llegada de SiteLink, los clientes ahora pueden habilitar la site-to-site conectividad directa para su ubicación local que termina en una ubicación. AWS Direct Connect Utilice su circuito Direct Connect para proporcionar site-to-site conectividad sin tener que enrutar el tráfico a través de sus VPC, lo que evita por completo la región de AWS.

Ahora puede crear pay-as-you-go conexiones globales y confiables entre las oficinas y los centros de datos de su red global mediante el envío de datos a través de la ruta más rápida entre AWS Direct Connect ubicaciones.

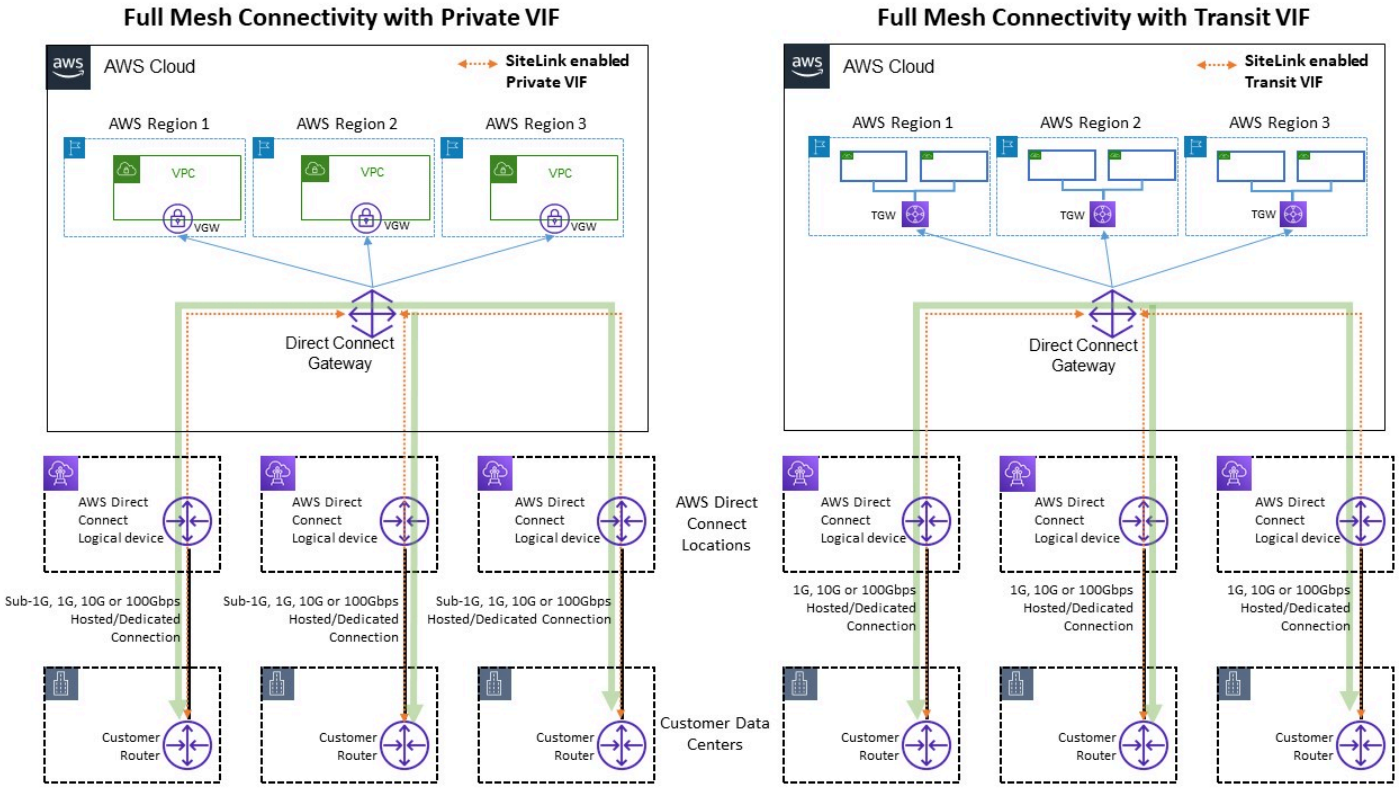


Ejemplo de arquitectura de referencia para AWS Direct Connect SiteLink

Al usarlo SiteLink, primero debe conectar sus redes locales a AWS en cualquiera de las más de 100 AWS Direct Connect ubicaciones de todo el mundo. A continuación, debe crear interfaces virtuales (VIF) en esas conexiones y activarlas. SiteLink Una vez que todas las VIF estén conectadas a la misma AWS Direct Connect puerta de enlace (DXGW), puede empezar a enviar datos entre ellas. Sus datos siguen el camino más corto entre AWS Direct Connect las ubicaciones hasta su destino, utilizando la red global de AWS, rápida, segura y confiable. No necesita disponer de ningún recurso Región de AWS para poder utilizarlo SiteLink.

De este SiteLink modo, el DXGW aprende los prefijos IPv4/IPv6 de los enrutadores a través de los VIF SiteLink habilitados, ejecuta el algoritmo de mejor ruta para el BGP, actualiza atributos como AS_Path NextHop y vuelve a anunciar estos prefijos BGP al resto de los VIF habilitados asociados a ese DXGW. SiteLink Si deshabilita SiteLink un VIF, el DXGW no anunciará los prefijos locales aprendidos sobre este VIF a los demás VIF SiteLink habilitados. Los prefijos locales de un VIF

SiteLink desactivado solo se anuncian a las asociaciones de DXGW Gateways, como las instancias de AWS Virtual Private Gateways (vGWS) o Transit Gateway (TGW) asociadas al DXGW.



Ejemplo de enlace de sitio que permite flujos de tráfico

SiteLink permite a los clientes utilizar la red global de AWS para funcionar como una conexión principal o secundaria o de respaldo entre sus ubicaciones remotas, con gran ancho de banda y baja latencia, con enrutamiento dinámico para controlar qué ubicaciones pueden comunicarse entre sí y con los recursos regionales de AWS.

Para obtener más información, consulte Introducción. AWS Direct Connect SiteLink

Salida centralizada a Internet

A medida que despliegues aplicaciones en tu entorno de múltiples cuentas, muchas de ellas requerirán acceso a Internet únicamente de forma saliente (por ejemplo, para descargar bibliotecas, parches o actualizaciones del sistema operativo). Esto se puede lograr tanto para el tráfico como para el tráfico. IPv4 IPv6 IPv4Pues esto puede lograrse mediante la traducción de direcciones de red (NAT) en forma de NAT puerta de enlace (se recomienda) o, alternativamente, mediante una NAT instancia autogestionada que se ejecute en una EC2 instancia de Amazon, como medio para el acceso a Internet de salida. Las aplicaciones internas residen en subredes privadas, mientras que NAT las EC2 NAT instancias de Gateways y Amazon residen en una subred pública.

AWSrecomienda que utilice NAT puertas de enlace porque ofrecen mejor disponibilidad y ancho de banda y requieren menos esfuerzo de su parte para administrarlas. Para obtener más información, consulte Comparación de NAT pasarelas e instancias. NAT

En cuanto al IPv6 tráfico, el tráfico de salida se puede configurar para que salga de cada uno de ellos VPC a través de una pasarela de Internet solo de salida de forma descentralizada o se puede configurar para que se envíe a una ubicación centralizada VPC mediante NAT instancias o instancias proxy. Los IPv6 patrones se describen en. Salida centralizada para IPv6

Temas

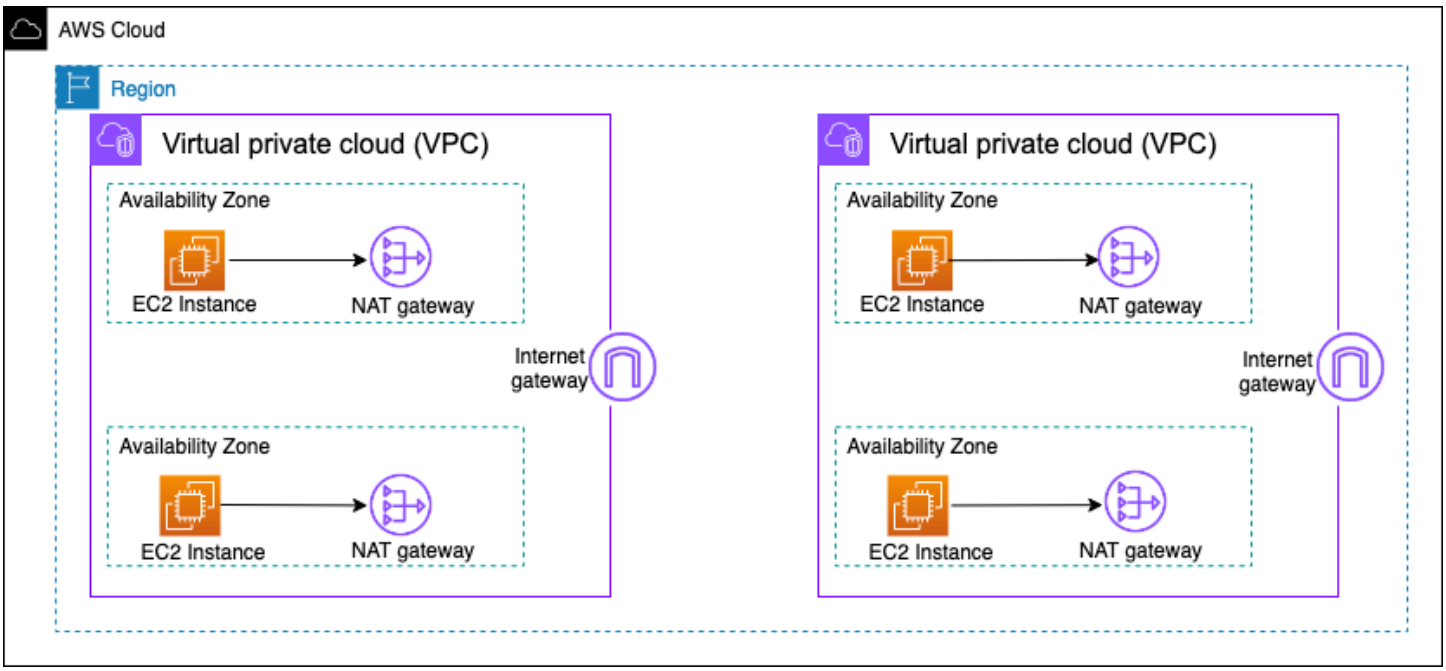
- Uso de la NAT puerta de enlace para la IPv4 salida centralizada
- Uso de la NAT puerta de AWS Network Firewall enlace con IPv4 salida centralizada
- Uso de la NAT puerta de enlace y del Load Balancer de puerta de enlace con EC2 instancias de Amazon para una salida centralizada IPv4
- Salida centralizada para IPv6

Uso de la NAT puerta de enlace para la IPv4 salida centralizada

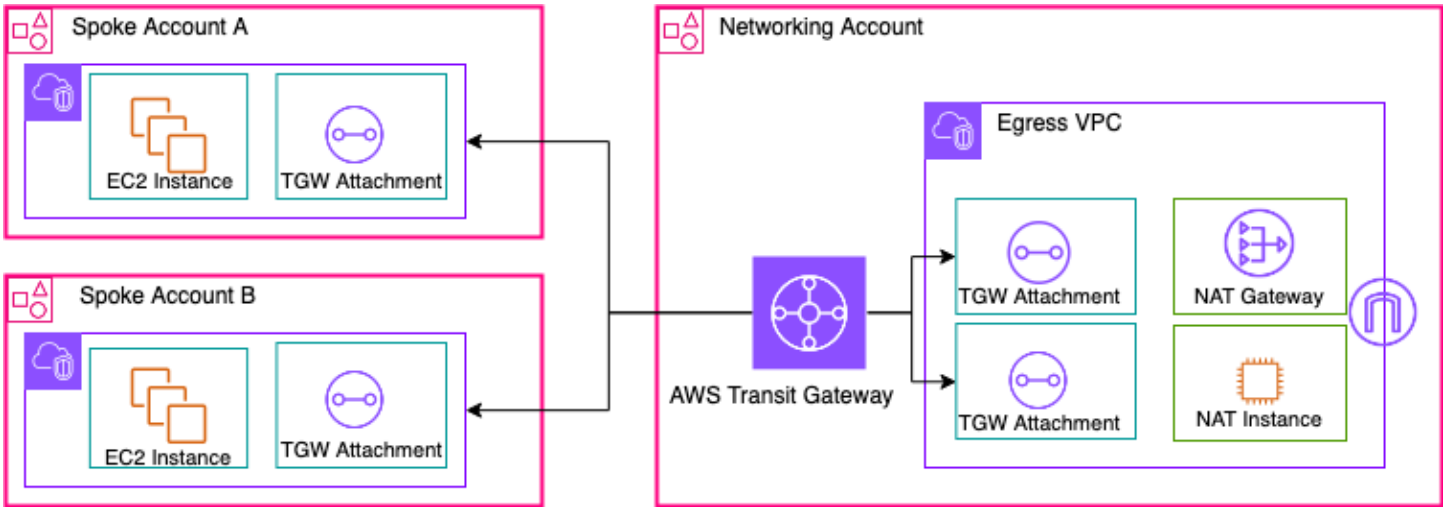
NATgateway es un servicio gestionado de traducción de direcciones de red. Implementar una NAT puerta de enlace en cada radio VPC puede resultar prohibitivo, ya que se paga una tarifa por hora por cada NAT puerta de enlace que se implemente (consulte los VPCprecios de Amazon). Centralizar NAT las pasarelas puede ser una opción viable para reducir los costes. Para centralizar, debe crear una salida independiente VPC en la cuenta de servicios de red, implementar NAT puertas de enlace en la salida y enrutar todo el tráfico de salida VPC del radio VPCs a las NAT puertas de

enlace que residen en la salida mediante Transit VPC Gateway o CloudWAN, como se muestra en la siguiente figura.

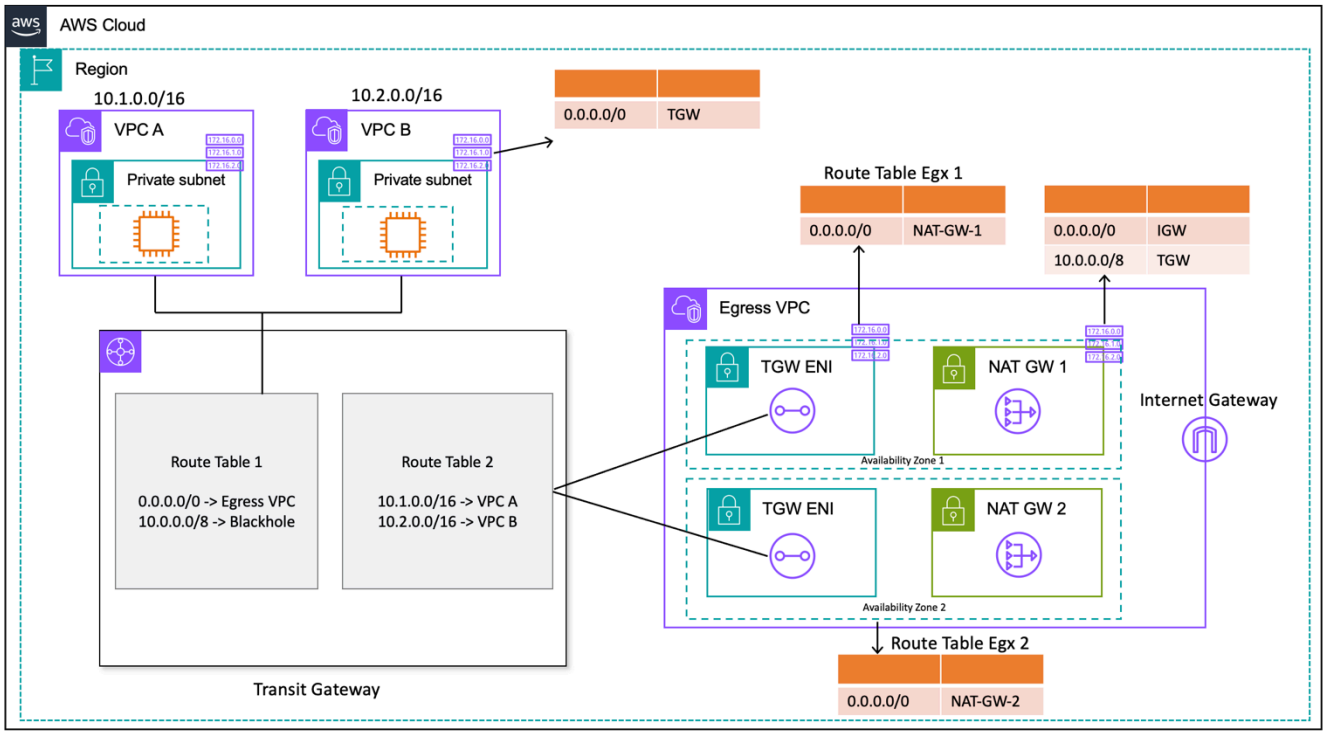
> **Note**
>
> Cuando centralizas la NAT pasarela con Transit Gateway, pagas un cargo adicional por procesamiento de datos de Transit Gateway, en comparación con el enfoque descentralizado que supone gestionar una NAT pasarela en todos los VPC países. En algunos casos extremos, cuando se envían grandes cantidades de datos a través de una NAT puerta de enlace desde una puerta de enlaceVPC, mantener el NAT local dentro VPC para evitar el cargo por procesamiento de datos de Transit Gateway podría ser una opción más rentable.



