Guía del administrador

AWS Client VPN

AWS Client VPN: Guía del administrador

Table of Contents

¿Qué es AWS Client VPN?

AWS Client VPN es un servicio de VPN gestionado y basado en clientes que le permite acceder de forma segura a sus AWS recursos y recursos de la red local. Con Client VPN, puede acceder a los recursos desde cualquier ubicación utilizando un cliente de VPN basado en OpenVPN.

Temas

Características de Client VPN

Client VPN cuenta con las siguientes características y funcionalidades:

- Conexiones seguras: establece conexiones TLS cifradas desde cualquier ubicación a través del cliente OpenVPN, lo que garantiza la privacidad y la integridad de los datos.
- Servicio administrado: elimina la carga operativa que supone la implementación y el mantenimiento de soluciones de VPN de acceso remoto de terceros mediante la administración completa de AWS.
- Alta disponibilidad y elasticidad: se escala de forma dinámica para adaptar un número variable de usuarios que se conectan a los recursos de AWS y en las instalaciones sin intervención manual.
- Autenticación: admite varios métodos de autenticación, como la integración de Active Directory, la autenticación federada y la autenticación basada en certificados para una administración flexible de identidades.
- Control granular: implementa controles de seguridad precisos a través de reglas de acceso basadas en la red configurables en el nivel de grupo de Active Directory y el control de acceso basado en grupos de seguridad.
- Facilidad de uso: proporciona acceso unificado a recursos de AWS y en las instalaciones a través de un único túnel de VPN, lo que simplifica la experiencia del usuario final.

- Capacidad de administración: ofrece visibilidad completa a través de registros de conexiones detallados y funciones de administración en tiempo real, incluida la capacidad de monitorizar y finalizar conexiones activas de los clientes cuando sea necesario.
- Integración profunda: se integra perfectamente con los servicios de AWS existentes, incluida AWS Directory Service Amazon VPC, lo que mejora las capacidades de conectividad de su infraestructura de nube.
- Arquitectura de red flexible: admite asociaciones de subredes de VPC y adjuntos directos de Transit Gateway. Para obtener más información, consulte Integración de Transit Gateway con Client VPN.
- IPv6 soporte: permite una IPv6 conectividad total para los puntos finales Client VPN y admite conexiones a IPv6 los recursos de su red VPCs y desde los clientes de IPv6 las redes para los requisitos de red modernos.

Componentes de Client VPN

Estos son los conceptos clave de Client VPN:

Punto de enlace de Client VPN

El punto de enlace de Client VPN es el recurso que usted crea y configura para activar y administrar sesiones de Client VPN. Es el punto de terminación de todas las sesiones de Client VPN.

Red de destino

Una red de destino es la red que se asocia a un punto de enlace de Client VPN. Puede asociar subredes de VPC o conectarlas directamente a una Transit Gateway AWS . Para obtener más información sobre la integración de Transit Gateway, consulteIntegración de Transit Gateway con Client VPN.

Ruta

Cada punto de enlace de Client VPN tiene una tabla de ruta que describe las rutas de la red de destino disponibles. Cada ruta de la tabla de enrutamiento especifica la ruta del tráfico a recursos o redes específicos.

Reglas de autorización

Una regla de autorización restringe los usuarios que pueden obtener acceso a una red. Para una red especificada, se configura el grupo de proveedor de identidades (IdP) o de Active Directory

al que se permite el acceso. Solo los usuarios que pertenezcan a este grupo pueden obtener acceso a la red especificada. De forma predeterminada, no hay reglas de autorización, por lo que debe configurarlas para permitir que los usuarios obtengan acceso a los recursos y redes.

Cliente

Usuario final que se conecta al punto de enlace de Client VPN para establecer una sesión de VPN. Los usuarios finales tienen que descargar un cliente OpenVPN y utilizar el archivo de configuración de la VPN de cliente que creó para establecer una sesión de VPN.

Rango de CIDR del cliente

Un rango de direcciones IP desde el que asignar direcciones IP del cliente. A cada conexión con el punto de enlace de Client VPN se le asigna una dirección IP única del intervalo CIDR del cliente. Para IPv4 el tráfico, usted elige el rango CIDR del cliente, por ejemplo,`10.2.0.0/16`. Para IPv6 el tráfico, asigna AWS Client VPN automáticamente el rango CIDR del cliente.

Puertos de Client VPN

AWS Client VPN admite los puertos 443 y 1194 tanto para TCP como para UDP. El valor predeterminado es el puerto 443.

Interfaces de red de Client VPN

Cuando asocia una subred con el punto de enlace de Client VPN, se crean interfaces de red de Client VPN en esa subred. El tráfico que se envía a la VPC desde el punto de enlace de Client VPN se envía a través de una interfaz de red de Client VPN. Para IPv4 el tráfico, se aplica la traducción de direcciones de red de origen (SNAT), donde la dirección IP de origen del rango CIDR del cliente se traduce a la dirección IP de la interfaz de red de Client VPN. Para IPv6 el tráfico, no se aplica la SNAT, lo que proporciona una mayor visibilidad de la dirección IP del usuario conectado.

Registro de conexión

Puede activar los registros de conexión en el punto de enlace de Client VPN para que los eventos de conexión queden registrados. Esta información puede resultar útil para ejecutar análisis forenses, analizar cómo se está utilizando el punto de enlace de Client VPN o depurar problemas de conexión.

Portal de autoservicio

Client VPN proporciona un portal de autoservicio como página web para que los usuarios finales descarguen la versión más reciente de AWS VPN Desktop Client y del archivo de

configuración del punto de enlace de Client VPN, que contiene la configuración necesaria con el fin de conectarse al punto de enlace. El administrador del punto de enlace de Client VPN puede habilitar o desactivar un portal de autoservicio para el punto de enlace de Client VPN. El portal de autoservicio es un servicio global respaldado por paquetes de servicios en las siguientes regiones: EE. UU. Este (Virginia del Norte), Asia Pacífico (Tokio), Europa (Irlanda) y AWS GovCloud (EE. UU. Oeste).

Tipo de dirección IP de punto de conexión

El tipo de dirección IP del punto final Client VPN, que puede ser IPv4 IPv6, o de doble pila (ambos IPv4 IPv6).

Tipo de dirección IP de tráfico

El tipo de dirección IP del tráfico que fluye a través del punto final Client VPN, que puede ser IPv4 IPv6, o de doble pila (ambos IPv4 IPv6). Determina el tipo de tráfico interno (la carga útil real o el tráfico original que se canaliza a través de la conexión de VPN), los intervalos de CIDR del cliente, la asociación de subredes, las rutas y las reglas por punto de conexión.

Uso de Client VPN

Puede utilizar Client VPN de cualquiera de las siguientes formas:

Consola de administración de AWS

La consola proporciona una interfaz de usuario basada en web para Client VPN.

La consola proporciona una interfaz de usuario basada en web para Client VPN con dos métodos de configuración:

- Configuración de inicio rápido: creación simplificada de terminales con los valores predeterminados recomendados por AWS
- Configuración estándar: control total sobre todas las opciones de configuración

Si se ha registrado en una Cuenta de AWS, puede iniciar sesión en la consola de Amazon VPC y seleccionar Client VPN en el panel de navegación.

AWS Command Line Interface (AWS CLI)

AWS CLI Proporciona acceso directo al público de Client VPN APIs. Es compatible con Windows, macOS y Linux. Para obtener más información sobre cómo empezar a utilizarla AWS CLI, consulte la Guía del AWS Command Line Interface usuario. Para obtener más información

acerca de los comandos de Client VPN, consulte la sección de EC2 de la Referencia de línea de comandos de Amazon EC2.

AWS Tools for Windows PowerShell

AWS proporciona comandos para un amplio conjunto de AWS ofertas para quienes escriben en el PowerShell entorno. Para obtener más información acerca de cómo empezar a trabajar con AWS Tools for Windows PowerShell, consulte la Guía del usuario de AWS Tools for Windows PowerShell. Para obtener más información acerca de los cmdlets de Client VPN, consulte la Referencia de Cmdlet de AWS Tools for Windows PowerShell.

API de consulta

La API de consulta HTTPS de Client VPN le brinda acceso programático a Client VPN y AWS. La API de consulta HTTPS le permite emitir solicitudes HTTPS directamente al servicio. Cuando use la API HTTPS, debe incluir código para firmar digitalmente las solicitudes utilizando sus credenciales. Para obtener más información, consulte las acciones de AWS Client VPN.

Precios de Client VPN

Se le cobra por cada asociación de puntos de conexión y cada conexión VPN cada hora. El uso IPv6 de los terminales de doble pila no supone ningún coste adicional; se cobra la misma tarifa que los terminales. IPv4 Para obtener más información, consulte Precios de AWS Client VPN.

Se le cobra la transferencia de datos desde Amazon EC2 a Internet. Para obtener más información, consulte la sección Data Transfer (Transferencia de datos) en la página Precios bajo demanda de Amazon EC2.

Si habilita el registro de conexiones para su terminal Client VPN, debe crear un grupo de CloudWatch registros en su cuenta. Se aplican cargos por el uso de grupos de registro. Para obtener más información, consulta CloudWatch los precios de Amazon (en el nivel de pago, selecciona Logs).

Si activa el controlador de la conexión del cliente en el punto de enlace de Client VPN, debe crear e invocar una función Lambda. Se aplicarán cargos por invocar funciones de Lambda. Para más información, consulte Precios de AWS Lambda.

Los puntos de conexión de Client VPN están asociados con una red de destino, que es una subred en una VPC. Si esta VPC tiene una puerta de enlace a Internet, asociamos las direcciones IP elásticas a las interfaces de red elásticas de Client VPN ()ENIs. Estas direcciones IP elásticas se cobran como direcciones públicas IPv4 en uso. Para obtener más información, consulte la pestaña Public IPv4 Address en la página de precios de la VPC.

> **Note**
>
> Los puntos de enlace de Client VPN requieren direcciones IP elásticas cuando se asocian a una subred de VPC que tiene una puerta de enlace de Internet, ya EIPs que permiten la conectividad directa a Internet para los clientes de VPN. Cuando se conectan a través de un punto de conexión de Client VPN, necesitan una dirección IP pública para comunicarse con los recursos de Internet. Elastic IPs cumple este propósito al proporcionar un punto final coherente y orientado al público. EIPs Se conectan a las interfaces de red elásticas de Client VPN (ENIs) y son esenciales para mantener un acceso a Internet estable y seguro para los clientes de VPN y, al mismo tiempo, garantizar el enrutamiento adecuado del tráfico. Dado que estas direcciones IP elásticas se asignan y utilizan activamente para el servicio Client VPN, las AWS cobra como IPv4 direcciones públicas en uso, siguiendo su modelo de precios estándar de asignación y asociación. EIPs

Reglas y mejores prácticas de uso AWS Client VPN

En las secciones siguientes, se describen las reglas y prácticas recomendadas para utilizar AWS Client VPN:

Temas

Requisitos de red y ancho de banda

- AWS Client VPN es un servicio totalmente gestionado que se escala automáticamente para adaptarse a las conexiones de usuario adicionales y a los requisitos de ancho de banda. Cada conexión de usuario tiene un ancho de banda base máximo de 50 Mbps.

  El ancho de banda real que experimenta al conectarse a través de un punto de conexión de Client VPN puede variar en función de varios factores. Se trata de factores como el tamaño del paquete, la composición del tráfico (combinación de TCP/UDP), las políticas de red (moldeado o limitación)

de las redes intermedias, las condiciones de Internet, los requisitos específicos de la aplicación y el número total de conexiones simultáneas de usuarios. Si alcanza el límite de ancho de banda máximo, puede solicitar un aumento a AWS Support.

- Los intervalos CIDR del cliente no pueden solaparse con el CIDR local de la VPC donde se encuentra la subred asociada ni con ninguna ruta que se haya agregado manualmente a la tabla de enrutamiento del punto de enlace de Client VPN.
- Los rangos de CIDR del cliente deben tener un tamaño de bloque de al menos /22 y no tienen que ser superiores a /12.
- Una parte de las direcciones del intervalo CIDR del cliente se utiliza para permitir el modelo de disponibilidad del punto de enlace de Client VPN y no se puede asignar a los clientes. Por lo tanto, es recomendable que asigne un bloque de CIDR que contenga el doble de direcciones IP de las necesarias para permitir el máximo número de conexiones simultáneas que tenga previsto admitir en el punto de enlace de Client VPN.
- El intervalo CIDR del cliente no se puede cambiar después de crear el punto de enlace de Client VPN.
- Client VPN admite IPv4 tráfico de doble pila (ambos IPv4 y IPv6). IPv6 Para obtener más información sobre el IPv6 soporte, consulte Consideraciones sobre IPv6 para AWS Client VPN.
- • La dirección IP de origen se traduce a la dirección IP del punto de conexión de Client VPN.
  - El número de puerto de origen original del cliente permanece inalterado.
- Client VPN realiza la traducción de direcciones de puertos (PAT) solo cuando los usuarios simultáneos se conectan al mismo destino. La traducción de puertos es automática y necesaria para admitir múltiples conexiones simultáneas a través del mismo punto de conexión de VPN.
  - Para la traducción de IP de origen, la dirección IP de origen se traduce a la dirección IP de VPN del cliente.
  - Para la traducción de puertos de origen para conexiones de un solo cliente, es posible que el número de puerto de origen original permanezca inalterado.
  - Para la traducción de puertos de origen para varios clientes que se conectan al mismo destino (la misma dirección IP y puerto de destino), Client VPN realiza la traducción de puertos para garantizar conexiones únicas.

  Por ejemplo, cuando dos clientes, cliente 1 y cliente 2, se conectan al mismo servidor y puerto de destino a través de un punto de conexión de Client VPN:

  - El puerto original del cliente 1, por ejemplo, 9999, podría traducirse a un puerto diferente, por ejemplo, el puerto 4306.

  - El puerto original del cliente 2, por ejemplo, 9999, podría traducirse a un puerto único diferente del cliente 1, por ejemplo, el puerto 63922.
- Para IPv6 el tráfico, Client VPN no realiza la traducción de direcciones de red (NAT). Esto proporciona una mayor visibilidad de la IPv6 dirección del usuario conectado.

Configuración de subred y de VPC

- Las subredes asociadas a un punto de enlace de Client VPN deben estar en la misma VPC.
- No puede asociar varias subredes de la misma zona de disponibilidad con un punto de enlace de Client VPN.
- Los puntos de enlace de Client VPN no admiten asociaciones de subredes en una VPC con tenencia dedicada.
- Para el IPv6 tráfico de doble pila, las subredes asociadas deben tener rangos de CIDR de doble pila IPv6 o de doble pila.
- Para puntos de conexión de doble pila, no puede asociar más de una subred por zona de disponibilidad.

Autenticación y seguridad

- El portal de autoservicio no está disponible para los clientes que utilizan la autenticación mutua.
- Si la autenticación multifactor (MFA) está deshabilitada para Active Directory, las contraseñas de usuario no pueden tener el siguiente formato.

```
SCRV1:base64_encoded_string:base64_encoded_string
```

- Los certificados que se utilizan en AWS Client VPN deben cumplir RFC 5280: perfil del certificado de infraestructura de clave pública X.509 de Internet y de la lista de revocación de certificados (CRL), incluidas las extensiones del certificado que se especifican en la sección 4.2 de la nota.
- Los nombres de usuario con caracteres especiales pueden provocar errores de conexión.
- La longitud máxima del nombre de usuario es de 1024 bytes. Se rechazarán las conexiones con nombres de usuario más largos.

Requisitos de conexión y DNS

- No se recomienda conectarse a un punto de conexión de Client VPN mediante direcciones IP. Como Client VPN es un servicio administrado, ocasionalmente verá cambios en las direcciones IP que resuelve el nombre de DNS. Además, verá las interfaces de red Client VPN eliminadas y recreadas en sus CloudTrail registros. Se recomienda conectarse al punto de conexión de Client VPN utilizando el nombre de DNS proporcionado.
- El servicio de Client VPN requiere que la dirección IP a la que se conecta el cliente coincida con la IP que resuelve el nombre de DNS de punto de conexión de Client VPN. En otras palabras, si configura un registro DNS personalizado para el punto final Client VPN y, a continuación, reenvía el tráfico a la dirección IP real a la que se dirige el nombre DNS del punto final, esta configuración no funcionará con los clientes AWS proporcionados recientemente. Esta regla se agregó para mitigar un ataque IP al servidor como se describe aquí: TunnelCrack.
- Puede usar un cliente AWS proporcionado para conectarse a varias sesiones DNS simultáneas. Sin embargo, para que la resolución de nombres funcione correctamente, los servidores de DNS de todas las conexiones deben tener registros sincronizados.
- El servicio de Client VPN requiere que los rangos de direcciones IP de la red de área local (LAN) de los dispositivos cliente estén dentro de los siguientes rangos de direcciones IP privadas estándar: `10.0.0.0/8`, `172.16.0.0/12`, `192.168.0.0/16` o `169.254.0.0/16`. Si se detecta que el rango de direcciones LAN del cliente se encuentra fuera de los rangos anteriores, el punto de conexión de Client VPN enviará automáticamente la directiva de OpenVPN “redirect-gateway block-local” al cliente, lo que forzará todo el tráfico de LAN en la VPN. Por lo tanto, si necesita acceso de LAN durante las conexiones de VPN, se recomienda que utilice los rangos de direcciones convencionales mostrados anteriormente para la LAN. Esta regla se aplica para mitigar las posibilidades de un ataque a la red local, como se describe aquí: TunnelCrack.
- En Windows, cuando se utiliza un punto final de túnel completo, todo el tráfico de DNS pasa por el túnel, independientemente del tipo de dirección IP del punto final (IPv4 IPv6o pila doble). Para que DNS funcione, se debe configurar un servidor de DNS al que se pueda acceder en el túnel.

Restricciones y limitaciones

- Actualmente, no se admite el reenvío de IP cuando se utiliza la aplicación de AWS Client VPN escritorio. Otros clientes admiten el reenvío de IP.
- Client VPN no admite la replicación en varias regiones en AWS Managed Microsoft AD. El punto final Client VPN debe estar en la misma región que el AWS Managed Microsoft AD recurso.

- No puede establecer una conexión VPN desde un ordenador si hay varios usuarios conectados al sistema operativo.
- Client-to-client los IPv6 clientes no admiten la comunicación. Si un IPv6 cliente intenta comunicarse con otro IPv6 cliente, se interrumpirá el tráfico.
- IPv6 y los terminales de doble pila requieren que los dispositivos de los usuarios y los proveedores de servicios de Internet (ISPs) admitan la configuración de IP correspondiente.

Cómo funciona AWS Client VPN

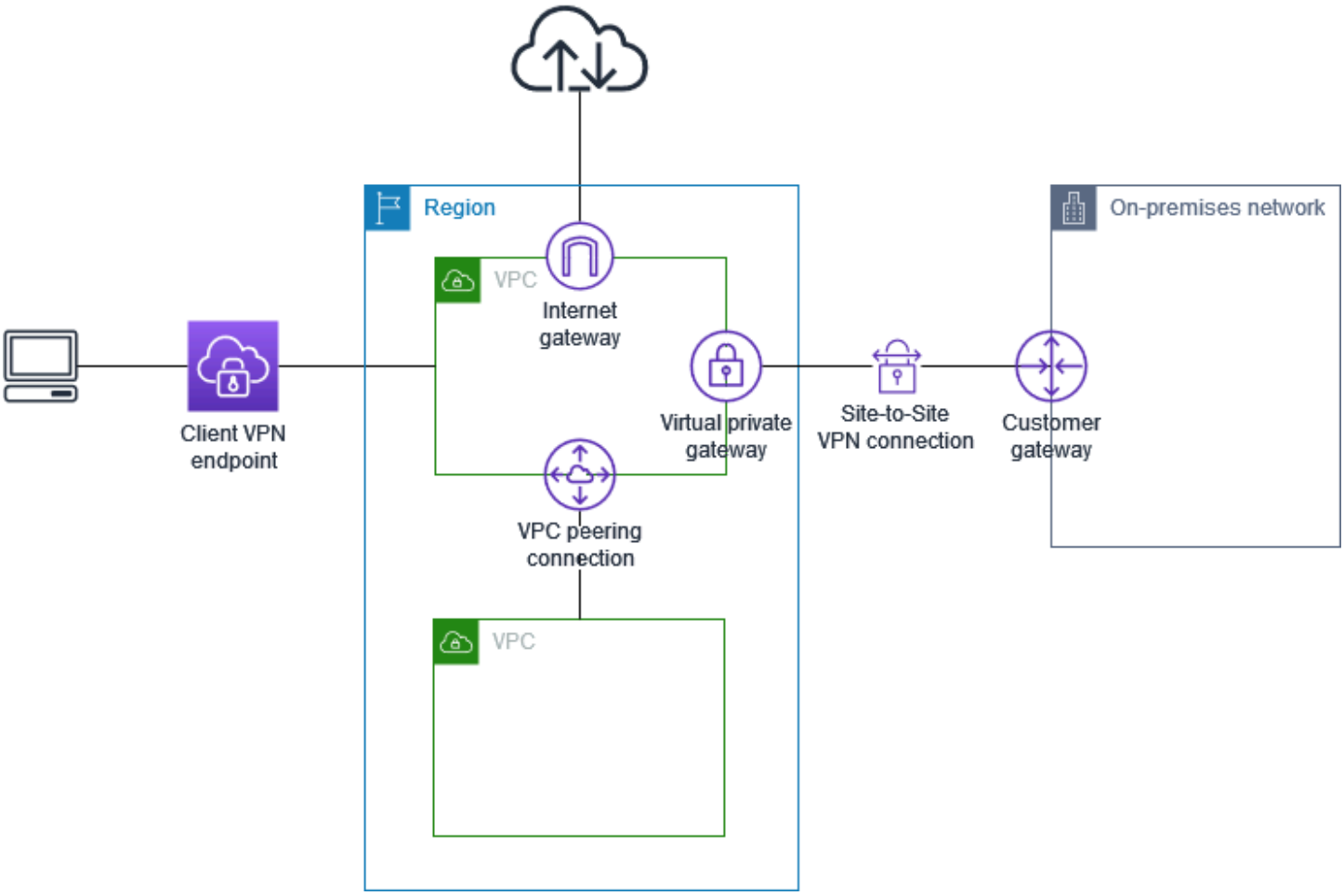
Con AWS Client VPN, hay dos tipos de usuarios que interactúan con el punto de conexión de Client VPN: administradores y clientes.

Client VPN admite conectividad IPv4, IPv6 y de doble pila (tanto IPv4 como IPv6). Puede crear puntos de conexión que utilicen IPv4, IPv6 o ambos, lo que le permitirá conectarse a los recursos de IPv6 de sus VPC o conectarse desde clientes de redes IPv6. Esta flexibilidad ayuda a las organizaciones que ya han implementado o están realizando la transición a una infraestructura de IPv6.

El administrador es responsable de la instalación y configuración del servicio. Esto incluye la creación del punto de conexión de Client VPN, la asociación de la red de destino, la configuración de reglas de autorización y de otras rutas (si es necesario). Una vez que el punto de enlace de Client VPN está instalado y configurado, el administrador descarga el archivo de configuración del punto de enlace de Client VPN y lo distribuye a los clientes que necesitan acceso. El archivo de configuración del punto de conexión de Client VPN contiene el nombre de DNS del punto de conexión de Client VPN y la información de autenticación necesaria para establecer una sesión de VPN. Para obtener más información sobre la configuración del servicio, consulte Comience con AWS Client VPN.

El cliente es el usuario final. Esta es la persona que se conecta al punto de enlace de Client VPN para establecer una sesión de VPN. El cliente establece la sesión de VPN desde su equipo local o un dispositivo móvil mediante una aplicación cliente de VPN basada en OpenVPN. Después de haber establecido la sesión de VPN, puede obtener acceso de forma segura a los recursos de la VPC en la que se encuentra la subred asociada. También puede obtener acceso a otros recursos de AWS, una red en las instalaciones u otros clientes si se han configurado las reglas de autorización y ruta necesarias. Para obtener más información acerca de la conexión a un punto de conexión de Client VPN para establecer una sesión de VPN, consulte Introducción en la Guía del usuario de AWS Client VPN.

En el gráfico siguiente, se ilustra la arquitectura básica de Client VPN.



Escenarios y ejemplos para Client VPN

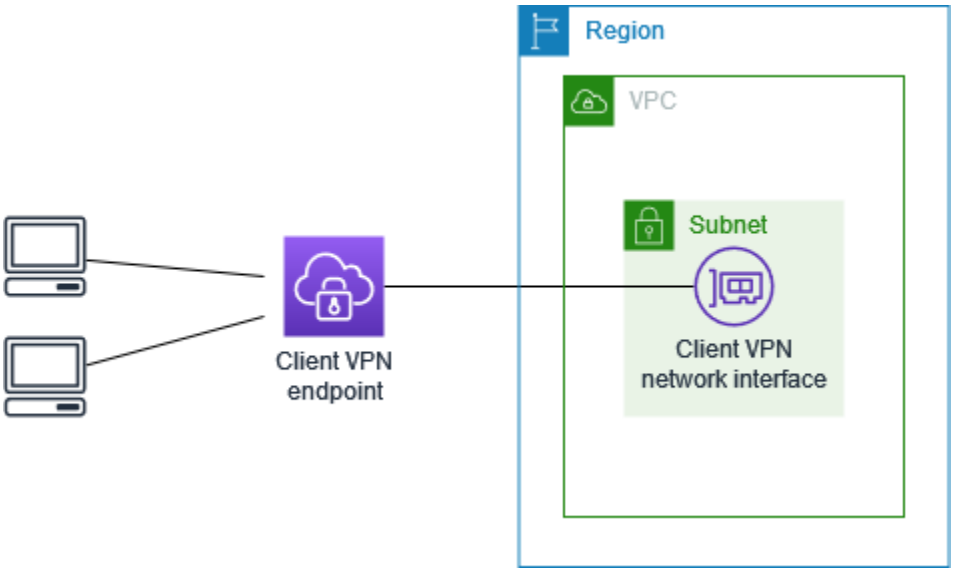
AWS Client VPN es una solución de VPN de acceso remoto totalmente administrada que se utiliza para permitir a los clientes un acceso seguro a los recursos dentro de AWS y de la red en las instalaciones. Existen varias opciones para configurar el acceso. Esta sección contiene ejemplos para crear y configurar el acceso de Client VPN de sus clientes.

Escenarios

- the section called “Acceso a una VPC”
- the section called “Acceso a una VPC interconectada”
- the section called “Acceso a una red en las instalaciones”
- the section called “Acceder a Internet”
- the section called “Acceso entre clientes”
- the section called “Restringir el acceso a la red”

Acceso a una VPC mediante Client VPN

La configuración de AWS Client VPN para este escenario incluye una VPC de destino única. Se recomienda esta configuración si tiene que ofrecer a los clientes acceso a los recursos solo en una única VPC.



Antes de comenzar, haga lo siguiente:

- Cree o identifique una VPC con al menos una subred. Identifique la subred de la VPC que desee asociar con el punto de conexión de Client VPN y anote los intervalos CIDR IPv4.
- Identifique un intervalo de CIDR adecuado para las direcciones IP del cliente que no se superponga con el CIDR de la VPC.
- Revise las reglas y limitaciones de los puntos de enlace de Client VPN en Reglas y mejores prácticas de uso AWS Client VPN.

Para implementar esta configuración

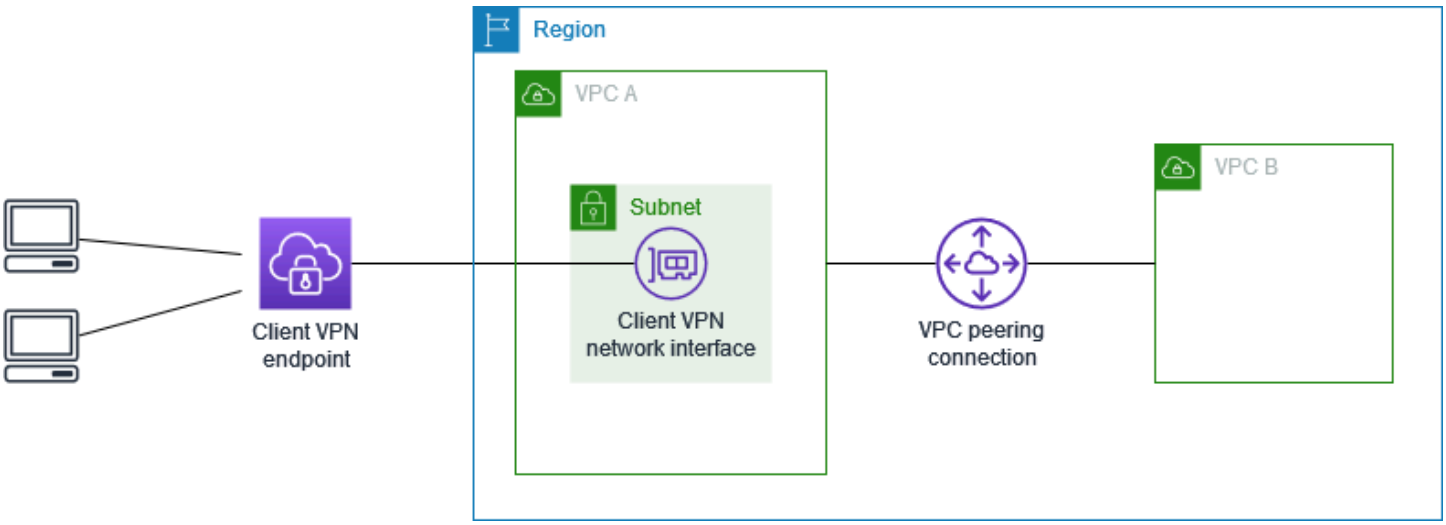
1. Cree un punto de enlace de Client VPN en la misma región que la VPC. Para ello, siga los pasos que se describen en Crear un AWS Client VPN punto final.
2. Asocie la subred con el punto de enlace de Client VPN. Para ello, siga los pasos que se describen en Asociar una red de destino a un AWS Client VPN punto final y seleccione la subred y la VPC que identificó anteriormente.
3. Añada una regla de autorización para dar a los clientes acceso a la VPC. Para ello, siga los pasos que se indican en Agregación de una regla de autorización y, en Destination network (Red de destino), escriba el intervalo CIDR IPv4 de la VPC.

4. Agregue una regla a los grupos de seguridad de sus recursos para permitir el tráfico del grupo de seguridad que se aplicó a la asociación de subred en el paso 2. Para obtener más información, consulte Grupos de seguridad.

Acceso a una VPC mediante Client VPN

La configuración de AWS Client VPN para este escenario incluye una VPC de destino (VPC A) que está interconectada con una VPC adicional (VPC B). Se recomienda esta configuración si tiene que ofrecer a los clientes acceso a los recursos internos de una VPC de destino y otras VPC interconectadas con ella (como la VPC B).

> **Note**
>
> El procedimiento para permitir el acceso a una VPC interconectada (descrito en el siguiente diagrama de red) solo es necesario si el punto de conexión de Client VPN se ha configurado para el modo de división de túneles. En modo de túnel completo, el acceso a la VPC interconectada de forma predeterminada está permitido.



Antes de comenzar, haga lo siguiente:

- Cree o identifique una VPC con al menos una subred. Identifique la subred de la VPC que desee asociar con el punto de conexión de Client VPN y anote los intervalos CIDR IPv4.
- Identifique un intervalo de CIDR adecuado para las direcciones IP del cliente que no se superponga con el CIDR de la VPC.

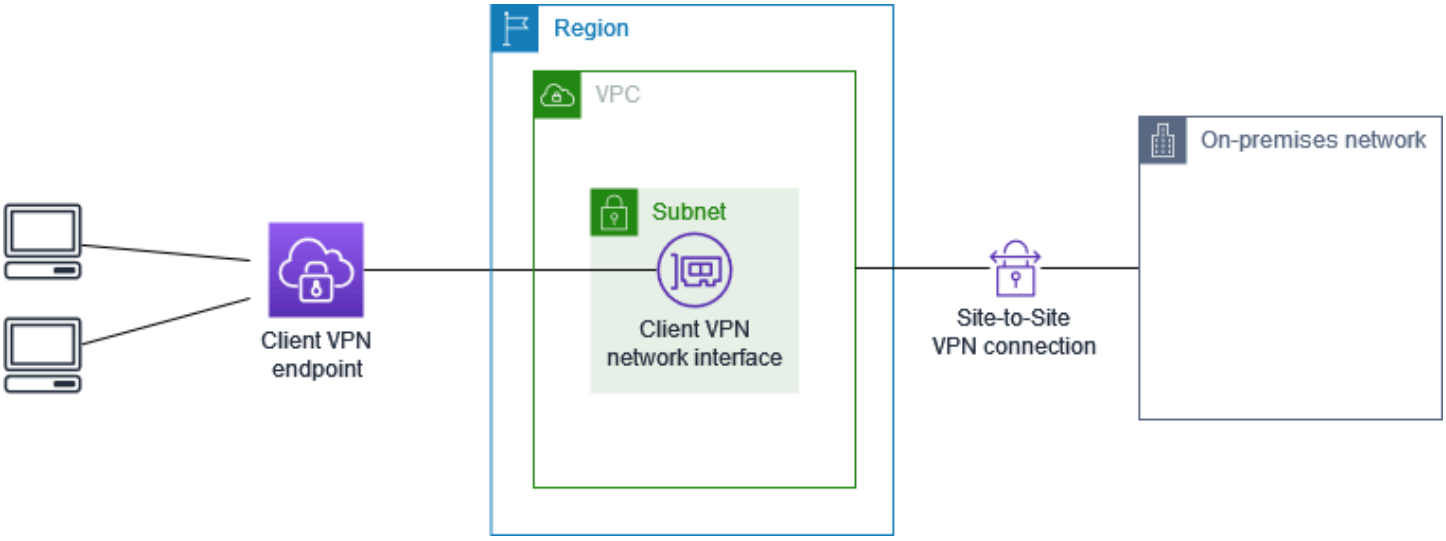
- Revise las reglas y limitaciones de los puntos de enlace de Client VPN en Reglas y mejores prácticas de uso AWS Client VPN.

Para implementar esta configuración

1. Establezca la interconexión de VPC entre las VPC. Siga los pasos que se indican en el artículo Creación y aceptación de interconexiones de VPC de la Guía de interconexión de Amazon VPC. Confirme que las instancias de la VPC A puedan comunicarse con las instancias de la VPC B mediante la conexión de emparejamiento.
2. Cree un punto de enlace de Client VPN en la misma región que la VPC de destino. En el diagrama, es VPC A. Realice los pasos descritos en Crear un AWS Client VPN punto final.
3. Asocie la subred que identificó con el punto de conexión de Client VPN que ha creado. Para ello, siga los pasos que se indican en Asociar una red de destino a un AWS Client VPN punto final, seleccione la VPC y la subred. De forma predeterminada, asociamos el grupo de seguridad predeterminado de la VPC con el punto de conexión de Client VPN. Puede asociar un grupo de seguridad diferente siguiendo los pasos que se describen en the section called “Aplicación de un grupo de seguridad a una red de destino”.
4. Agregue una regla de autorización para proporcionar a los clientes acceso a la VPC de destino. Para ello, siga los pasos que se describen en Agregación de una regla de autorización. En Destination network to enable (Red de destino que se va a habilitar), escriba el intervalo CIDR IPv4 de la VPC.
5. Añada una ruta para dirigir el tráfico hacia la VPC interconectada. En el diagrama, es VPC B. Para ello, siga los pasos que se describen en Creación de una ruta de punto de conexión de AWS Client VPN. Para el Destino de la ruta, ingrese el intervalo CIDR IPv4 de la VPC interconectada. En ID de subred de VPC de destino, seleccione la subred que está asociada al punto de conexión de Client VPN.
6. Añada una regla de autorización para ofrecer a los clientes acceso a la VPC interconectada. Para ello, siga los pasos que se describen en Agregación de una regla de autorización. En Red de destino, escriba el intervalo CIDR IPv4 de la VPC interconectada.
7. Agregue una regla a los grupos de seguridad para las instancias en la VPC A y VPC B para permitir el tráfico del grupo de seguridad que solicitó el punto de conexión de Client VPN en el paso 3. Para obtener más información, consulte Grupos de seguridad.

Acceso a una red en las instalaciones mediante Client VPN

La configuración de AWS Client VPN para este escenario incluye acceso a una red solo en las instalaciones. Se recomienda esta configuración si tiene que ofrecer a los clientes acceso a los recursos que hay únicamente en una red local.



Antes de comenzar, haga lo siguiente:

- Cree o identifique una VPC con al menos una subred. Identifique la subred de la VPC que desee asociar con el punto de conexión de Client VPN y anote los intervalos CIDR IPv4.
- Identifique un intervalo de CIDR adecuado para las direcciones IP del cliente que no se superponga con el CIDR de la VPC.
- Revise las reglas y limitaciones de los puntos de enlace de Client VPN en Reglas y mejores prácticas de uso AWS Client VPN.

Para implementar esta configuración

1. Habilite la comunicación entre la VPC y su propia red en las instalaciones a través de una conexión Site-to-Site VPN de AWS. Para ello, siga los pasos descritos en la Introducción de la Guía del usuario de AWS Site-to-Site VPN.

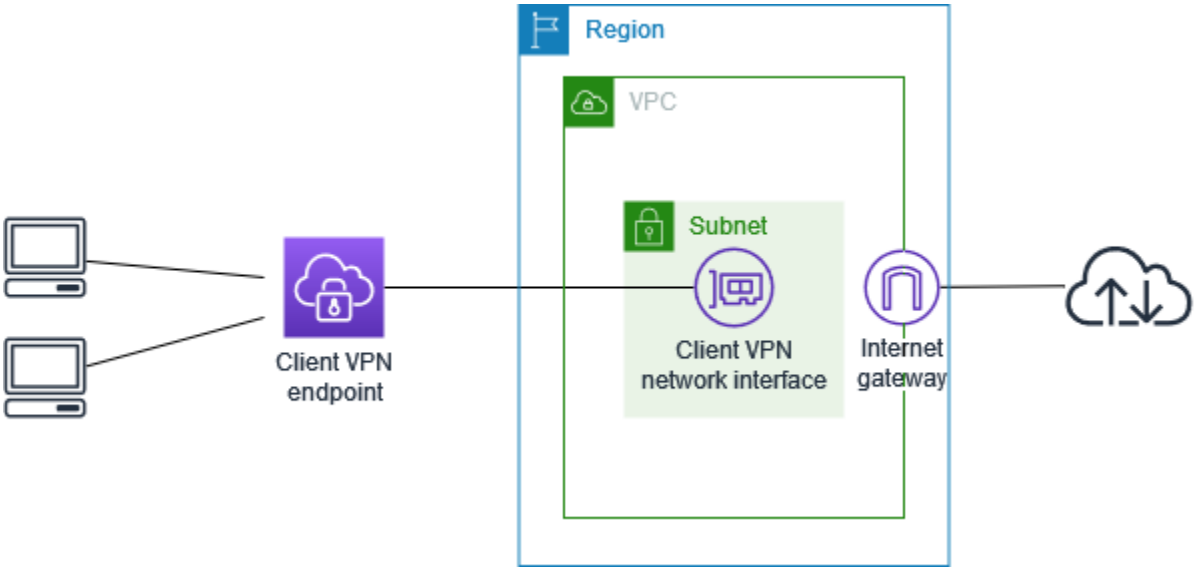
> **Note**
>
> Como opción, puede implementar esta situación mediante una conexión de Direct Connect entre la VPC y la red en las instalaciones. Para obtener más información, consulte la Guía del usuario de Direct Connect.

2. Pruebe la conexión de Site-to-Site VPN de AWS que creó en el paso anterior. Para ello, siga los pasos que se indican en la sección Comprobación de la conexión de Site-to-Site VPN de la Guía del usuario de AWS Site-to-Site VPN. Si la conexión de VPN funciona tal y como se esperaba, continúe en el siguiente paso.
3. Cree un punto de enlace de Client VPN en la misma región que la VPC. Para ello, siga los pasos que se describen en Crear un AWS Client VPN punto final.
4. Asocie la subred que identificó anteriormente con el punto de enlace de Client VPN. Para ello, siga los pasos que se describen en Asociar una red de destino a un AWS Client VPN punto final y seleccione la VPC y la subred.
5. Añada una ruta que permita el acceso a la conexión de Site-to-Site VPN de AWS. Para ello, siga los pasos que se indican en Creación de una ruta de punto de conexión de AWS Client VPN; a continuación, en Route destination (Destino de ruta), ingrese el rango IPv4 CIDR de la conexión de Site-to-Site VPN de AWS y, en Target VPC Subnet ID (ID de subred de la VPC de destino), seleccione la subred que asoció al punto de enlace de Client VPN.
6. Añada una regla de autorización para proporcionar a los clientes acceso a la conexión de Site-to-Site VPN de AWS. Para ello, siga los pasos que se indican en Agregar una regla de autorización a un AWS Client VPN punto final; en Destination network (Red de destino), ingrese el intervalo CIDR IPv4 de la conexión de Site-to-Site VPN de AWS.

Acceso a Internet mediante Client VPN

La configuración de AWS Client VPN para este escenario incluye una única VPC de destino y acceso a Internet. Se recomienda esta configuración si tiene que ofrecer a los clientes acceso a los recursos que están en una única VPC de destino y también permitir el acceso a Internet.

Si completó el tutorial Comience con AWS Client VPN, entonces ya ha implementado este escenario.



Antes de comenzar, haga lo siguiente:

- Cree o identifique una VPC con al menos una subred. Identifique la subred de la VPC que desee asociar con el punto de conexión de Client VPN y anote los intervalos CIDR IPv4.
- Identifique un intervalo de CIDR adecuado para las direcciones IP del cliente que no se superponga con el CIDR de la VPC.
- Revise las reglas y limitaciones de los puntos de enlace de Client VPN en Reglas y mejores prácticas de uso AWS Client VPN.

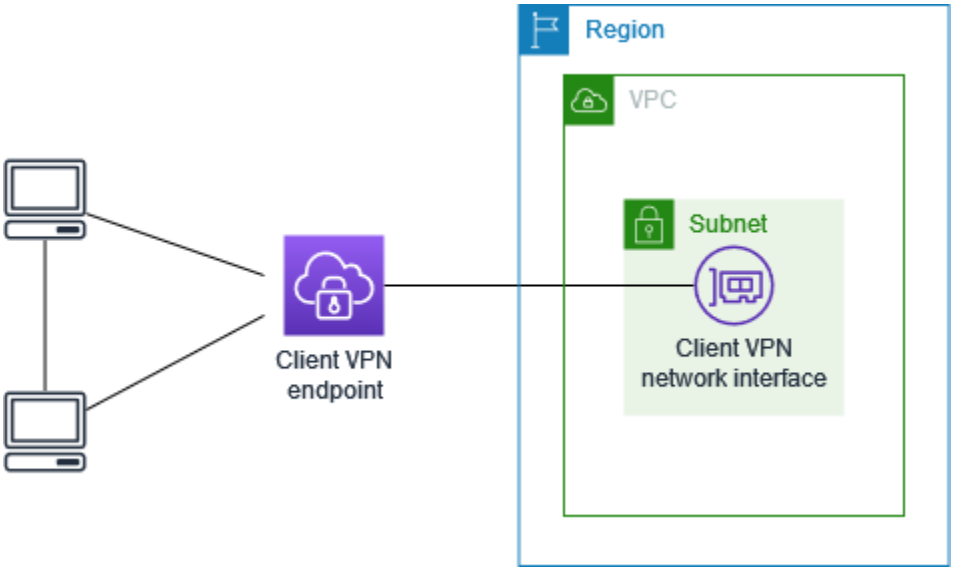
Para implementar esta configuración

1. Asegúrese de que el grupo de seguridad que va a utilizar con el punto de conexión de Client VPN permita el tráfico de Internet de salida. Para ello, agregue reglas de salida que permitan el tráfico hacia 0.0.0.0/0 para el tráfico HTTP y HTTPS.
2. Cree una gateway de Internet y asóciela a su VPC Para obtener más información, consulte Crear y asociar una gateway de Internet en la Guía del usuario de Amazon VPC.
3. Haga que su subred sea pública añadiendo una ruta al gateway de Internet en su tabla de ruteo. En la consola de VPC, elija Subnets (Subredes), seleccione la subred que desea asociar con el punto de enlace de Client VPN, haga clic en Route Table (Tabla de enrutamiento) y elija el ID de la tabla de enrutamiento. Elija Actions (Acciones), seleccione Edit routes (Editar rutas) y luego Add route (Añadir ruta). En Destination (Destino), escriba `0.0.0.0/0` y, en Target (Destino), elija la gateway de Internet del paso anterior.

4. Cree un punto de enlace de Client VPN en la misma región que la VPC. Para ello, siga los pasos que se describen en Crear un AWS Client VPN punto final.
5. Asocie la subred que identificó anteriormente con el punto de enlace de Client VPN. Para ello, siga los pasos que se describen en Asociar una red de destino a un AWS Client VPN punto final y seleccione la VPC y la subred.
6. Añada una regla de autorización para dar a los clientes acceso a la VPC. Para ello, siga los pasos que se indican en Agregación de una regla de autorización y, en Destination network to enable (Red de destino que se va a activar), escriba el intervalo CIDR IPv4 de la VPC.
7. Agregue una ruta que permita que el tráfico a Internet. Para ello, siga los pasos que se indican en Creación de una ruta de punto de conexión de AWS Client VPN; a continuación, en Route destination (Destino de ruta), escriba `0.0.0.0/0` y, en Target VPC Subnet ID (ID de subred de la VPC de destino), seleccione la subred que asoció con el punto de enlace de Client VPN.
8. Agregue una regla de autorización para dar a los clientes acceso a Internet. Para ello, siga los pasos que se indican en Agregación de una regla de autorización y, a continuación, en Destination network (Red de destino), escriba `0.0.0.0/0`.
9. Asegúrese de que los grupos de seguridad de los recursos de la VPC tengan una regla que permita el acceso desde el grupo de seguridad asociado con el punto de conexión de Client VPN. Esto permite a sus clientes acceder a los recursos de su VPC.

Acceso de cliente a cliente mediante Client VPN

La configuración de AWS Client VPN para este escenario permite a los clientes acceder a una sola VPC y enrutar el tráfico entre sí. Esta es la configuración recomendada si los clientes que se conectan al mismo punto de enlace de Client VPN también necesitan comunicarse entre sí. Los clientes pueden comunicarse entre sí utilizando la dirección IP única que se les asigna desde el intervalo CIDR del cliente cuando se conectan al punto de enlace de Client VPN.



Antes de comenzar, haga lo siguiente:

- Cree o identifique una VPC con al menos una subred. Identifique la subred de la VPC que desee asociar con el punto de conexión de Client VPN y anote los intervalos CIDR IPv4.
- Identifique un intervalo de CIDR adecuado para las direcciones IP del cliente que no se superponga con el CIDR de la VPC.
- Revise las reglas y limitaciones de los puntos de enlace de Client VPN en Reglas y mejores prácticas de uso AWS Client VPN.

> **Note**
>
> Las reglas de autorización basadas en la red que utilizan grupos de Active Directory o grupos de IdP basados en SAML no están soportados en este escenario.

Para implementar esta configuración

1. Cree un punto de enlace de Client VPN en la misma región que la VPC. Para ello, siga los pasos que se describen en Crear un AWS Client VPN punto final.
2. Asocie la subred que identificó anteriormente con el punto de enlace de Client VPN. Para ello, siga los pasos que se describen en Asociar una red de destino a un AWS Client VPN punto final y seleccione la VPC y la subred.

3. Agregue una ruta a la red local en la tabla de enrutamiento. Para ello, siga los pasos que se describen en Creación de una ruta de punto de conexión de AWS Client VPN. En Route destination (Destino de ruta), escriba el intervalo CIDR del cliente y, en Target VPC Subnet ID (ID de subred de VPC de destino), especifique `local`.
4. Añada una regla de autorización para dar a los clientes acceso a la VPC. Para ello, siga los pasos que se describen en Agregación de una regla de autorización. En Destination network to enable (Red de destino que se va a habilitar), escriba el intervalo CIDR IPv4 de la VPC.
5. Agregue una regla de autorización para proporcionar a los clientes acceso al intervalo CIDR del cliente. Para ello, siga los pasos que se describen en Agregación de una regla de autorización. En Destination network to enable (Red de destino que se va a habilitar), escriba el intervalo CIDR del cliente.

Restricción del acceso a su red mediante Client VPN

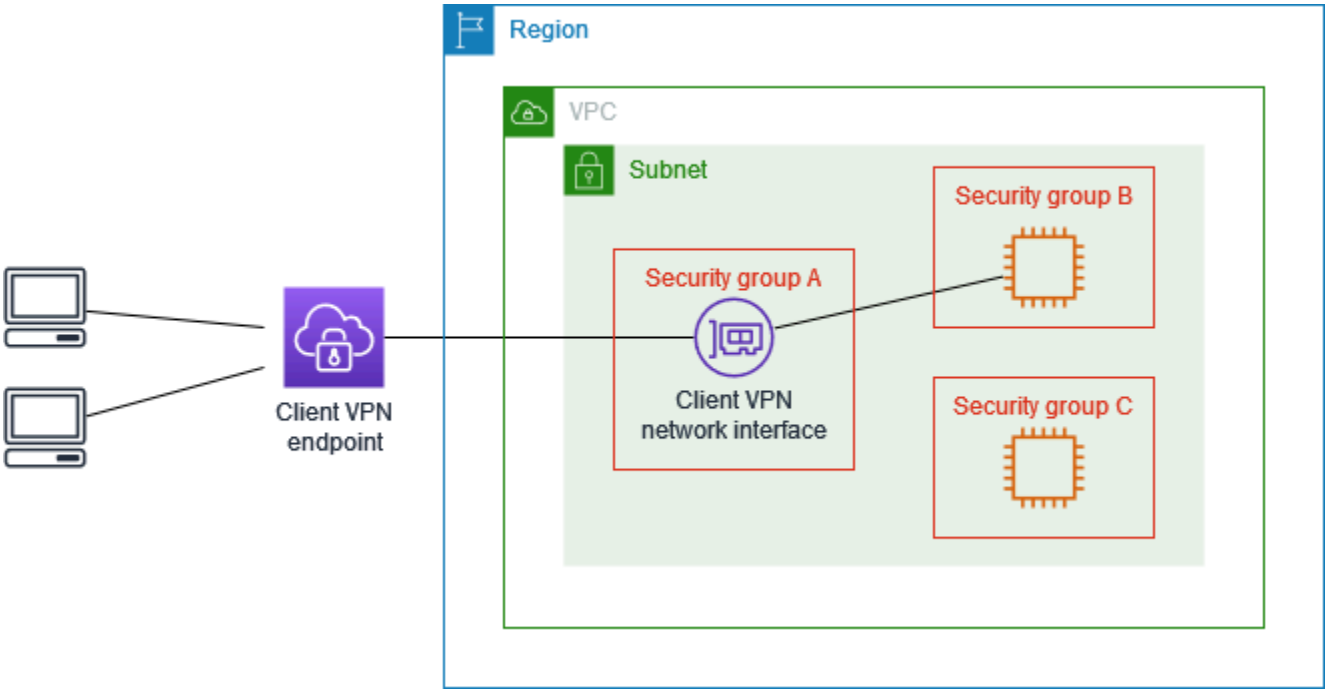
Puede configurar el punto de enlace de AWS Client VPN para restringir el acceso a recursos específicos de la VPC. En la autenticación basada en usuarios, también puede restringir el acceso a partes de la red en función del grupo de usuarios que accede al punto de enlace de Client VPN.

Restringir el acceso mediante grupos de seguridad

Puede conceder o denegar el acceso a recursos específicos de la VPC. Para ello, solo tiene que agregar o quitar reglas del grupo de seguridad que hagan referencia al grupo de seguridad que se aplicó a la asociación de red de destino (el grupo de seguridad de Client VPN). Esta configuración se amplía en el escenario que se describe en Acceso a una VPC mediante Client VPN. Esta configuración se aplica de manera adicional a la regla de autorización configurada en ese escenario.

Para conceder acceso a un recurso específico, identifique el grupo de seguridad asociado a la instancia en la que se está ejecutando el recurso. A continuación, cree una regla que permita el tráfico desde el grupo de seguridad de Client VPN.

En el siguiente diagrama, el grupo de seguridad A es el grupo de seguridad de Client VPN, el grupo de seguridad B está asociado a una instancia de EC2 y el grupo de seguridad C está asociado a una instancia de EC2. Si añade una regla al grupo de seguridad B que permita el acceso desde el grupo de seguridad A, los clientes podrán acceder a la instancia asociada al grupo de seguridad B. Si el grupo de seguridad C no tiene una regla que permita el acceso desde el grupo de seguridad A, los clientes no podrán acceder a la instancia asociada al grupo de seguridad C.



Antes de comenzar, compruebe si el grupo de seguridad de Client VPN está asociado a otros recursos de la VPC. Si agrega o quita reglas que hacen referencia al grupo de seguridad de Client VPN, puede darse el caso de que también conceda o deniegue el acceso a otros recursos asociados. Para evitar esto, utilice un grupo de seguridad creado específicamente para el punto de enlace de Client VPN.

Para crear una regla de un grupo de seguridad

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Security Groups (Grupos de seguridad).
3. Elija el grupo de seguridad asociado a la instancia en la que se ejecute el recurso.
4. Seleccione Actions (Acciones), Edit inbound rules (Editar reglas de entrada).
5. Elija Add Rule (Agregar regla) y, a continuación, haga lo siguiente:
   - En Type (Tipo), elija All traffic (Todo el tráfico) o un tipo específico de tráfico que desee permitir.
   - En Source (Origen), elija Custom (Personalizado) y, a continuación, escriba o elija el ID del grupo de seguridad de Client VPN.
6. Seleccione Save rules (Guardar reglas).

Para quitar el acceso a un recurso específico, compruebe el grupo de seguridad asociado a la instancia en la que se está ejecutando el recurso. Si hay una regla que permite el tráfico desde el grupo de seguridad de Client VPN, elimínela.

Para comprobar las reglas del grupo de seguridad

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Security Groups (Grupos de seguridad).
3. Seleccione Inbound Rules (Reglas de entrada).
4. Revise la lista de reglas. Si hay una regla en la que Source (Origen) es el grupo de seguridad de Client VPN, elija Edit rules (Editar reglas) y, en la regla, haga clic en Delete (Eliminar) (el icono x). Seleccione Save rules (Guardar reglas).

Restringir el acceso en función de grupos de usuarios

Si el punto de enlace de Client VPN está configurado para utilizar la autenticación basada en usuarios, puede permitir que grupos específicos de usuarios tengan acceso a partes concretas de la red. Para ello, siga los pasos que se describen a continuación:

1. Configure usuarios y grupos en Directory Service o en su IdP. Para obtener más información, consulte los siguientes temas:
   - Autenticación con Active Directory en Client VPN
   - Requisitos y consideraciones de la autenticación federada basada en SAML
2. Cree una regla de autorización para el punto de enlace de Client VPN que permita que un grupo especificado pueda acceder a toda la red o a parte ella. Para obtener más información, consulte AWS Client VPN reglas de autorización.

Si el punto de enlace de Client VPN está configurado para utilizar la autenticación mutua, no se pueden configurar grupos de usuarios. Al crear una regla de autorización, debe conceder acceso a todos los usuarios. Para permitir que grupos específicos de usuarios tengan acceso a partes específicas de la red, puede crear varios puntos de enlace de Client VPN. Por ejemplo, para cada grupo de usuarios que tiene acceso a la red, haga lo siguiente:

1. Cree un conjunto de certificados y claves de servidor y cliente para ese grupo de usuarios. Para obtener más información, consulte Autenticación mutua en AWS Client VPN.