Arquitectura de NAT puerta de enlace descentralizada de alta disponibilidad



NATPasarela centralizada mediante Transit Gateway (descripción general)



Puerta de NAT enlace centralizada mediante Transit Gateway (diseño de tabla de rutas)

En esta configuración, VPC los radios adjuntos se asocian a la tabla de rutas 1 (RT1) y se propagan a la tabla de rutas 2 (RT2). Existe una ruta Blackhole para impedir que los dos se comuniquen VPCs entre sí. Si desea permitir la VPC intercomunicación, puede eliminar la entrada de la `10.0.0.0/8 -> Blackhole` ruta. RT1 Esto les permite comunicarse a través de la pasarela de tránsito. También puede propagar los radios VPC adjuntos a RT1 (o, como alternativa, puede utilizar una tabla de rutas

y asociar/propagar todo a ella), lo que permite un flujo de tráfico directo entre la Transit Gateway que utilice. VPCs

Agrega una ruta estática para dirigir todo el tráfico hacia la salidaRT1. VPC Debido a esta ruta estática, Transit Gateway envía todo el tráfico de Internet a través de su ENIs ruta de salidaVPC. Una vez en la salidaVPC, el tráfico sigue las rutas definidas en la tabla de rutas de subred donde están presentes estas Transit Gateway. ENIs Agregue una ruta en las tablas de rutas de subred que dirija todo el tráfico hacia la NAT puerta de enlace correspondiente en la misma zona de disponibilidad para minimizar el tráfico entre zonas de disponibilidad (AZ). La tabla de rutas de subred de la NAT puerta de enlace tiene la puerta de enlace a Internet (IGW) como siguiente salto. Para que el tráfico de retorno fluya hacia atrás, debe añadir una entrada de tabla de enrutamiento estática en la tabla de enrutamiento de subred de la NAT puerta de enlace que dirija todo el VPC tráfico con radio a Transit Gateway como siguiente salto.

Alta disponibilidad

Para una alta disponibilidad, debe usar más de una NAT puerta de enlace (una en cada zona de disponibilidad). Si una NAT puerta de enlace no está disponible, es posible que se interrumpa el tráfico en la zona de disponibilidad que atraviesa la puerta de enlace afectadaNAT. Si una zona de disponibilidad no está disponible, el punto final de Transit Gateway junto con la NAT puerta de enlace de esa zona de disponibilidad fallarán y todo el tráfico fluirá a través de los puntos de enlace de Transit Gateway y de la NAT puerta de enlace de la otra zona de disponibilidad.

Seguridad

Puede confiar en los grupos de seguridad de las instancias de origen, en las rutas de agujero negro de las tablas de rutas de Transit Gateway y en la red ACL de la subred en la que se encuentra la NAT puerta de enlace. Por ejemplo, los clientes pueden usar ACLs las subredes públicas de NAT Gateway para permitir o bloquear las direcciones IP de origen o destino. Como alternativa, puede usar NAT Gateway with AWS Network Firewall para la salida centralizada que se describe en la siguiente sección para cumplir con este requisito.

Escalabilidad

Una sola NAT puerta de enlace puede admitir hasta 55 000 conexiones simultáneas por dirección IP asignada a cada destino único. Puede solicitar un ajuste de cuota para permitir la asignación de hasta ocho direcciones IP, lo que permitirá establecer 440 000 conexiones simultáneas a un único puerto e IP de destino. NATLa puerta de enlace proporciona 5 Gbps de ancho de banda y se escala

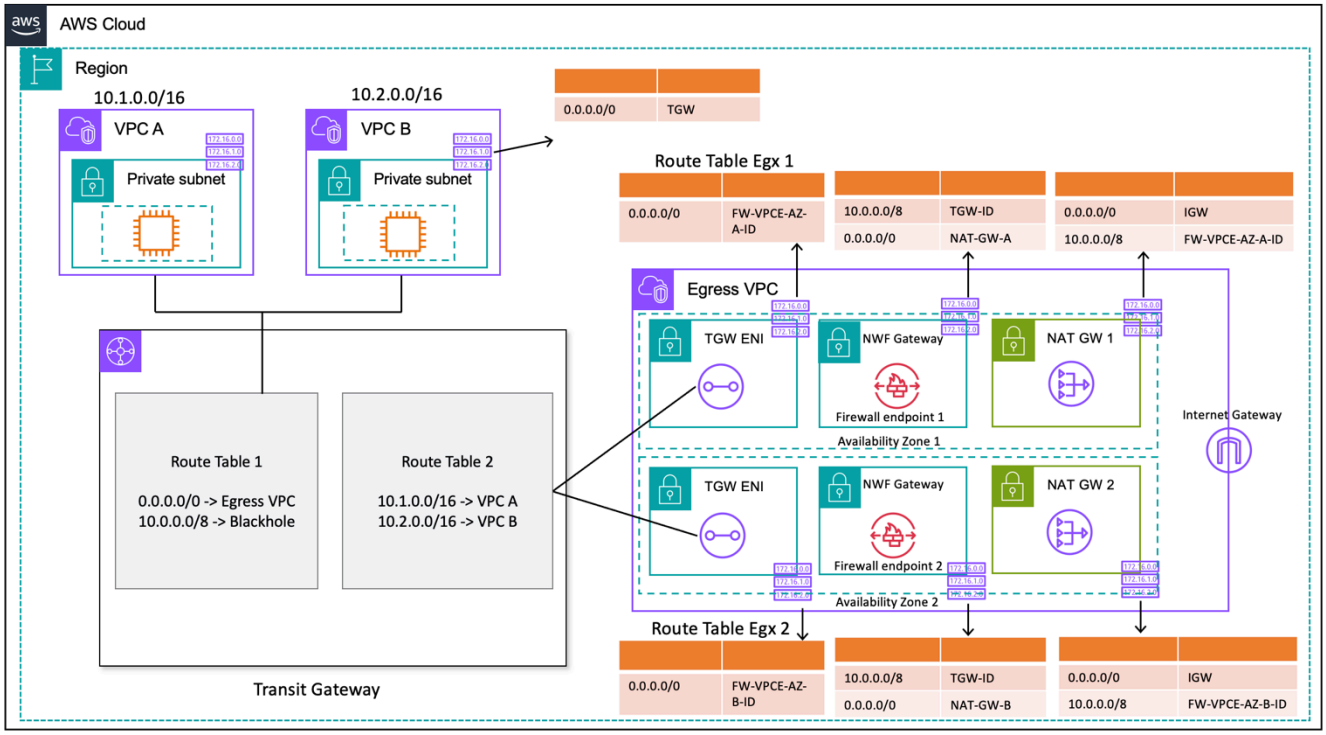
automáticamente a 100 Gbps. Por lo general, Transit Gateway no actúa como un equilibrador de carga y no distribuiría el tráfico de manera uniforme entre NAT las puertas de enlace de las múltiples zonas de disponibilidad. Si es posible, el tráfico a través de Transit Gateway permanecerá dentro de una zona de disponibilidad. Si la EC2 instancia de Amazon que inicia el tráfico se encuentra en la zona de disponibilidad 1, el tráfico saldrá de la interfaz de red elástica Transit Gateway en la misma zona de disponibilidad 1 en la salida VPC y pasará al siguiente salto en función de la tabla de enrutamiento de subred en la que reside la interfaz de red elástica. Para obtener una lista completa de reglas, consulte las NATpasarelas en la documentación de Amazon Virtual Private Cloud.

Para obtener más información, consulte la entrada del blog Cómo crear un único punto de salida de Internet a partir de varios VPCs dispositivos AWS Using Transit Gateway.

Uso de la NAT puerta de AWS Network Firewall enlace con IPv4 salida centralizada

Si desea inspeccionar y filtrar el tráfico saliente, puede incorporar AWS Network Firewall con NAT puerta de enlace en su arquitectura de salida centralizada. AWS Network Firewall es un servicio gestionado que facilita la implementación de las protecciones de red esenciales para todos sus dispositivos. VPCs Proporciona control y visibilidad del tráfico de red de nivel 3 a 7 para todo VPC su tráfico. Puede filtrar el tráfico saliente por nombre de URL dominio, dirección IP y contenido para evitar posibles pérdidas de datos, cumplir con los requisitos de conformidad y bloquear las comunicaciones de malware conocidas. AWS Network Firewall admite miles de reglas que pueden filtrar el tráfico de red destinado a direcciones IP o nombres de dominio incorrectos conocidos. También puede utilizar las reglas de Suricata como parte del AWS Network Firewall servicio importando conjuntos de IPS reglas de código abierto o creando sus propias reglas del Sistema de Prevención de Intrusiones () IPS mediante la sintaxis de reglas de Suricata. AWS Network Firewall también le permite importar reglas compatibles procedentes de socios. AWS

En la arquitectura de salida centralizada con inspección, el AWS Network Firewall punto final es un objetivo predeterminado de la tabla de enrutamiento en la tabla de enrutamiento de subred adjunta a la pasarela de tránsito para la salida. VPC El tráfico entre los radios VPCs e Internet se inspecciona AWS Network Firewall tal como se muestra en el siguiente diagrama.



Salida centralizada con una NAT puerta de enlace (AWS Network Firewall diseño de tabla de enrutamiento)

Para un modelo de implementación centralizada con Transit Gateway, se AWS recomienda implementar AWS Network Firewall puntos finales en varias zonas de disponibilidad. Debe haber un punto final de firewall en cada zona de disponibilidad en la que el cliente ejecute las cargas de trabajo, como se muestra en el diagrama anterior. Como práctica recomendada, la subred del firewall no debe contener ningún otro tráfico porque AWS Network Firewall no puede inspeccionar el tráfico procedente de las fuentes o los destinos dentro de una subred de firewall.

Al igual que en la configuración anterior, los VPC archivos adjuntos a los radios se asocian a la tabla de rutas 1 (RT1) y se propagan a la tabla de rutas 2 (). RT2 Se añade explícitamente una ruta Blackhole para impedir que ambas se comuniquen VPCs entre sí.

Siga utilizando una ruta predeterminada para dirigir todo el RT1 tráfico hacia la salida. VPC Transit Gateway reenviará todos los flujos de tráfico a una de las dos zonas de disponibilidad de la salidaVPC. Cuando el tráfico llegue a una de las Transit Gateway ENIs en la salidaVPC, tomarás una ruta predeterminada que reenviará el tráfico a uno de los AWS Network Firewall puntos finales de sus respectivas zonas de disponibilidad. AWS Network Firewall A continuación, inspeccionará el tráfico según las reglas que hayas establecido antes de reenviar el tráfico a la NAT pasarela mediante una ruta predeterminada.

Este caso no requiere el modo de dispositivo Transit Gateway, ya que no se envía tráfico entre archivos adjuntos.

> **Note**
>
> AWS Network Firewall no realiza la traducción de direcciones de red por usted, la NAT puerta de enlace gestionaría esta función una vez inspeccionada el tráfico a través del AWS Network Firewall. En este caso, no se requiere el enrutamiento de entrada, ya que el tráfico de retorno se reenviará al de forma NATGW IPs predeterminada.

Como está utilizando una Transit Gateway, aquí podemos colocar el firewall antes de la NAT puerta de enlace. En este modelo, el firewall puede ver la IP de origen detrás de la Transit Gateway.

Si lo hace de una sola vezVPC, podemos utilizar las mejoras de VPC enrutamiento que le permiten inspeccionar el tráfico entre las subredes de la mismaVPC. Para obtener más información, consulte la entrada del blog sobre modelos de implementación AWS Network Firewall con mejoras de VPC enrutamiento.

Escalabilidad

AWS Network Firewall puede aumentar o reducir automáticamente la capacidad del firewall en función de la carga de tráfico para mantener un rendimiento estable y predecible y minimizar los costos. AWS Network Firewall está diseñado para admitir decenas de miles de reglas de firewall y puede ampliarse hasta 100 Gbps por zona de disponibilidad.

Consideraciones clave

- Cada terminal de firewall puede gestionar unos 100 Gbps de tráfico. Si necesita una ráfaga mayor o un rendimiento sostenido, póngase en contacto con el servicio de asistencia. AWS
- Si decide crear una NAT puerta de enlace en su AWS cuenta junto con Network Firewall, no se cobrarán los cargos de procesamiento estándar de la NAT puerta de enlace ni de uso por hora, sino que el procesamiento por GB y las horas de uso se cobrarán por su firewall. one-to-one
- También puede considerar la posibilidad de utilizar puntos finales de firewall distribuidos AWS Firewall Manager sin Transit Gateway.
- Pruebe las reglas del firewall antes de pasarlas a producción, de forma similar a una lista de control de acceso a la red, ya que el orden importa.

- Se requieren reglas avanzadas de Suricata para una inspección más profunda. El firewall de red admite la inspección del tráfico cifrado tanto para el tráfico de entrada como para el de salida.
- La variable del grupo de `HOME_NET` reglas definió el rango de IP de origen que podía procesarse en el motor Stateful. Con un enfoque centralizado, debe agregar todos los datos adicionales VPC CIDRs adjuntos a Transit Gateway para que sean aptos para su procesamiento. Consulte la documentación de Network Firewall para obtener más información sobre la variable del grupo de `HOME_NET` reglas.
- Considere la posibilidad de implementar Transit Gateway y egress VPC en una cuenta de servicios de red independiente para segregar el acceso en función de la delegación de funciones; por ejemplo, solo los administradores de red pueden acceder a la cuenta de servicios de red.
- Para simplificar la implementación y la administración AWS Network Firewall de este modelo, se AWS Firewall Manager puede utilizar. Firewall Manager le permite administrar de forma centralizada sus diferentes firewalls al aplicar automáticamente la protección que cree en la ubicación centralizada a varias cuentas. Firewall Manager admite modelos de implementación distribuidos y centralizados para Network Firewall. Para obtener más información, consulte la entrada del blog Cómo implementar AWS Network Firewall mediante el uso AWS Firewall Manager.

Uso de la NAT puerta de enlace y del Load Balancer de puerta de enlace con EC2 instancias de Amazon para una salida centralizada IPv4

El uso de un dispositivo virtual basado en software (en AmazonEC2) desde AWS Marketplace y AWS Partner Network como punto de salida es similar a la configuración de la NAT puerta de enlace. Esta opción se puede utilizar si desea utilizar el avanzado sistema de detección y prevención de intrusiones (IPS/IDS) de nivel 7 y las capacidades de inspección profunda de paquetes que ofrecen los distintos proveedores.