2. Cree un punto de enlace de Client VPN. Para obtener más información, consulte Crear un AWS Client VPN punto final.
3. Cree una regla de autorización que conceda acceso a la totalidad o parte de la red. Por ejemplo, si se trata de un punto de enlace de Client VPN que van a utilizar los administradores, puede crear una regla de autorización que conceda acceso a toda la red. Para obtener más información, consulte Agregación de una regla de autorización.

Autenticación de cliente en AWS Client VPN

La autenticación del cliente se implementa en el primer punto de entrada a la AWS nube. Se utiliza para determinar si los clientes tienen permiso para conectarse al punto de enlace de Client VPN. Si la autenticación se realiza correctamente, los clientes se conectan al punto de enlace de Client VPN y establecen una sesión de VPN. Si la autenticación falla, se deniega la conexión y el cliente no podrá establecer una sesión de VPN.

Client VPN permite utilizar los siguientes tipos de autenticación de cliente:

- Autenticación con Active Directory (basada en el usuario)
- Autenticación mutua (basada en certificados)
- Inicio de sesión único (autenticación federada basada en SAML) (basada en el usuario)

Puede utilizar solo uno de los métodos anteriores o una combinación de autenticación mutua con un método basado en usuarios como el siguiente:

- Autenticación mutua y autenticación federada
- Autenticación mutua y autenticación con Active Directory

> **Important**
>
> - Para crear un punto de conexión de Client VPN, debe aprovisionar un certificado de servidor en AWS Certificate Manager, independientemente del tipo de autenticación que utilice. Para obtener más información acerca de cómo crear y aprovisionar un certificado de servidor, consulte los pasos de Autenticación mutua en AWS Client VPN.

- Si utiliza una combinación de autenticación mutua y autenticación basada en el usuario, debe utilizar ambos métodos para autenticarse correctamente en la VPN.

Autenticación con Active Directory en Client VPN

Client VPN proporciona compatibilidad con Active Directory al integrarse con Directory Service. Con la autenticación de Active Directory, los clientes se autentican en grupos de Active Directory existentes. Si Directory Service lo usa, Client VPN puede conectarse a Active Directories existentes aprovisionados en su red local AWS o dentro de ella. Esto le permite utilizar su infraestructura de autenticación del cliente existente. Si utiliza un Active Directory local y no tiene un Microsoft AD AWS administrado existente, debe configurar un conector de Active Directory (AD Connector). Puede utilizar un servidor de Active Directory para autenticar a los usuarios. Para obtener más información acerca de la integración de Active Directory, consulte la Guía de administración de AWS Directory Service.

Client VPN admite la autenticación multifactor (MFA) cuando está habilitada para AWS Managed Microsoft AD o AD Connector. Si la MFA está activada, los clientes tienen que especificar un nombre de usuario, una contraseña y un código de MFA al conectarse a un punto de enlace de Client VPN. Para obtener más información acerca de cómo habilitar la MFA, consulte Habilitar la autenticación multifactor para AWS Managed Microsoft AD y Habilitar la autenticación multifactor para AD Connector en la Guía de administración de AWS Directory Service .

Para obtener información sobre las cuotas y las reglas para configurar usuarios y grupos en Active Directory, consulte Cuotas de usuarios y grupos.

Autenticación mutua en AWS Client VPN

Con la autenticación mutua, Client VPN utiliza certificados para realizar la autenticación entre el cliente y el servidor. Los certificados son un formulario digital de identificación emitido por una entidad de certificación (CA). El servidor utiliza certificados de cliente para autenticar a los clientes cuando intentan conectarse al punto de enlace de Client VPN. Debe crear un certificado y una clave de servidor y al menos un certificado y una clave de cliente.

Debe cargar el certificado del servidor en AWS Certificate Manager (ACM) y especificarlo al crear un punto final Client VPN. Cuando se carga el certificado de servidor en ACM, también se especifica la entidad de certificación (CA). Solo tiene que cargar el certificado de cliente en ACM cuando la entidad de certificación del certificado de cliente es diferente de la entidad de certificación del

certificado de servidor. Para obtener más información acerca de ACM, consulte la Guía del usuario de AWS Certificate Manager.

Puede crear una clave y un certificado de cliente diferentes para cada uno de los clientes que se conecte al punto de enlace de Client VPN. De esta forma, puede revocar un certificado de cliente específico si un usuario abandona la organización. En este caso, cuando cree el punto de enlace de Client VPN, puede especificar el ARN del certificado de servidor para el certificado de cliente, siempre que la misma entidad de certificación haya emitido los dos certificados.

Los certificados que se utilizan en AWS Client VPN deben cumplir RFC 5280: perfil del certificado de infraestructura de clave pública X.509 de Internet y de la lista de revocación de certificados (CRL), incluidas las extensiones del certificado que se especifican en la sección 4.2 de la nota.

> **Note**
>
> Los puntos de enlace de Client VPN solo admiten claves RSA con un tamaño de 1024 bits y 2048 bits. Además, el certificado de cliente debe tener el atributo CN en el campo Subject (Asunto).
>
> Cuando se actualicen los certificados usados con el servicio Client VPN, ya sea mediante la rotación automática de ACM, importando manualmente un nuevo certificado o actualizaciones de metadatos al Centro de identidades de IAM, el servicio Client VPN actualizará automáticamente el punto de conexión de Client VPN con el certificado más reciente. Se trata de un proceso automatizado que puede tardar hasta 5 horas.

Tareas

- Habilitar la autenticación mutua para AWS Client VPN
- Renovación del certificado de servidor para AWS Client VPN

Habilitar la autenticación mutua para AWS Client VPN

Puede habilitar la autenticación mutua en Client VPN en Windows Linux/MacOS o en Windows.

Linux/macOS

En el procedimiento siguiente, se usa easy-rsa de OpenVPN para generar los certificados y las claves del servidor y el cliente, y después se cargan la clave y el certificado del servidor en ACM. Para obtener más información, consulte Easy-RSA 3 Quickstart README.

Para generar las claves y los certificados del cliente y el servidor, y cargarlos en ACM

1. Clone el repositorio easy-rsa de OpenVPN en su equipo local y navegue a la carpeta `easy-rsa/easyrsa3`.

```
$ git clone https://github.com/OpenVPN/easy-rsa.git
```

```
$ cd easy-rsa/easyrsa3
```

2. Inicialice un nuevo entorno de PKI.

```
$ ./easyrsa init-pki
```

3. Para crear una nueva entidad de certificación (CA), ejecute este comando y siga las indicaciones.

```
$ ./easyrsa build-ca nopass
```

4. Genere el certificado y la clave del servidor.

```
$ ./easyrsa --san=DNS:server build-server-full server nopass
```

5. Genere el certificado y la clave del cliente.

   Asegúrese de guardar el certificado del cliente y la clave privada del cliente, ya que los necesitará para configurar el cliente.

```
$ ./easyrsa build-client-full client1.domain.tld nopass
```

   Tiene la opción de repetir este paso para cada cliente (usuario final) que requiera un certificado y una clave de cliente.

6. Copie el certificado y la clave del servidor y el certificado y la clave del cliente en una carpeta personalizada y, a continuación, vaya a la carpeta personalizada.

   Antes de copiar los certificados y las claves, cree la carpeta personalizada; para ello, ejecute el comando `mkdir`. En el ejemplo siguiente se crea una carpeta personalizada en el directorio principal.

```
$ mkdir ~/custom_folder/
```

```
$ cp pki/ca.crt ~/custom_folder/
$ cp pki/issued/server.crt ~/custom_folder/
$ cp pki/private/server.key ~/custom_folder/
$ cp pki/issued/client1.domain.tld.crt ~/custom_folder
$ cp pki/private/client1.domain.tld.key ~/custom_folder/
$ cd ~/custom_folder/
```

7. Cargue las claves y los certificados del cliente y el servidor en ACM. No olvide cargarlos en la misma región en la que quiere crear el punto de enlace de Client VPN. Los siguientes comandos utilizan la AWS CLI para cargar los certificados. Para cargar los certificados a través de la consola de ACM en su lugar, consulte Importar un certificado en la Guía del usuario de AWS Certificate Manager .

```
$ aws acm import-certificate --certificate fileb://server.crt --private-key
 fileb://server.key --certificate-chain fileb://ca.crt
```

```
$ aws acm import-certificate --certificate fileb://client1.domain.tld.crt --
private-key fileb://client1.domain.tld.key --certificate-chain fileb://ca.crt
```

No es necesario cargar el certificado de cliente en ACM. Si el servidor y los certificados del cliente los ha emitido la misma entidad de certificación (CA), puede utilizar el ARN del certificado del servidor para el servidor y el cliente cuando cree el punto de enlace de Client VPN. En los pasos anteriores, se ha utilizado la misma CA para crear ambos certificados. Sin embargo, se incluyen los pasos para cargar el certificado de cliente con ánimo de exhaustividad.

Windows

El siguiente procedimiento instala el software Easy-RSA 3.x y lo utiliza para generar los certificados y claves de servidor y cliente.

Para generar las claves y los certificados del cliente y el servidor y cargarlos en ACM

1. Abra la página de versiones de EasyRSA y descargue el archivo ZIP para extraer la versión de Windows.
2. Abra un símbolo del sistema y vaya a la ubicación en la que se extrajo la carpeta `EasyRSA-3.x`.
3. Ejecute el siguiente comando para abrir el shell de EasyRSA 3.

```
C:\Program Files\EasyRSA-3.x> .\EasyRSA-Start.bat
```

4. Inicialice un nuevo entorno de PKI.

```
# ./easyrsa init-pki
```

5. Para crear una nueva entidad de certificación (CA), ejecute este comando y siga las indicaciones.

```
# ./easyrsa build-ca nopass
```

6. Genere el certificado y la clave del servidor.

```
# ./easyrsa --san=DNS:server build-server-full server nopass
```

7. Genere el certificado y la clave del cliente.

```
# ./easyrsa build-client-full client1.domain.tld nopass
```

   Tiene la opción de repetir este paso para cada cliente (usuario final) que requiera un certificado y una clave de cliente.

8. Salga del shell de EasyRSA 3.

```
# exit
```

9. Copie el certificado y la clave del servidor y el certificado y la clave del cliente en una carpeta personalizada y, a continuación, vaya a la carpeta personalizada.

   Antes de copiar los certificados y las claves, cree la carpeta personalizada; para ello, ejecute el comando `mkdir`. En el ejemplo siguiente se crea una carpeta personalizada en su unidad C:\.

```
C:\Program Files\EasyRSA-3.x> mkdir C:\custom_folder
C:\Program Files\EasyRSA-3.x> copy pki\ca.crt C:\custom_folder
C:\Program Files\EasyRSA-3.x> copy pki\issued\server.crt C:\custom_folder
C:\Program Files\EasyRSA-3.x> copy pki\private\server.key C:\custom_folder
C:\Program Files\EasyRSA-3.x> copy pki\issued\client1.domain.tld.crt C:
\custom_folder
```

```
C:\Program Files\EasyRSA-3.x> copy pki\private\client1.domain.tld.key C:
\custom_folder
C:\Program Files\EasyRSA-3.x> cd C:\custom_folder
```

10. Cargue las claves y los certificados del cliente y el servidor en ACM. No olvide cargarlos en la misma región en la que quiere crear el punto de enlace de Client VPN. Los siguientes comandos utilizan el AWS CLI para cargar los certificados. Para cargar los certificados a través de la consola de ACM en su lugar, consulte Importar un certificado en la Guía del usuario de AWS Certificate Manager .

```
aws acm import-certificate \
    --certificate fileb://server.crt \
    --private-key fileb://server.key \
    --certificate-chain fileb://ca.crt
```

```
aws acm import-certificate \
    --certificate fileb://client1.domain.tld.crt \
    --private-key fileb://client1.domain.tld.key \
    --certificate-chain fileb://ca.crt
```

No es necesario cargar el certificado de cliente en ACM. Si el servidor y los certificados del cliente los ha emitido la misma entidad de certificación (CA), puede utilizar el ARN del certificado del servidor para el servidor y el cliente cuando cree el punto de enlace de Client VPN. En los pasos anteriores, se ha utilizado la misma CA para crear ambos certificados. Sin embargo, se incluyen los pasos para cargar el certificado de cliente con ánimo de exhaustividad.

Renovación del certificado de servidor para AWS Client VPN

Puede renovar y volver a importar un certificado de servidor de Client VPN que haya caducado. En función de la versión de OpenVPN easy-rsa que utilice, el procedimiento variará. Consulte la documentación de renovación y revocación del certificado de Easy-RSA 3 para obtener más información.

Renovación del certificado de servidor

1. Realice una de las siguientes acciones siguientes:
   - Versión 3.1.x de Easy-RSA

- Ejecute el comando de renovación de certificados.

```
$ ./easyrsa renew server nopass
```

- Versión 3.2.x de Easy-RSA

a. Ejecute el comando expire.

```
$ ./easyrsa expire server
```

b. Firme un certificado nuevo.

```
$ ./easyrsa --san=DNS:server sign-req server server
```

2. Cree una carpeta personalizada, copie los nuevos archivos en ella y, a continuación, navegue hasta la carpeta.

```
$ mkdir ~/custom_folder2
$ cp pki/ca.crt ~/custom_folder2/
$ cp pki/issued/server.crt ~/custom_folder2/
$ cp pki/private/server.key ~/custom_folder2/
$ cd ~/custom_folder2/
```

3. Importe los archivos nuevos en ACM. Asegúrese de importarlos en la misma región que el punto de conexión de Client VPN.

```
$ aws acm import-certificate \
    --certificate fileb://server.crt \
    --private-key fileb://server.key \
    --certificate-chain fileb://ca.crt \
    --certificate-arn
 arn:aws:acm:region:123456789012:certificate/12345678-1234-1234-1234-12345678901
```

Inicio de sesión único (autenticación federada basada en SAML 2.0) en Client VPN

AWS Client VPN admite la federación de identidades con Security Assertion Markup Language 2.0 (SAML 2.0) para terminales Client VPN. Puede usar proveedores de identidad (IdPs) compatibles con SAML 2.0 para crear identidades de usuario centralizadas. A continuación, puede configurar un

punto de enlace de Client VPN para utilizar la autenticación federada basada en SAML y asociarlo al proveedor de identidades. Los usuarios se conectarán entonces al punto de enlace de Client VPN utilizando sus credenciales centralizadas.

Temas

Habilitar SAML para AWS Client VPN

Puede habilitar SAML para el inicio de sesión único en Client VPN siguiendo estos pasos. Asimismo, si habilitó el portal de autoservicio del punto de enlace de Client VPN, también puede pedirle a los usuarios que lo utilicen para obtener el archivo de configuración y el cliente proporcionado por AWS . Para obtener más información, consulte Acceso de AWS Client VPN al portal de la autoservicio.

Para que el proveedor de identidades basado en SAML funcione con un punto de enlace de Client VPN, debe hacer lo siguiente.

1. Cree una aplicación basada en SAML en el IDP que elija para usarla con una aplicación existente o utilice una AWS Client VPN aplicación existente.
2. Configure el IdP para establecer una relación de confianza con AWS. Para obtener información sobre los recursos, consulte Recursos de configuración de IdP basados en SAML.
3. En su IdP, genere y descargue un documento de metadatos de federación que describa su organización como proveedor de identidades.

   Este documento XML firmado se utiliza para establecer la relación de confianza entre AWS y el IdP.
4. Cree un proveedor de identidades SAML de IAM en la misma AWS cuenta que el punto final Client VPN.

   El proveedor de identidad SAML de IAM define la relación entre el IdP y la AWS confianza de su organización mediante el documento de metadatos generado por el IdP. Para obtener más información, consulte Creación de proveedores de identidad SAML de IAM en la Guía del usuario de IAM. Si, más adelante, actualiza la configuración de la aplicación en el proveedor de

identidades, genere un nuevo documento de metadatos y actualice el proveedor de identidades SAML de IAM.

> **Note**
>
> No es necesario que cree un rol de IAM para utilizar el proveedor de identidades SAML de IAM.

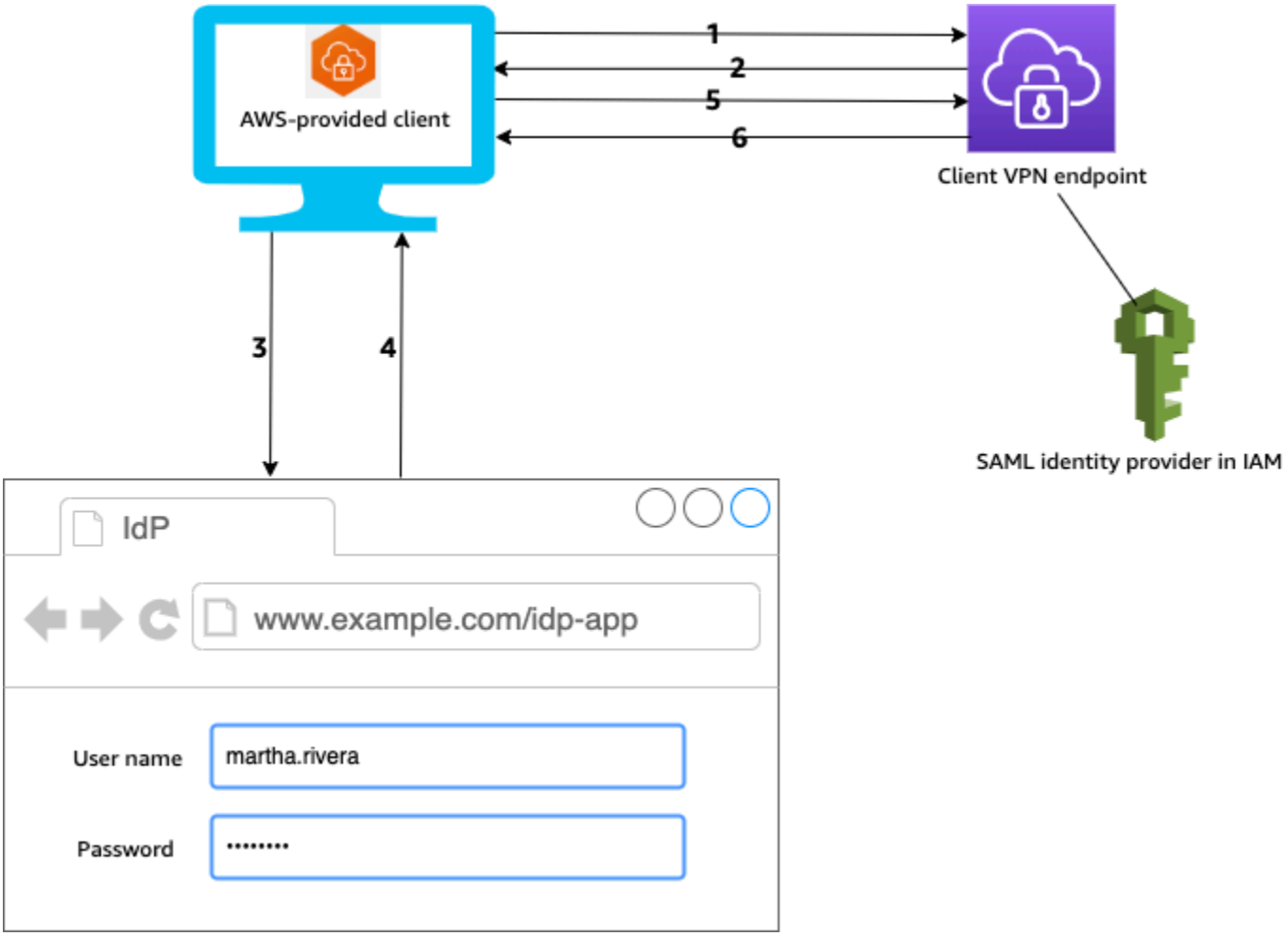
5. Cree un punto de enlace de Client VPN.

   Especifique la autenticación federada como tipo de autenticación y el proveedor de identidades SAML de IAM que ha creado. Para obtener más información, consulte Crear un AWS Client VPN punto final.

6. Exporte el archivo de configuración de cliente y distribúyalo a los usuarios. Indique a los usuarios que descarguen la versión más reciente del cliente proporcionado por AWS y que lo utilicen para cargar el archivo de configuración y conectarse al punto de enlace de Client VPN.

Flujo de trabajo de autenticación

El diagrama siguiente proporciona información general sobre el flujo de trabajo de autenticación de un punto de enlace de Client VPN que utiliza la autenticación federada basada en SAML. Cuando y configure el punto de enlace de Client VPN, tendrá que especificar el proveedor de identidades SAML de IAM.



1. El usuario abre el cliente AWS proporcionado en su dispositivo e inicia una conexión con el punto final Client VPN.
2. El punto de enlace de Client VPN devuelve al cliente una dirección URL del proveedor de identidades y una solicitud de autenticación en función de la información proporcionada en el proveedor de identidades SAML de IAM.
3. El cliente AWS proporcionado abre una nueva ventana del navegador en el dispositivo del usuario. El navegador realiza una solicitud al IdP y muestra una página de inicio de sesión.
4. El usuario escribe sus credenciales en la página de inicio de sesión y el IdP devuelve una aserción SAML firmada al cliente.
5. El cliente AWS proporcionado envía la aserción SAML al punto final Client VPN.
6. El punto de enlace de Client VPN valida la aserción y permite o deniega el acceso al usuario.

Requisitos y consideraciones de la autenticación federada basada en SAML

A continuación, se indican las consideraciones y los requisitos relativos a la autenticación federada basada en SAML.

- Para obtener información sobre las cuotas y las reglas para configurar usuarios y grupos en un proveedor de identidades basado en SAML, consulte Cuotas de usuarios y grupos.
- La aserción y la respuesta de SAML deben estar firmadas.
- AWS Client VPN solo admite las condiciones «AudienceRestriction» y «NotBefore y NotOnOrAfter» en las aserciones de SAML.
- El tamaño máximo admitido para las respuestas SAML es de 128 KB.
- AWS Client VPN no proporciona solicitudes de autenticación firmadas.
- No se admite el cierre de sesión único de SAML. Los usuarios pueden cerrar sesión desconectándose del cliente AWS proporcionado o usted puede finalizar las conexiones.
- Los puntos de enlace de Client VPN solo admiten un único proveedor de identidades.
- Multi-Factor Authentication (MFA) se admite si está habilitada en el IdP.
- Los usuarios deben usar el cliente AWS proporcionado para conectarse al punto final Client VPN. Deben usar la versión 1.2.0 o posterior. Para obtener más información, consulte Conectarse mediante el cliente AWS proporcionado.
- Los navegadores siguientes son compatibles con la autenticación de proveedores de identidades: Apple Safari, Google Chrome, Microsoft Edge y Mozilla Firefox.
- El cliente AWS proporcionado reserva el puerto TCP 35001 en los dispositivos de los usuarios para la respuesta SAML.
- Si el documento de metadatos del proveedor de identidades SAML de IAM se actualiza con una dirección URL incorrecta o malintencionada, pueden generarse problemas de autenticación de los usuarios o ataques de suplantación de identidad (phishing). Por lo tanto, se recomienda utilizar AWS CloudTrail para monitorear las actualizaciones que se realizan en el proveedor de identidades SAML de IAM. Para obtener más información, consulte Registro de llamadas a IAM y AWS STS con AWS CloudTrail en la Guía del usuario de IAM.
- AWS Client VPN envía una solicitud AuthN al IDP a través de un enlace de redireccionamiento HTTP. Por lo tanto, el IdP debe ser compatible con los enlaces de redirección HTTP y debe estar presente en el documento de metadatos del IdP.
- Para la aserción SAML, debe utilizar un formato de dirección de correo electrónico para el atributo `NameID`.

- La longitud máxima del nombre de usuario (`NameID`) es de 1024 bytes. Se rechazarán las conexiones con nombres de usuario más largos.
- Cuando se actualicen los certificados usados con el servicio Client VPN, ya sea mediante la rotación automática de ACM, importando manualmente un nuevo certificado o actualizaciones de metadatos al Centro de identidades de IAM, el servicio Client VPN actualizará automáticamente el punto de conexión de Client VPN con el certificado más reciente. Se trata de un proceso automatizado que puede tardar hasta 5 horas.

Recursos de configuración de IdP basados en SAML

En la siguiente tabla, se enumeran los recursos basados en SAML con AWS Client VPN los IdPs que hemos probado y los recursos que pueden ayudarlo a configurar el IdP.

IdP	Recurso
Okta	Autentique AWS Client VPN a los usuarios con SAML
Microsoft Entra ID (anteriormente Azure Active Directory)	Para obtener más información, consulte el tutorial: Integración del inicio de sesión único (SSO) de Microsoft Entra con AWS ClientVPN en el sitio web de documentación de Microsoft.
JumpCloud	Intégrelo con AWS Client VPN
AWS IAM Identity Center	Uso de IAM Identity Center con AWS Client VPN fines de autenticación y autorización

Información del proveedor de servicios para crear una aplicación

Para crear una aplicación basada en SAML con un IdP que no aparezca en la tabla anterior, utilice la siguiente información para configurar la información del AWS Client VPN proveedor de servicios.

- Dirección URL de Assertion Consumer Service (ACS): `http://127.0.0.1:35001`
- URI de audiencia: `urn:amazon:webservices:clientvpn`

Se debe incluir al menos un atributo en la respuesta SAML del IdP. A continuación, se muestran ejemplos de atributos.

Atributo	Description (Descripción)
`FirstName`	El nombre del usuario.
`LastName`	El apellido del usuario.
`memberOf`	El grupo o los grupos a los que pertenece el usuario.

> **Note**
>
> El atributo `memberOf` es necesario para usar las reglas de autorización basadas en grupos de Active Directory o SAML IdP. Distingue también mayúsculas y minúsculas y se debe configurar exactamente como se especifica. Para obtener más información, consulte Autorización basada en red y AWS Client VPN reglas de autorización.

Compatibilidad con el portal de autoservicio

Si activa el portal de autoservicio en el punto de enlace de Client VPN, los usuarios iniciarán sesión en él utilizando las credenciales del proveedor de identidades basado en SAML.

Si su IdP admite varios Assertion Consumer Service (ACS) URLs, añada la siguiente URL de ACS a su aplicación.

```
https://self-service.clientvpn.amazonaws.com/api/auth/sso/saml
```

Si utiliza el punto final Client VPN en una GovCloud región, utilice la siguiente URL de ACS en su lugar. Si usa la misma aplicación de IDP para autenticarse tanto en el estándar como en las GovCloud regiones, puede agregar ambas. URLs

```
https://gov.self-service.clientvpn.amazonaws.com/api/auth/sso/saml
```

Si su IdP no admite varios ACS URLs, haga lo siguiente:

1. Cree otra aplicación basada en SAML en el proveedor de identidades y especifique la siguiente URL de ACS.

```
https://self-service.clientvpn.amazonaws.com/api/auth/sso/saml
```

2. Genere y descargue un documento de metadatos de federación.
3. Cree un proveedor de identidades SAML de IAM en la misma AWS cuenta que el punto final Client VPN. Para obtener más información, consulte Creación de proveedores de identidad SAML de IAM en la Guía del usuario de IAM.

> **Note**
>
> Cree este proveedor de identidades SAML de IAM además del que va a crear para la aplicación principal.

4. Cree el punto de enlace de Client VPN y especifique los dos proveedores de identidades SAML de IAM que ha creado.

Autorización de cliente en AWS Client VPN

Client VPN admite dos tipos de autorización de cliente: los grupos de seguridad y la autorización basada en red (mediante reglas de autorización).

Grupos de seguridad

Cuando cree un punto de enlace de Client VPN, puede especificar los grupos de seguridad de una determinada VPC para aplicarlos al punto de enlace de Client VPN. Al asociar una subred con un punto de enlace de Client VPN, se aplica automáticamente el grupo de seguridad predeterminado de la VPC. Los grupos de seguridad se pueden cambiar después de crear el punto de enlace de Client VPN. Para obtener más información, consulte Aplicar un grupo de seguridad a una red de destino en AWS Client VPN. Los grupos de seguridad están asociados a interfaces de red de Client VPN.