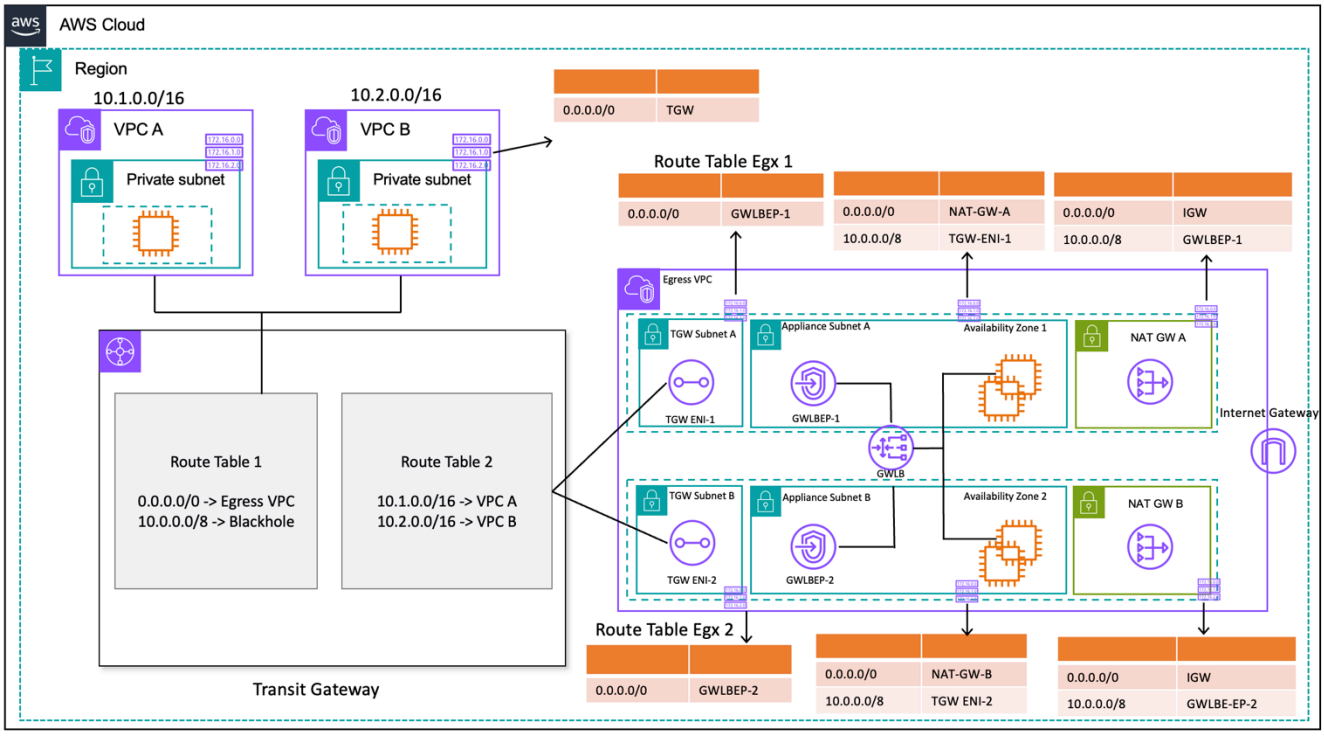
En la siguiente figura, además de la NAT puerta de enlace, se implementan dispositivos virtuales mediante EC2 instancias detrás de un Load Balancer de puerta de enlace ()GWLB. En esta configuraciónGWLB, el Gateway Load Balancer Endpoint (GWLBE), los dispositivos virtuales y NAT las pasarelas se despliegan de forma centralizada y VPC se conectan a Transit Gateway mediante un adjunto. VPC Los radios también VPCs se conectan a la Transit Gateway mediante un VPC accesorio. Como GWLBEs se trata de un objetivo enrutable, puede enrutar el tráfico que se mueve hacia y desde Transit Gateway a la flota de dispositivos virtuales que están configurados como

objetivos detrás de unGWLB. GWLBactúa como un dispositivo virtual de terceros bump-in-the-wire y lo transfiere de forma transparente a través de dispositivos virtuales de terceros y, por lo tanto, es invisible para el origen y el destino del tráfico. Por lo tanto, esta arquitectura le permite inspeccionar de forma centralizada todo el tráfico de salida que pasa por Transit Gateway.

Para obtener más información sobre cómo fluye el tráfico de las aplicaciones a Internet y viceversa VPCs a través de esta configuración, consulte Arquitectura de inspección centralizada con AWS Gateway Load Balancer y. AWS Transit Gateway

Puede activar el modo dispositivo en Transit Gateway para mantener la simetría del flujo a través de los dispositivos virtuales. Esto significa que el tráfico bidireccional se enruta a través del mismo dispositivo y de la zona de disponibilidad durante todo el flujo. Esta configuración es especialmente importante para los firewalls con estado que realizan una inspección profunda de paquetes. La activación del modo dispositivo elimina la necesidad de soluciones alternativas complejas, como la traducción de la dirección de red de origen (SNAT), para obligar al tráfico a volver al dispositivo correcto para mantener la simetría. Consulte las prácticas recomendadas para implementar Gateway Load Balancer para obtener más información.

También es posible implementar GWLB puntos finales de forma distribuida sin Transit Gateway para permitir la inspección de egreso. Obtenga más información sobre este patrón arquitectónico en la entrada del blog Introducing AWS Gateway Load Balancer: Supported architecture patterns.



Salida centralizada con Gateway Load Balancer EC2 e instancia (diseño de tabla de enrutamiento)

Alta disponibilidad

AWSrecomienda implementar los balanceadores de carga de Gateway y los dispositivos virtuales en varias zonas de disponibilidad para aumentar la disponibilidad.

Gateway Load Balancer puede realizar comprobaciones de estado para detectar errores en los dispositivos virtuales. En caso de que un dispositivo no funcione correctamente, GWLB redirige los nuevos flujos a dispositivos en buen estado. Los flujos existentes siempre se dirigen al mismo objetivo, independientemente del estado de salud del objetivo. Esto permite que la conexión se agote y se adapta a los fallos en las comprobaciones de estado debidos a los CPU picos de tensión en los aparatos. Para obtener más información, consulte la sección 4: Conozca los escenarios de error del dispositivo y la zona de disponibilidad en la entrada del blog Mejores prácticas para implementar Gateway Load Balancer. Gateway Load Balancer puede usar grupos de autoescalado como objetivos. Esta ventaja elimina la pesada tarea de administrar la disponibilidad y la escalabilidad de las flotas de dispositivos.

Ventajas

Los puntos finales Gateway Load Balancer y Gateway Load Balancer están alimentados AWS PrivateLink por, lo que permite el intercambio de tráfico a través de las VPC fronteras de forma segura sin necesidad de atravesar la Internet pública.

Gateway Load Balancer es un servicio gestionado que elimina el pesado trabajo indiferenciado de gestionar, implementar y escalar dispositivos de seguridad virtuales para que pueda centrarse en las cosas que importan. Gateway Load Balancer puede exponer la pila de firewalls como un servicio de punto final al que los clientes pueden suscribirse mediante. AWS Marketplace Esto se denomina Firewall as a Service (FWaaS); introduce una implementación simplificada y elimina la necesidad de confiar en el tráfico BGP y ECMP distribuirlo entre varias EC2 instancias de Amazon.

Consideraciones clave

- Los dispositivos deben ser compatibles con el protocolo de encapsulación Geneve para poder integrarse con él. GWLB
- Algunos dispositivos de terceros pueden admitir SNAT y superponer el enrutamiento (modo de dos brazos), lo que elimina la necesidad de crear NAT pasarelas para ahorrar costos. Sin embargo, consulte con un AWS socio de su elección antes de utilizar este modo, ya que esto depende del soporte y la implementación del proveedor.

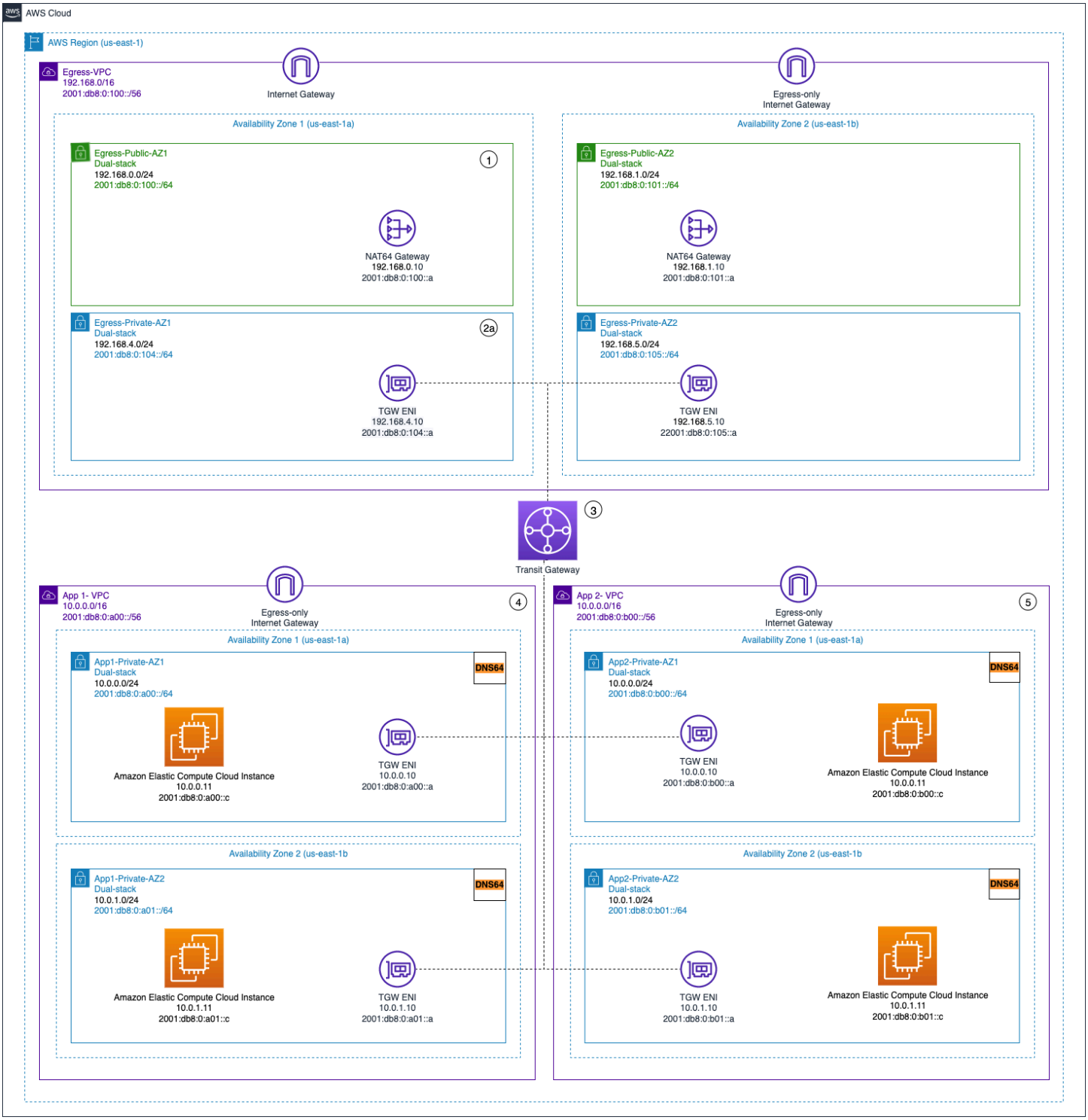
- Tome nota del tiempo de espera de GWLBinactividad. Esto puede provocar tiempos de espera de conexión en los clientes. Para evitarlo, puede ajustar los tiempos de espera a nivel de cliente, servidor, firewall y sistema operativo. Consulte la Sección 1: Ajustar los valores TCP de mantenimiento activo o de tiempo de espera para admitir TCP flujos de larga duración en la entrada del blog Prácticas recomendadas para implementar Gateway Load Balancer para obtener más información.
- GWLBEestán alimentados por, por AWS PrivateLink lo que se aplicarán cargos. AWS PrivateLink Puedes obtener más información en la página AWS PrivateLink de precios. Si utiliza el modelo centralizado con Transit Gateway, se aplicarán los cargos por procesamiento de TGW datos.
- Considere la posibilidad de implementar Transit Gateway y Egress VPC en una cuenta de servicios de red independiente para segregar el acceso en función de la delegación de funciones, ya que solo los administradores de red pueden acceder a la cuenta de servicios de red.

Salida centralizada para IPv6

Para admitir la IPv6 salida en las implementaciones de doble pila que tienen una IPv4 salida centralizada, se debe elegir uno de estos dos patrones:

- Salida centralizada con IPv4 salida descentralizada IPv6
- Salida centralizada y IPv4 salida centralizada IPv6

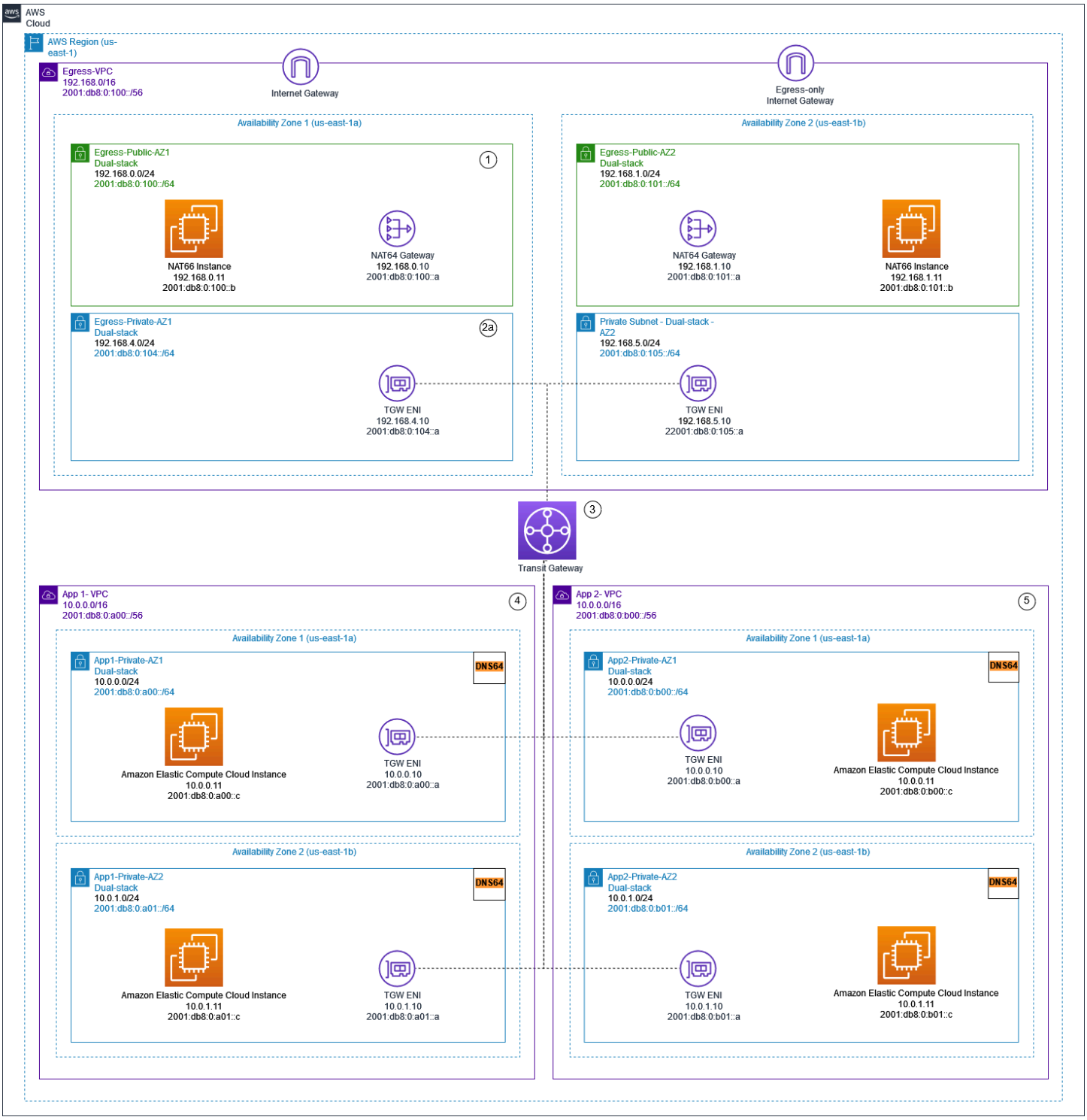
En el primer patrón, que se muestra en el siguiente diagrama, se implementan pasarelas de Internet solo de salida en cada radio. VPC Las pasarelas de Internet solo de salida son pasarelas de escalado horizontal, redundantes y de alta disponibilidad que permiten la comunicación saliente desde instancias internas. IPv6 VPC Impiden que Internet inicie conexiones con sus instancias. IPv6 Las pasarelas de Internet que solo permiten el acceso a Internet son gratuitas. En este modelo de implementación, el IPv6 tráfico sale de las pasarelas de Internet de solo salida de cada una de ellas VPC y IPv4 el tráfico fluye a través de las pasarelas centralizadas desplegadas. NAT