Puede permitir que los usuarios de Client VPN obtengan acceso a las aplicaciones de una VPC agregando una regla a los grupos de seguridad de las aplicaciones que permita el tráfico desde el grupo de seguridad que se ha aplicado a la asociación.

Por el contrario, puede restringir el acceso de los usuarios de Client VPN no especificando el grupo de seguridad que se aplicó a la asociación o quitando la regla que hace referencia al grupo de

seguridad del punto de enlace de Client VPN. Las reglas de grupos de seguridad que necesite también podrían depender del tipo de acceso de VPN que desee configurar. Para obtener más información, consulte Escenarios y ejemplos para Client VPN.

Para obtener más información sobre los grupos de seguridad, consulte Grupos de seguridad de su VPC en la Guía de usuario de Amazon VPC.

Autorización basada en red

La autorización basada en red se implementa mediante reglas de autorización. Por cada red en la que desee permitir el acceso, debe configurar reglas de autorización que limiten los usuarios que tienen acceso. Para una red especificada, debe configurar el grupo de Active Directory o el grupo de IdP basado en SAML que tiene permiso de acceso. Solo los usuarios que pertenecen al grupo especificado pueden obtener acceso a la red especificada. Si no va a utilizar la autenticación federada basada en SAML o Active Directory, o desea permitir el acceso a todos los usuarios, puede especificar una regla que conceda acceso a todos los clientes. Para obtener más información, consulte AWS Client VPN reglas de autorización.

Tareas

- Crear una regla de grupo de seguridad de AWS Client VPN punto final

Crear una regla de grupo de seguridad de AWS Client VPN punto final

El grupo de seguridad predeterminado para la VPC que se aplica al asociar una subred a una Client VPN podría restringir el tráfico del grupo de seguridad predeterminado que se quiere permitir y, al mismo tiempo, permitir el tráfico que no se desea. Siga los siguientes pasos para crear una regla de grupo de seguridad de punto de conexión de Client VPN que permita o restrinja el tráfico de un grupo de seguridad de punto de conexión asociado a un recurso o una aplicación. Para obtener más información sobre reglas de grupos de seguridad, consulte Grupos de seguridad de su VPC en la Guía de usuario de Amazon VPC.

Para agregar una regla que permita el tráfico desde el grupo de seguridad del punto de enlace de Client VPN

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Grupos de seguridad.
3. Elija el grupo de seguridad asociado a su recurso o aplicación y elija Acciones, Editar reglas de entrada.

4. Seleccione Agregar regla.
5. En Tipo, seleccione Todo el tráfico. Como opción, puede restringir el acceso a un tipo específico de tráfico, por ejemplo, SSH.

   En Source (Origen), especifique el ID del grupo de seguridad que está asociado a la red de destino (subred) del punto de enlace de Client VPN.
6. Seleccione Guardar reglas.

Autorización de conexión en AWS Client VPN

Puede configurar un controlador de la conexión del cliente en el punto de enlace de Client VPN. Este controlador le permite ejecutar una lógica personalizada que autorice las nuevas conexiones en función de los atributos del dispositivo, el usuario y la conexión. El controlador de la conexión del cliente se ejecuta una vez que el servicio de Client VPN ha autenticado el dispositivo y el usuario.

Para configurar un controlador de la conexión del cliente en el punto de enlace de Client VPN, cree una función de AWS Lambda que tome los atributos del dispositivo, el usuario y la conexión como entrada y devuelva una decisión al servicio Client VPN sobre si se va a permitir o denegar una nueva conexión. Especifique la función Lambda en el punto de enlace de Client VPN. Cuando los dispositivos se conectan al punto de enlace de Client VPN, el servicio Client VPN invoca la función Lambda en su nombre. Solo las conexiones autorizadas por la función Lambda pueden conectarse al punto de enlace de Client VPN.

> **Note**
>
> Actualmente, el único tipo de controlador de conexión del cliente que se admite son las funciones Lambda.

Requisitos y consideraciones

A continuación se explican las consideraciones y los requisitos relacionados con el controlador de la conexión del cliente:

- El nombre de la función Lambda debe comenzar con el prefijo `AWSClientVPN-`.
- Las funciones Lambda calificadas son compatibles.

- La función Lambda debe estar en la misma AWS región y en la misma AWS cuenta que el punto final Client VPN.
- El tiempo de espera de la función Lambda se agota después de 30 segundos. Este valor no se puede modificar.
- La función Lambda se invoca de manera sincrónica. Se invoca después de la autenticación del dispositivo y del usuario, y antes de que se evalúen las reglas de autorización.
- Si la función Lambda se invoca para una nueva conexión y el servicio Client VPN no obtiene una respuesta esperada de la función, el servicio Client VPN deniega la solicitud de conexión. Esto puede ocurrir, por ejemplo, si la función Lambda tiene alguna limitación controlada, se agota su tiempo de espera o se producen otros errores inesperados, o bien si la respuesta de la función no tiene un formato válido.
- Es conveniente que configure la simultaneidad aprovisionada de la función Lambda para que pueda escalarse sin que se produzcan fluctuaciones en la latencia.
- Si actualiza la función Lambda, las conexiones existentes con el punto de enlace de Client VPN no se verán afectadas. Puede terminar las conexiones existentes y pedirle después a sus clientes que establezcan nuevas conexiones. Para obtener más información, consulte Finalizar una conexión de AWS Client VPN cliente.
- Si los clientes utilizan el cliente AWS proporcionado para conectarse al punto final Client VPN, deben usar la versión 1.2.6 o posterior para Windows y la versión 1.2.4 o posterior para macOS. Para obtener más información, consulte Conexión mediante el cliente proporcionado por AWS.

Interfaz de Lambda

La función Lambda toma atributos del dispositivo, del usuario y de la conexión como entrada del servicio Client VPN. A continuación, debe devolver una decisión al servicio Client VPN acerca de si se va a permitir o denegar la conexión.

Esquema de la solicitud

La función Lambda toma un blob JSON que contiene los siguientes campos como entrada.

```
{
    "connection-id": <connection ID>,
    "endpoint-id": <client VPN endpoint ID>,
    "common-name": <cert-common-name>,
    "username": <user identifier>,
    "platform": <OS platform>,
```

```
    "platform-version": <OS version>,
    "public-ip": <public IP address>,
    "client-openvpn-version": <client OpenVPN version>,
    "aws-client-version": <AWS client version>,
    "groups": <group identifier>,
    "schema-version": "v3"
}
```

- `connection-id`: ID de la conexión del cliente con el punto de enlace de Client VPN.
- `endpoint-id`: ID del punto de enlace de Client VPN.
- `common-name`: identificador del dispositivo. En el certificado de cliente que va a crear para el dispositivo, el nombre común identifica de forma inequívoca el dispositivo.
- `username`: identificador del usuario, si procede. En la autenticación de Active Directory, es el nombre de usuario. En la autenticación federada basada en SAML, es `NameID`. En la autenticación mutua, este campo está vacío.
- `platform`: plataforma del sistema operativo cliente.
- `platform-version`: versión del sistema operativo. El servicio Client VPN proporciona un valor si la directiva `--push-peer-info` está presente en la configuración del cliente de OpenVPN cuando los clientes se conectan a un punto de enlace de Client VPN y cuando el cliente ejecuta la plataforma Windows.
- `public-ip`: dirección IP pública del dispositivo de conexión.
- `client-openvpn-version`: versión de OpenVPN que se utiliza en el cliente.
- `aws-client-version`— La versión del AWS cliente.
- `groups`: identificador del grupo, si procede. Para la autenticación de Active Directory, será una lista de grupos de Active Directory. Para la autenticación federada basada en SAML, será una lista de grupos de proveedores de identidades (IdP). En la autenticación mutua, este campo está vacío.
- `schema-version`: versión del esquema. El valor predeterminado es `v3`.

Esquema de respuesta

La función Lambda debe devolver los siguientes campos.

```
{
    "allow": boolean,
    "error-msg-on-denied-connection": "",
    "posture-compliance-statuses": [],
```

```
    "schema-version": "v3"
}
```

- `allow`: obligatorio. Valor booleano (`true` | `false`) que indica si se va a permitir o denegar la nueva conexión.
- `error-msg-on-denied-connection`: obligatorio. Cadena de hasta 255 caracteres que se puede utilizar para proporcionar pasos y directrices a los clientes si la función Lambda deniega la conexión. Si se producen errores durante la ejecución de la función de Lambda (por ejemplo, debido a una limitación controlada), el servicio Client VPN devuelve a los clientes el siguiente mensaje predeterminado.

  ```
  Error establishing connection. Please contact your administrator.
  ```

- `posture-compliance-statuses`: obligatorio. Si utiliza la función Lambda para evaluar la posición, es una lista de estados del dispositivo de conexión. Los nombres de estado se definen de acuerdo con las categorías de evaluación de la posición de los dispositivos; por ejemplo, `compliant`, `quarantined`, `unknown`, etc. Un nombre puede tener 255 caracteres como máximo. Puede especificar hasta 10 estados.
- `schema-version`: obligatorio. Versión del esquema. El valor predeterminado es `v3`.

Puede utilizar la misma función Lambda con varios puntos de enlace de Client VPN de la misma región.

Para obtener más información acerca de cómo crear una función de Lambda, consulte Introducción a AWS Lambda en la Guía para desarrolladores de AWS Lambda .

Uso del controlador de la conexión del cliente para evaluar la posición

Puede utilizar el controlador de la conexión del cliente para integrar el punto de enlace de Client VPN con la solución de administración de dispositivos existente y evaluar la conformidad de la posición de los dispositivos de conexión. Para que la función Lambda trabaje como un controlador de autorización de dispositivos, utilice la autenticación mutua con el punto de enlace de Client VPN. Cree un certificado de cliente único y una clave para cada cliente (dispositivo) que se conecte al punto de enlace de Client VPN. La función Lambda puede utilizar el nombre común único del certificado de cliente (que se pasa desde el servicio Client VPN) para identificar el dispositivo y obtener su estado de conformidad de posición de la solución de administración de dispositivos. Puede utilizar la autenticación mutua combinada con la autenticación basada en usuarios.

Si lo desea, también puede realizar una evaluación básica de la posición de la propia función Lambda. Por ejemplo, puede evaluar los campos `platform` y `platform-version` que el servicio Client VPN pasa a la función Lambda.

> **Note**
>
> Si bien el controlador de conexión se puede utilizar para imponer una versión mínima de la AWS Client VPN aplicación, el campo `aws-client-version` del controlador de conexión solo se aplica a la AWS Client VPN aplicación y se rellena a partir de las variables de entorno del dispositivo del usuario.

Habilitación del controlador de la conexión del cliente

Para habilitar el controlador de la conexión del cliente, cree o modifique un punto de enlace de Client VPN y especifique el nombre de recurso de Amazon (ARN) de la función Lambda. Para obtener más información, consulte Crear un AWS Client VPN punto final y Modificación de un punto de conexión de AWS Client VPN.

Función vinculada al servicio

AWS Client VPN crea automáticamente un rol vinculado al servicio en tu cuenta llamado. AWSServiceRoleForClientVPNConnections El rol tiene permisos para invocar la función Lambda cuando se realiza una conexión con el punto de enlace de Client VPN. Para obtener más información, consulte Uso de roles vinculados a servicios para AWS Client VPN.

Supervisión de errores de autorización de la conexión

Puede ver el estado de la autorización de las conexiones con el punto de enlace de Client VPN. Para obtener más información, consulte Visualización de conexiones de clientes de AWS Client VPN.

Cuando se utiliza el controlador de la conexión del cliente para evaluar la posición, también se pueden ver los estados de conformidad de la posición de los dispositivos que se conectan al punto de enlace de Client VPN en los registros de conexión. Para obtener más información, consulte Registro de conexiones para un punto de conexión de AWS Client VPN.

Si un dispositivo no consigue la autorización de conexión, el campo `connection-attempt-failure-reason` de los registros de conexión devuelve uno de los siguientes motivos de error:

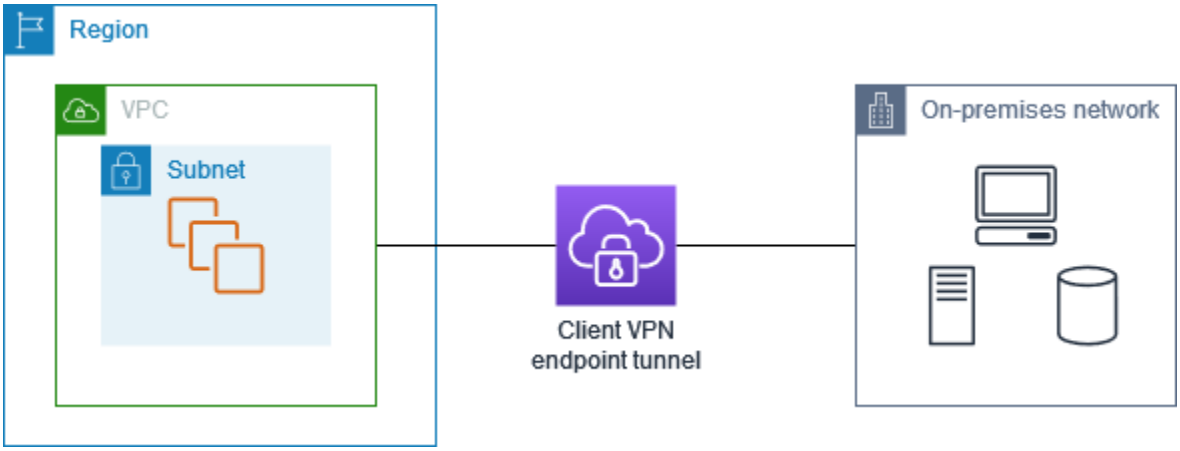
- `client-connect-failed`: la función Lambda impidió que se estableciera la conexión.
- `client-connect-handler-timed-out`: se agotó el tiempo de espera de la función Lambda.
- `client-connect-handler-other-execution-error`: la función Lambda encontró un error inesperado.
- `client-connect-handler-throttled`: se aplicaron limitaciones en la función Lambda.
- `client-connect-handler-invalid-response`: la función Lambda devolvió una respuesta que no era válida.
- `client-connect-handler-service-error`: se produjo un error en el lado del servicio durante el intento de conexión.

Túnel dividido en puntos de enlace de AWS Client VPN

De forma predeterminada, cuando tiene un punto de enlace de Client VPN, todo el tráfico de los clientes se direcciona a través del túnel de Client VPN. Cuando activa un túnel dividido en el punto de enlace de Client VPN, las rutas de la tabla de enrutamiento del punto de enlace de Client VPN se insertan en el dispositivo que está conectado al punto de enlace de Client VPN. De esta forma, el único tráfico que se direcciona a través del túnel de Client VPN es el tráfico dirigido a la red que coincide con una ruta de la tabla de enrutamiento del punto de enlace de Client VPN.

Puede utilizar un punto de enlace de Client VPN con un túnel dividido cuando no quiera que todo el tráfico de los usuarios se direccione a través del punto de enlace de Client VPN.

En el ejemplo siguiente, hay un túnel dividido activado en el punto de enlace de Client VPN. El único tráfico que se direcciona a través del túnel de Client VPN es el que tiene como destino la VPC (`172.31.0.0/16`). El tráfico con destino a los recursos locales no se direcciona a través del túnel de Client VPN.



Beneficios del túnel dividido

El túnel dividido de los puntos de enlace de Client VPN brinda los siguientes beneficios:

- Puede optimizar el enrutamiento del tráfico de los clientes al hacer que solo el tráfico destinado a AWS atraviese el túnel de la VPN.
- Puede reducir el volumen de tráfico saliente de AWS, lo que reduce el costo de transferencia de datos.

Consideraciones del enrutamiento

- Cuando habilite el modo de túnel dividido, todas las rutas de la tabla de enrutamiento del punto de conexión de Client VPN se agregan a la tabla de enrutamiento del cliente cuando se establece la conexión de VPN. Esta operación es diferente del comportamiento predeterminado, que sobrescribe la tabla de enrutamiento del cliente con la entrada `0.0.0.0/0` para enrutar todo el tráfico a través de la VPN.

  > **Note**
  >
  > Agregar una ruta 0.0.0/0 a la tabla de enrutamiento del punto de conexión de Client VPN cuando se utiliza el modo de túnel dividido puede provocar interrupciones en la conectividad, por lo que no se recomienda

- Cuando el modo de túnel dividido está activado, cualquier modificación en la tabla de enrutamiento del punto de conexión de Client VPN provocará el restablecimiento de todas las conexiones de cliente.

Habilitación del túnel-dividido

Puede activar el túnel dividido en un punto de enlace de Client VPN nuevo o existente. Para obtener más información, consulte los temas siguientes:

- Crear un AWS Client VPN punto final
- Modificación de un punto de conexión de AWS Client VPN

Registro de conexiones para un punto de conexión de AWS Client VPN

El registro de conexión es una característica de AWS Client VPN que le permite capturar registros de conexión del punto de enlace de Client VPN.

Un registro de conexiones contiene entradas de registro de conexiones que capturan información sobre eventos de conexión, que es cuando un cliente (usuario final) se conecta, intenta conectarse o se desconecta del punto de conexión de Client VPN. Esta información puede resultar útil para ejecutar análisis forenses, analizar cómo se está utilizando el punto de enlace de Client VPN o depurar problemas de conexión.

El registro de conexión está disponible en todas las regiones donde AWS Client VPN está disponible. Los registros de conexión se publican en un grupo de registros de CloudWatch Logs de la cuenta.

> **Note**
>
> Los intentos fallidos de autenticación mutua no se registran.

Entradas de registro de conexión

Una entrada de registro de conexión es un blob con formato JSON de pares clave-valor. A continuación, se muestra una entrada de registro de conexión de ejemplo.

```
{
    "connection-log-type": "connection-attempt",
    "connection-attempt-status": "successful",
    "connection-reset-status": "NA",
    "connection-attempt-failure-reason": "NA",
    "connection-id": "cvpn-connection-abc123abc123abc12",
    "client-vpn-endpoint-id": "cvpn-endpoint-aaa111bbb222ccc33",
    "transport-protocol": "udp",
    "connection-start-time": "2020-03-26 20:37:15",
    "connection-last-update-time": "2020-03-26 20:37:15",
    "client-ip": "10.0.1.2",
    "common-name": "client1",
    "device-type": "mac",
    "device-ip": "98.247.202.82",
```

```
    "port": "50096",
    "ingress-bytes": "0",
    "egress-bytes": "0",
    "ingress-packets": "0",
    "egress-packets": "0",
    "connection-end-time": "NA",
    "username": "joe"
    }
```

Una entrada de registro de conexión contiene las siguientes claves:

- `connection-log-type`: tipo de entrada del registro de conexión (`connection-attempt` o `connection-reset`).
- `connection-attempt-status`: estado de la solicitud de conexión (`successful`, `failed`, `waiting-for-assertion` o `NA`).
- `connection-reset-status`: estado de un evento de restablecimiento de conexión (`NA` o `assertion-received`).
- `connection-attempt-failure-reason`: motivo del error de conexión, si procede.
- `connection-id`: ID de la conexión.
- `client-vpn-endpoint-id`: ID del punto de enlace de Client VPN con el que se realizó la conexión.
- `transport-protocol`: protocolo de transporte que se utilizó para la conexión.
- `connection-start-time`: hora de inicio de la conexión.
- `connection-last-update-time`: hora de la última actualización de la conexión. Este valor se actualiza periódicamente en los registros.
- `client-ip`: dirección IP del cliente, que se asigna desde el intervalo CIDR IPv4 del cliente al punto de enlace de Client VPN.
- `common-name`: nombre común del certificado utilizado para la autenticación basada en certificados.
- `device-type`: tipo de dispositivo utilizado por el usuario final para la conexión.
- `device-ip`: dirección IP pública del dispositivo.
- `port`: número de puerto de la conexión.
- `ingress-bytes`: número de bytes de entrada de la conexión. Este valor se actualiza periódicamente en los registros.

- `egress-bytes`: número de bytes de salida de la conexión. Este valor se actualiza periódicamente en los registros.
- `ingress-packets`: número de paquetes de entrada de la conexión. Este valor se actualiza periódicamente en los registros.
- `egress-packets`: número de paquetes de salida de la conexión. Este valor se actualiza periódicamente en los registros.
- `connection-end-time`: hora de finalización de la conexión. El valor es `NA` si la conexión sigue en curso o si el intento de conexión devolvió un error.
- `posture-compliance-statuses`: estados de conformidad de la posición devueltos por el controlador de la conexión del cliente, si procede.
- `username`: el nombre de usuario se registra cuando se utiliza la autenticación basada en el usuario (AD o SAML) para el punto de conexión.
- `connection-duration-seconds`: duración de una conexión en segundos. Igual a la diferencia entre la «hora de inicio de la conexión» y la «hora de finalización de la conexión».

Para obtener más información acerca de cómo activar los registros de conexión, consulte registros de conexiones de AWS Client VPN.

Consideraciones de escalado de Client VPN

Cuando cree un punto de enlace de Client VPN, tenga en cuenta el número máximo de conexiones VPN simultáneas que planea admitir. Debe tener en cuenta el número de clientes que admite actualmente y si el punto de conexión de Client VPN puede escalar para cumplir una demanda adicional si es necesario.

Los siguientes factores afectan al número máximo de conexiones VPN simultáneas que se pueden admitir en un punto de conexión de Client VPN:

Tamaño del rango CIDR del cliente

Al crear un punto de enlace de Client VPN, debe especificar un intervalo CIDR de cliente, que es un bloque CIDR IPv4 entre una máscara de red /12 y /22. A cada conexión VPN con el punto de enlace de Client VPN se le asigna una dirección IP única del intervalo CIDR del cliente. Una parte de las direcciones del intervalo CIDR del cliente se utiliza para admitir el modelo de disponibilidad del punto de enlace de Client VPN y no se puede asignar a los clientes. No puede cambiar el intervalo CIDR del cliente después de crear el punto de enlace de Client VPN.

En general, se recomienda especificar un intervalo CIDR de cliente que contenga el doble del número de direcciones IP (y, por lo tanto, conexiones simultáneas) que va a admitir en el punto de enlace de Client VPN.

Número de subredes asociadas

Cuando asocia una subred con un punto de enlace de Client VPN, permite a los usuarios establecer sesiones VPN en el punto de enlace de Client VPN. Puede asociar varias subredes con un punto de enlace de Client VPN para obtener alta disponibilidad y habilitar capacidad de conexión adicional.

A continuación se muestra el número de conexiones VPN simultáneas admitidas en función del número de asociaciones de subred para el punto de enlace de Client VPN.

Asociaciones de subred	Número de conexiones admitidas
1	7000
2	36 500
3	66 500
4	96 500
5	126 000

No puede asociar varias subredes de la misma zona de disponibilidad con un punto de enlace de Client VPN. Por lo tanto, el número de asociaciones de subred también depende del número de zonas de disponibilidad disponibles en una región de AWS.

Por ejemplo, si espera admitir 8000 conexiones VPN al punto de enlace de Client VPN, especifique un tamaño mínimo de intervalo CIDR de cliente de `/18` (16 384 direcciones IP) y asocie al menos 2 subredes con el punto de enlace de Client VPN.

Si no está seguro de cuál es el número de conexiones VPN esperadas para el punto de enlace de Client VPN, recomendamos que especifique un bloque `/16` CIDR de tamaño o mayor.

A fin de obtener más información acerca de las reglas y limitaciones para trabajar con rangos CIDR de cliente y redes de destino, consulte Reglas y mejores prácticas de uso AWS Client VPN.

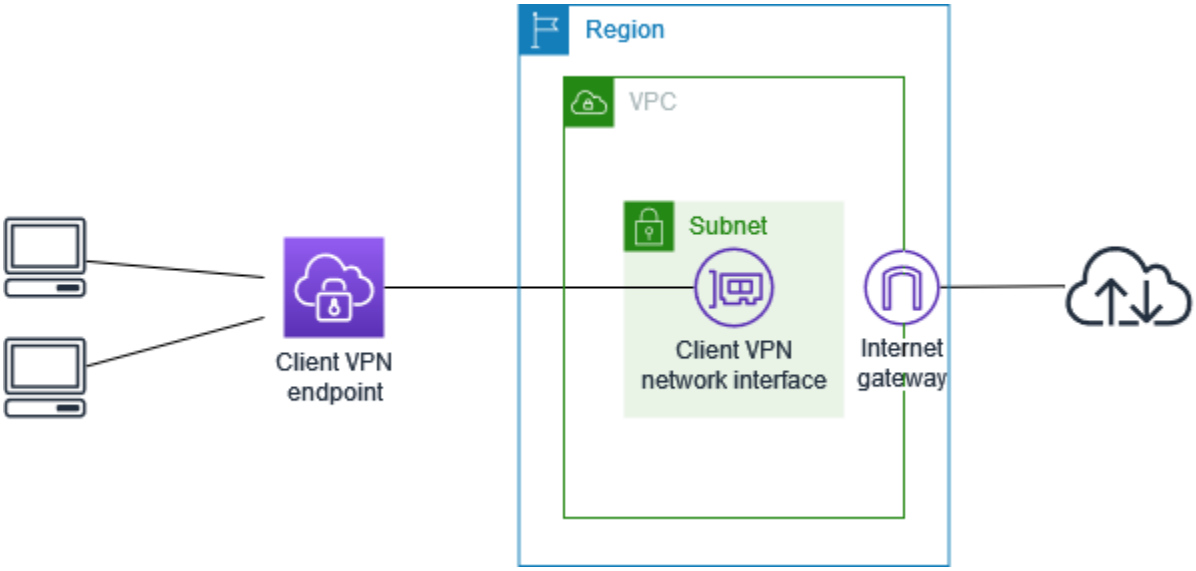
Para obtener más información acerca de las cuotas para el punto de enlace de Client VPN, consulte AWS Client VPNCuotas de.

Comience con AWS Client VPN

En este tutorial, creará un AWS Client VPN punto final que haga lo siguiente:

- Proporciona a todos los clientes acceso a una única VPC.
- Proporciona a todos los clientes acceso a Internet.
- Utiliza la autenticación mutua.

En el siguiente diagrama, se ilustra la configuración de la VPC y el punto de enlace de Client VPN después de completar este tutorial.



Steps

- Requisitos previos
- Paso 1: elija el tipo de punto final
- Paso 2: Generar certificados y claves de servidor y cliente
- Paso 3: Crear un punto final Client VPN
- Paso 4: Asocie una red de destino
- Paso 5: Añadir una regla de autorización para la VPC
- Paso 6: Proporcione acceso a Internet
- Paso 7: Compruebe los requisitos de los grupos de seguridad
- Paso 8: Descargar el archivo de configuración del punto final de Client VPN

- Paso 9: Conectarse al punto final Client VPN

Requisitos previos

Antes de comenzar este tutorial de introducción, asegúrese de tener lo siguiente:

- Los permisos necesarios para trabajar con puntos de enlace de Client VPN.
- Los permisos necesarios para importar certificados en AWS Certificate Manager.
- Una VPC con al menos una subred y un gateway de Internet. La tabla de rutas asociada a la subred debe tener una ruta al gateway de Internet.

Paso 1: elija el tipo de punto final

Client VPN admite dos tipos de terminales: asociación de subredes de VPC para el acceso de una sola VPC y asociación de Transit Gateway para escenarios de redes híbridas y de múltiples VPC. Este tutorial cubre los puntos finales asociados a la VPC. Para ver los puntos finales de Transit Gateway, consulteIntegración de Transit Gateway con Client VPN.

Paso 2: Generar certificados y claves de servidor y cliente

En este tutorial, se utiliza la autenticación mutua. Con la autenticación mutua, Client VPN utiliza certificados para realizar la autenticación entre los clientes y el punto de conexión de Client VPN. Deberá tener un certificado y una clave de servidor y al menos un certificado y una clave de cliente. Como mínimo, el certificado del servidor deberá importarse a AWS Certificate Manager (ACM) y especificarse al crear el punto final Client VPN. La importación del certificado de cliente en ACM es opcional.

Si aún no dispone de certificados para utilizarlos con este fin, se pueden crear con la utilidad easy-rsa de OpenVPN. Para conocer los pasos detallados para generar los certificados y las claves del servidor y del cliente mediante la utilidad easy-rsa de OpenVPN e importarlos a ACM, consulte Autenticación mutua en AWS Client VPN.

> **Note**
>
> El certificado de servidor debe aprovisionarse o importarse a AWS Certificate Manager (ACM) en la misma AWS región en la que creará el punto final Client VPN.

Paso 3: Crear un punto final Client VPN

El punto de enlace de Client VPN es el recurso que usted crea y configura para activar y administrar sesiones de Client VPN. Es el punto de terminación de todas las sesiones de Client VPN.

Para crear un punto de conexión de Client VPN

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN Endpoints (Puntos de conexión de Client VPN) y Create Client VPN Endpoint (Crear punto de conexión de Client VPN).
3. (Opcional) Escriba una etiqueta de nombre y una descripción del punto de conexión de Client VPN.
4. Para el IPv4 CIDR del cliente, especifique un rango de direcciones IP, en notación CIDR, desde el que asignar las direcciones IP de los clientes.

   > **Note**
   >
   > El intervalo de direcciones no puede solaparse al intervalo de direcciones de la red de destino, al intervalo de direcciones de la VPC ni a ninguna de las rutas que se asociarán con el punto de conexión de Client VPN. El intervalo de direcciones del cliente debe tener un tamaño de bloque de CIDR mínimo de /22 y no superior a /12. No puede cambiar el intervalo de direcciones del cliente después de crear el punto de conexión de Client VPN.

5. Para el ARN del certificado de servidor, seleccione el ARN del certificado de servidor que generó en el paso 2.
6. En Authentication options (Opciones de autenticación), elija Use mutual authentication (Usar autenticación mutua) y, a continuación, en Client certificate ARN (ARN de certificado de cliente), seleccione el ARN del certificado que desea utilizar como certificado de cliente.

   Si los certificados de servidor y de cliente están firmados por la misma entidad de certificación (CA), tiene la opción de especificar el ARN del certificado de servidor para los certificados de cliente y de servidor. En este escenario, cualquier certificado de cliente que se corresponda con el certificado de servidor se puede utilizar para la autenticación.
7. (Opcional) Especifique qué servidores DNS se van a utilizar para la resolución de DNS. Para utilizar servidores DNS personalizados, en DNS Server 1 IP address (Dirección IP de servidor de DNS 1) yDNS Server 2 IP address (Dirección IP de servidor de DNS 2), especifique las

direcciones IP de los servidores DNS que se van a utilizar. Para utilizar un servidor DNS de la VPC, en DNS Server 1 IP address (Dirección IP del servidor DNS 1) o DNS Server 2 IP address (Dirección IP del servidor DNS 2), especifique las direcciones IP y agregue la dirección IP del servidor DNS de la VPC.

> **Note**
>
> Asegúrese de que los clientes pueden acceder a los servidores DNS.

8. Mantenga los demás valores predeterminados y elija Create Client VPN Endpoint (Crear punto de conexión de Client VPN).

Después de crear el punto de enlace de Client VPN, su estado es `pending-associate`. Los clientes solo pueden establecer una conexión de VPN después de que se haya asociado al menos una red de destino.

Para obtener más información sobre las opciones que puede especificar para un punto de conexión de Client VPN, consulte Crear un AWS Client VPN punto final.

Paso 4: Asocie una red de destino

Para permitir que los clientes establezcan una sesión de VPN, debe asociar una red de destino con el punto de conexión de Client VPN. Una red de destino es una subred en una VPC.

Para asociar una red de destino con el punto de conexión de Client VPN

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN Endpoints (Puntos de enlace de Client VPN).
3. Seleccione el punto de conexión de Client VPN que creó en el procedimiento anterior y, a continuación, elija Target network associations (Asociaciones de red de destino), Associate target network (Asociar red de destino).
4. En VPC, elija la VPC en la que se encuentra la subred.
5. En Choose a subnet to associate (Elija una subred para asociar), elija la subred que desee asociar con el punto de conexión de Client VPN.
6. Elija Associate target network (Asociar red de destino).

7. Si las reglas de autorización lo permiten, basta con una asociación de subred para que los clientes obtengan acceso a toda la red de una VPC. Puede asociar más subredes para ofrecer una alta disponibilidad en caso de que una de las zonas de disponibilidad deje de funcionar.

Al asociar la primera subred con el punto de enlace de Client VPN, sucede lo siguiente:

- El estado del punto de enlace de Client VPN cambia a `available`. Los clientes ahora pueden establecer una conexión de VPN, pero no pueden acceder a los recursos de la VPC hasta que se añadan las reglas de autorización.
- La ruta local de la VPC se agrega automáticamente a la tabla de enrutamiento del punto de enlace de Client VPN.
- El grupo de seguridad predeterminado de la VPC se aplica automáticamente para el punto de conexión de Client VPN.

Paso 5: Añadir una regla de autorización para la VPC

Para que los clientes puedan acceder a la VPC, es necesario que haya una ruta a la VPC en la tabla de enrutamiento del punto de conexión de Client VPN y una regla de autorización. La ruta ya se agregó automáticamente en el paso anterior. En este tutorial, deseamos conceder a todos los usuarios el acceso a la VPC.

Para agregar una regla de autorización para la VPC

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN Endpoints (Puntos de enlace de Client VPN).
3. Seleccione el punto de conexión de Client VPN al que se agregará la regla de autorización. Elija Authorization rules (Reglas de autorización) y, a continuación, Add authorization rule (Agregar regla de autorización).
4. En Destination network to enable access (Red de destino para habilitar el acceso), ingrese el CIDR de la red para la que desea conceder acceso. Por ejemplo, para permitir el acceso a toda la VPC, especifique el bloque IPv4 CIDR de la VPC.
5. En Grant access to (Conceder acceso a), elija Allow access to all users (Permitir acceso a todos los usuarios).
6. (Opcional) En Description (Descripción), ingrese una breve descripción de la regla de autorización.

7. Seleccione Add authorization rule (Añadir regla de autorización).

Paso 6: Proporcione acceso a Internet

Puede proporcionar acceso a redes adicionales conectadas a la VPC, como AWS servicios, redes interconectadas VPCs, locales e Internet. Para cada red adicional, se agrega una ruta a la red en la tabla de enrutamiento del punto de conexión de Client VPN y se configura una regla de autorización para conceder acceso a los clientes.

Para este tutorial, deseamos conceder a todos los usuarios acceso a Internet y también a la VPC. Ya ha configurado el acceso a la VPC, así que este paso es para el acceso a Internet.

Para proporcionar acceso a Internet

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN Endpoints (Puntos de enlace de Client VPN).
3. Seleccione el punto de conexión de Client VPN que creó para este tutorial. Elija Route Table (Tabla de enrutamiento) y, a continuación, Create Route (Crear ruta).
4. En Route destination (Destino de ruta), escriba `0.0.0.0/0`. En Subnet ID for target network association (ID de subred para la asociación de red de destino), especifique el ID de la subred a través de la cual se va a dirigir el tráfico.
5. Elija Create Route (Crear ruta).
6. Elija Authorization rules (Reglas de autorización) y, a continuación, Add authorization rule (Agregar regla de autorización).
7. En Destination network to enable access (Red de destino para permitir el acceso), ingrese `0.0.0.0/0` y elija Allow access to all users (Permitir acceso a todos los usuarios).
8. Seleccione Add authorization rule (Añadir regla de autorización).

Paso 7: Compruebe los requisitos de los grupos de seguridad

En este tutorial, no se especificó ningún grupo de seguridad durante la creación del punto final Client VPN en el paso 3. Esto significa que el grupo de seguridad predeterminado para la VPC se aplica automáticamente al punto de conexión de Client VPN cuando se asocia una red de destino. Como resultado, el grupo de seguridad predeterminado para la VPC debería estar ahora asociado con el punto de conexión de Client VPN.

Verifique los siguientes requisitos del grupo de seguridad

- Que el grupo de seguridad asociado a la subred por la que está dirigiendo el tráfico (en este caso, el grupo de seguridad de la VPC predeterminada) permita el tráfico saliente hacia Internet. Para ello, agregue una regla de salida que permita todo el tráfico hacia el destino `0.0.0.0/0`.
- Que los grupos de seguridad de los recursos de su VPC tengan una regla que permita el acceso desde el grupo de seguridad que se aplica al punto de conexión de Client VPN (en este caso, el grupo de seguridad predeterminado de VPC). Esto permite a sus clientes acceder a los recursos de su VPC.

Para obtener más información, consulte Grupos de seguridad.

Paso 8: Descargar el archivo de configuración del punto final de Client VPN

El siguiente paso que tiene que realizar es descargar y preparar el archivo de configuración del punto de conexión de Client VPN. El archivo de configuración contiene los detalles del punto de conexión de Client VPN y la información del certificado necesaria para establecer una conexión de VPN. Este archivo se proporciona a los usuarios finales que necesitan conectarse al punto de conexión de Client VPN. El usuario final utiliza el archivo para configurar su aplicación cliente de VPN.

Para descargar y preparar el archivo de configuración del punto de enlace de Client VPN

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN Endpoints (Puntos de enlace de Client VPN).
3. Seleccione el punto de conexión de Client VPN que creó para este tutorial y elija Download client configuration (Descargar la configuración del cliente).
4. Localice el certificado y la clave del cliente que se generaron en el paso 2. El certificado y la clave del cliente se encuentran en las siguientes ubicaciones del repositorio easy-rsa de OpenVPN clonado:
   - Certificado del client — `easy-rsa/easyrsa3/pki/issued/client1.domain.tld.crt`
   - Clave de client — `easy-rsa/easyrsa3/pki/private/client1.domain.tld.key`
5. Abra el archivo de configuración del punto de enlace de Client VPN con el editor de texto que prefiera. Agregue las etiquetas `<cert></cert>` y `<key></key>` al archivo. Coloque

el contenido del certificado del cliente y el contenido de la clave privada entre las etiquetas correspondientes, del siguiente modo:

```
<cert>
Contents of client certificate (.crt) file
</cert>

<key>
Contents of private key (.key) file
</key>
```

6. Guarde y cierre el archivo de configuración del punto de enlace de Client VPN.
7. Distribuya el archivo de configuración del punto de conexión de Client VPN a sus usuarios finales.

Para obtener más información sobre el archivo de configuración del punto de enlace de Client VPN, consulte AWS Client VPN exportación de archivos de configuración de terminales.

Paso 9: Conectarse al punto final Client VPN

Puede conectarse al punto final Client VPN mediante el cliente AWS proporcionado u otra aplicación cliente basada en OpenVPN y el archivo de configuración que acaba de crear. Para obtener más información, consulte la Guía del usuario de AWS Client VPN.

Trabaja con AWS Client VPN

En los siguientes temas se explican las principales tareas administrativas necesarias para trabajar con Client VPN:

- Acceso al portal de autoservicio: configure el acceso al portal de autoservicio de Client VPN para que los clientes puedan descargar por sí mismos el archivo de configuración del punto de conexión de Client VPN. Para obtener información sobre cómo acceder al portal de autoservicio, consulte the section called “Acceso al portal de autoservicio”.
- Reglas de autorización: agregue reglas de autorización para controlar el acceso de los clientes a redes específicas. Para obtener información sobre cómo agregar reglas de autorización, consulte the section called “Reglas de autorización”.
- Listas de revocación de certificados de cliente: use listas de revocación de certificados de cliente para revocar el acceso a un punto de conexión de Client VPN. Para obtener información sobre listas de revocación de certificados del cliente, consulte the section called “Listas de revocación de certificados del cliente”.
- Conexiones de cliente: permite ver o finalizar una conexión de cliente a un punto de conexión de Client VPN. Para obtener información sobre cómo ver o finalizar una conexión de cliente, consulte the section called “Conexiones de clientes”.
- Banner de inicio de sesión de cliente: agregue un banner de texto en una aplicación de escritorio de Client VPN cuando se establece una sesión de VPN. Puede usar el banner de texto para satisfacer sus necesidades normativas y de conformidad. Para obtener información sobre los banners de inicio de sesión, consulte the section called “Banners de inicio de sesión de cliente”.
- Client Route Enforcement: aplique rutas definidas por el administrador en los dispositivos conectados a través de la VPN. Para obtener más información sobre Client Route Enforcement, consulte the section called “Client Route Enforcement”.
- Puntos de conexión de Client VPN: configure los puntos de conexión de Client VPN para administrar y controlar todas las sesiones de VPN. Para obtener información sobre la configuración de los puntos de conexión, consulte the section called “Puntos de conexión”.
- Registros de conexiones: habilite el registro de conexión de puntos de conexión de Client VPN nuevos o existentes para comenzar a capturar registros de conexiones. Para obtener información sobre el registro de conexiones, consulte the section called “Registros de conexiones”.
- Exportación del archivo de configuración del cliente: configure el archivo de configuración del cliente que los clientes de Client VPN necesitan para establecer las conexiones de VPN. Tras configurar el archivo, descárguelo (expórtelo) para distribuirlo a los clientes. Para obtener más

información sobre la exportación de un archivo de configuración del cliente, consulte the section called “Exportación de archivos de configuración de cliente”.

- Rutas: configure reglas de autorización para cada ruta de Client VPN para especificar qué clientes tienen acceso a la red de destino. Para obtener información acerca de la configuración de reglas de autorización, consulte the section called “Reglas de autorización”
- Redes de destino: asocie subredes de VPC o conéctelas directamente a una AWS Transit Gateway para permitir que los clientes se conecten y establezcan una conexión VPN. Para obtener más información sobre las redes de destino, consulte the section called “Redes de destino”. Para obtener información sobre la integración de Transit Gateway, consultethe section called “Integración de Transit Gateway con Client VPN”.
- Duración máxima de la sesión de VPN: establezca opciones para la duración máxima de la sesión de VPN para cumplir los requisitos de seguridad y conformidad. Para obtener información acerca de la duración máxima de la sesión de VPN, consulte the section called “Duración máxima de la sesión de VPN”.

Acceso de AWS Client VPN al portal de la autoservicio

Si ha habilitado el portal de autoservicio en el punto de enlace de Client VPN, puede proporcionar a sus clientes una URL del portal de autoservicio. Los clientes pueden acceder al portal en un explorador web y utilizar sus credenciales basadas en usuarios para iniciar sesión. En el portal, los clientes pueden descargar el archivo de configuración del punto de enlace de Client VPN y la versión más reciente del cliente proporcionado por AWS.

Se aplican las siguientes reglas:

- El portal de autoservicio no está disponible para los clientes que utilizan la autenticación mutua.
- El archivo de configuración que está disponible en el portal de autoservicio es el mismo que se exporta a través de la consola de Amazon VPC o la AWS CLI. Si necesita personalizar el archivo de configuración antes de distribuirlo a los clientes, deberá encargarse usted mismo de distribuir el archivo personalizado a los clientes.
- Debe habilitar la opción del portal de autoservicio en el punto de enlace de Client VPN o los clientes no podrán acceder al portal. Si esta opción no está habilitada, puede modificar el punto de enlace de Client VPN para habilitarla.

Una vez que la opción del portal de autoservicio esté habilitada, proporcione a sus clientes una de las siguientes direcciones URL:

- `https://self-service.clientvpn.amazonaws.com/`

  Si los clientes acceden al portal mediante esta dirección URL, deben especificar el ID del punto de enlace de Client VPN para poder iniciar sesión.
- `https://self-service.clientvpn.amazonaws.com/endpoints/<endpoint-id>`

  En la URL anterior, sustituya *<endpoint-id>* por el ID del punto de enlace de Client VPN; por ejemplo, `cvpn-endpoint-0123456abcd123456`.

También puede ver la URL del portal de autoservicio en la salida del comando describe-client-vpn-endpoints de la AWS CLI. Por otro lado, la URL también está disponible en la pestaña Details (Detalles) de la página VPN Client Endpoints (Puntos de conexión de Client VPN) de la consola de Amazon VPC.

Para obtener más información acerca de cómo configurar el portal de autoservicio para usarlo con la autenticación federada, consulte Compatibilidad con el portal de autoservicio.

AWS Client VPN reglas de autorización

Las reglas de autorización actúan como reglas de firewall que conceden acceso a redes. Al agregar reglas de autorización, debe conceder a los clientes específicos acceso a la red especificada. Debe tener una regla de autorización para cada red a la que desea conceder acceso. Puede agregar reglas de autorización a un punto de enlace de Client VPN a través de la consola y la AWS CLI.

> **Note**
>
> Client VPN utiliza la coincidencia de prefijos más larga al evaluar las reglas de autorización. Consulte el tema sobre solución de problemas Solución de problemas AWS Client VPN: las reglas de autorización para los grupos de Active Directory no funcionan según lo esperado y Prioridad de la ruta en la Guía del usuario de Amazon VPC para obtener más información.

Puntos clave para entender las reglas de autorización

En los siguientes puntos se explican algunos de los comportamientos de las reglas de autorización:

- Para permitir el acceso a una red de destino, debe agregarse explícitamente una regla de autorización. El comportamiento predeterminado es denegar el acceso.

- No puede agregar una regla de autorización para restringir el acceso a una red de destino.
- El CIDR `0.0.0.0/0` se gestiona como un caso especial. Se procesa en último lugar, independientemente del orden en que se crearon las reglas de autorización.
- El CIDR `0.0.0.0/0` puede considerarse como "cualquier destino" o "cualquier destino no definido por otras reglas de autorización".
- La coincidencia del prefijo más largo es la regla que tiene prioridad.

Temas

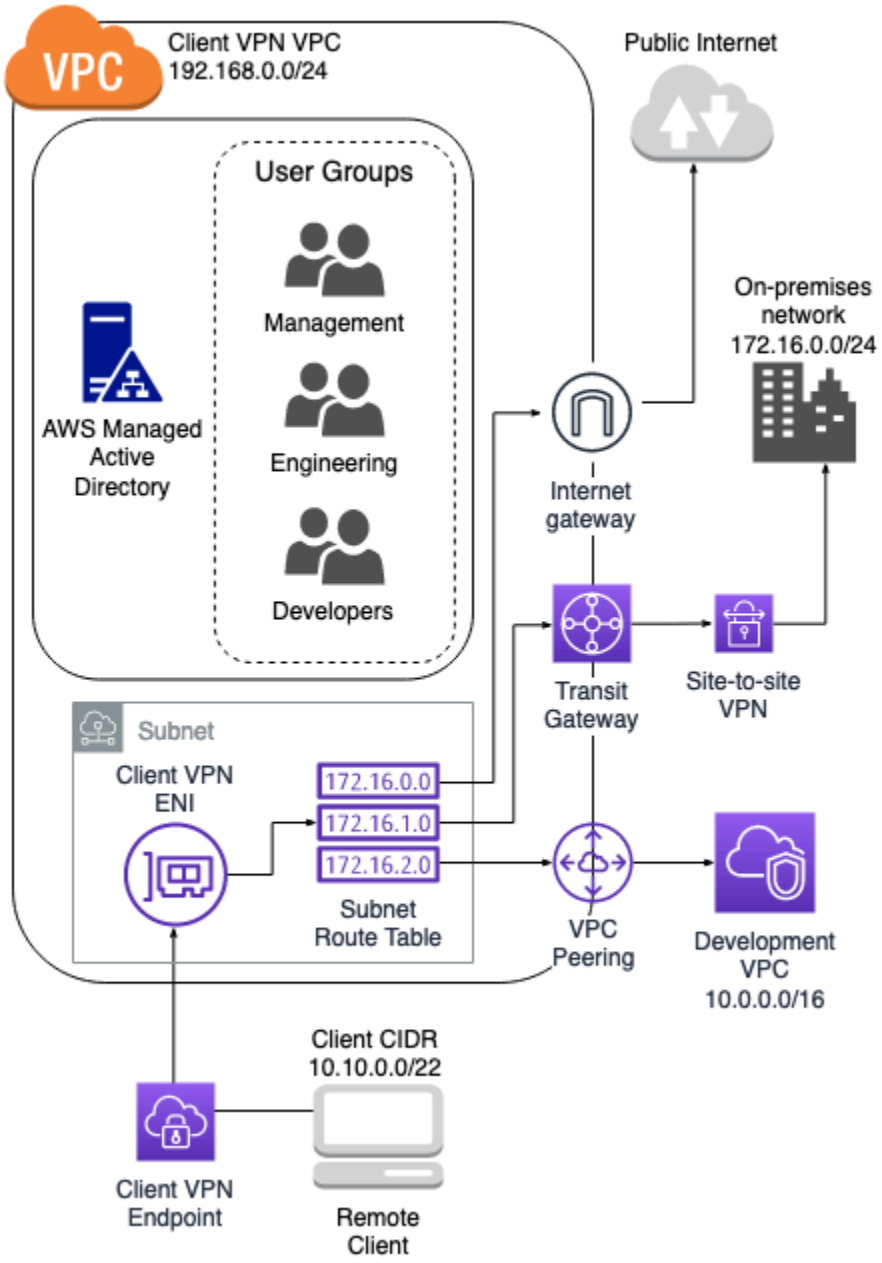
Escenarios de ejemplo para las reglas de autorización de Client VPN

En esta sección se describe cómo funcionan las reglas de autorización para AWS Client VPN. Incluye puntos clave para entender las reglas de autorización, una arquitectura de ejemplo y la explicación de escenarios de ejemplo que se asignan a la arquitectura de ejemplo.

Escenarios

Ejemplo de arquitectura para escenarios de reglas de autorización

En el siguiente diagrama se muestra la arquitectura de ejemplo que se utiliza para los escenarios de ejemplo que se encuentran en esta sección.



Acceso a un único destino

Descripción de la regla	ID de grupo	Permitir el acceso a todos los usuarios	CIDR de destino

Descripción de la regla	ID de grupo	Permitir el acceso a todos los usuarios	CIDR de destino
Proporcionar acceso al grupo de ingeniería a la red en las instalaciones	S-xxxxx14	False	172.16.0.0/24
Proporcionar acceso al grupo de desarrollo a la VPC de desarrollo	S-xxxxx15	False	10.0.0.0/16
Proporcionar acceso al grupo de administración a la VPC de Client VPN	S-xxxxx16	False	192.168.0.0/24

Comportamiento resultante

- El grupo de ingeniería puede acceder solo a `172.16.0.0/24`.
- El grupo de desarrollo puede acceder solo a `10.0.0.0/16`.
- El grupo de administradores puede acceder solo a `192.168.0.0/24`.
- El punto de conexión de Client VPN descarta el resto del tráfico.

> **Note**
>
> En este escenario, ningún grupo de usuarios tiene acceso al Internet público.

Utilice cualquier CIDR de destino (0.0.0.0/0)

Descripción de la regla	ID de grupo	Permitir el acceso a todos los usuarios	CIDR de destino

Descripción de la regla	ID de grupo	Permitir el acceso a todos los usuarios	CIDR de destino
Proporcionar acceso al grupo de ingeniería a la red en las instalaciones	S-xxxxx14	False	172.16.0.0/24
Proporcionar acceso al grupo de desarrollo a la VPC de desarrollo	S-xxxxx15	False	10.0.0.0/16
Proporcionar acceso al grupo de administradores a cualquier destino	S-xxxxx16	False	0.0.0.0/0

Comportamiento resultante

- El grupo de ingeniería puede acceder solo a `172.16.0.0/24`.
- El grupo de desarrollo puede acceder solo a `10.0.0.0/16`.
- El grupo de administradores puede acceder al Internet público y a `192.168.0.0/24`, pero no puede acceder a `172.16.0.0/24` ni `10.0.0/16`.

> **Note**
>
> En este escenario, como no hay reglas que hagan referencia a `192.168.0.0/24`, el acceso a esa red también lo proporciona la regla `0.0.0.0/0`.
> Una regla que contenga `0.0.0.0/0` siempre se evalúa en último lugar, independientemente del orden en que se crearon las reglas. Por ello, hay que tener en cuenta que las reglas evaluadas antes que `0.0.0.0/0` desempeñan un rol en la determinación de las redes a las que `0.0.0.0/0` concede acceso.

La concordancia de prefijo IP más larga

Descripción de la regla	ID de grupo	Permitir el acceso a todos los usuarios	CIDR de destino
Proporcionar acceso al grupo de ingeniería a la red en las instalaciones	S-xxxxx14	False	172.16.0.0/24
Proporcionar acceso al grupo de desarrollo a la VPC de desarrollo	S-xxxxx15	False	10.0.0.0/16
Proporcionar acceso al grupo de administradores a cualquier destino	S-xxxxx16	False	0.0.0.0/0
Proporcionar acceso al grupo de administradores a un único host en la VPC de desarrollo	S-xxxxx16	False	10.0.2.119/32

Comportamiento resultante

- El grupo de ingeniería puede acceder solo a `172.16.0.0/24`.
- El grupo de desarrollo puede acceder a `10.0.0.0/16`, excepto al host individual `10.0.2.119/32`.
- El grupo de administradores puede acceder al Internet público, `192.168.0.0/24` y a un host individual (`10.0.2.119/32`) en la VPC de desarrollo, pero no tiene acceso a `172.16.0.0/24` ni a ninguno de los restantes hosts de la VPC de desarrollo.

> **Note**
>
> Aquí se ve cómo una regla con un prefijo IP más largo tiene prioridad sobre una regla con un prefijo IP más corto. Si desea que el grupo de desarrollo tenga acceso a `10.0.2.119/32`, es necesario agregar una regla adicional que conceda acceso a `10.0.2.119/32` al equipo de desarrollo.

CIDR superpuesto (mismo grupo)

Descripción de la regla	ID de grupo	Permitir el acceso a todos los usuarios	CIDR de destino
Proporcionar acceso al grupo de ingeniería a la red en las instalaciones	S-xxxxx14	False	172.16.0.0/24
Proporcionar acceso al grupo de desarrollo a la VPC de desarrollo	S-xxxxx15	False	10.0.0.0/16
Proporcionar acceso al grupo de administradores a cualquier destino	S-xxxxx16	False	0.0.0.0/0
Proporcionar acceso al grupo de administradores a un único host en la VPC de desarrollo	S-xxxxx16	False	10.0.2.119/32
	S-xxxxx14	False	172.16.0.128/25

Descripción de la regla	ID de grupo	Permitir el acceso a todos los usuarios	CIDR de destino
Proporcionar acceso al grupo de ingeniería a una subred más pequeña en las instalaciones			

Comportamiento resultante

- El grupo de desarrollo puede acceder a `10.0.0.0/16`, excepto al host individual `10.0.2.119/32`.
- El grupo de administradores puede acceder al Internet público, `192.168.0.0/24` y a un host individual (`10.0.2.119/32`) en la red `10.0.0.0/16`, pero no tiene acceso a `172.16.0.0/24` ni a ninguno de los restantes hosts de la red `10.0.0.0/16`.
- El grupo de ingeniería tiene acceso a `172.16.0.0/24`, incluida la subred más específica `172.16.0.128/25`.

Regla 0.0.0.0/0 adicional

Descripción de la regla	ID de grupo	Permitir el acceso a todos los usuarios	CIDR de destino
Proporcionar acceso al grupo de ingeniería a la red en las instalaciones	S-xxxxx14	False	172.16.0.0/24
Proporcionar acceso al grupo de desarrollo a la VPC de desarrollo	S-xxxxx15	False	10.0.0.0/16

Descripción de la regla	ID de grupo	Permitir el acceso a todos los usuarios	CIDR de destino
Proporcionar acceso al grupo de administradores a cualquier destino	S-xxxxx16	False	0.0.0.0/0
Proporcionar acceso al grupo de administradores a un único host en la VPC de desarrollo	S-xxxxx16	False	10.0.2.119/32
Proporcionar acceso al grupo de ingeniería a una subred más pequeña en las instalaciones	S-xxxxx14	False	172.16.0.128/25
Proporcionar acceso al grupo de ingeniería a cualquier destino	S-xxxxx14	False	0.0.0.0/0

Comportamiento resultante

- El grupo de desarrollo puede acceder a `10.0.0.0/16`, excepto al host individual `10.0.2.119/32`.
- El grupo de administradores puede acceder al Internet público, `192.168.0.0/24` y a un host individual (`10.0.2.119/32`) en la red `10.0.0.0/16`, pero no tiene acceso a `172.16.0.0/24` ni a ninguno de los restantes hosts de la red `10.0.0.0/16`.
- El grupo de ingeniería puede acceder al Internet público, `192.168.0.0/24` y `172.16.0.0/24`, incluida la subred más específica `172.16.0.128/25`.