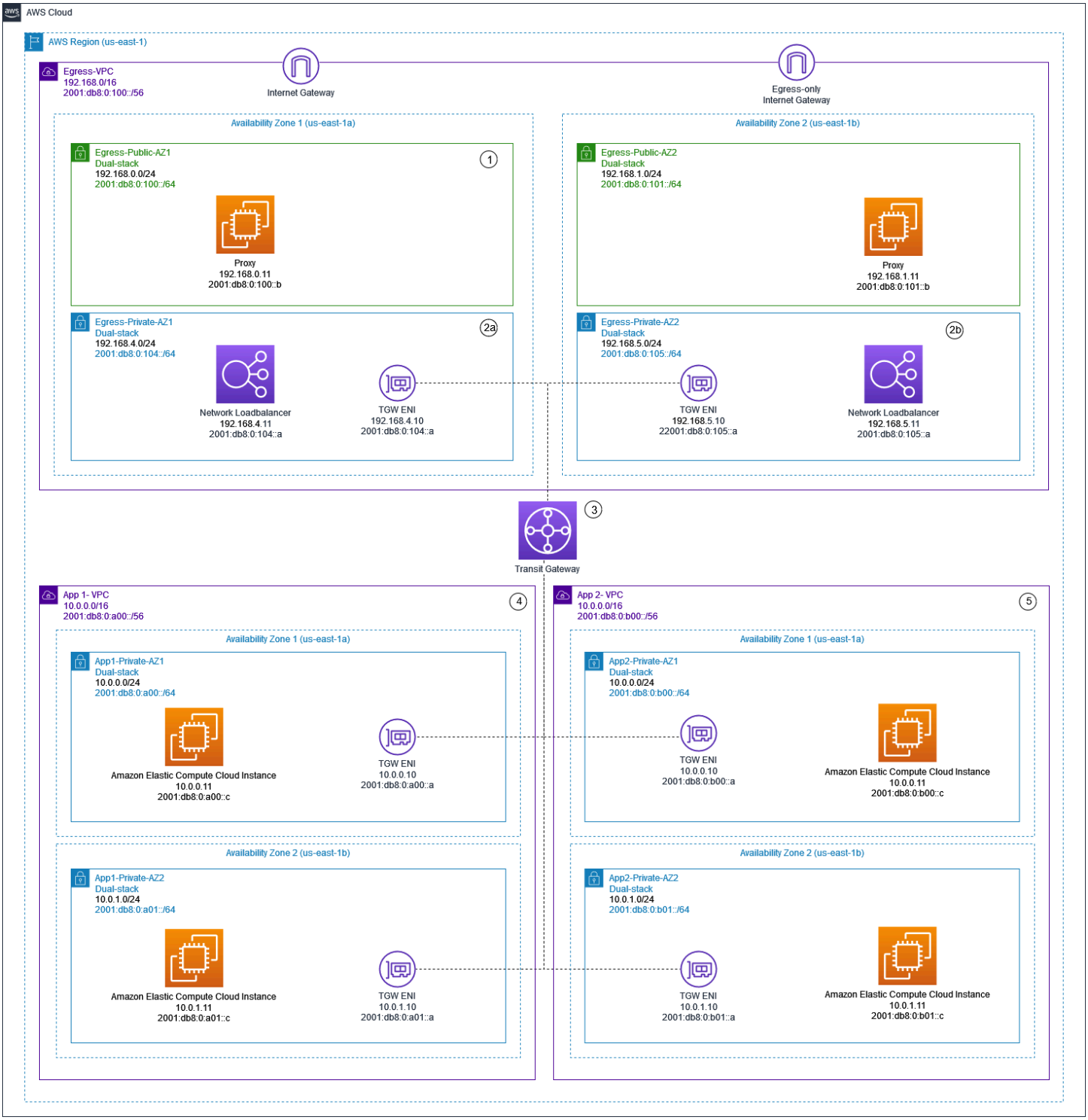
Salida centralizada y IPV4 salida solo saliente descentralizada IPv6

En el segundo patrón, que se muestra en los siguientes diagramas, el IPv6 tráfico de salida de las instancias se envía a una instancia centralizada. VPC Esto se puede lograr mediante la traducción IPv6 -to- de prefijo de IPv6 red (NPTv6) con NAT66 instancias y NAT puertas de enlace o mediante

instancias proxy y Network Load Balancer. Este patrón se aplica si se requiere una inspección centralizada del tráfico saliente y no se puede realizar en cada radio. VPC



Salida centralizada mediante IPv6 pasarelas e instancias NAT NAT66



Centralizado IPv4 y de IPv6 salida mediante instancias proxy y Network Load Balancer

IPv6En el AWS documento técnico se describen los patrones de salida centralizados. IPv6 Los patrones de IPv6 salida se analizan con más detalle en el blog Tráfico de Internet saliente

centralizado para doble pila IPv4 y IPv6 VPCs, junto con consideraciones especiales, ejemplos de soluciones y diagramas.

Seguridad de red centralizada para el tráfico de VPC a VPC y de las instalaciones a VPC

Puede haber situaciones en las que un cliente desee implementar un firewall/IP/IDS de capa 3 a 7 en su entorno de múltiples cuentas para inspeccionar los flujos de tráfico entre las VPC (tráfico este-oeste) o entre un centro de datos local y una VPC (tráfico norte-sur). Esto se puede lograr de diferentes maneras, según el caso de uso y los requisitos. Por ejemplo, puede incorporar Gateway Load Balancer, Network Firewall, Transit VPC o utilizar arquitecturas centralizadas con Transit Gateways. Estos escenarios se analizan en la siguiente sección.

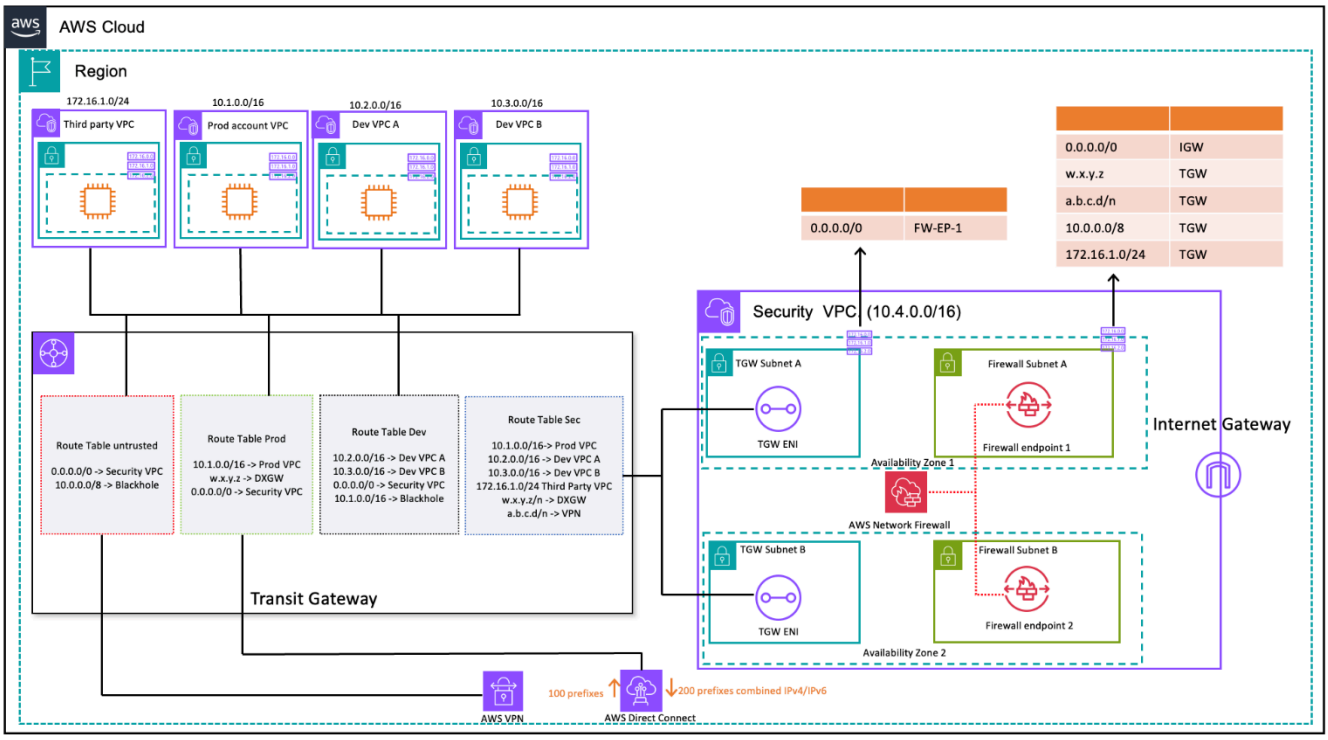
Consideraciones sobre el uso de un modelo de inspección de seguridad de red centralizado

Para reducir los costes, debes ser selectivo en cuanto al tráfico que pasa por tu Load Balancer AWS Network Firewall o por Gateway Load Balancer. Una forma de proceder es definir las zonas de seguridad e inspeccionar el tráfico entre las zonas que no son de confianza. Una zona que no sea de confianza puede ser un sitio remoto gestionado por un tercero, una VPC de un proveedor que no controle o no confíe, o una VPC sandbox/de desarrollo, que tiene reglas de seguridad más relajadas en comparación con el resto de su entorno. En este ejemplo, hay cuatro zonas:

- Zona no confiable: se aplica a cualquier tráfico que provenga de la «VPN a un sitio remoto que no sea de confianza» o de la VPC de un proveedor externo.
- Zona de producción (producción): contiene el tráfico de la VPC de producción y del centro de distribución del cliente local.
- Zona de desarrollo (desarrollo): contiene el tráfico de las dos VPC de desarrollo.
- Zona de seguridad (sec): contiene nuestros componentes de firewall Network Firewall o Gateway Load Balancer.

Esta configuración tiene cuatro zonas de seguridad, pero es posible que tengas más. Puede usar varias tablas de rutas y rutas con agujeros negros para lograr un aislamiento de seguridad y un flujo de tráfico óptimo. La elección del conjunto correcto de zonas depende de la estrategia general de diseño de la zona de aterrizaje (estructura contable, diseño de VPC). Puede disponer de zonas para permitir el aislamiento entre las unidades de negocio (BUs), las aplicaciones, los entornos, etc.

Si desea inspeccionar y filtrar su tráfico de VPC a VPC, entre zonas y tráfico de VPC local, puede incorporar Transit AWS Network Firewall Gateway en su arquitectura centralizada. Al disponer del hub-and-spoke modelo de, se puede lograr un modelo de despliegue AWS Transit Gateway centralizado. AWS Network Firewall Se implementa en una VPC de seguridad independiente. Una VPC de seguridad independiente proporciona un enfoque simplificado y central para gestionar la inspección. Esta arquitectura de VPC proporciona visibilidad de la IP AWS Network Firewall de origen y destino. Se conservan las IP de origen y destino. Esta VPC de seguridad consta de dos subredes en cada zona de disponibilidad: una subred está dedicada a la AWS Transit Gateway conexión y la otra está dedicada al punto final del firewall. Las subredes de esta VPC solo deben AWS Network Firewall contener puntos finales, ya que Network Firewall no puede inspeccionar el tráfico en las mismas subredes que los puntos finales. Cuando utiliza Network Firewall para inspeccionar el tráfico de forma centralizada, puede realizar una inspección profunda de paquetes (DPI) en el tráfico de entrada. El patrón de DPI se amplía en la sección de inspección entrante centralizada de este documento.



Inspección del tráfico de VPC a VPC y de las instalaciones a VPC mediante Transit Gateway y (diseño de tabla de rutas) AWS Network Firewall

En la arquitectura centralizada con inspección, las subredes de Transit Gateway requieren una tabla de enrutamiento de VPC independiente para garantizar que el tráfico se reenvíe al punto final del firewall dentro de la misma zona de disponibilidad. Para el tráfico de retorno, se configura una tabla de enrutamiento de VPC única que contiene una ruta predeterminada hacia Transit Gateway. El

tráfico se devuelve a AWS Transit Gateway la misma zona de disponibilidad una vez inspeccionado por AWS Network Firewall. Esto es posible gracias a la función de modo dispositivo de la Transit Gateway. La función de modo dispositivo de Transit Gateway también ayuda AWS Network Firewall a disponer de una capacidad de inspección de tráfico con estado dentro de la VPC de seguridad.

Con el modo dispositivo activado en una pasarela de tránsito, selecciona una única interfaz de red mediante el algoritmo de hash de flujo durante toda la vida útil de la conexión. La puerta de enlace de tránsito utiliza la misma interfaz de red para el tráfico de retorno. Esto garantiza que el tráfico bidireccional se enrute simétricamente: se enruta a través de la misma zona de disponibilidad en la conexión de VPC durante el tiempo de vida del flujo. Para obtener más información sobre el modo de dispositivo, consulte Dispositivos con estado y modo de dispositivo en la documentación de Amazon VPC.

Para conocer las diferentes opciones de implementación de una VPC de seguridad con AWS Network Firewall Transit Gateway, consulte la entrada del blog sobre los modelos de implementación de AWS Network Firewall.

Uso de Gateway Load Balancer con Transit Gateway para una seguridad de red centralizada

A menudo, los clientes desean incorporar dispositivos virtuales para gestionar el filtrado del tráfico y proporcionar capacidades de inspección de seguridad. En estos casos de uso, pueden integrar Gateway Load Balancer, dispositivos virtuales y Transit Gateway para implementar una arquitectura centralizada que inspeccione el tráfico de VPC a VPC y VPC. to-on-premises

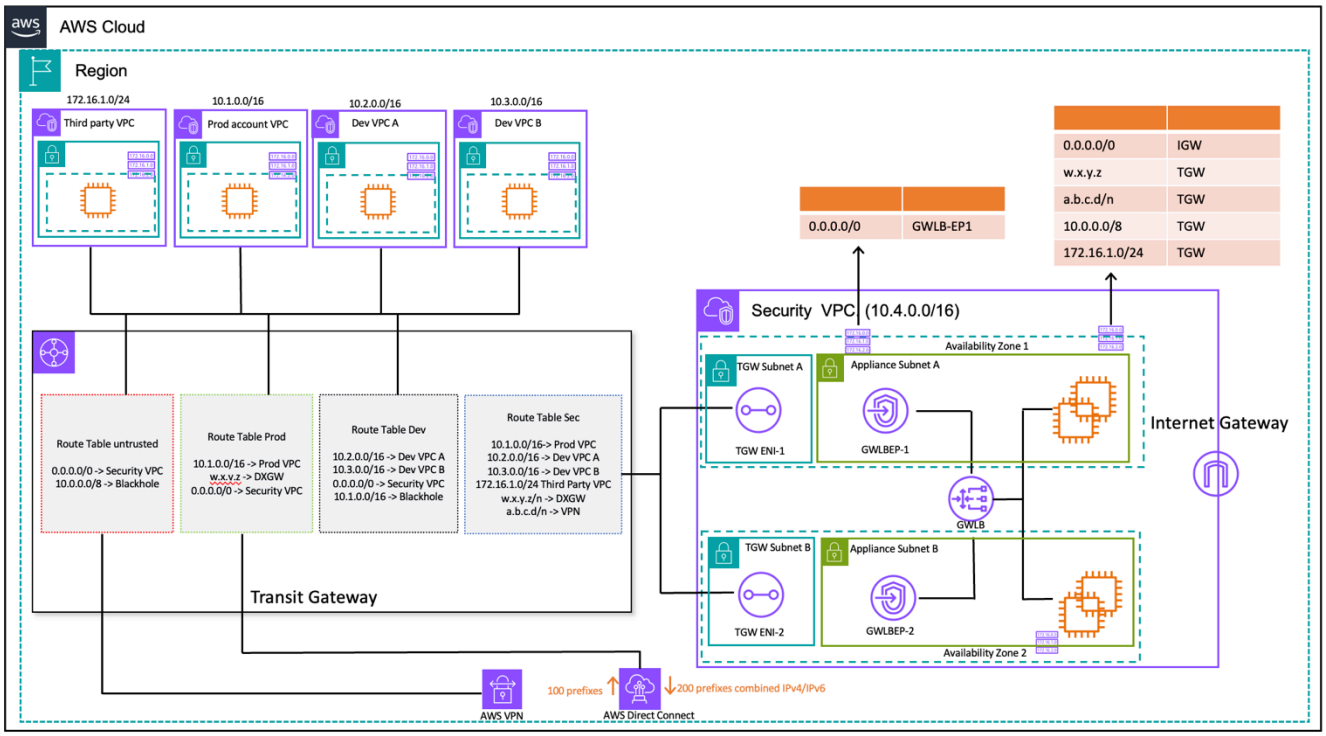
Gateway Load Balancer se implementa en una VPC de seguridad independiente junto con los dispositivos virtuales. Los dispositivos virtuales que inspeccionarán el tráfico se configuran como objetivos detrás del Gateway Load Balancer. Como los puntos finales del Gateway Load Balancer son un objetivo enrutable, los clientes pueden enrutar el tráfico que se mueve hacia y desde Transit Gateway a la flota de dispositivos virtuales. Para garantizar la simetría del flujo, el modo dispositivo está activado en la Transit Gateway.

Cada VPC radial tiene una tabla de enrutamiento asociada a la Transit Gateway, que tiene la ruta predeterminada al adjunto de la VPC de seguridad como siguiente salto.

La VPC de seguridad centralizada consta de subredes de dispositivos en cada zona de disponibilidad, que tienen los puntos finales del Gateway Load Balancer y los dispositivos

virtuales. También tiene subredes para los archivos adjuntos de Transit Gateway en cada zona de disponibilidad, como se muestra en la siguiente figura.

Para obtener más información sobre la inspección de seguridad centralizada con Gateway Load Balancer y Transit Gateway, consulte la arquitectura de inspección centralizada con AWS Gateway Load Balancer AWS Transit Gateway y la entrada del blog.



on-premises-toInspección del tráfico de VPC a VPC y -VPC mediante Transit Gateway y AWS Gateway Load Balancer (diseño de tabla de rutas)

Consideraciones clave para un AWS Network FirewallAWS Gateway Load Balancer

- El modo electrodoméstico debe estar activado en la Transit Gateway al realizar una inspección de este a oeste.
- Puede implementar el mismo modelo para inspeccionar el tráfico a otros Regiones de AWS mediante el peering interregional de AWS Transit Gateway.
- De forma predeterminada, cada Load Balancer de puerta de enlace implementado en una zona de disponibilidad distribuye el tráfico únicamente entre los destinos registrados dentro de la misma zona de disponibilidad. Esto se denomina afinidad entre zonas de disponibilidad. Si habilita el equilibrio de carga entre zonas, Gateway Load Balancer distribuye el tráfico entre todos los

destinos registrados y en buen estado en todas las zonas de disponibilidad habilitadas. Si todos los destinos de todas las zonas de disponibilidad están en mal estado, Gateway Load Balancer no se abrirá. Consulte la sección 4: Conozca los escenarios de error del dispositivo y de la zona de disponibilidad en la entrada del blog Prácticas recomendadas para implementar Gateway Load Balancer para obtener más información.