> **Note**
>
> Observe que tanto el grupo de ingenieros como el de administradores ahora pueden acceder a `192.168.0.0/24`. Esto se debe a que ambos grupos tienen acceso a `0.0.0.0/0` (cualquier destino) y no hay otras reglas que hagan referencia a `192.168.0.0/24`.

Agregación de una regla para 192.168.0.0/24

Descripción de la regla	ID de grupo	Permitir el acceso a todos los usuarios	CIDR de destino
Proporcionar acceso al grupo de ingeniería a la red en las instalaciones	S-xxxxx14	False	172.16.0.0/24
Proporcionar acceso al grupo de desarrollo a la VPC de desarrollo	S-xxxxx15	False	10.0.0.0/16
Proporcionar acceso al grupo de administradores a cualquier destino	S-xxxxx16	False	0.0.0.0/0
Proporcionar acceso al grupo de administradores a un único host en la VPC de desarrollo	S-xxxxx16	False	10.0.2.119/32
Proporcionar acceso al grupo de ingeniería	S-xxxxx14	False	172.16.0.128/25

Descripción de la regla	ID de grupo	Permitir el acceso a todos los usuarios	CIDR de destino
a a una subred en la red en las instalaciones			
Proporcionar acceso al grupo de ingeniería a cualquier destino	S-xxxxx14	False	0.0.0.0/0
Proporcionar acceso al grupo de administración a la VPC de Client VPN	S-xxxxx16	False	192.168.0.0/24

Comportamiento resultante

- El grupo de desarrollo puede acceder a `10.0.0.0/16`, excepto al host individual `10.0.2.119/32`.
- El grupo de administradores puede acceder al Internet público, `192.168.0.0/24` y a un host individual (`10.0.2.119/32`) en la red `10.0.0.0/16`, pero no tiene acceso a `172.16.0.0/24` ni a ninguno de los restantes hosts de la red `10.0.0.0/16`.
- El grupo de ingeniería puede acceder al Internet público, `172.16.0.0/24` y `172.16.0.128/25`.

> **Note**
>
> Observe cómo al agregar la regla para que el grupo de administradores acceda a `192.168.0.0/24`, el grupo de desarrollo deja de tener acceso a esa red de destino.

Autenticación federada SAML

Descripción de la regla	ID de grupo	Permitir el acceso a todos los usuarios	CIDR de destino
Proporcionar acceso al grupo de ingeniería a la red en las instalaciones	Diseño	False	172.16.0.0/24
Proporcionar acceso al grupo de desarrollo a la VPC de desarrollo	Desarrolladores	False	10.0.0.0/16
Proporcionar acceso al grupo de administración a la VPC de Client VPN	Administradores	False	192.168.0.0/24

Comportamiento resultante

- Los usuarios autenticados mediante SAML con el atributo de grupo “Ingeniería” solo pueden acceder a `172.16.0.0/24`.
- Los usuarios autenticados mediante SAML con el atributo de grupo “Desarrolladores” solo pueden acceder a `10.0.0.0/16`.
- Los usuarios autenticados mediante SAML con el atributo de grupo “Administradores” solo pueden acceder a `192.168.0.0/24`.
- El punto de conexión de Client VPN descarta el resto del tráfico.

> **Note**
>
> Cuando se utiliza la autenticación federada de SAML, el campo de ID de grupo corresponde al valor del atributo SAML que identifica la pertenencia al grupo del usuario. Este atributo

se configura en el proveedor de identidad SAML y se pasa a Client VPN durante la autenticación.

Acceso para todos los grupos de usuarios

Descripción de la regla	ID de grupo	Permitir el acceso a todos los usuarios	CIDR de destino
Proporcionar acceso al grupo de ingeniería a la red en las instalaciones	S-xxxxx14	False	172.16.0.0/24
Proporcionar acceso al grupo de desarrollo a la VPC de desarrollo	S-xxxxx15	False	10.0.0.0/16
Proporcionar acceso al grupo de administradores a cualquier destino	S-xxxxx16	False	0.0.0.0/0
Proporcionar acceso al grupo de administradores a un único host en la VPC de desarrollo	S-xxxxx16	False	10.0.2.119/32
Proporcionar acceso al grupo de ingeniería a una subred en la	S-xxxxx14	False	172.16.0.128/25

Descripción de la regla	ID de grupo	Permitir el acceso a todos los usuarios	CIDR de destino
red en las instalaciones			
Proporcionar acceso al grupo de ingeniería a todas las redes	S-xxxxx14	False	0.0.0.0/0
Proporcionar acceso al grupo de administración a la VPC de Client VPN	S-xxxxx16	False	192.168.0.0/24
Proporcionar acceso a todos los grupos	N/A	True	0.0.0.0/0

Comportamiento resultante

- El grupo de desarrollo puede acceder a `10.0.0.0/16`, excepto al host individual `10.0.2.119/32`.
- El grupo de administradores puede acceder al Internet público, `192.168.0.0/24` y a un host individual (`10.0.2.119/32`) en la red `10.0.0.0/16`, pero no tiene acceso a `172.16.0.0/24` ni a ninguno de los restantes hosts de la red `10.0.0.0/16`.
- El grupo de ingeniería puede acceder al Internet público, `172.16.0.0/24` y `172.16.0.128/25`.
- Cualquier otro grupo de usuarios, por ejemplo, el "grupo de administradores", puede acceder al Internet público, pero no a otras redes de destino definidas en las demás reglas.

Agregar una regla de autorización a un AWS Client VPN punto final

Puede agregar una regla de autorización para conceder o restringir el acceso a un punto de conexión de Client VPN a través de Consola de administración de AWS. Se puede agregar una regla de

autorización a un punto de conexión de Client VPN a través de la consola de Amazon VPC o a través de la línea de comandos o API.

Para agregar una regla de autorización a un punto final de Client VPN mediante Consola de administración de AWS

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN Endpoints (Puntos de enlace de Client VPN).
3. Seleccione el punto de conexión de Client VPN al que va a agregar la regla de autorización y elija Authorization rules (Reglas de autorización) y Add authorization rule (Agregar regla de autorización).
4. En Destination network to enable access (Red de destino para habilitar acceso), ingrese la dirección IP, en notación CIDR, de la red a la que desea que accedan los usuarios (por ejemplo, el bloque de CIDR de la VPC).
5. Especifique qué clientes pueden obtener acceso a la red especificada. En For grant access to (Para conceder acceso a), realice una de las siguientes operaciones::

   - Para conceder acceso a todos los clientes, seleccione Allow access to all users (Permitir acceso a todos los usuarios).
   - Para restringir el acceso a clientes específicos, elija Permitir acceso a los usuarios de un grupo de acceso específico y, a continuación, en ID de grupo de acceso, escriba el ID del grupo al que se va a conceder acceso. Por ejemplo, el identificador de seguridad (SID) de un grupo de Active Directory o el ID/name de un grupo definido en un proveedor de identidad (IdP) basado en SAML.
     - (Active Directory) Para obtener el SID, puede usar el ADGroup cmdlet Get- de Microsoft Powershell, por ejemplo:

       ```
       Get-ADGroup -Filter 'Name -eq "<Name of the AD Group>"'
       ```

       También puede abrir la herramienta de usuarios y equipos de Active Directory, consultar las propiedades del grupo, ir a la pestaña del editor de atributos y obtener el valor de `objectSID`. Si es necesario, primero elija View (Ver), Advanced Features (Características avanzadas) para habilitar la pestaña del editor de atributos.
     - (Autenticación federada basada en SAML) El grupo ID/name debe coincidir con la información de atributos del grupo que se devuelve en la afirmación SAML.
6. En Description (Descripción), escriba una breve descripción de la regla de autorización.

7. Seleccione Add authorization rule (Añadir regla de autorización).

Agregar una regla de autorización a un punto de enlace de Client VPN (AWS CLI)

Utilice el comando authorize-client-vpn-ingress.

Eliminar una regla de autorización de un AWS Client VPN punto final

Puede eliminar las reglas de autorización de un punto de conexión de Client VPN específico a través de la consola y AWS CLI.

Eliminación de reglas de autorización (consola)

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN Endpoints (Puntos de enlace de Client VPN).
3. Seleccione el punto de conexión de Client VPN para el que se agregó la regla de autorización y, a continuación, elija Reglas de autorización.
4. Seleccione la regla de autorización a eliminar, elija Eliminación de regla de autorización y, a continuación, elija Eliminar regla de autorización.

Eliminación de reglas de autorización (AWS CLI)

Utilice el comando revoke-client-vpn-ingress.

Visualización de reglas de autorización de AWS Client VPN

Puede consultar las reglas de autorización de un punto de enlace de Client VPN específico a través de la consola y AWS CLI.

Para ver las reglas de autorización (consola)

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN Endpoints (Puntos de enlace de Client VPN).
3. Seleccione el punto de conexión de Client VPN cuyas reglas de autorización desee ver y elija Authorization rules (Reglas de autorización).

Para ver las reglas de autorización (AWS CLI)

Utilice el comando describe-client-vpn-authorization-rules.

AWS Client VPN listas de revocación de certificados de cliente

Las listas de revocación de certificados de cliente de Client VPN se usan para revocar el acceso a un punto de conexión de Client VPN para certificados de cliente específicos. Puede generar una lista de revocación o importar una lista existente. También puede exportar la lista actual a un archivo de lista de revocación. La generación de una lista se realiza mediante el software OpenVPN en Windows Linux/macOS o en Windows. La importación y la exportación se pueden realizar mediante la consola de Amazon VPC o mediante la CLI AWS .

Para obtener más información sobre cómo generar los certificados y las claves del cliente y el servidor, consulte Autenticación mutua en AWS Client VPN

> **Note**
>
> Si esta lista ha caducado, no puede conectarse al punto de conexión de Client VPN. Deberá crear una nueva e importarla al punto de conexión de Client VPN.

Puede agregar solo un número de entradas limitado a una lista de revocación de certificados de cliente. Para obtener más información sobre la cantidad de entradas que puede agregar a una lista de revocación, consulte Cuotas de Client VPN.

Tareas

- Generar una lista de revocaciones de certificados de AWS Client VPN cliente
- Importar una lista de revocaciones de certificados de AWS Client VPN cliente
- Exportar una lista de revocaciones de certificados de AWS Client VPN cliente

Generar una lista de revocaciones de certificados de AWS Client VPN cliente

Puede generar una lista de revocaciones de certificados de Client VPN en un sistema operativo Linux/macOS o Windows. La lista de revocación se utiliza para revocar el acceso a un punto de conexión de Client VPN para certificados específicos. Para obtener más información sobre listas de revocación de certificados del cliente, consulte Listas de revocación de certificados del cliente.

Linux/macOS

En el procedimiento siguiente, genera una lista de revocación de certificados del cliente mediante la utilidad de línea de comandos easy-rsa de OpenVPN.

Para generar una lista de revocación de certificados del cliente mediante easy-rsa de OpenVPN

1. Inicie sesión en el servidor que aloja la instalación easyrsa que se usó para generar el certificado.
2. Vaya a la carpeta `easy-rsa/easyrsa3` de su repositorio local.

```
$ cd easy-rsa/easyrsa3
```

3. Revocar el certificado de cliente y generar la lista de revocación de cliente.

```
$ ./easyrsa revoke client1.domain.tld
$ ./easyrsa gen-crl
```

Ingrese `yes` cuando se le pida.

Windows

El siguiente procedimiento utiliza el software OpenVPN para generar una lista de revocación de clientes. Se supone que ha seguido los pasos para utilizar el software OpenVPN para generar los certificados y claves de cliente y servidor.

Para generar una lista de revocación de certificados de cliente utilizando EasyRSA versión 3.x.x

1. Abra un símbolo del sistema y navegue hasta el directorio EasyRSA-3.x.x, que dependerá de dónde esté instalado en el sistema.

```
C:\> cd c:\Users\windows\EasyRSA-3.x.x
```

2. Ejecute el archivo `EasyRSA-Start.bat` para iniciar el intérprete de comandos de EasyRSA.

```
C:\> .\EasyRSA-Start.bat
```

3. Revoque el certificado del cliente en el shell de EasyRSA.

```
# ./easyrsa revoke client_certificate_name
```

4. Ingrese `yes` cuando se le pida.
5. Genere la lista de revocación de clientes.

```
# ./easyrsa gen-crl
```

6. La lista de revocación de clientes se creará en la siguiente ubicación:

```
c:\Users\windows\EasyRSA-3.x.x\pki\crl.pem
```

Para generar una lista de revocación de certificados de cliente utilizando versiones anteriores de EasyRSA

1. Abra un símbolo del sistema y vaya al directorio de OpenVPN.

```
C:\> cd \Program Files\OpenVPN\easy-rsa
```

2. Ejecute el archivo `vars.bat`.

```
C:\> vars
```

3. Revocar el certificado de cliente y generar la lista de revocación de cliente.

```
C:\> revoke-full client_certificate_name
C:\> more crl.pem
```

Importar una lista de revocaciones de certificados de AWS Client VPN cliente

Debe tener un archivo de lista de revocación de certificados del cliente de Client VPN para importarlo. Para obtener más información sobre cómo generar una lista de revocación de certificados del cliente, consulte Generar una lista de revocaciones de certificados de AWS Client VPN cliente.

Puede importar una lista de revocación de certificados del cliente mediante la consola y la AWS CLI.

Para importar una lista de revocación de certificados del cliente (consola)

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN Endpoints (Puntos de enlace de Client VPN).
3. Seleccione el punto de enlace de Client VPN para el que va a importar la lista de revocación de certificados del cliente.
4. Elija Actions (Acciones) y seleccione Import Client Certificate CRL (Importar CRL de certificados de cliente).
5. En Certificate Revocation List (Lista de revocación de certificados), ingrese el archivo de la lista de revocación de certificados del cliente y seleccione Import client certificate CRL (Importar CRL de certificados de cliente).

Para importar una lista de revocación de certificados del cliente (AWS CLI)

Utilice el certificate-revocation-list comando import-client-vpn-client-.

```
$ aws ec2 import-client-vpn-client-certificate-revocation-list --certificate-
revocation-list file://path_to_CRL_file --client-vpn-endpoint-id endpoint_id --
region region
```

Exportar una lista de revocaciones de certificados de AWS Client VPN cliente

Puede exportar listas de revocación de certificados de cliente de Client VPN mediante la consola y la AWS CLI.

Para exportar una lista de revocación de certificados del cliente (consola)

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN Endpoints (Puntos de enlace de Client VPN).
3. Seleccione el punto de enlace de Client VPN para el que va a exportar la lista de revocación de certificados del cliente.
4. Elija Actions (Acciones), seleccione Export Client Certificate CRL (Exportar CRL de certificados de cliente) y elija Export Client Certificate CRL (Exportar CRL de certificados de cliente).

Para exportar una lista de revocación de certificados del cliente (AWS CLI)

Utilice el certificate-revocation-list comando export-client-vpn-client-.

Conexiones de clientes de AWS Client VPN

Las conexiones de AWS Client VPN son sesiones de VPN activas que los clientes han establecido en un punto de conexión de Client VPN específico, así como conexiones que se hayan finalizado en los últimos 60 minutos para ese punto de conexión. Una conexión se establece cuando un cliente se conecta correctamente a un punto de enlace de Client VPN. Al finalizar una sesión, se finaliza la conexión del cliente con el punto de conexión de Client VPN.

Puede ver y finalizar las conexiones de Client VPN. La visualización de la información de conexión devuelve información como la dirección IP asignada del rango de bloques de CIDR del cliente, el ID del punto de conexión y la marca temporal. Al finalizar una sesión, se finaliza la conexión de la VPN especificada con el punto de conexión. La visualización y la finalización de las sesiones se pueden realizar mediante la consola de Amazon VPC o la CLI de AWS. Si no puede conectarse al punto de conexión y, en función del error, consulte Solución de problemas para ver las medidas que debe tomar para resolver el problema.

Tareas

- Visualización de conexiones de clientes de AWS Client VPN
- Finalizar una conexión de AWS Client VPN cliente

Visualización de conexiones de clientes de AWS Client VPN

Puede ver las conexiones de Client VPN activas mediante la consola de Amazon VPC o la CLI de AWS.

Visualización de las conexiones de clientes de Client VPN (consola)

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN Endpoints (Puntos de enlace de Client VPN).
3. Seleccione el punto de enlace de Client VPN cuyas conexiones de clientes desee ver.
4. Elija la pestaña Connections (Conexiones). En la pestaña Connections (Conexiones) se incluyen todas las conexiones de clientes activas y terminadas.

Visualización de las conexiones de clientes de Client VPN (AWS CLI)

Utilice el comando describe-client-vpn-connections.

Finalizar una conexión de AWS Client VPN cliente

Puede finalizar la conexión de un cliente Client VPN mediante la consola de Amazon VPC o la CLI AWS .

Terminación de una conexión de cliente de Client VPN (consola)

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN Endpoints (Puntos de enlace de Client VPN).
3. Seleccione el punto de conexión de Client VPN al que está conectado el cliente y elija Connections.
4. Seleccione la conexión que va a terminar, elija Terminar conexión y, a continuación, elija Terminar conexión de nuevo para confirmar la terminación.

Terminación de una conexión de cliente de Client VPN (AWS CLI)

Utilice el comando terminate-client-vpn-connections.

Banners de inicio de sesión de cliente de AWS Client VPN

AWS Client VPN ofrece la opción de mostrar un banner de texto en AWS proporciona aplicaciones de escritorio de Client VPN cuando se establece una sesión VPN. Puede definir el contenido del banner de texto para satisfacer sus necesidades normativas y de conformidad. Se pueden utilizar un máximo de 1400 caracteres codificados de UTF-8.

> **Note**
>
> Cuando se ha habilitado un banner de inicio de sesión de cliente, solo se mostrará en las sesiones VPN recién creadas. Las sesiones VPN existentes no se interrumpen, aunque el banner se mostrará cuando se restablezca una sesión existente.

Creación de un banner

Los banners de inicio de sesión se crean y se habilitan inicialmente durante la creación del punto de conexión de Client VPN. Para obtener los pasos para habilitar un banner de inicio de sesión de

cliente durante la creación de un punto de conexión de Client VPN, consulte Crear un AWS Client VPN punto final.

Tareas

- Configurar un banner de inicio de sesión de cliente para un AWS Client VPN punto final existente
- Desactivar un banner de inicio de sesión de cliente para un punto final existente AWS Client VPN
- Modificar el texto del encabezado existente en un AWS Client VPN punto final
- Ver un banner de inicio de AWS Client VPN sesión configurado actualmente

Configurar un banner de inicio de sesión de cliente para un AWS Client VPN punto final existente

Siga los siguientes pasos para configurar un banner de inicio de sesión de cliente para un punto de conexión de Client VPN existente.

Habilitar el banner de inicio de sesión de cliente en un punto de conexión de Client VPN (consola)

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN Endpoints (Puntos de enlace de Client VPN).
3. Seleccione el punto de conexión de Client VPN que desee modificar, elija Actions (Acciones) y, a continuación, elija Modify Client VPN Endpoint (Modificar punto de conexión de Client VPN).
4. Desplácese por la página hasta la sección Other parameters (Otros parámetros).
5. Active Enable client login banner (Habilitar banner de inicio de sesión de cliente).
6. En el texto del encabezado de inicio de sesión del cliente, introduzca el texto que se mostrará en un banner en los clientes AWS proporcionados cuando se establezca una sesión de VPN. Utilice sólo caracteres codificados en UTF-8, con un máximo de 1400 caracteres permitidos.
7. Elija Modify Client VPN endpoint (Modificar punto de conexión de Client VPN).

Habilitar el banner de inicio de sesión de cliente en un punto de conexión de Client VPN (AWS CLI)

Utilice el comando modify-client-vpn-endpoint.

Desactivar un banner de inicio de sesión de cliente para un punto final existente AWS Client VPN

Siga estos pasos para desactivar un banner de inicio de sesión de cliente para un punto de conexión de Client VPN existente.

Desactivar el banner de inicio de sesión de cliente en un punto de conexión de Client VPN (consola)

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN Endpoints (Puntos de enlace de Client VPN).
3. Seleccione el punto de conexión de Client VPN que desee modificar, elija Actions (Acciones) y, a continuación, elija Modify Client VPN endpoint (Modificar punto de conexión de Client VPN).
4. Desplácese por la página hasta la sección Other parameters (Otros parámetros).
5. Desactive Enable client login banner (Habilitar banner de inicio de sesión de cliente).
6. Elija Modify Client VPN endpoint (Modificar punto de conexión de Client VPN).

Desactivar el banner de inicio de sesión de cliente en un punto de conexión de Client VPN (AWS CLI)

Utilice el comando modify-client-vpn-endpoint.

Modificar el texto del encabezado existente en un AWS Client VPN punto final

Siga estos pasos para modificar el texto existente en un banner de inicio de sesión de cliente de Client VPN.

Modificación del texto del banner existente en un punto de conexión de Client VPN (consola)

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN Endpoints (Puntos de enlace de Client VPN).
3. Seleccione el punto de conexión de Client VPN que desee modificar, elija Actions (Acciones) y, a continuación, elija Modify Client VPN endpoint (Modificar punto de conexión de Client VPN).
4. En Enable client login banner?(¿Habilitar banner de inicio de sesión de cliente?), verifique que se ha activado.

5. En el texto del encabezado de inicio de sesión del cliente, sustituya el texto existente por el texto nuevo que desee que aparezca en un banner en los clientes AWS proporcionados cuando se establezca una sesión de VPN. Utilice sólo caracteres codificados en UTF-8, con un máximo de 1400 caracteres.
6. Elija Modify Client VPN endpoint (Modificar punto de conexión de Client VPN).

Modificación de un banner de inicio de sesión de cliente en un punto de conexión de Client VPN (AWS CLI)

Utilice el comando modify-client-vpn-endpoint.

Ver un banner de inicio de AWS Client VPN sesión configurado actualmente

Utilice los pasos siguientes para ver un banner de inicio de sesión de cliente de Client VPN configurado actualmente.

Ver el banner de inicio de sesión actual para un punto de conexión de Client VPN (consola)

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN Endpoints (Puntos de enlace de Client VPN).
3. Seleccione el punto de conexión de Client VPN que desea ver.
4. Verifique que la pestaña Details (Detalles) esté seleccionada.
5. Vea el texto del banner de inicio de sesión configurado actualmente junto a Client login banner text (Texto del banner de inicio de sesión de cliente).

Ver un banner de inicio de sesión configurado actualmente en un punto de conexión de Client VPN (AWS CLI)

Utilice el comando describe-client-vpn-endpoints.

AWS Client VPN Aplicación de rutas del cliente

Client Route Enforcement ayuda a aplicar las rutas definidas por el administrador en los dispositivos conectados a través de la VPN. Esta característica ayuda a mejorar su nivel de seguridad al garantizar que el tráfico de red que se origina en un cliente conectado no se envíe por error fuera del túnel de la VPN.

Client Route Enforcement monitoriza la tabla de enrutamiento principal del dispositivo conectado y se asegura de que el tráfico de red saliente vaya a un túnel de VPN, de acuerdo con las rutas de red configuradas en el punto de conexión de la VPN cliente. Esto incluye la modificación de las tablas de enrutamiento de un dispositivo si se detectan rutas que entran en conflicto con el túnel de VPN. Client Route Enforcement apoya tanto IPv4 a las familias como a las de IPv6 direcciones.

Requisitos

Client Route Enforcement solo funciona con las siguientes versiones de Client VPN AWS proporcionadas:

- Windows versión 5.2.0 o superior (IPv4 compatible)
- macOS versión 5.2.0 o superior (IPv4 compatible)
- Ubuntu versión 5.2.0 o superior (compatible) IPv4
- Windows versión 5.3.0 o superior (compatible) IPv6
- macOS versión 5.3.0 o superior (IPv6 compatible)
- Ubuntu versión 5.3.0 o superior (compatible) IPv6

En el caso de los puntos finales de doble pila, la configuración de cumplimiento de rutas del cliente se aplica a ambos IPv4 y IPv6 a las pilas simultáneamente. No es posible habilitar Client Route Enforcement para una sola pila.

Conflictos de enrutamiento

Mientras un cliente está conectado a la VPN, se realiza una comparación entre la tabla de enrutamiento local del cliente y las rutas de red del punto de conexión. Se producirá un conflicto de enrutamiento si hay solapamiento de redes entre dos entradas de la tabla de enrutamiento. Un ejemplo de redes solapadas es:

- `172.31.0.0/16`
- `172.31.1.0/24`

En este ejemplo, estos bloques de CIDR constituyen un conflicto de enrutamiento. Por ejemplo, `172.31.0.0/16` podría ser el CIDR del túnel de VPN. Dado que `172.31.1.0/24` es más específico porque tiene un prefijo más largo, normalmente tiene prioridad y, potencialmente, redirige el tráfico de VPN en el intervalo de IP de `172.31.1.0/24` a otro destino. Esto podría provocar

un comportamiento de enrutamiento no deseado. Sin embargo, cuando se habilita Client Route Enforcement, se elimina este último CIDR. Al utilizar esta característica, se deben tener en cuenta posibles conflictos de enrutamiento.

Las conexiones de VPN de túnel completo dirigen todo el tráfico de red a través de la conexión de VPN. Por ello, los dispositivos conectados a la VPN no podrán acceder a los recursos de la red local (LAN) si la característica Client Route Enforcement está habilitada. Si se requiere acceso a una LAN local, considere la posibilidad de utilizar el modo de túnel dividido en lugar del modo de túnel completo. Para obtener más información acerca del túnel dividido, consulte Client VPN con un túnel dividido.

Consideraciones

Debe tenerse en cuenta la siguiente información antes de activar Client Route Enforcement.

- En el momento de la conexión, si se detecta un conflicto de enrutamiento, la característica actualizará la tabla de enrutamiento del cliente para dirigir el tráfico al túnel de VPN. Se restaurarán las rutas que existían antes de que se estableciera la conexión y que esta característica eliminó.
- La característica solo se aplica en la tabla de enrutamiento principal y no se aplica a otros mecanismos de enrutamiento. Por ejemplo, la aplicación no se aplica a lo siguiente:
  - enrutamiento basado en políticas
  - enrutamiento en el ámbito de interfaz
- Client Route Enforcement protege el túnel de VPN mientras está abierto. No hay protección después de desconectar el túnel o mientras el cliente se vuelve a conectar.

Las directivas de OpenVPN afectan a Client Route Enforcement

Algunas directivas personalizadas del archivo de configuración de OpenVPN tienen interacciones específicas con Client Route Enforcement:

- La directiva `route`
  - Al añadir rutas a una puerta de enlace de VPN. Por ejemplo, al agregar la ruta `192.168.100.0 255.255.255.0` a una puerta de enlace de VPN.

El Client Route Enforcement monitoriza las rutas agregadas a una puerta de enlace VPN de forma similar a cualquier otra ruta de VPN. Se detectarán y eliminarán todas las rutas en conflicto.

- Al agregar rutas a una puerta de enlace de VPN. Por ejemplo, al agregar la ruta `192.168.200.0 255.255.255.0 net_gateway`.

  Las rutas agregadas a una puerta de enlace que no sea de VPN se excluyen de Client Route Enforcement, ya que omiten el túnel de la VPN. Se permiten rutas en conflicto. En el ejemplo anterior, la ruta quedará excluida de la monitorización de Client Route Enforcement.

- Al igual que en IPv4 las rutas, las IPv6 rutas agregadas a una puerta de enlace VPN son monitoreadas por Client Route Enforcement, mientras que las rutas agregadas a una puerta de enlace que no es de VPN se excluyen de la supervisión.

Rutas ignoradas

Client Route Enforcement ignorará IPv4 las rutas a las siguientes redes:

- `127.0.0.0/8`: reservado para el host local
- `169.254.0.0/16`: reservado para direcciones locales de enlace
- `224.0.0.0/4`: reservado para multidifusión
- `255.255.255.255/32`: reservado para transmisión

Client Route Enforcement ignorará IPv6 las rutas a las siguientes redes:

- `::1/128`: reservado para bucles invertidos
- `fe80::/10`: reservado para direcciones locales de enlace
- `ff00::/8`: reservado para multidifusión

Temas

- Active Client Route Enforcement para un AWS Client VPN punto final
- Desactive Client Route Enforcement desde un punto final AWS Client VPN
- Solucionar problemas de IPv6 Client Route Enforcement

Active Client Route Enforcement para un AWS Client VPN punto final

Puede activar Client Route Enforcement en los puntos de conexión de Client VPN existentes mediante la consola o la AWS CLI.

Cómo activar Client Route Enforcement mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN endpoints (Puntos de conexión de Client VPN).
3. Seleccione el punto de conexión de Client VPN que desee modificar, elija Acciones y, a continuación, elija Modificar punto de conexión de Client VPN.
4. Desplácese por la página hasta la sección Other parameters (Otros parámetros).
5. Active Client Route Enforcement.
6. Elija Modify Client VPN endpoint (Modificar punto de conexión de Client VPN).

Cómo activar Client Route Enforcement mediante la AWS CLI:

- Utilice el comando modify-client-vpn-endpoint.

Desactive Client Route Enforcement desde un punto final AWS Client VPN

Puede desactivar Client Route Enforcement en los puntos de conexión de Client VPN mediante la consola o la AWS CLI.

Cómo desactivar Client Route Enforcement mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN endpoints (Puntos de conexión de Client VPN).
3. Seleccione el punto de conexión de Client VPN que desee modificar, elija Acciones y, a continuación, elija Modificar punto de conexión de Client VPN.
4. Desplácese por la página hasta la sección Other parameters (Otros parámetros).
5. Desactive Client Route Enforcement.
6. Elija Modify Client VPN endpoint (Modificar punto de conexión de Client VPN).

Para desactivar Client Route Enforcement mediante el AWS CLI

- Utilice el comando modify-client-vpn-endpoint.

Solucionar problemas de IPv6 Client Route Enforcement

Si tiene problemas con la aplicación de rutas por IPv6 parte del cliente, tenga en cuenta los siguientes pasos de solución de problemas:

Verificación de la versión del cliente

Asegúrese de utilizar la versión 5.3.0 o superior del cliente VPN de AWS, que es necesaria para el soporte de IPv6 Client Route Enforcement.

Comprobación de la configuración de punto de conexión

Compruebe que el terminal tenga activado Client Route Enforcement y que esté configurado para el tráfico IPv6 de doble pila.

Examen de registros de clientes

Revise los registros del cliente VPN de AWS para ver si hay algún mensaje de error relacionado con la aplicación de rutas de IPv6 clientes. Busque entradas que contengan «» y IPv6 «Client Route Enforcement» o «CRM».

Inspección de tablas de enrutamiento

Use el comando apropiado para su sistema operativo para ver la tabla de IPv6 enrutamiento:

- Windows: `netsh interface ipv6 show route`
- macOS: `netstat -rn -f inet6`
- Linux: `ip -6 route`

Comprobación de rutas en conflicto

Busque cualquier IPv6 ruta que pueda entrar en conflicto con las rutas de la VPN. Preste especial atención a las rutas con el mismo destino, pero con diferentes puertas de enlace.

Verifica el soporte del ISP IPv6

Asegúrese de que su proveedor de servicios de Internet (ISP) sea compatible adecuadamente. IPv6

Si sigue teniendo problemas con IPv6 Client Route Enforcement después de seguir estos pasos de solución de problemas, póngase en contacto con AWS Support para obtener más ayuda.

AWS Client VPN puntos finales

Todas las AWS Client VPN sesiones establecen comunicación con un punto final Client VPN. Puede administrar el punto de conexión de Client VPN para crear, modificar, ver y eliminar sesiones de Client VPN con ese punto de conexión. Los puntos de conexión se pueden crear y modificar mediante la consola de Amazon VPC o mediante la CLI de AWS .

Requisitos para crear puntos de conexión de Client VPN

> **Important**
>
> Se debe crear un punto final Client VPN en la misma AWS cuenta en la que se aprovisiona la red de destino prevista. También tendrá que generar un certificado de servidor y, si es necesario, un certificado de cliente. Para obtener más información, consulte Autenticación de cliente en AWS Client VPN.

Antes de comenzar, asegúrese de hacer lo siguiente:

- Revise las reglas y las limitaciones en Reglas y mejores prácticas de uso AWS Client VPN.
- Genere el certificado de servidor y, si es necesario, el certificado de cliente. Para obtener más información, consulte Autenticación de cliente en AWS Client VPN.

Tipos de direcciones IP

AWS Client VPN admite configuraciones IPv4 de solo pila, solo y IPv6 de doble pila para la conectividad de los puntos finales y el enrutamiento del tráfico. La siguiente guía le ayuda a seleccionar el tipo de dirección IP adecuado en función de las capacidades del dispositivo cliente, la infraestructura de red y los requisitos de la aplicación.

Tipo de dirección del punto de conexión

El tipo de dirección del punto de conexión determina qué protocolos IP admite el punto de conexión de Client VPN para las conexiones de los clientes. Este ajuste no se puede cambiar después de la creación del punto de conexión.

Elija -solo cuando IPv4:

- Sus dispositivos cliente solo admiten conexiones IPv4 VPN
- Sus herramientas de seguridad están optimizadas para la inspección IPv4 del tráfico

Elija IPv6 -solo cuando:

- Todos los dispositivos cliente son totalmente compatibles IPv6 con las conexiones
- Estás en redes en las que las IPv4 direcciones están agotadas

Elija doble pila cuando:

- Tenga una combinación de dispositivos cliente con diferentes capacidades de IP
- Estás realizando una transición gradual de a IPv4 IPv6

Tipo de dirección IP de tráfico

El tipo de dirección IP de tráfico controla la forma en que Client VPN enruta el tráfico entre los clientes y sus recursos de VPC, independientemente que admita el punto de conexión.

Dirija el tráfico como IPv4 cuando:

- Solo admite aplicaciones de destino en su VPC IPv4
- Tiene redes y grupos IPv4 de seguridad complejos ACLs
- Se esté conectando a sistemas heredados

Redirija el tráfico como IPv6 cuando:

- Su infraestructura de VPC es principalmente IPv6
- Quiera preparar la arquitectura de red para el futuro
- Tiene aplicaciones modernas diseñadas para IPv6

Modificación de puntos de conexión

> **Note**
>
> Los puntos finales de Client VPN creados mediante la configuración de inicio rápido se pueden modificar mediante los mismos procedimientos que los puntos finales creados con la configuración estándar. Todas las opciones de configuración están disponibles independientemente del método de configuración utilizado durante la creación.

Después de crear una conexión de Client VPN, se puede modificar cualquiera de los siguientes ajustes:

- La descripción
- El certificado de servidor
- Las opciones de registro de la conexión de cliente
- La opción del controlador de la conexión del cliente
- Los servidores DNS
- La opción de túnel dividido
- Rutas (cuando se utiliza la opción de túnel dividido)
- Lista de revocación de certificados (CRL)
- Reglas de autorización
- Las asociaciones de grupos de seguridad y VPC
- El número de puerto de VPN
- La opción del portal de autoservicio
- El máximo de duración de la sesión VPN
- Habilitación o deshabilitación de reconexión automática cuando se agota el tiempo de espera de sesión
- Habilitar o desactivar el texto del banner de inicio de sesión de cliente
- Texto del banner de inicio de sesión de cliente

> **Note**
>
> Las modificaciones de los puntos de conexión de Client VPN, incluidos los cambios en la lista de revocación de certificados (CRL), surtirán efecto hasta cuatro horas después de que el servicio Client VPN acepte una solicitud.
> No puede modificar el rango IPv4 CIDR del cliente, las opciones de autenticación, el certificado del cliente o el protocolo de transporte una vez creado el punto final Client VPN.

Cuando modifica cualquiera de los siguientes parámetros en un punto de enlace de Client VPN, la conexión se restablece:

- El certificado de servidor
- Los servidores DNS
- La opción de túnel dividido (activar o desactivar el soporte)
- Rutas (cuando se utiliza la opción de túnel dividido)
- Lista de revocación de certificados (CRL)
- Reglas de autorización
- El número de puerto de VPN

Tareas

- Crear un AWS Client VPN punto final
- Visualización de puntos de enlace de AWS Client VPN
- Modificación de un punto de conexión de AWS Client VPN
- Eliminación de un punto de conexión de AWS Client VPN

Crear un AWS Client VPN punto final

Cree un AWS Client VPN punto final para que sus clientes puedan establecer una sesión de VPN mediante la consola Amazon VPC o la VPN AWS CLI.Client que admite todas las combinaciones del tipo de punto final (túnel dividido y túnel completo) con el tipo de tráfico (IPv4 IPv6, y pila doble) durante la creación inicial.

Antes de crear un punto de conexión, familiarícese con los requisitos. Para obtener más información, consulte the section called “Requisitos para crear puntos de conexión de Client VPN”.

Para crear un punto de conexión de Client VPN mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN Endpoints (Puntos de enlace de Client VPN) y Create Client VPN Endpoint (Crear punto de enlace de Client VPN).
3. En «Elegir método de configuración», seleccione una de las siguientes opciones:
   - Inicio rápido: cree un punto final con los valores predeterminados recomendados por AWS
   - Estándar: configure manualmente todos los ajustes del punto final

Configuración de inicio rápido:

1. En «Elegir método de configuración», selecciona Inicio rápido.
2. En « IPv4 CIDR de cliente», introduzca el rango de direcciones IP desde el que desea asignar las direcciones IP de los clientes. AWS recomienda usar un bloque CIDR /22 (por ejemplo, 10.0.0.0/22).
3. En «VPC», seleccione la VPC que desee asociar al punto final de Client VPN.
4. En «Subredes», seleccione una o más subredes en la VPC. Estas subredes se utilizarán para las asociaciones de redes de destino.
5. En Server certificate ARN (ARN del certificado del servidor), especifique el ARN del certificado TLS que va a utilizar el servidor. Los clientes utilizan el certificado de servidor para autenticar el punto de enlace de Client VPN al que están conectados.
6. Elija «Crear punto final Client VPN».

AWS crea automáticamente los siguientes recursos:

- Regla de autorización que permite a todos los usuarios acceder al CIDR de la VPC
- Asociación de la red de destino con las subredes de VPC seleccionadas
- Entradas de la tabla de enrutamiento para el CIDR de la VPC

Una vez creado el punto final, puede descargar el archivo de configuración del cliente desde la página de detalles del dispositivo final y distribuirlo entre los usuarios junto con el certificado y la clave del cliente.

Configuración estándar:

1. En «Elegir método de configuración», selecciona Estándar.
2. (Opcional) Escriba una etiqueta de nombre y una descripción del punto de conexión de Client VPN.
3. En Tipo de dirección IP de punto de conexión, elija el tipo de dirección IP para el punto de conexión.
   - IPv4: El punto final usa IPv4 direcciones para el tráfico del túnel VPN externo.
   - IPv6: El punto final usa IPv6 direcciones para el tráfico del túnel VPN externo.
   - Pila doble: el punto final utiliza ambas IPv6 direcciones IPv4 y para el tráfico del túnel VPN exterior.
4. En Tipo de dirección IP del tráfico, elija el tipo de dirección IP para el tráfico que fluye a través del punto de conexión.
   - IPv4: El punto final solo admite IPv4 tráfico.
   - IPv6: El punto final solo admite IPv6 tráfico.
   - Doble pila: el punto final admite ambos tipos IPv4 de IPv6 tráfico.
5. Para el IPv4 CIDR del cliente, especifique un rango de direcciones IP, en notación CIDR, desde el que asignar las direcciones IP de los clientes. Por ejemplo, `10.0.0.0/22`. Esto es obligatorio si ha seleccionado IPv4 una pila doble para el tipo de dirección IP de tráfico.

   > **Note**
   >
   > - El intervalo de direcciones no puede solaparse al intervalo de direcciones de la red de destino, al intervalo de direcciones de la VPC ni a ninguna de las rutas que se asociarán con el punto de conexión de Client VPN. El intervalo de direcciones del cliente debe tener un tamaño de bloque de CIDR mínimo de /22 y no superior a /12. No puede cambiar el intervalo de direcciones del cliente después de crear el punto de conexión de Client VPN.
   > - IPv6 Al seleccionar el tipo de dirección IP del punto final, el campo IPv4 CIDR del cliente se deshabilita. El punto final Client VPN asigna IPv6 las direcciones de los clientes de una subred asociada y usted puede asociar la subred después de crear el punto final.

> **Note**
>
> Para el IPv6 tráfico, no es necesario especificar un rango de CIDR de cliente. Amazon asigna automáticamente los rangos de IPv6 CIDR a los clientes.

6. En Server certificate ARN (ARN del certificado del servidor), especifique el ARN del certificado TLS que va a utilizar el servidor. Los clientes utilizan el certificado de servidor para autenticar el punto de enlace de Client VPN al que están conectados.

> **Note**
>
> El certificado del servidor debe estar presente en AWS Certificate Manager(ACM) en la región en la que va a crear el punto final Client VPN. El certificado se puede aprovisionar con ACM o importarse a ACM.
> Para conocer los pasos para aprovisionar o importar un certificado a ACM, consulte Certificados de AWS Certificate Manager en la Guía del usuario de AWS Certificate Manager.

7. Especifique el método de autenticación que se va a utilizar para autenticar los clientes al establecer una conexión de VPN. Debe seleccionar un método de autenticación.

   - Para usar la autenticación basada en usuarios, seleccione Utilizar la autenticación basada en usuarios y, a continuación, elija una de las opciones siguientes:
     - Autenticación con Active Directory: elija esta opción para la autenticación con Active Directory. Para ID de directorio, especifique el ID de Active Directory que se va a utilizar.
     - Autenticación federada: elija esta opción para la autenticación federada basada en SAML.

       Para ARN del proveedor SAML, especifique el ARN del proveedor de identidades SAML de IAM.

       (Opcional) En Self-service SAML provider ARN (ARN del proveedor SAML de autoservicio), especifique el ARN del proveedor de identidades SAML de IAM que creó para poder utilizar el portal de autoservicio, si procede.
   - Para usar la autenticación con certificado mutuo, seleccione Usar autenticación mutua y, a continuación, en el ARN del certificado de cliente, especifique el ARN del certificado de cliente aprovisionado en (ACM).AWS Certificate Manager

> **Note**
>
> Si los certificados de servidor y cliente los ha emitido la misma entidad de certificación (CA), puede utilizar el ARN del certificado de servidor para el servidor y el cliente. Si el certificado de cliente fue emitido por una entidad de certificación distinta, debe especificarse el ARN del certificado de cliente.

8. (Opcional) Para el registro de conexiones, especifique si desea registrar los datos sobre las conexiones de los clientes mediante Amazon CloudWatch Logs. Active Enable log details on client connections (Habilitar los detalles de registro en las conexiones de cliente). En el nombre del grupo de CloudWatch registros, introduzca el nombre del grupo de registros que se va a utilizar. En el caso del nombre del flujo de registro de CloudWatch registros, introduzca el nombre del flujo de registro que desee utilizar o deje esta opción en blanco para que podamos crear un flujo de registro para usted.
9. (Opcional) En Client Connect Handler (Controlador de conexión de cliente), active Enable client connect handler (Habilitar controlador de conexión de cliente) para ejecutar código personalizado que permita o deniegue una nueva conexión con el punto de conexión de Client VPN. En Client Connect Handler ARN (ARN del controlador de la conexión del cliente), especifique el nombre de recurso de Amazon (ARN) de la función Lambda que contiene la lógica que va a permitir o a denegar las conexiones.
10. (Opcional) Especifique qué servidores DNS se van a utilizar para la resolución de DNS. Para usar servidores DNS personalizados, para la dirección IP del servidor DNS 1 y la dirección IP del servidor DNS 2, especifique las IPv4 direcciones de los servidores DNS que se van a utilizar. Para los puntos finales IPv6 o de doble pila, también puede especificar las direcciones del servidor DNS IPv6 1 y del servidor DNS IPv6 2. Para utilizar un servidor DNS de la VPC, en DNS Server 1 IP address (Dirección IP del servidor DNS 1) o DNS Server 2 IP address (Dirección IP del servidor DNS 2), especifique las direcciones IP y agregue la dirección IP del servidor DNS de la VPC.

> **Note**
>
> Asegúrese de que los clientes pueden acceder a los servidores DNS.

11. (Opcional) De forma predeterminada, el punto de conexión de Client VPN utiliza el protocolo de transporte `UDP`. Para utilizar el protocolo de transporte `TCP` en su lugar, en Transport Protocol (Protocolo de transporte), seleccione TCP.

> **Note**
>
> Normalmente UDP tiene mejor rendimiento que TCP. El protocolo de transporte no se puede cambiar una vez creado el punto de enlace de Client VPN.

12. (Opcional) Para que el punto de conexión sea un punto de conexión de Client VPN de túnel dividido, active Enable split-tunnel (Habilitar túnel dividido). De forma predeterminada, el túnel dividido en un punto de conexión de Client VPN está desactivado.
13. (Opcional) En VPC ID (ID de VPC), elija la VPC que desea asociar con el punto de enlace de Client VPN. En Security Group IDs, elija uno o más de los grupos de seguridad de la VPC para aplicarlos al punto final Client VPN.
14. (Opcional) En VPN port (Puerto de VPN), elija el número de puerto de VPN. El valor predeterminado es 443.
15. (Opcional) Si desea generar una URL del portal de autoservicio para los clientes, active Enable self-service portal (Habilitar portal de autoservicio).
16. (Opcional) Para Session timeout hours (Tiempo de espera de la sesión), elija el tiempo máximo de duración de la sesión VPN deseado en horas de las opciones disponibles o deje el valor predeterminado de 24 horas.
17. (Opcional) Para Desconectarse al finalizar el tiempo de espera de la sesión, elija si desea terminar la sesión cuando se llegue al tiempo máximo de sesión. La elección de esta opción requiere que los usuarios se vuelvan a conectar manualmente al punto de conexión al finalizar el tiempo de espera de la sesión; de lo contrario, Client VPN intentará volver a conectarse automáticamente.
18. (Opcional) Especifique si desea habilitar el texto del banner de inicio de sesión de cliente. Active Enable client login banner (Habilitar banner de inicio de sesión de cliente). En Client Login Banner Text (Texto de banner de inicio de sesión de cliente), ingrese el texto que se mostrará en un banner en los clientes proporcionados por AWS cuando se establezca una sesión de VPN. Solo caracteres con codificación UTF-8. Máximo de 1400 caracteres.
19. Elija Create Client VPN endpoint (Crear punto de conexión de Client VPN).

Cuando haya creado el punto de enlace de Client VPN, haga lo siguiente para completar la configuración y permitir que los clientes se conecten:

- El estado inicial del punto de enlace de Client VPN es `pending-associate`. Los clientes solo pueden conectarse al punto de enlace de Client VPN después de asociar la primera red de destino.
- Cree una regla de autorización para especificar qué clientes tienen acceso a la red.
- Descargue y prepare el archivo de configuración del punto de enlace de Client VPN para distribuirlo a sus clientes.
- Indique a sus clientes que utilicen el cliente AWS proporcionado u otra aplicación cliente basada en OpenVPN para conectarse al punto final Client VPN. Para obtener más información, consulte la Guía del usuario de AWS Client VPN.

Para crear un punto final Client VPN mediante el AWS CLI

Utilice el comando create-client-vpn-endpoint.

Ejemplo de creación de un IPv4 punto final:

```
aws ec2 create-client-vpn-endpoint \
  --client-cidr-block "172.31.0.0/16" \
  --server-certificate-arn arn:aws:acm:ap-south-1:123456789012:certificate/
a1b2c3d4-5678-90ab-cdef-11111EXAMPLE \
  --authentication-options Type=certificate-
authentication,MutualAuthentication={ClientRootCertificateChainArn=arn:aws:acm:ap-
south-1:123456789012:certificate/a1b2c3d4-5678-90ab-cdef-22222EXAMPLE} \
  --connection-log-options Enabled=false
```

Ejemplo de creación de un IPv6 punto final:

```
aws ec2 create-client-vpn-endpoint \
  --endpoint-ip-address-type "ipv6" \
  --traffic-ip-address-type "ipv6" \
  --server-certificate-arn arn:aws:acm:ap-south-1:123456789012:certificate/
a1b2c3d4-5678-90ab-cdef-11111EXAMPLE \
  --authentication-options Type=certificate-
authentication,MutualAuthentication={ClientRootCertificateChainArn=arn:aws:acm:ap-
south-1:123456789012:certificate/a1b2c3d4-5678-90ab-cdef-22222EXAMPLE} \
  --connection-log-options Enabled=false
```

Ejemplo de creación de un punto de conexión de doble pila:

```
aws ec2 create-client-vpn-endpoint \
```

```
  --endpoint-ip-address-type "dual-stack" \
  --traffic-ip-address-type "dual-stack" \
  --client-cidr-block "172.31.0.0/16" \
  --server-certificate-arn arn:aws:acm:ap-south-1:123456789012:certificate/
a1b2c3d4-5678-90ab-cdef-11111EXAMPLE \
  --authentication-options Type=certificate-
authentication,MutualAuthentication={ClientRootCertificateChainArn=arn:aws:acm:ap-
south-1:123456789012:certificate/a1b2c3d4-5678-90ab-cdef-22222EXAMPLE} \
  --connection-log-options Enabled=false
```

Visualización de puntos de enlace de AWS Client VPN

Puede consultar información sobre los puntos de conexión de Client VPN a través de la consola de Amazon VPC o la AWS CLI.

Para ver los puntos de conexión de Client VPN (consola)

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN Endpoints (Puntos de enlace de Client VPN).
3. Seleccione el punto de enlace de Client VPN que desea ver.
4. Use las pestañas Detalles, Asociaciones de red de destino, Grupos de seguridad, Reglas de autorización, Tabla de enrutamiento, Conexiones y Etiquetas para ver la información sobre los puntos de conexión de Client VPN existentes.

   También puede usar filtros para mejorar la búsqueda.

Para ver los puntos de conexión de Client VPN (AWS CLI)

Utilice el comando describe-client-vpn-endpoints.

Modificación de un punto de conexión de AWS Client VPN

Puede modificar un punto de conexión de Client VPN mediante la consola de Amazon VPC o la AWS CLI. Para obtener más información acerca de los campos que puede modificar de Client VPN, consulte the section called “Modificación de puntos de conexión”.

Limitaciones

Se aplican las siguientes limitaciones para modificar un punto de conexión:

- Las modificaciones de los puntos de conexión de Client VPN, incluidos los cambios en la lista de revocación de certificados (CRL), surtirán efecto hasta cuatro horas después de que el servicio Client VPN acepte una solicitud.
- No puede modificar el intervalo CIDR IPv4 del cliente, las opciones de autenticación, el certificado de cliente ni el protocolo de transporte después de crear el punto de conexión de Client VPN.
- Puede modificar los puntos de conexión IPv4 existentes para convertirlos a doble pila, tanto los tipos de IP de punto de conexión como de tráfico. Si solo necesita IPv6 para IP de punto de conexión e IP de tráfico, debe crear un nuevo punto de conexión.
- Client VPN no admite la modificación del tipo de punto de conexión (IPv4, IPv6, doble pila) ni del tipo de tráfico (IPv4, IPv6, doble pila) después de la creación.
- No se admite la modificación de una Client VPN con una combinación específica de tipo de punto de conexión y tipo de tráfico. No puede cambiar a ninguna otra combinación. El punto de conexión se debe eliminar y volver a crear con la configuración deseada.
- Los clientes IPv6 no admiten la comunicación de cliente a cliente.

Modificación de un punto de enlace de Client VPN.

Los puntos de conexión de Client VPN se pueden modificar a través de la consola o la AWS CLI.

Cómo modificar un punto de conexión de Client VPN mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN Endpoints (Puntos de enlace de Client VPN).
3. Seleccione el punto de conexión de Client VPN que desea modificar, elija Actions (Acciones) y haga clic en Modify Client VPN Endpoint (Modificar punto de conexión de Client VPN).
4. En Description (Descripción), escriba una breve descripción del punto de enlace de Client VPN.
5. En Tipo de dirección IP de punto de conexión, puede modificar un punto de conexión IPv4 existente para que sea de doble pila. Esta opción solo está disponible para puntos de conexión IPv4.
6. En Tipo de dirección IP de tráfico, puede modificar un punto de conexión IPv4 existente para que sea de doble pila. Esta opción solo está disponible para puntos de conexión IPv4.
7. En Server certificate ARN (ARN del certificado del servidor), especifique el ARN del certificado TLS que va a utilizar el servidor. Los clientes utilizan el certificado de servidor para autenticar el punto de enlace de Client VPN al que están conectados.

> **Note**
>
> El certificado de servidor debe estar presente en AWS Certificate Manager (ACM) en la región en la que está creando el punto de enlace de Client VPN. El certificado se puede aprovisionar con ACM o importarse a ACM.

8. Indique si desea registrar datos sobre las conexiones del cliente a través de Amazon CloudWatch Logs. En Enable log details on client connections (Habilitar los detalles de registro en las conexiones de cliente), realice una de las siguientes acciones:

   - Para activar el registro de la conexión del cliente, active Enable log details on client connections (Habilitar los detalles de registro en las conexiones de cliente). En CloudWatch Logs log group name (Nombre del grupo de registro de CloudWatch Logs), seleccione el nombre del grupo de registro que se va a utilizar. En CloudWatch Logs log stream name (Nombre de la secuencia de registro de CloudWatch), seleccione el nombre de la secuencia de registro que se va a utilizar o deje esta opción en blanco para permitirnos crear una secuencia de registro automáticamente.
   - Para desactivar el registro de la conexión del cliente, desactive Enable log details on client connections (Habilitar los detalles de registro en las conexiones de cliente).

9. En Client connect handler (Controlador de conexión de cliente), para activar el controlador de conexión de cliente, active Enable client connect handler (Habilitar controlador de conexión de cliente). En Client Connect Handler ARN (ARN del controlador de la conexión del cliente), especifique el nombre de recurso de Amazon (ARN) de la función Lambda que contiene la lógica que va a permitir o a denegar las conexiones.

10. Active o desactive Enable DNS servers (Habilitar servidores DNS). Para utilizar servidores DNS personalizados, en DNS Server 1 IP address (Dirección IP de servidor de DNS 1) yDNS Server 2 IP address (Dirección IP de servidor de DNS 2), especifique las direcciones IPv4 de los servidores DNS que se van a utilizar. Para los puntos de conexión IPv6 o de doble pila, también puede especificar las direcciones IPv6 1 de servidor de DNS e IPv6 2 de servidor de DNS. Para utilizar un servidor DNS de la VPC, en DNS Server 1 IP address (Dirección IP del servidor DNS 1) o DNS Server 2 IP address (Dirección IP del servidor DNS 2), especifique las direcciones IP y agregue la dirección IP del servidor DNS de la VPC.

> **Note**
>
> Asegúrese de que los clientes pueden acceder a los servidores DNS.