- Para la implementación en varias regiones, se AWS recomienda configurar VPC de inspección independientes en las regiones locales respectivas para evitar las dependencias interregionales y reducir los costos de transferencia de datos asociados. Debe inspeccionar el tráfico en la región local en lugar de centralizar la inspección en otra región.
- El costo de ejecutar un par adicional de alta disponibilidad (HA) basado en EC2 en implementaciones multirregionales puede aumentar. Para obtener más información, consulta la entrada del blog Best practices for deploy Gateway Load Balancer.

AWS Network Firewall frente a Gateway Load Balancer

Tabla 2: AWS Network Firewall frente a Gateway Load Balancer

Criterios	AWS Network Firewall	Balanceador de carga de gateway
Caso de uso	Firewall de red gestionado y funcional con capacidad de servicio de detección y prevención de intrusiones compatible con Suricata.	Servicio gestionado que facilita la implementación, el escalado y la gestión de dispositivos virtuales de terceros
Complejidad	AWS servicio gestionado. AWS gestiona la escalabilidad y la disponibilidad del servicio.	Servicio gestionado de AWS. AWS gestionará la escalabilidad y la disponibilidad del servicio Gateway Load Balancer. El cliente es responsable de administrar el escalado y la disponibilidad de los dispositivos virtuales detrás de Gateway Load Balancer.

Criterios	AWS Network Firewall	Balanceador de carga de gateway
Escala	AWS Network Firewall los puntos finales funcionan con. AWS PrivateLink Network Firewall admite hasta 100 Gbps de tráfico de red por punto final de firewall.	Los puntos finales Gateway Load Balancer admiten un ancho de banda máximo de hasta 100 Gbps por punto final
Costo	AWS Network Firewall coste del terminal más gastos de procesamiento de datos	Gateway Load Balancer + puntos finales de Gateway Load Balancer + dispositivos virtuales + cargos por procesamiento de datos

Inspección de entrada centralizada

Las aplicaciones orientadas a Internet, por su naturaleza, tienen una mayor superficie de ataque y están expuestas a categorías de amenazas a las que la mayoría de los demás tipos de aplicaciones no tienen que enfrentarse. Contar con la protección necesaria contra los ataques a este tipo de aplicaciones y minimizar la superficie de impacto son elementos fundamentales de cualquier estrategia de seguridad.

A medida que despliegue aplicaciones en su zona de destino, los usuarios accederán a muchas de ellas a través de la Internet pública (por ejemplo, a través de una red de entrega de contenido (CDN) o a través de una aplicación web pública), mediante un balanceador de carga público, una puerta de enlace de API o directamente a través de una puerta de enlace de Internet. En este caso, puede proteger sus cargas de trabajo y aplicaciones con AWS Web Application Firewall (AWS WAF) para la inspección de aplicaciones entrantes o, alternativamente, con IDS/IPS Inbound Inspection con Gateway Load Balancer o. AWS Network Firewall

A medida que vaya implementando aplicaciones en su zona de destino, es posible que tenga que inspeccionar el tráfico entrante de Internet. Puede lograrlo de varias maneras: mediante arquitecturas de inspección distribuidas, centralizadas o combinadas, mediante Gateway Load Balancer que ejecuta dispositivos de firewall de terceros AWS Network Firewall o con capacidades avanzadas de DPI e IDS/IPS mediante el uso de reglas de Suricata de código abierto. En esta sección, se describe tanto el Load Balancer de puertas de enlace como AWS Network Firewall las implementaciones centralizadas, que utilizan la función AWS Transit Gateway de concentrador central para el enrutamiento del tráfico.

AWS WAF y AWS Firewall Manager para inspeccionar el tráfico entrante de Internet

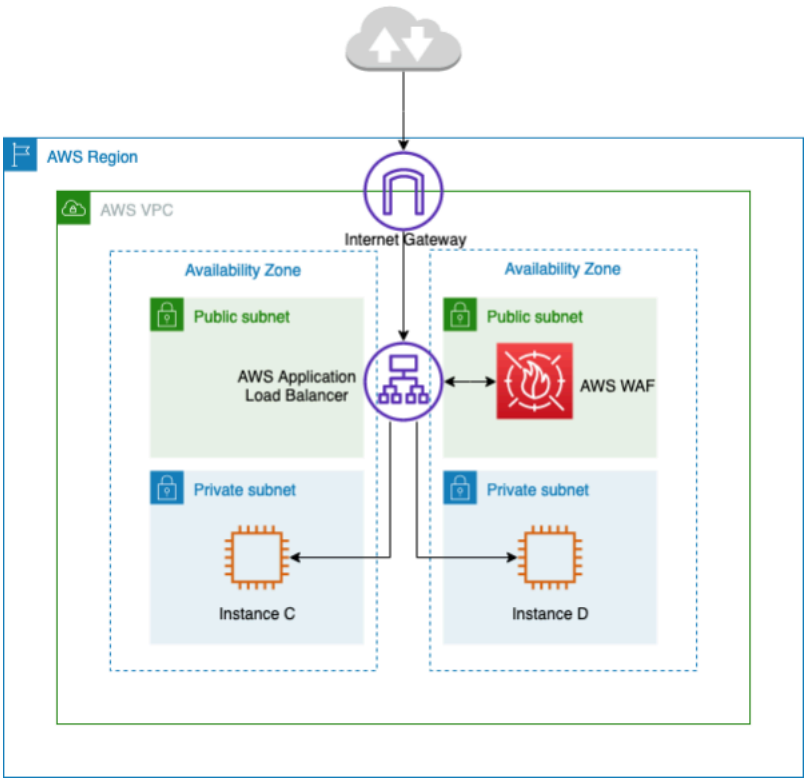
AWS WAF es un firewall de aplicaciones web que ayuda a proteger sus aplicaciones web o API contra los exploits web y los bots más comunes que pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos. AWS WAF le permite controlar la forma en que el tráfico llega a sus aplicaciones, ya que le permite crear reglas de seguridad que controlan el tráfico de bots y bloquean los patrones de ataque más comunes, como la inyección de SQL o los scripts entre sitios (XSS). También puede personalizar las reglas que filtran patrones de tráfico específicos.

Puede implementarlo AWS WAF en Amazon CloudFront como parte de su solución de CDN, el Application Load Balancer que se encuentra en sus servidores web, Amazon API Gateway para sus API REST AWS AppSync o para sus API de GraphQL.

Una vez implementadas AWS WAF, puede crear sus propias reglas de filtrado de tráfico mediante el generador visual de reglas, el código en JSON, las reglas administradas por ellas AWS o puede suscribirse a reglas de terceros desde. AWS Marketplace Estas reglas pueden filtrar el tráfico no deseado al evaluar el tráfico en función de los patrones especificados. También puedes usar Amazon CloudWatch para monitorear las estadísticas y el registro del tráfico entrante.

Para una administración centralizada de todas sus cuentas y aplicaciones AWS Organizations, puede utilizar AWS Firewall Manager. AWS Firewall Manager es un servicio de administración de seguridad que le permite configurar y administrar de forma centralizada las reglas del firewall. A medida que se crean nuevas aplicaciones, AWS Firewall Manager facilita el cumplimiento de las nuevas aplicaciones y recursos mediante la aplicación de un conjunto común de reglas de seguridad.

Con AWS Firewall Managerél, puede implementar fácilmente AWS WAF reglas para sus balanceadores de carga de aplicaciones, instancias de API Gateway y CloudFront distribuciones de Amazon. AWS Firewall Manager se integra con Reglas administradas de AWS for AWS WAF, lo que le proporciona una forma sencilla de implementar AWS WAF reglas preconfiguradas y seleccionadas en sus aplicaciones. Para obtener más información sobre la gestión centralizada AWS WAF con AWS Firewall Manager, consulte Gestión centralizada AWS WAF (API v2) y Reglas administradas de AWS escalabilidad con AWS Firewall Manager.



Inspección centralizada del tráfico entrante mediante AWS WAF

En la arquitectura anterior, las aplicaciones se ejecutan en instancias de Amazon EC2 en varias zonas de disponibilidad de las subredes privadas. Hay un Application Load Balancer (ALB) orientado al público que se implementa delante de las instancias de Amazon EC2, que equilibra la carga de las solicitudes entre los diferentes destinos. AWS WAF Está asociado al ALB.

Ventajas

- Con AWS WAF Bot Control, obtiene visibilidad y control sobre el tráfico de bots común y generalizado que llega a sus aplicaciones.
- Con Managed Rules for AWS WAF, puede comenzar rápidamente y proteger su aplicación web o sus API contra las amenazas más comunes. Puede seleccionar entre muchos tipos de reglas, como las que abordan cuestiones como los 10 principales riesgos de seguridad del Proyecto Abierto de Seguridad de Aplicaciones Web (OWASP), las amenazas específicas de los sistemas de gestión de contenido (CMS), como Joomla, WordPress o incluso las emergentes vulnerabilidades y exposiciones comunes (CVE). Las reglas administradas se actualizan automáticamente a medida que surgen nuevos problemas, para que pueda dedicar más tiempo a crear aplicaciones.

- AWS WAF es un servicio gestionado y en esta arquitectura no se necesita ningún dispositivo para su inspección. Además, proporciona registros prácticamente en tiempo real a través de Amazon Data Firehose. AWS WAF proporciona visibilidad casi en tiempo real de tu tráfico web, que puedes utilizar para crear nuevas reglas o alertas en Amazon. CloudWatch

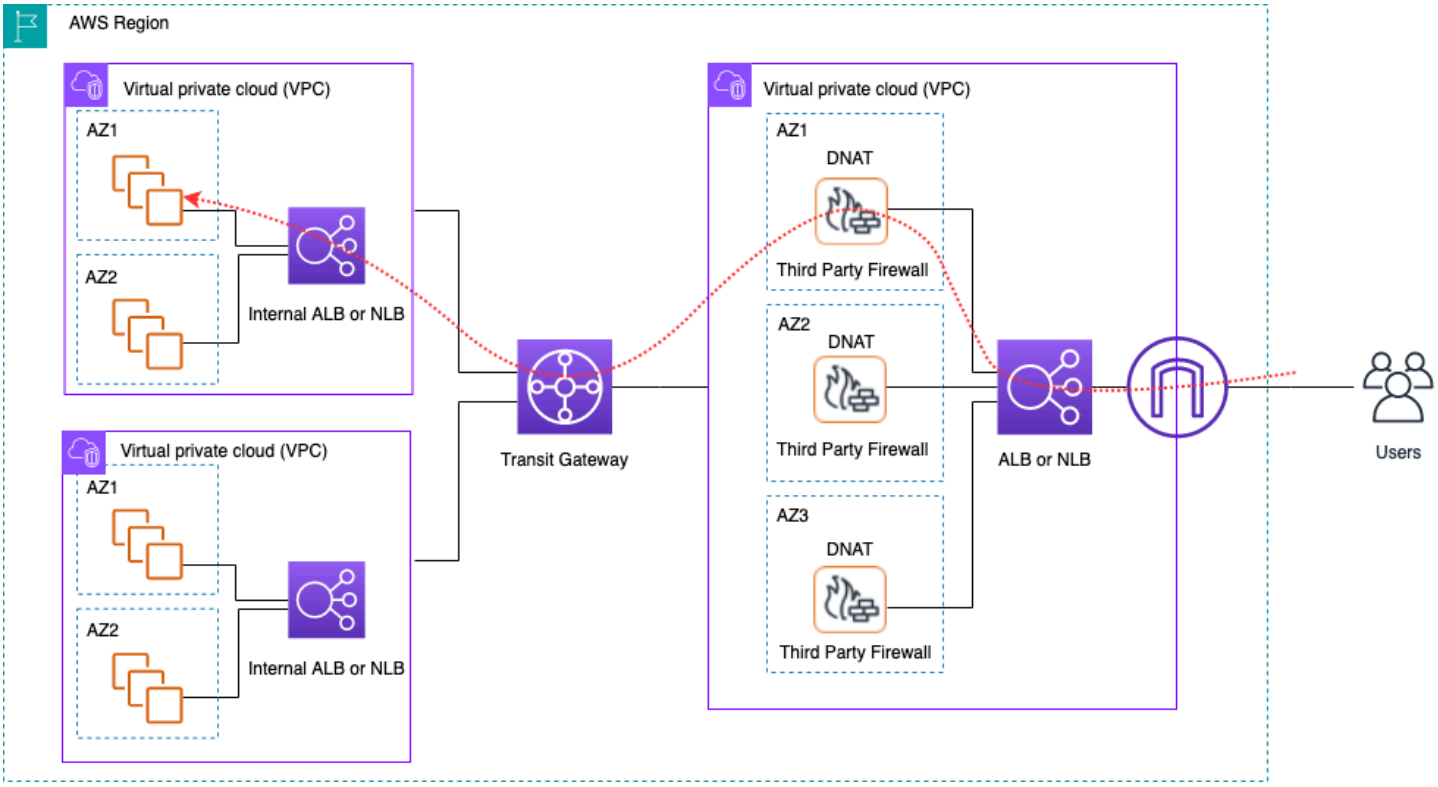
Consideraciones clave

- Esta arquitectura es la más adecuada para la inspección de encabezados HTTP y las inspecciones distribuidas, ya que AWS WAF está integrada en una API Gateway por ALB, una CloudFront distribución y una API Gateway. AWS WAF no registra el cuerpo de la solicitud.
- Es posible que el tráfico que se dirige a un segundo conjunto de ALB (si está presente) no sea inspeccionado por la misma AWS WAF instancia, ya que se haría una nueva solicitud al segundo conjunto de ALB.

Inspección centralizada de entradas con dispositivos de terceros

En este patrón de diseño arquitectónico, se implementan dispositivos de firewall de terceros en Amazon EC2 en varias zonas de disponibilidad detrás de un Elastic Load Balancer (ELB), como un balanceador de carga de aplicaciones o redes, en una VPC de inspección independiente.

La VPC de inspección, junto con otras VPC Spoke, se conectan entre sí a través de una Transit Gateway como accesorios de VPC. Las aplicaciones de los Spoke VPC están gestionadas por un ELB interno, que puede ser ALB o NLB, según el tipo de aplicación. Los clientes a través de Internet se conectan al DNS del ELB externo en la VPC de inspección, que enruta el tráfico a uno de los dispositivos de firewall. El firewall inspecciona el tráfico y, a continuación, lo enruta a la VPC Spoke a través de Transit Gateway mediante el DNS del ELB interno, como se muestra en la siguiente figura. Para obtener más información sobre la inspección de seguridad entrante con dispositivos de terceros, consulte la entrada del blog Cómo integrar dispositivos de firewall de terceros en un entorno de AWS.



Inspección centralizada del tráfico de entrada mediante dispositivos de terceros y ELB

Ventajas

- Esta arquitectura puede admitir cualquier tipo de aplicación de inspección y las funciones de inspección avanzada que ofrecen los dispositivos de firewall de terceros.
- Este patrón admite el enrutamiento basado en DNS desde los dispositivos de firewall a las VPC con radios, lo que permite que las aplicaciones de las VPC Spoke se escalen de forma independiente detrás de un ELB.
- Puede usar Auto Scaling con el ELB para escalar los dispositivos de firewall de la VPC de inspección.

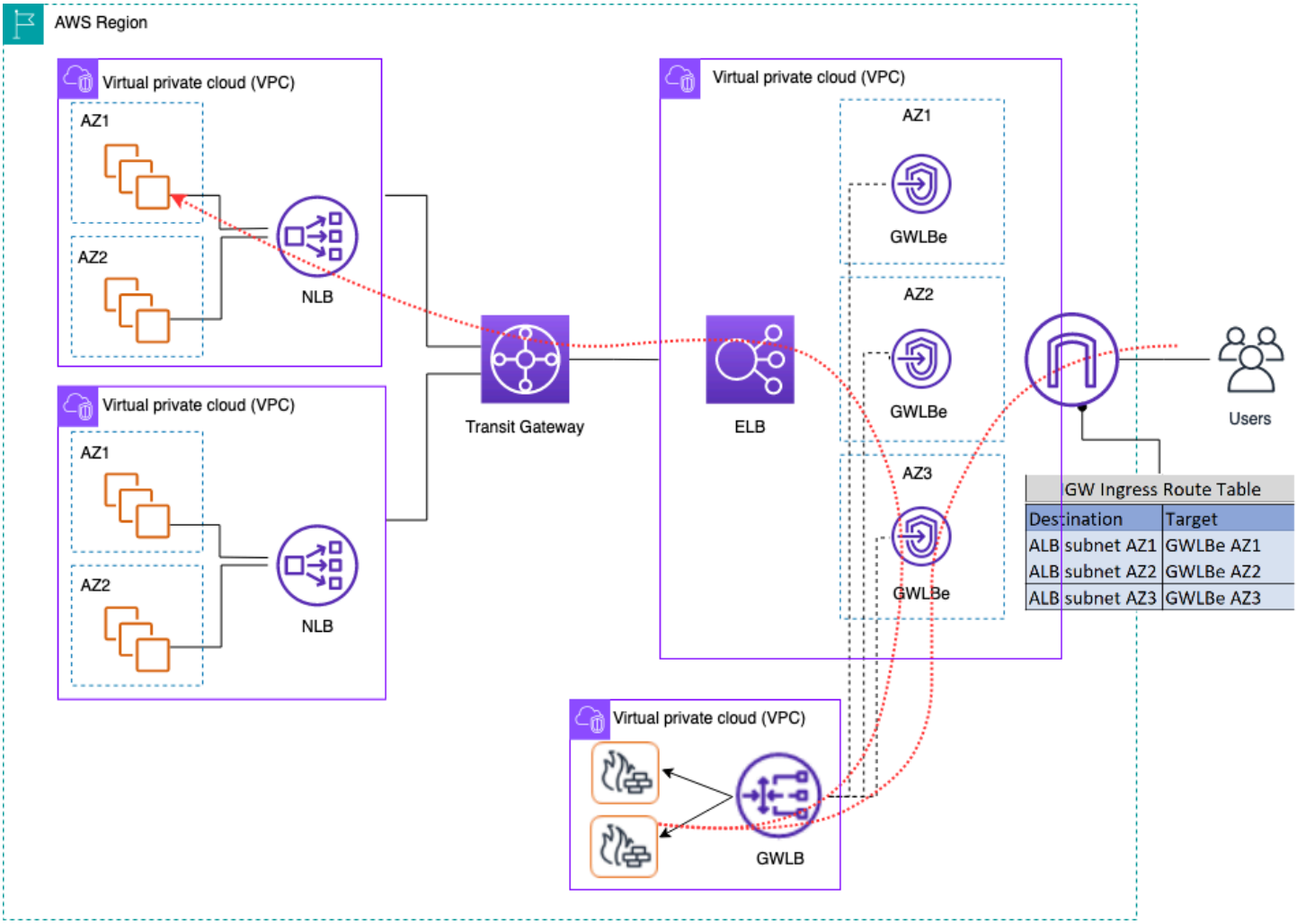
Consideraciones clave

- Para obtener una alta disponibilidad, debe implementar varios dispositivos de firewall en las zonas de disponibilidad.
- El firewall debe configurarse con la NAT de origen y ejecutarla para mantener la simetría del flujo, lo que significa que la aplicación no podrá ver la dirección IP del cliente.

- Considere la posibilidad de implementar Transit Gateway y Inspection VPC en la cuenta de servicios de red.
- Coste adicional de licencias y soporte de firewalls de proveedores externos. Los cargos de Amazon EC2 dependen del tipo de instancia.

Inspección del tráfico entrante de Internet mediante dispositivos de firewall con Gateway Load Balancer

Los clientes utilizan firewalls de última generación (NGFW) y sistemas de prevención de intrusiones (IPS) de terceros como parte de su estrategia de defensa exhaustiva. Tradicionalmente, suelen ser dispositivos virtuales o de hardware o software dedicados. Puede usar Gateway Load Balancer para escalar estos dispositivos virtuales de forma horizontal e inspeccionar el tráfico desde y hacia la VPC, como se muestra en la siguiente figura.



Inspección centralizada del tráfico de entrada mediante dispositivos de firewall con Gateway Load Balancer

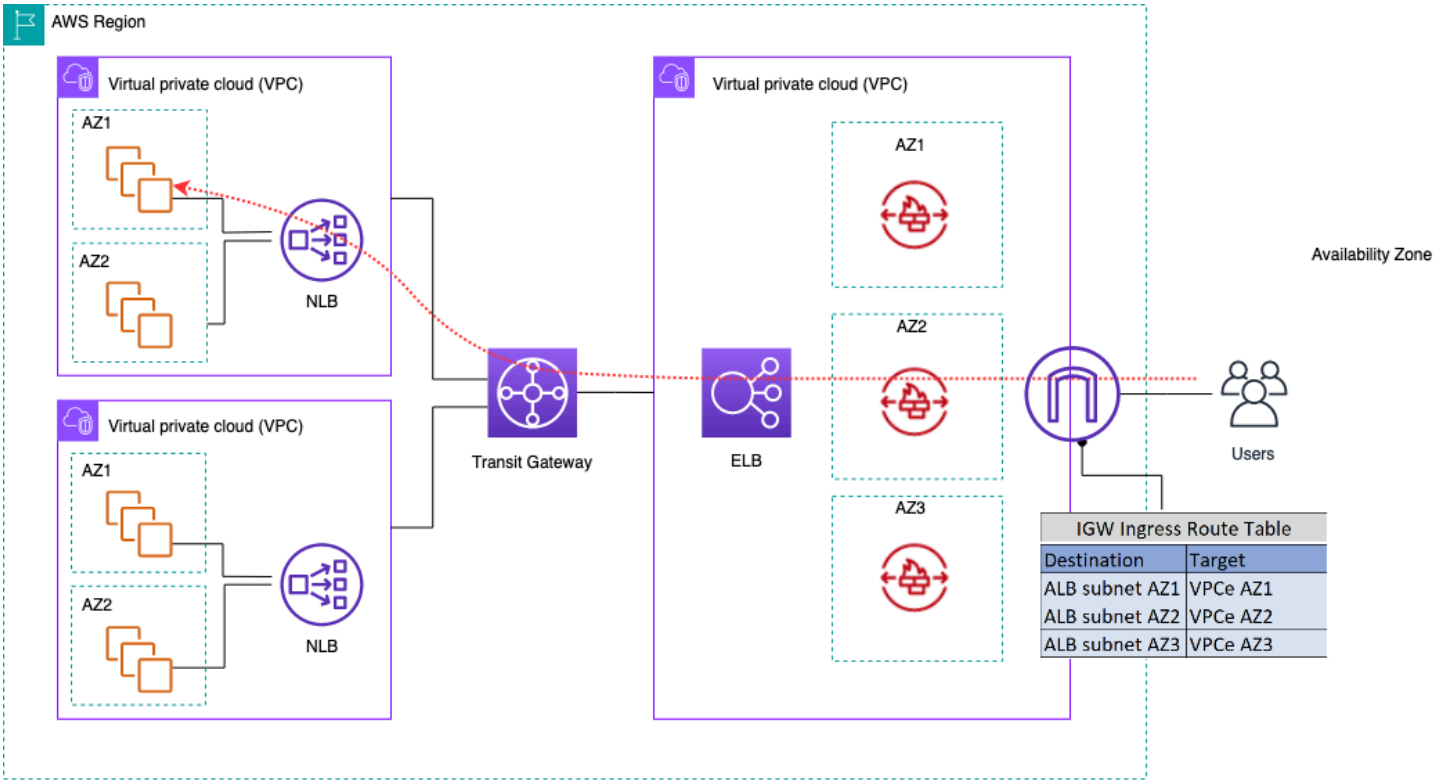
En la arquitectura anterior, los puntos finales del Gateway Load Balancer se implementan en cada zona de disponibilidad en una VPC perimetral independiente. Los firewalls, los sistemas de prevención de intrusiones, etc. de próxima generación se implementan detrás del Gateway Load Balancer en la VPC centralizada del dispositivo. La VPC de este dispositivo puede estar en la misma cuenta de AWS que las VPC de radio o en una cuenta de AWS diferente. Los dispositivos virtuales se pueden configurar para usar grupos de Auto Scaling y se registran automáticamente en el Gateway Load Balancer, lo que permite el escalado automático de la capa de seguridad.

Estos dispositivos virtuales se pueden administrar accediendo a sus interfaces de administración a través de una puerta de enlace de Internet (IGW) o mediante una configuración de host bastión en la VPC del dispositivo.

Mediante la función de enrutamiento de entrada de VPC, la tabla de enrutamiento perimetral se actualiza para enrutar el tráfico entrante de Internet a los dispositivos de firewall detrás de Gateway Load Balancer. El tráfico inspeccionado se enruta a través de los puntos finales del Gateway Load Balancer a la instancia de VPC de destino. Consulte la entrada del blog Introducing AWS Gateway Load Balancer: Supported architecture patterns para obtener más información sobre las distintas formas de utilizar Gateway Load Balancer.

Utilizándolo AWS Network Firewall para una entrada centralizada

En esta arquitectura, el tráfico de entrada se inspecciona AWS Network Firewall antes de llegar al resto de las VPC. En esta configuración, el tráfico se divide entre todos los puntos finales de firewall implementados en la VPC de Edge. Se implementa una subred pública entre el punto final del firewall y la subred Transit Gateway. Puedes usar un ALB o un NLB, que contienen objetivos IP en tus VPC radiales y, al mismo tiempo, controlan el Auto Scaling para los objetivos que están detrás de ellos.

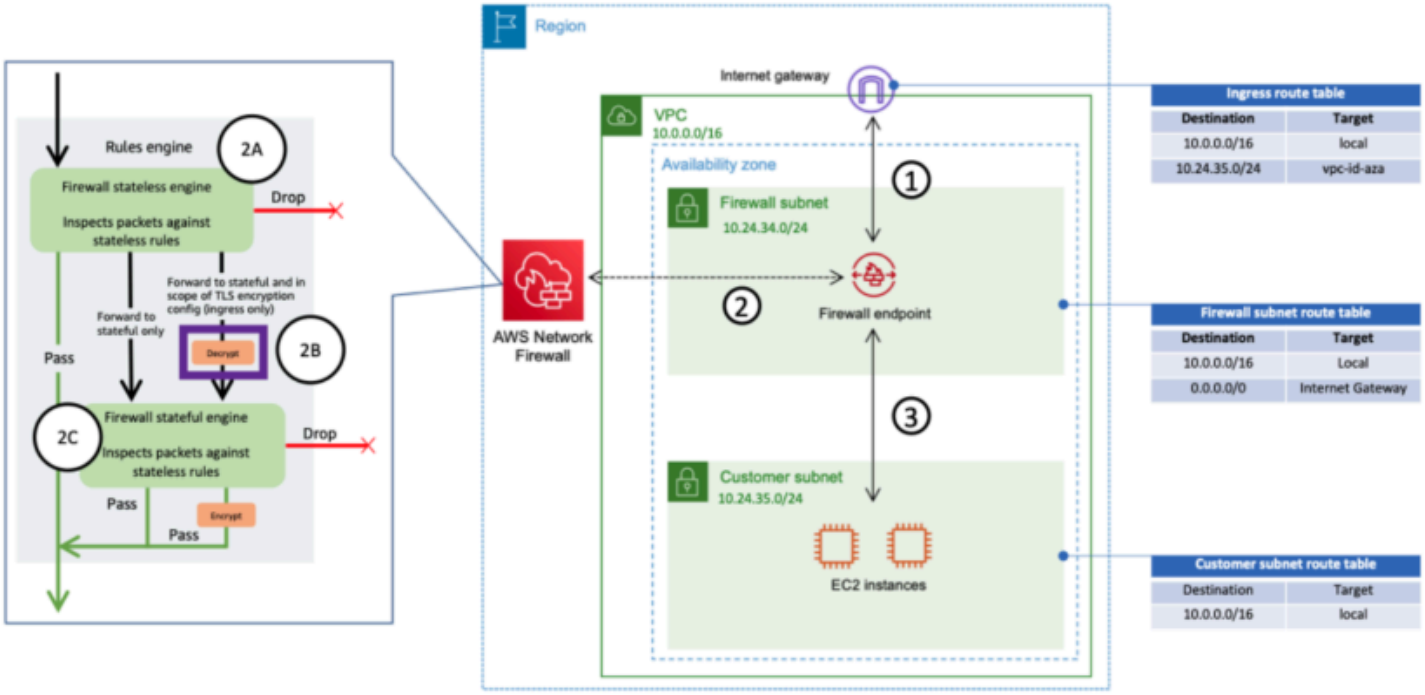


Inspección del tráfico de entrada mediante AWS Network Firewall

Para simplificar la implementación y la administración AWS Network Firewall de este modelo, se AWS Firewall Manager puede utilizar. Firewall Manager le permite administrar de forma centralizada sus diferentes firewalls al aplicar automáticamente la protección que cree en la ubicación centralizada a varias cuentas. Firewall Manager admite modelos de implementación distribuidos y centralizados para Network Firewall. La entrada del blog Cómo implementar AWS Network Firewall mediante el uso AWS Firewall Manager proporciona más detalles sobre el modelo.

Inspección profunda de paquetes (DPI) con AWS Network Firewall

Network Firewall puede realizar una inspección profunda de paquetes (DPI) en el tráfico de entrada. Al utilizar un certificado de seguridad de la capa de transporte (TLS) almacenado en AWS Certificate Manager (ACM), Network Firewall puede descifrar paquetes, realizar DPI y volver a cifrarlos. Hay algunas consideraciones a la hora de configurar el DPI con un firewall de red. En primer lugar, se debe almacenar un certificado TLS de confianza en ACM. En segundo lugar, las reglas de Network Firewall deben configurarse para enviar correctamente los paquetes para su descifrado y recrifrado. Consulte la entrada del blog sobre la configuración de la inspección de TLS para ver el tráfico cifrado y AWS Network Firewall obtener más información.



Inspección del tráfico de entrada mediante Network Firewall con DPI

Consideraciones clave para AWS Network Firewall una arquitectura de entrada centralizada

- Elastic Load Balancing en la VPC de Edge solo puede tener direcciones IP como tipos de destino, no un nombre de host. En la figura anterior, los destinos son las IP privadas del Network Load Balancer en las VPC radiales. El uso de objetivos IP detrás del ELB en la VPC perimetral provoca la pérdida de Auto Scaling.
- Considere la posibilidad de AWS Firewall Manager utilizarlos como un panel de vidrio único para los puntos finales de su firewall.
- Este modelo de implementación utiliza la inspección de tráfico justo cuando entra en la VPC perimetral, por lo que tiene el potencial de reducir el coste total de la arquitectura de inspección.

DNS

Al lanzar una instancia en una VPC, excluida la VPC predeterminada, AWS proporciona a la instancia un nombre de host de DNS privado (y, posiblemente, un nombre de host de DNS público) en función de los atributos de DNS que especifique para la VPC y de si la instancia tiene una dirección IPv4 pública. Cuando el `enableDnsSupport` atributo se establece en `true`, obtiene una resolución de DNS dentro de la VPC desde Route 53 Resolver (+2 de compensación de IP con respecto al CIDR de la VPC). De forma predeterminada, Route 53 Resolver responde a las consultas de DNS de los nombres de dominio de VPC, como los nombres de dominio de las instancias EC2 o los balanceadores de carga de Elastic Load Balancing. Con el emparejamiento de VPC, los hosts de una VPC pueden convertir los nombres de host de DNS públicos en direcciones IP privadas para las instancias de las VPC interconectadas, siempre que la opción esté habilitada. Lo mismo se aplica a las VPC conectadas mediante. AWS Transit Gateway Para obtener más información, consulte Habilitar el soporte de resolución de DNS para una conexión de emparejamiento de VPC.

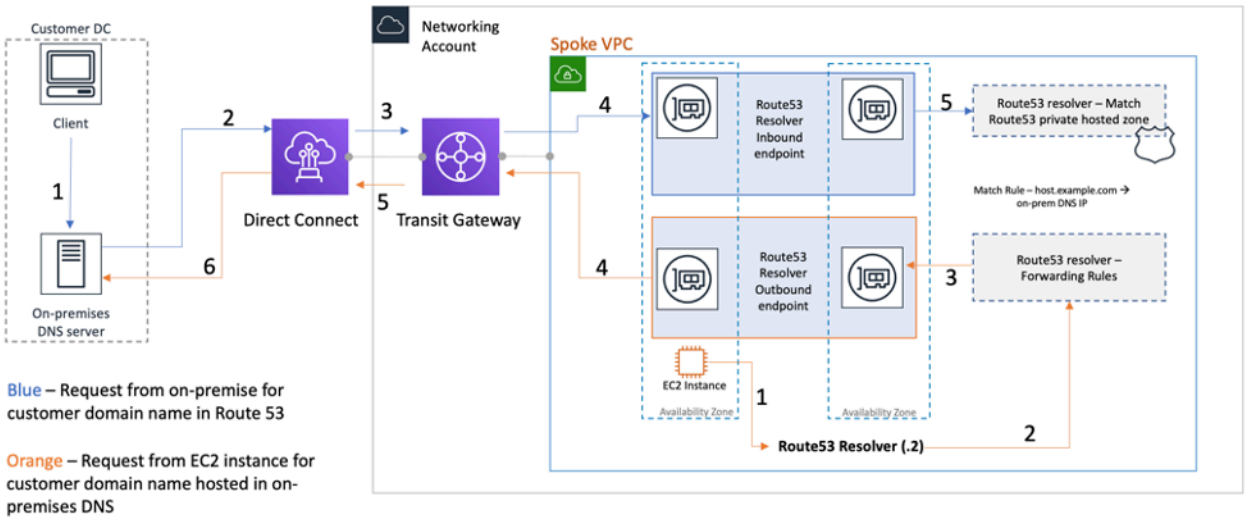
Si desea asignar sus instancias a un nombre de dominio personalizado, puede usar Amazon Route 53 para crear un registro de mapeo de DNS a IP personalizado. Una zona alojada de Amazon Route 53 es un contenedor que contiene información sobre cómo desea que Amazon Route 53 responda a las consultas de DNS de un dominio y sus subdominios. Las zonas alojadas públicas contienen información de DNS que se puede resolver a través de la Internet pública, mientras que las zonas alojadas privadas son una implementación específica que solo presenta información a las VPC que se hayan conectado a la zona alojada privada específica. En una configuración de zona de destino en la que tenga varias VPC o cuentas, puede asociar una única zona alojada privada a varias VPC en todas las cuentas y regiones de AWS (solo es posible con SDK/CLI/API). Los hosts finales de las VPC utilizan su IP de resolución de Route 53 respectiva (+2 compensan el CIDR de la VPC) como servidor de nombres para las consultas de DNS. El solucionador de Route 53 de la VPC solo acepta consultas de DNS de los recursos de una VPC.

DNS híbrido

El DNS es un componente fundamental de cualquier infraestructura, híbrida o no, ya que proporciona la resolución de nombre de host a dirección IP en la que se basan las aplicaciones. Los clientes que implementan entornos híbridos suelen disponer ya de un sistema de resolución de DNS y desean una solución de DNS que funcione en conjunto con su sistema actual. No se puede acceder al solucionador nativo de Route 53 (+2 del conjunto del CIDR de la VPC base) desde las redes locales mediante una VPN o. AWS Direct Connect Por lo tanto, cuando integra el DNS de las VPC de una

región de AWS con el DNS de su red, necesita un punto de enlace de entrada de Route 53 Resolver (para las consultas de DNS que reenvía a sus VPC) y un punto de enlace de salida de Route 53 Resolver (para las consultas que reenvía desde las VPC a la red).

Como se muestra en la siguiente figura, puede configurar los puntos de enlace salientes del Resolver para que reenvíen las consultas que reciba de las instancias de Amazon EC2 de sus VPC a los servidores DNS de su red. Para reenviar consultas seleccionadas, desde una VPC a una red local, cree reglas de resolución de Route 53 que especifiquen los nombres de dominio de las consultas de DNS que desea reenviar (como example.com) y las direcciones IP de los solucionadores de DNS de la red a los que desea reenviar las consultas. Para las consultas entrantes desde las redes locales a las zonas alojadas de Route 53, los servidores DNS de la red pueden reenviar las consultas a los puntos finales de Resolver entrantes en una VPC específica.



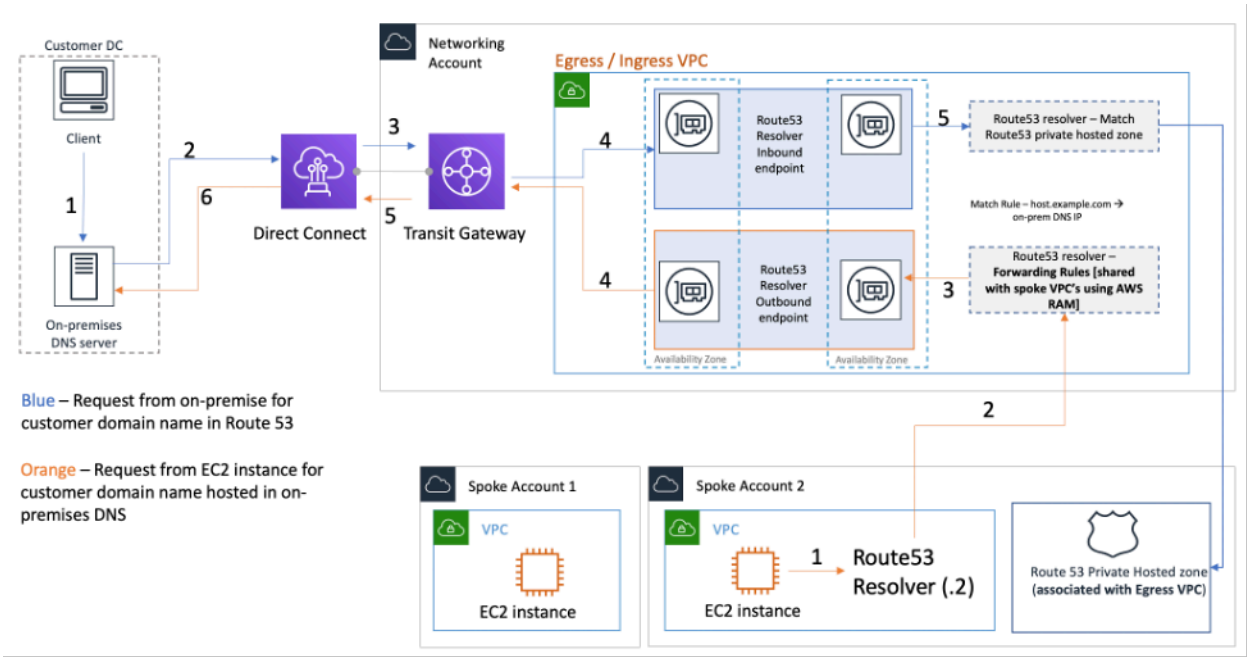
Resolución de DNS híbrido mediante Route 53 Resolver

Esto permite a sus solucionadores de DNS locales resolver fácilmente los nombres de dominio de los recursos de AWS, como las instancias o los registros de Amazon EC2 en una zona alojada privada de Route 53 asociada a esa VPC. Además, los puntos de enlace de Route 53 Resolver pueden gestionar hasta aproximadamente 10 000 consultas por segundo por ENI, por lo que pueden escalar fácilmente hasta alcanzar un volumen de consultas de DNS mucho mayor. Consulte las prácticas recomendadas para Resolver en la documentación de Amazon Route 53 para obtener más información.

No se recomienda crear puntos finales de Route 53 Resolver en cada VPC de la zona de aterrizaje. Centralícelos en una VPC de salida central (en la cuenta de servicios de red). Este enfoque permite una mejor capacidad de administración y, al mismo tiempo, mantiene los costos bajos (se le cobrará

una tarifa por hora por cada terminal de resolución entrante/saliente que cree). Compartes el punto final centralizado de entrada y salida con el resto de la zona de aterrizaje.

- Resolución de salida: utilice la cuenta de servicios de red para escribir reglas de resolución (en función de las cuales las consultas de DNS se reenviarán a los servidores DNS locales). Con Resource Access Manager (RAM), comparta estas reglas de Route 53 Resolver con varias cuentas (y asócelas a las VPC de las cuentas). Las instancias EC2 de las VPC radiales pueden enviar consultas de DNS al Solucionador de Route 53 y el Servicio de Resolver de Route 53 reenviará estas consultas al servidor DNS local a través de los puntos de conexión salientes del Resolver de Route 53 en la VPC de salida. No es necesario unir las VPC con radios a la VPC de salida ni conectarlas a través de Transit Gateway. No utilice la IP del punto final de resolución saliente como DNS principal en las VPC radiales. Las VPC de Spoke deben usar Route 53 Resolver (para compensar el CIDR de la VPC) en su VPC.



Centralización de los puntos finales de Route 53 Resolver en la VPC de entrada y salida

- Resolución de DNS entrante: cree puntos finales de entrada de Route 53 Resolver en una VPC centralizada y asocie todas las zonas alojadas privadas de su zona de destino a esta VPC centralizada. Para obtener más información, consulte Asociar más VPC a una zona alojada privada. No se pueden superponer varias zonas alojadas privadas (PHZ) asociadas a una VPC. Como se muestra en la figura anterior, esta asociación de PHZ con la VPC centralizada permitirá a los servidores locales resolver el DNS de cualquier entrada en cualquier zona alojada privada

(asociada a la VPC central) mediante el punto final de entrada de la VPC centralizada. Para obtener más información sobre las configuraciones de DNS híbrido, consulte Administración centralizada del DNS de la nube híbrida con Amazon Route 53 y AWS Transit Gateway y Opciones de DNS de nube híbrida para Amazon VPC.

Firewall DNS Route 53

Amazon Route 53 Resolver El firewall de DNS ayuda a filtrar y regular el tráfico DNS saliente de sus VPC. Uno de los usos principales del firewall de DNS es ayudar a evitar la exfiltración de datos mediante la definición de listas de nombres de dominio permitidos que permiten a los recursos de su VPC realizar solicitudes de DNS salientes solo para los sitios en los que su organización confía. También ofrece a los clientes la posibilidad de crear listas de bloqueo para los dominios con los que no desean que los recursos de una VPC se comuniquen a través de DNS. Amazon Route 53 Resolver El firewall de DNS tiene las siguientes características:

Los clientes pueden crear reglas para definir cómo se responden las consultas de DNS. Las acciones que se pueden definir para los nombres de dominio incluyen`NODATA`, `OVERRIDE` y`NXDOMAIN`.

Los clientes pueden crear alertas tanto para las listas de permitidos como para las de denegación a fin de supervisar la actividad de las reglas. Esto puede resultar útil cuando los clientes desean probar la regla antes de pasarla a producción.

Para obtener más información, consulte la entrada del blog How to Get Amazon Route 53 Resolver Started with DNS Firewall for Amazon VPC.

Acceso centralizado a VPC puntos finales privados

Un VPC punto final le permite conectarse de forma privada VPC a AWS los servicios compatibles sin necesidad de una pasarela de Internet ni de un NAT dispositivo, VPN conexión o AWS Direct Connect conexión. Por lo tanto, no VPC está expuesto a la Internet pública. Las instancias de su servidor VPC no requieren direcciones IP públicas para comunicarse con los puntos finales del AWS servicio a través de este punto final de la interfaz. El tráfico entre sus servicios VPC y otros no sale de la AWS red troncal. VPCLos puntos finales son dispositivos virtuales. Son componentes de escala horizontal, redundantes y de alta disponibilidad. VPC Actualmente, se pueden aprovisionar dos tipos de puntos finales: puntos finales de interfaz (alimentados por AWS PrivateLink) y puntos finales de puerta de enlace. Los puntos de enlace de enlace se pueden utilizar para acceder a los servicios de Amazon S3 y Amazon DynamoDB de forma privada. El uso de puntos de enlace de gateway no supone ningún cargo adicional. Se aplicará la tarifa estándar por la transferencia de datos y el uso de recursos.

Puntos de enlace de VPC de interfaz

Un punto final de interfaz consta de una o más interfaces de red elásticas con una dirección IP privada que sirve como punto de entrada para el tráfico destinado a un servicio compatible. AWS Al aprovisionar un punto final de interfaz, se incurre en un coste por cada hora de funcionamiento del punto final, además de los gastos de procesamiento de datos. De forma predeterminada, se crea un punto final de interfaz en cada punto VPC desde el que se desee acceder al AWS servicio. Esto puede resultar prohibitivo y difícil de gestionar en la configuración de la zona de aterrizaje, en la que un cliente quiere interactuar con un AWS servicio específico a través de varios canales. VPCs Para evitarlo, puede alojar los puntos finales de la interfaz de forma centralizada. VPC Todos los radios VPCs utilizarán estos puntos finales centralizados a través de Transit Gateway.

Cuando creas un VPC punto final para un AWS servicio, puedes habilitar el modo privadoDNS. Cuando está habilitada, la configuración crea una zona alojada privada de Route 53 AWS administrada (PHZ), que permite convertir el punto final del AWS servicio público en la IP privada del punto final de la interfaz. El gestionado PHZ solo funciona dentro del VPC punto final de la interfaz. En nuestra configuración, cuando queremos que Speaking pueda VPCs resolver un VPC punto final DNS alojado en un servidor centralizadoVPC, el gestionado no PHZ funcionará. Para solucionar este problema, deshabilite la opción que crea automáticamente el punto final de la interfaz DNS cuando se crea un punto final de interfaz. A continuación, cree manualmente una zona alojada privada de Route 53 que coincida con el nombre del punto de conexión del servicio y agregue un registro de

alias con el nombre completo del Servicio de AWS punto de conexión que apunte al punto final de la interfaz.

1. Inicie sesión en Route 53 AWS Management Console y navegue hasta allí.
2. Seleccione la zona alojada privada y vaya a Crear registro.
3. Rellene el campo Nombre del registro, seleccione el tipo de registro como A y active el alias.

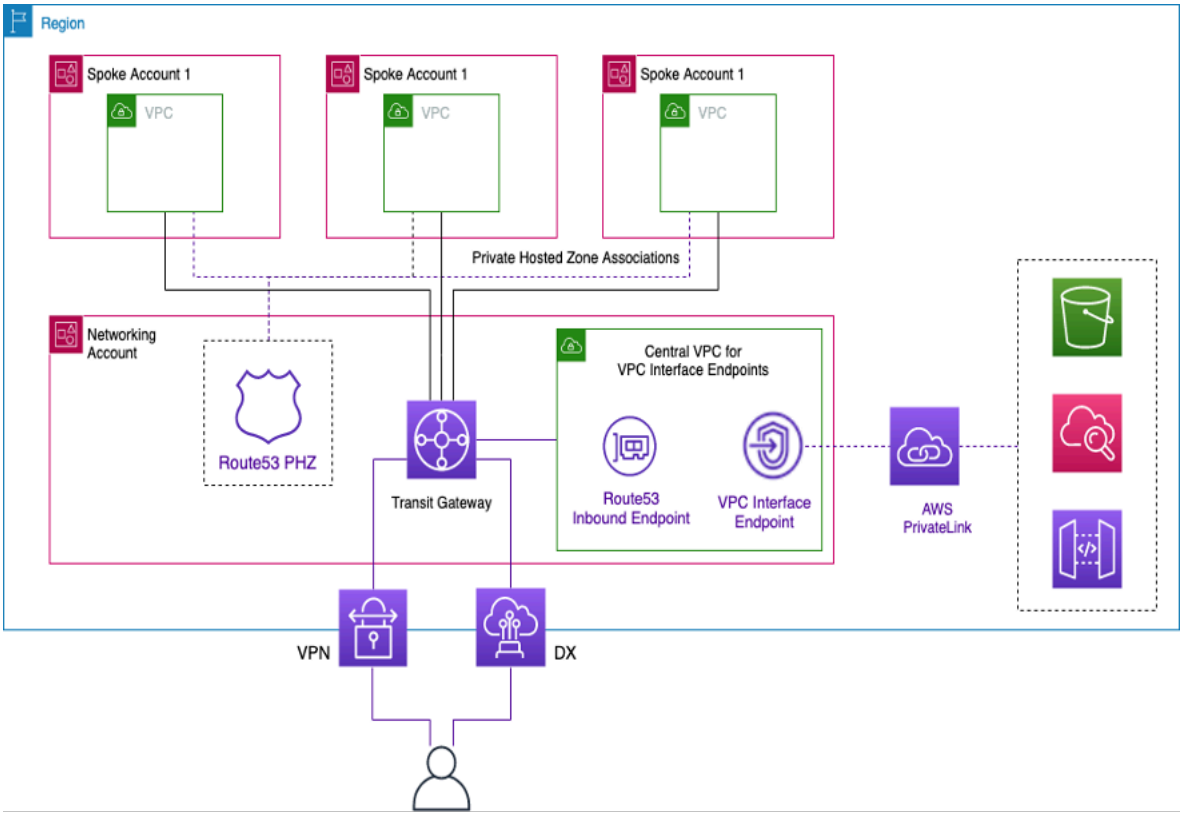
   Tenga en cuenta que algunos servicios, como los terminales de Docker y del OCI cliente (**`dkr.ecr`**), requieren que se utilice un alias comodín (**`*`**) para el nombre del registro.
4. En la sección Enrutar el tráfico a, seleccione el servicio al que se debe enviar el tráfico y seleccione la región en la lista desplegable.
5. Seleccione la política de enrutamiento adecuada y habilite la opción de evaluar el estado del objetivo.

Asocias esta zona alojada privada con otras VPCs dentro de la zona de aterrizaje. Esta configuración permite que el radio resuelva VPCs los nombres de los puntos finales de servicio completo para los puntos finales de la interfaz centralizada. VPC

> **Note**
>
> Para acceder a la zona alojada privada compartida, los hosts del radio VPCs deben utilizar la IP del Route 53 Resolver de sus servidores. VPC También se puede acceder a los puntos finales de la interfaz desde las redes locales a través de VPN Direct Connect. Utilice reglas de reenvío condicional para enviar todo el DNS tráfico de los nombres de los puntos de conexión de servicio completo a los puntos de conexión entrantes de Route 53 Resolver, que resolverá DNS las solicitudes en función de la zona alojada privada.

En la siguiente figura, Transit Gateway permite el flujo de tráfico desde los puntos finales de la interfaz radial VPCs hasta los puntos finales de la interfaz centralizada. Cree VPC los puntos finales y la zona alojada privada para ellos en la cuenta de servicios de red y compártalos con las cuentas spoke VPCs in the spoke. Para obtener más información sobre cómo compartir información de puntos de conexión con otras VPCs personas, consulte la entrada del blog Integrating AWS Transit Gateway with AWS PrivateLink and Amazon Route 53 Resolver.

> **Note**
>
> Un enfoque de VPC punto final distribuido, es decir, un punto final por punto final, VPC le permite aplicar políticas de privilegios mínimos en los VPC puntos finales. Con un enfoque centralizado, aplicará y gestionará las políticas de VPC acceso remoto desde un único punto final. Con un número cada vez mayor de ellasVPCs, podría aumentar la complejidad de mantener los privilegios mínimos con un único documento de política. Un único documento de política también da como resultado un radio de explosión mayor. También está restringido el tamaño del documento de política (20.480 caracteres).



Centralización de los puntos finales de la interfaz VPC

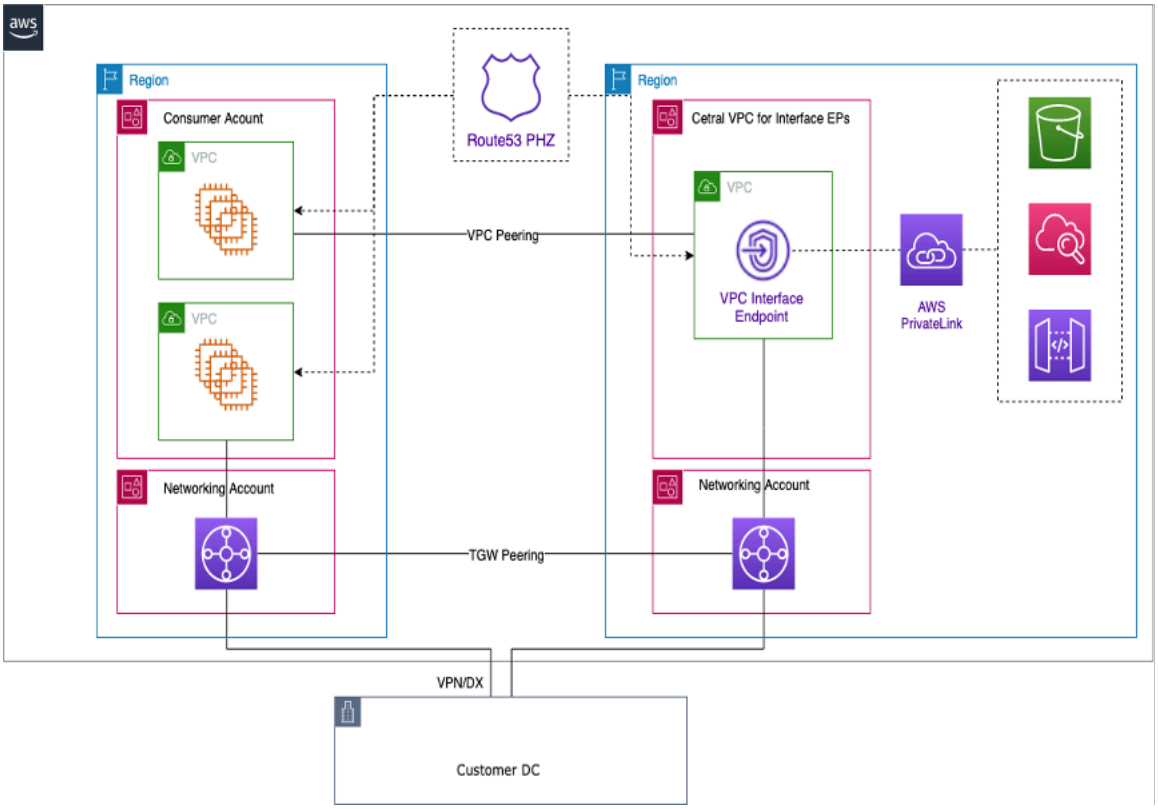
Acceso a puntos finales entre regiones

Si desea VPCs configurar varios dispositivos en diferentes regiones que compartan un VPC punto final común, utilice unPHZ, tal y como se ha descrito anteriormente. Ambas VPCs en cada región se asociarán PHZ con el alias del punto final. Para enrutar el tráfico entre ellas VPCs en una arquitectura multirregional, las pasarelas de tránsito de cada región deben estar conectadas entre sí.

Para obtener más información, consulte este blog: Uso de zonas alojadas privadas de Route 53 para arquitecturas multirregionales entre cuentas.

VPCsdesde diferentes regiones se pueden enrutar entre sí mediante Transit Gateways o Peering. VPC Use la siguiente documentación para interconectar las pasarelas de tránsito: Adjuntos de interconexión de las pasarelas de tránsito.

En este ejemplo, la EC2 instancia de Amazon de la VPC `us-west-1` región utilizará la PHZ para obtener la dirección IP privada del punto final de la `us-west-2` región y enrutar el tráfico a la región a VPC través de la `us-west-2` interconexión o interconexión de Transit GatewayVPC. Con esta arquitectura, el tráfico permanece dentro de la AWS red, lo que permite a la EC2 instancia acceder `us-west-1` al VPC servicio de forma segura `us-west-2` sin tener que recurrir a Internet.



Puntos finales multirregionales VPC

> **Note**
>
> Se aplican cargos por transferencia de datos entre regiones al acceder a los puntos finales en todas las regiones.

Haciendo referencia a la figura anterior, se crea un servicio de punto final VPC en una región. `us-west-2` Este servicio de punto final proporciona acceso a un AWS servicio en esa región. Para que las instancias de otra región (por ejemplo`us-east-1`) puedan acceder al punto final de la `us-west-2` región, debe crear un registro de direcciones PHZ con un alias para el VPC punto final deseado.

En primer lugar, asegúrese de que las VPCs de cada región estén asociadas a la PHZ que creó.

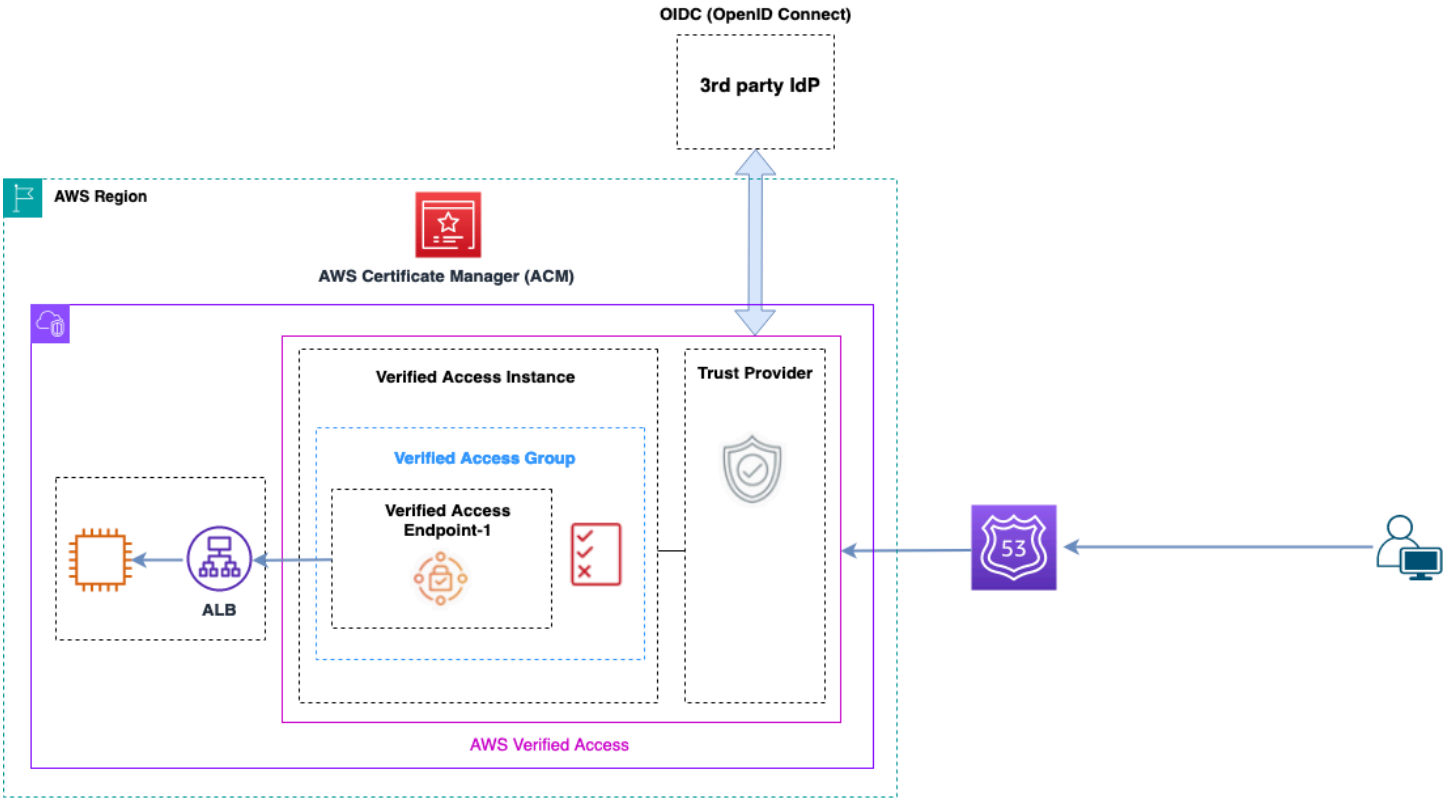
Al implementar un punto final en varias zonas de disponibilidad, la dirección IP del punto final devuelto DNS procederá de cualquiera de las subredes de la zona de disponibilidad que esté asignada.

Al invocar el punto final, utilice el nombre de dominio completo (FQDN) que se encuentra en. PHZ

Acceso verificado de AWS

Acceso verificado de AWS ofrece acceso seguro a las aplicaciones en una red privada sin unVPN. Evalúa las solicitudes en tiempo real, como la identidad, el dispositivo y la ubicación. Este servicio permite el acceso a las aplicaciones en función de la política y conecta a los usuarios mediante la mejora de la seguridad de la organización. El acceso verificado proporciona acceso a aplicaciones privadas al actuar como un proxy inverso que reconoce la identidad. La identidad del usuario y el estado del dispositivo, si corresponde, se analizan antes de enrutar el tráfico a la aplicación.

El siguiente diagrama brinda información general de alto nivel sobre Acceso verificado. Los usuarios envían solicitudes para acceder a una aplicación. Acceso verificado evalúa la solicitud en función de la política de acceso del grupo y de cualquier política de punto de conexión específica de la aplicación. Si se permite el acceso, la solicitud se envía a la aplicación a través del punto de conexión.



Descripción general del acceso verificado

Los componentes principales de una Acceso verificado de AWS arquitectura son:

- Instancias de Acceso verificado: una instancia evalúa las solicitudes de aplicación y concede el acceso solo cuando se cumplen los requisitos de seguridad.
- Puntos de conexión de Acceso verificado: cada punto de conexión representa una aplicación. Un punto final puede ser NLB una interfaz de red ALB o una interfaz de red.
- Grupo de Acceso verificado: conjunto de puntos de conexión de Acceso verificado. Se recomienda agrupar los puntos de conexión de las aplicaciones con requisitos de seguridad similares a fin de simplificar la administración de las políticas.
- Políticas de acceso: conjunto de reglas definidas por el usuario que determinan si se debe permitir o denegar el acceso a una aplicación.
- Proveedores de confianza: el acceso verificado es un servicio que facilita la administración de las identidades de los usuarios y los estados de seguridad de los dispositivos. Es compatible con proveedores de confianza AWS tanto como con proveedores de confianza de terceros, por lo que es necesario adjuntar al menos un proveedor de confianza a cada instancia de Verified Access. Cada una de estas instancias puede incluir un único proveedor de confianza de identidad, así como varios proveedores de confianza de dispositivos.

- Datos de confianza: los datos de seguridad que tu proveedor de confianza envía a Verified Access, como la dirección de correo electrónico de un usuario o el grupo al que pertenece, se evalúan en función de tus políticas de acceso cada vez que se recibe una solicitud de solicitud.

Puedes encontrar más información en las publicaciones del blog de Verified Access.

Conclusión

A medida que amplía el uso de las aplicaciones AWS y las implementa en la zona de AWS destino, aumenta la cantidad de VPC y componentes de red. En este documento técnico se explica cómo se puede gestionar esta infraestructura en crecimiento garantizando la escalabilidad, la alta disponibilidad y la seguridad y, al mismo tiempo, manteniendo los costes bajos. Es fundamental tomar las decisiones de diseño correctas cuando se utilizan servicios como Transit Gateway, Shared VPC, puntos de enlace de AWS Direct Connect VPC, Gateway Load Balancer, AWS Network Firewall Amazon Route 53 y dispositivos de software de terceros. Es importante comprender las consideraciones clave de cada enfoque y analizar sus requisitos para determinar qué opción o combinación de opciones se adapta mejor a sus necesidades.

Colaboradores

Las siguientes personas y organizaciones han colaborado en este documento:

- Sohaib Tahir, arquitecto de soluciones, Amazon Web Services
- Shirin Bhambhani, arquitecta de soluciones, Amazon Web Services
- Kunal Pansari, arquitecto de soluciones, Amazon Web Services
- Eric Vasquez, arquitecto de soluciones, Amazon Web Services
- Tushar Jagdale, arquitecto de soluciones, Amazon Web Services
- Ameer Shariff, arquitecto de soluciones, Amazon Web Services
- Glenn Davis, arquitecto de soluciones, Amazon Web Services
- Nick Kniveton, arquitecto de soluciones, Amazon Web Services
- Sidhartha Chauhan, arquitecta principal de soluciones, Amazon Web Services

Historial del documento

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

Cambio	Descripción	Fecha
Actualización importante	Actualizaciones en todo el documento técnico sobre los cambios en CloudWAN, Amazon VPC Lattice, ENA Express, conectividad híbrida, AWS Direct Connect Sitelink, Deep Packet Inspection y. Acceso verificado de AWS	17 de abril de 2024
Actualización menor	Se actualizaron los diagramas para ser más coherentes, se actualizaron las opciones de conectividad DX para incluir una VPN con IP privada y se introdujeron numerosos cambios menores en todas ellas.	6 de julio de 2023
Actualización menor	AWS Control Tower La información se actualizó , reflejó los nuevos límites de rendimiento para varios servicios, se actualizó el diagrama de la puerta de enlace NAT y se actualizó la sección de seguridad para centralizar las salidas.	4 de abril de 2023

Actualización menor	Se agregó una sección: Acceso a puntos finales entre regiones.	19 de julio de 2022
Actualización importante	Se actualizó la sección Transit Gateway con Transit Gateway Connect, se actualizó la sección Transit VPC; se actualizó AWS Direct Connect la sección con MACsec y recomendaciones de resilienc ia; se actualizó la sección. AWS PrivateLink Se agregó una tabla comparativa entre VPC y Transit VPC y Transit Gateway; se agregó una sección de inspección entrante centralizada; se actualizó la seguridad de red centraliz ada para VPC a VPC y de VPC local a VPC y salida centralizada a Internet con patrones de diseño de AWS Network Firewall Gateway Load Balancer; se agregaron secciones de puerta de enlace NAT privada y firewall de DNS Amazon Route 53.	22 de febrero de 2022
Actualización menor	Se actualizó la sección de emparejamiento entre Transit Gateway y VPC	2 de abril de 2021
Documento técnico actualiza do	Se corrigió el texto para que coincidiera con las opciones ilustradas en la figura 7	10 de junio de 2020

Publicación inicial	Documento técnico publicado.	15 de noviembre de 2019

Avisos

Los clientes son responsables de realizar sus propias evaluaciones de la información contenida en este documento. Este documento: (a) solo tiene fines informativos, (b) representa las prácticas y las ofertas de productos vigentes de AWS, que están sujetas a cambios sin previo aviso, y (c) no crea ningún compromiso ni garantía de AWS y sus empresas filiales, proveedores o concesionarios de licencias. Los productos o servicios de AWS se proporcionan “tal cual”, sin garantías, representaciones ni condiciones de ningún tipo, ya sean explícitas o implícitas. Las responsabilidades y las obligaciones de AWS con respecto a sus clientes se controlan mediante los acuerdos de AWS. Además, este documento no forma parte de ningún acuerdo entre AWS y sus clientes ni lo modifica.

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.