11. Active o desactive Enable split-tunnel (Habilitar túnel dividido). De forma predeterminada, el túnel dividido en un punto de conexión de VPN está desactivado.
12. En VPC ID (ID de VPC), elija la VPC que desea asociar con el punto de conexión de Client VPN. En Security Group IDs (ID de grupo de seguridad), elija uno o varios grupos de seguridad de la VPC para aplicarlos al punto de enlace de Client VPN.
13. En VPN port (Puerto de VPN), elija el número de puerto de VPN. El valor predeterminado es 443.
14. Si desea generar una URL del portal de autoservicio para los clientes, active Enable self-service portal (Habilitar portal de autoservicio).
15. En Session timeout hours (Horas de tiempo de espera de la sesión), elija el tiempo máximo de duración de la sesión VPN deseado en horas de las opciones disponibles o deje el valor predeterminado de 24 horas.
16. En Desconectarse al finalizar el tiempo de espera de la sesión, elija si desea finalizar la sesión cuando termine el tiempo máximo de sesión. La elección de esta opción requiere que los usuarios se vuelvan a conectar manualmente al punto de conexión al finalizar el tiempo de espera de la sesión; de lo contrario, Client VPN intentará volver a conectarse automáticamente.
17. Active o desactive Enable client login banner (Habilitar banner de inicio de sesión de cliente). Si desea usar el banner de inicio de sesión de cliente, ingrese el texto que se mostrará en un banner en los clientes proporcionados por AWS cuando se establezca una sesión VPN. Solo caracteres con codificación UTF-8. Máximo de 1400 caracteres.
18. Elija Modify Client VPN endpoint (Modificar punto de conexión de Client VPN).

Cómo modificar un punto de conexión de Client VPN mediante la AWS CLI

Utilice el comando modify-client-vpn-endpoint.

Ejemplo de modificación de un punto de conexión IPv4 para que sea de doble pila:

```
aws ec2 modify-client-vpn-endpoint \
  --client-vpn-endpoint-id cvpn-endpoint-123456789123abcde \
  --endpoint-ip-address-type "dual-stack" \
  --traffic-ip-address-type "dual-stack" \
```

```
  --client-cidr-block "172.31.0.0/16"
```

Eliminación de un punto de conexión de AWS Client VPN

Tendrá que desconectar todas las redes de destino para poder eliminar un punto de conexión de Client VPN. Cuando se elimina un punto de enlace de Client VPN, su estado cambia a `deleting` y los clientes ya no pueden conectarse a él.

Los puntos de enlace de Client VPN pueden eliminarse a través de la consola o la AWS CLI.

Para eliminar un punto de enlace de Client VPN (consola)

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN Endpoints (Puntos de enlace de Client VPN).
3. Seleccione el punto de conexión de Client VPN que desea eliminar. Elija Actions (Acciones), Delete Client VPN endpoint (Eliminar punto de conexión de Client VPN).
4. Ingrese delete en la ventana de confirmación y elija Delete (Eliminar).

Eliminación de un punto de enlace de Client VPN (AWS CLI)

Utilice el comando delete-client-vpn-endpoint.

registros de conexiones de AWS Client VPN

Puede habilitar el registro de conexión de un punto de enlace de Client VPN nuevo o existente y comenzar a capturar registros de conexión. Los registros de conexiones muestran la secuencia de los eventos de registro del punto de conexión de Client VPN. Cuando habilita el registro de conexión, puede especificar el nombre de una secuencia de registros en el grupo de registros. Si no especifica ninguna secuencia de registros, el servicio Client VPN creará una automáticamente. A continuación, el registro de conexiones registra la siguiente información: las solicitudes de conexión del cliente, los resultados de la conexión del cliente (correcta o no), los motivos por los que la conexión no se realiza correctamente y la hora de finalización del cliente desde el punto de conexión.

Antes de comenzar, debe tener un grupo de registro de CloudWatch Logs en su cuenta. Para obtener más información, consulte este artículo sobre el uso de grupos y secuencias de registros en la Guía del usuario de Amazon CloudWatch Logs. Se aplican cargos por usar los registros de CloudWatch Logs. Para más información, consulte Precios de Amazon CloudWatch.

Los registros de conexiones de Client VPN se pueden crear mediante la consola de Amazon VPC o la CLI de AWS.

Tareas

- Habilitar el registro de conexiones para un nuevo AWS Client VPN punto final
- Habilitar el registro de conexiones para un AWS Client VPN punto final existente
- Visualización de los registros de conexiones de AWS Client VPN
- Desactivación del registro de conexiones de AWS Client VPN

Habilitar el registro de conexiones para un nuevo AWS Client VPN punto final

Puede activar el registro de conexión al crear un nuevo punto de enlace de Client VPN a través de la consola o la línea de comandos.

Para habilitar el registro de conexión de un nuevo punto de enlace de Client VPN a través de la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN Endpoints (Puntos de conexión de Client VPN) y Create Client VPN endpoint (Crear punto de conexión de Client VPN).
3. Complete las opciones hasta que llegue a la sección Registro de conexión. Para obtener más información sobre las opciones, consulte Crear un AWS Client VPN punto final.
4. En Connection logging (Registro de conexiones), active Enable log details on client connections (Habilitar los detalles de registro en las conexiones de cliente).
5. En el nombre del grupo de CloudWatch registros, elija el nombre del grupo de CloudWatch registros.
6. (Opcional) Para el nombre del flujo de registro de CloudWatch registros, elija el nombre del flujo de registro de CloudWatch registros.
7. Elija Create Client VPN endpoint (Crear punto de conexión de Client VPN).

Para habilitar el registro de conexiones para un nuevo punto final Client VPN mediante AWS CLI

Utilice el create-client-vpn-endpointcomando y especifique el `--connection-log-options` parámetro. Puede especificar la información de los registros de conexión en formato JSON, como se muestra en el siguiente ejemplo.

```
{
    "Enabled": true,
    "CloudwatchLogGroup": "ClientVpnConnectionLogs",
    "CloudwatchLogStream": "NewYorkOfficeVPN"
}
```

Habilitar el registro de conexiones para un AWS Client VPN punto final existente

Puede habilitar el registro de conexión en un punto de enlace de Client VPN existente a través de la consola o la línea de comandos.

Para habilitar el registro de conexión en un punto de enlace de Client VPN existente a través de la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN Endpoints (Puntos de enlace de Client VPN).
3. Seleccione el punto de conexión de Client VPN, elija Actions (Acciones) y, a continuación, elija Modify Client VPN endpoint (Modificar el punto de conexión de Client VPN).
4. En Connection logging (Registro de conexiones), active Enable log details on client connections (Habilitar los detalles de registro en las conexiones de cliente).
5. En el nombre del grupo de CloudWatch registros, elija el nombre del grupo de CloudWatch registros.
6. (Opcional) Para el nombre del flujo de registro de CloudWatch registros, elija el nombre del flujo de registro de CloudWatch registros.
7. Elija Modify Client VPN endpoint (Modificar punto de conexión de Client VPN).

Para habilitar el registro de conexiones para un punto final Client VPN existente mediante el AWS CLI

Utilice el comando modify-client-vpn-endpoint y especifique el parámetro `--connection-log-options`. Puede especificar la información de los registros de conexión en formato JSON, como se muestra en el siguiente ejemplo.

```
{
    "Enabled": true,
    "CloudwatchLogGroup": "ClientVpnConnectionLogs",
    "CloudwatchLogStream": "NewYorkOfficeVPN"
}
```

Visualización de los registros de conexiones de AWS Client VPN

Puede ver los registros de conexiones de Client VPN mediante la consola de CloudWatch Logs.

Para ver los registros de conexión mediante la consola

1. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, elija Grupos de registros y seleccione el grupo de registros que contiene los registros de conexión.
3. Seleccione la secuencia de registros del punto de enlace de Client VPN.

> **Note**
>
> En la columna Timestamp (Marca temporal), se muestra la hora a la que el registro de conexión se publicó en CloudWatch Logs, no la hora de la conexión.

Para obtener más información sobre la búsqueda de datos de registro, consulte Búsqueda de datos de registro mediante patrones de filtro en la Guía del usuario de Amazon CloudWatch Logs.

Desactivación del registro de conexiones de AWS Client VPN

Puede desactivar los registros de conexiones de un punto de conexión de Client VPN a través de la consola o la línea de comandos. Cuando desactiva el registro de conexiones, no se eliminan los registros de CloudWatch Logs existentes.

Para desactivar el registro de conexiones mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN Endpoints (Puntos de enlace de Client VPN).
3. Seleccione el punto de conexión de Client VPN, elija Actions (Acciones) y, a continuación, elija Modify Client VPN endpoint (Modificar el punto de conexión de Client VPN).

4. En Connection logging (Registro de conexiones), desactive Enable log details on client connections (Habilitar los detalles de registro en las conexiones de cliente).
5. Elija Modify Client VPN endpoint (Modificar punto de conexión de Client VPN).

Para desactivar el registro de conexiones mediante la AWS CLI

Utilice el comando modify-client-vpn-endpoint y especifique el parámetro `--connection-log-options`. Asegúrese de que `Enabled` está establecido en `false`.

AWS Client VPN exportación de archivos de configuración de terminales

El archivo de configuración del AWS Client VPN punto final es el archivo que los clientes (usuarios) utilizan para establecer una conexión VPN con el punto final Client VPN. Debe descargar (exportar) este archivo y distribuirlo a todos los clientes que necesitan acceder a la VPN. Alternativamente, si ha habilitado el portal de autoservicio para el punto de conexión de Client VPN, los clientes también pueden iniciar sesión en el portal y descargar el archivo de configuración ellos mismos. Para obtener más información, consulte Acceso de AWS Client VPN al portal de la autoservicio.

Si el punto de enlace de Client VPN utiliza la autenticación mutua, debe agregar el certificado y la clave privada del cliente al archivo de configuración .ovpn que descargue. Después de agregar la información, los clientes pueden importar el archivo .ovpn al software de cliente OpenVPN.

> **Important**
>
> Si no agrega el certificado de cliente y la información de la clave privada del cliente al archivo, los clientes que utilicen la autenticación mutua no podrán conectarse al punto de enlace de Client VPN.

De forma predeterminada, la opción «remote-random-hostname» de la configuración del cliente de OpenVPN habilita el DNS comodín. Dado que el DNS comodín está habilitado, el cliente no almacena en caché la dirección IP del punto de enlace, por lo que no podrá hacer ping al nombre de DNS del punto de enlace.

Si el punto de enlace de Client VPN utiliza la autenticación de Active Directory y habilita la autenticación multifactor (MFA) en el directorio después de distribuir el archivo de configuración del

cliente, deberá descargar un archivo nuevo y volver a distribuirlo entre sus clientes. Los clientes no pueden usar el archivo de configuración anterior para conectarse al punto de enlace de Client VPN.

Tareas

- Exportar el archivo de configuración del AWS Client VPN cliente
- Agregue el certificado del AWS Client VPN cliente y la información clave para la autenticación mutua

Exportar el archivo de configuración del AWS Client VPN cliente

Puede exportar la configuración del cliente de Client VPN mediante la consola o la AWS CLI.

Para exportar la configuración del cliente (consola)

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN Endpoints (Puntos de enlace de Client VPN).
3. Seleccione el punto de enlace de Client VPN cuyo archivo de configuración desea descargar y elija Download Client Configuration (Descargar configuración del cliente).

Para exportar la configuración del cliente (AWS CLI)

Utilice el comando export-client-vpn-client-configuration y especifique el nombre del archivo de salida.

```
$ aws ec2 export-client-vpn-client-configuration --client-vpn-endpoint-id endpoint_id
 --output text>config_filename.ovpn
```

Agregue el certificado del AWS Client VPN cliente y la información clave para la autenticación mutua

Si el punto de enlace de Client VPN utiliza la autenticación mutua, debe agregar el certificado y la clave privada del cliente al archivo de configuración .ovpn que descargue.

No se puede modificar el certificado de cliente cuando utiliza la autenticación mutua.

Para agregar el certificado de cliente y la información de la clave (autenticación mutua)

Puede utilizar una de las siguientes opciones.

(Opción 1) Distribuya la clave y el certificado de cliente entre los clientes junto con el archivo de configuración del punto de enlace de Client VPN. En este caso, especifique la ruta de acceso al certificado y la clave en el archivo de configuración. Abra el archivo de configuración utilizando el editor que prefiera y agregue lo siguiente al final del archivo. */path/*Sustitúyala por la ubicación del certificado y la clave del cliente (la ubicación es relativa al cliente que se conecta al punto final).

```
cert /path/client1.domain.tld.crt
key /path/client1.domain.tld.key
```

(Opción 2) Añada el contenido del certificado de cliente entre las etiquetas `<cert></cert>` y el contenido de la clave privada entre las etiquetas `<key></key>` al archivo de configuración. Si elige esta opción, distribuirá únicamente el archivo de configuración entre sus clientes.

Si ha generado certificados y claves de cliente diferentes para cada uno de los usuarios que se van a conectar al punto de enlace de Client VPN, repita este paso con todos los usuarios.

A continuación, se muestra un ejemplo del formato de un archivo de configuración de Client VPN que incluye la clave y el certificado de cliente.

```
client
dev tun
proto udp
remote cvpn-endpoint-0011abcabcabcabc1.prod.clientvpn.eu-west-2.amazonaws.com 443
remote-random-hostname
resolv-retry infinite
nobind
remote-cert-tls server
cipher AES-256-GCM
verb 3

<ca>
Contents of CA
</ca>

<cert>
Contents of client certificate (.crt) file
</cert>

<key>
Contents of private key (.key) file
</key>
```

```
reneg-sec 0
```

AWS Client VPN rutas

Cada AWS Client VPN punto final tiene una tabla de rutas que describe las rutas de red de destino disponibles. Cada ruta de la tabla de ruteo determina la ubicación a la que se dirige el tráfico de red. Debe configurar reglas de autorización en cada ruta del punto de enlace de Client VPN para especificar qué clientes tienen acceso a la red de destino.

Cuando asocia una subred de una VPC con un punto de enlace de Client VPN, se agrega automáticamente una ruta de la VPC a la tabla de enrutamiento del punto de enlace de Client VPN. Para habilitar el acceso a redes adicionales, como las redes locales interconectadas VPCs, la red local (para permitir que los clientes se comuniquen entre sí) o Internet, debe agregar manualmente una ruta a la tabla de rutas del punto final Client VPN.

> **Note**
>
> Si va a asociar varias subredes al punto de enlace de Client VPN, debe asegurarse de crear una ruta para cada subred tal como se describe aquí: Solución de problemas AWS Client VPN: el acceso a una VPC interconectada, Amazon S3 o Internet es intermitente. Cada subred asociada debe tener un conjunto de rutas idéntico.

Consideraciones sobre el uso de túneles divididos en los puntos de conexión de Client VPN

Cuando se utiliza un túnel dividido en un punto de enlace de Client VPN, todas las rutas que están en las tablas de enrutamiento de Client VPN se agregan a la tabla de enrutamiento del cliente al establecer la VPN. Si agrega una ruta después de establecer la VPN, tendrá que restablecer la conexión para que la nueva ruta se envíe al cliente.

Es conveniente que tenga en cuenta el número de rutas que el dispositivo cliente puede controlar antes de modificar la tabla de enrutamiento del punto de enlace de Client VPN.

Tareas

- Creación de una ruta de punto de conexión de AWS Client VPN
- Visualización de rutas de punto de conexión de AWS Client VPN

- Eliminación de una ruta de punto de conexión de AWS Client VPN

Creación de una ruta de punto de conexión de AWS Client VPN

Al crear una ruta de punto de conexión de Client VPN, debe especificar cómo se debe dirigir el tráfico de la red de destino.

Para permitir que los clientes obtengan acceso a Internet, añada una ruta `0.0.0.0/0` de destino.

Puede agregar rutas a un punto de enlace de Client VPN a través de la consola y la AWS CLI.

Para crear la ruta de un punto de enlace de Client VPN (consola)

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN Endpoints (Puntos de enlace de Client VPN).
3. Seleccione el punto de conexión de Client VPN al que desee agregar la ruta y elija Route table (Table de enrutamiento) y Create Route (Crear ruta).
4. En Route destination (Destino de ruta), especifique el rango de CIDR de IPv4 para la red de destino. Por ejemplo:
   - Para agregar una ruta para la VPC del punto de conexión de Client VPN, ingrese el intervalo CIDR IPv4 de la VPC.
   - Para agregar una ruta para acceder a Internet, escriba `0.0.0.0/0`.
   - Para agregar una ruta para una VPC interconectada, escriba el rango de CIDR de IPv4 de la VPC interconectada.
   - Para agregar la ruta de una red en las instalaciones, ingrese el rango CIDR IPv4 de la conexión de AWS Site-to-Site VPN.
5. En Subnet ID for target network association (ID de subred para la asociación de red de destino), seleccione la subred que está asociada al punto de conexión de Client VPN.

   Si va a agregar una ruta para la red local del punto de conexión de Client VPN, también puede seleccionar `local`.
6. (Opcional) En Description (Descripción), ingrese una breve descripción de la ruta.
7. Elija Create route (Crear ruta).

Para crear una ruta de punto de enlace de Client VPN (AWS CLI)

Utilice el comando create-client-vpn-route.

Visualización de rutas de punto de conexión de AWS Client VPN

Puede ver las rutas de un punto de enlace de Client VPN específico a través de la consola o la AWS CLI.

Para ver las rutas de un punto de enlace de Client VPN (consola)

1. En el panel de navegación, elija Client VPN Endpoints (Puntos de enlace de Client VPN).
2. Seleccione el punto de conexión de Client VPN cuyas rutas desee ver y elija Route Table (Tabla de enrutamiento).

Para ver las rutas de un punto de enlace de Client VPN (AWS CLI)

Ejecute el comando describe-client-vpn-routes.

Eliminación de una ruta de punto de conexión de AWS Client VPN

Solo puede eliminar las rutas de Client VPN que haya agregado manualmente. No se pueden eliminar las rutas que se hayan agregado automáticamente al asociar una subred con el punto de enlace de Client VPN. Para eliminar las rutas que se han agregado automáticamente, debe desconectar la subred que inició la creación de estas rutas del punto de enlace de Client VPN.

Puede eliminar una ruta de un punto de enlace de Client VPN a través de la consola o la AWS CLI.

Para eliminar una ruta de punto de enlace de Client VPN (consola)

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN Endpoints (Puntos de enlace de Client VPN).
3. Seleccione el punto de conexión de Client VPN del que desea eliminar la ruta y elija Route table (Tabla de enrutamiento).
4. Seleccione la ruta que va a eliminar, elija Delete route (Eliminar ruta) y seleccione Delete route (Eliminar ruta).

Para eliminar la ruta de un punto de enlace de Client VPN (AWS CLI)

Utilice el comando delete-client-vpn-route.

Redes de destino de AWS Client VPN

Una red de destino es una subred en una VPC. Un punto de conexión de AWS Client VPN debe tener al menos una red de destino para permitir que los clientes se conecten a ella y establecer una conexión de VPN.

Para obtener más información sobre los tipos de acceso que puede configurar (por ejemplo, permitir que los clientes accedan a Internet), consulte Escenarios y ejemplos para Client VPN.

Requisitos de la red de destino de Client VPN

Cuando se crea una red de destino, se aplican las reglas siguientes:

- La subred debe tener un bloque de CIDR con al menos una máscara de bits de /27, por ejemplo 10.0.0.0/27. La subred debe tener también al menos 20 direcciones IP disponibles en todo momento.
- El bloque de CIDR de la subred no se puede solapar con el intervalo CIDR del cliente del punto de enlace de Client VPN.
- Si asocia varias subredes con un punto de enlace de Client VPN, cada subred tendrá que estar en una zona de disponibilidad diferente. Le recomendamos que asocie al menos dos subredes para proporcionar redundancia a la zona de disponibilidad.
- Si al crear el punto de enlace de Client VPN especificó una subred, dicha subred tendrá que estar en la misma VPC. Si aún no ha asociado ninguna VPC con el punto de enlace de Client VPN, puede elegir cualquier subred de cualquier VPC.

  Todas las asociaciones de subred adicionales tienen que ser de la misma VPC. Para asociar una subred de una VPC diferente, primero tiene que modificar el punto de enlace de Client VPN y cambiar la VPC que tiene asociada. Para obtener más información, consulte Modificación de un punto de conexión de AWS Client VPN.

Al asociar una subred con un punto de enlace de Client VPN, la ruta local de la VPC en la que está aprovisionada la subred asociada se agrega automáticamente a la tabla de enrutamiento del punto de enlace de Client VPN.

> **Note**
>
> Una vez asociadas las redes de destino, cuando agregue o quite CIDR adicionales a la VPC conectada, debe realizar una de las siguientes operaciones para actualizar la ruta local para la tabla de enrutamiento del punto de enlace de Client VPN:
>
> - Desasocie el punto de enlace de Client VPN de la red de destino y, a continuación, asocie el punto de enlace de Client VPN a la red de destino.
> - Agregar manualmente o eliminar la ruta de la tabla de enrutamiento del punto de enlace de Client VPN.

Después de asociar la primera subred con el punto de enlace de Client VPN, el estado del punto de enlace de Client VPN cambia de `pending-associate` a `available` y los clientes pueden establecer una conexión de VPN.

Tareas

- Asociar una red de destino a un AWS Client VPN punto final
- Aplicar un grupo de seguridad a una red de destino en AWS Client VPN
- Visualización de redes de destino de AWS Client VPN
- Desasociar una red de destino de un punto final AWS Client VPN

Asociar una red de destino a un AWS Client VPN punto final

Puede asociar una o más redes de destino (subredes) a un punto final Client VPN mediante la consola de Amazon VPC o la AWS CLI. Antes de asociar una red de destino con un punto de conexión de Client VPN, familiarícese con los requisitos. Consulte Requisitos para crear una red de destino.

Para asociar una red de destino a un punto de enlace de Client VPN (consola)

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN Endpoints (Puntos de enlace de Client VPN).
3. Seleccione el punto de conexión de Client VPN con el que desee asociar la red de destino, elija Target network associations (Asociaciones de red de destino) y, a continuación, elija Associate target network (Asociar red de destino).

4. En VPC, elija la VPC en la que se encuentra la subred. Si al crear el punto de enlace de Client VPN especificó una VPC o si tiene asociaciones de subredes anteriores, debe ser la misma VPC.
5. En Choose a subnet to associate (Elija una subred para asociar), elija la subred que desee asociar con el punto de conexión de Client VPN.
6. Elija Associate target network (Asociar red de destino).

Asociación una red de destino con un punto de enlace de Client VPN (AWS CLI)

Utilice el comando associate-client-vpn-target-network.

Aplicar un grupo de seguridad a una red de destino en AWS Client VPN

Cuando cree un punto de enlace de Client VPN, puede especificar los grupos de seguridad que se aplicarán a la red de destino. Al asociar la primera red de destino con un punto de enlace de Client VPN, se aplica automáticamente el grupo de seguridad predeterminado de la VPC en la que se encuentra la subred asociada. Para obtener más información, consulte Grupos de seguridad.

Puede cambiar los grupos de seguridad del punto de enlace de Client VPN. Las reglas de los grupos de seguridad que necesite también pueden depender del tipo de acceso de VPN que desee configurar. Para obtener más información, consulte Escenarios y ejemplos para Client VPN.

Para aplicar un grupo de seguridad a una red de destino (consola)

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN Endpoints (Puntos de enlace de Client VPN).
3. Seleccione el punto de enlace de Client VPN al que se aplican los grupos de seguridad.
4. Elija Security Groups (Grupos de seguridad) y, luego, elija Apply Security Groups (Aplicar grupos de seguridad).
5. Seleccione los grupos de seguridad adecuados en Grupo de seguridad IDs.
6. Elija Apply Security Groups (Aplicar grupos de seguridad).

Para aplicar un grupo de seguridad a una red de destino (AWS CLI)

Utilice el client-vpn-target-network comando apply-security-groups-to-.

Visualización de redes de destino de AWS Client VPN

Puede ver los destinos asociados con un determinado punto de enlace de Client VPN a través de la consola o la AWS CLI.

Para ver las redes de destino (consola)

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN Endpoints (Puntos de enlace de Client VPN).
3. Seleccione el punto de conexión de Client VPN adecuado y elija Target network associations (Asociaciones de la red de destino).

Para ver las redes de destino mediante la AWS CLI

Utilice el comando describe-client-vpn-target-networks.

Desasociar una red de destino de un punto final AWS Client VPN

Cuando desasocie una red de destino, se eliminará cualquier ruta que se haya agregado manualmente a la tabla de enrutamiento del punto de conexión de la VPN de cliente, así como la ruta que se creó automáticamente cuando se realizó la asociación de la red de destino (la ruta local de la VPC). Si desconecta todas las redes de destino de un punto de enlace de Client VPN, los clientes ya no podrán establecer una conexión de VPN.

Para desconectar una red de destino de un punto de enlace de Client VPN (consola)

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN Endpoints (Puntos de enlace de Client VPN).
3. Seleccione el punto de conexión de Client VPN al que está asociada la red de destino y elija Target network associations (Asociaciones de red de destino).
4. Seleccione la red de destino que desea desasociar, elija Disassociate (Desasociar) y, a continuación, elija Disassociate target network (Desasociar red de destino).

Desconectar una red de destino de un punto de enlace de Client VPN (AWS CLI)

Utilice el comando disassociate-client-vpn-target-network.

AWS Client VPN tiempo de espera máximo de la sesión de VPN

AWS Client VPN proporciona varias opciones para la duración máxima de la sesión de VPN, que es el tiempo máximo permitido para la conexión de un cliente al punto final de Client VPN. Puede configurar una sesión VPN de duración máxima menor para ayudar a cumplir con los requisitos de seguridad y conformidad. De forma predeterminada, la duración máxima de la sesión VPN es de 24 horas. Una vez que haya establecido la duración máxima de la sesión, podrá controlar lo que ocurrirá con esa sesión al finalizar el tiempo de espera. La opción de desconexión al finalizar el tiempo de espera de la sesión le permite terminar la sesión o intentar volver a conectarse automáticamente al punto de conexión. La finalización de una sesión le permite tener más control sobre la seguridad de los puntos de conexión aplicando la duración máxima de la sesión de VPN. Si una sesión está configurada para finalizar al llegar al límite de tiempo, los usuarios deberán volver a conectarse y proporcionar sus credenciales de autenticación para restablecer la conexión de VPN.

Cuando la desconexión al finalizar el tiempo de espera de la sesión esté configurada para volver a conectarse automáticamente y se agote el tiempo máximo de la sesión,

- se establecerá automáticamente una nueva sesión en el caso de las credenciales de usuario almacenadas en caché (Active Directory) o de la autenticación basada en certificados (autenticación mutua). Para desconectarse por completo y no volver a conectarse automáticamente, estos usuarios se deben desconectar manualmente.
- no se establecerá automáticamente una nueva sesión en el caso de la autenticación federada (SAML). Estos usuarios deben volver a autenticarse una vez transcurrido el tiempo de espera de la sesión para restablecer la conexión de VPN.

> **Note**
>
> - Cuando el valor máximo de duración de la sesión de VPN disminuye con respecto a su valor actual, se desconecta cualquier sesión de VPN activa que esté conectada al punto de conexión durante un periodo de tiempo superior a la duración recién establecida.
> - Al cambiar la opción de desconexión al finalizar el tiempo de espera de la sesión, se aplicará la nueva configuración a todas las sesiones abiertas actualmente.

Configure la sesión VPN máxima durante la creación de un AWS Client VPN punto final

La duración de una sesión de VPN se configura durante la creación de un punto de conexión de Client VPN. Consulte Crear un AWS Client VPN punto final para los pasos, para crear un punto de conexión de Client VPN y establecer la duración máxima de la sesión.

Tareas

- Ver la duración máxima AWS Client VPN actual de la sesión de VPN
- Modificar la duración máxima de la AWS Client VPN sesión y el comportamiento del tiempo de espera

Ver la duración máxima AWS Client VPN actual de la sesión de VPN

Siga estos pasos para ver la duración de la sesión de VPN máxima de Client VPN actual.

Visualización de la duración máxima de la sesión de VPN para un punto de conexión de Client VPN (consola)

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN Endpoints (Puntos de enlace de Client VPN).
3. Seleccione el punto de conexión de Client VPN que desea ver.
4. Verifique que la pestaña Details (Detalles) esté seleccionada.
5. Consulte la duración máxima de la sesión de VPN actual junto a Horas de tiempo de espera de la sesión y si está habilitada o deshabilitada la opción Desconectarse al finalizar el tiempo de espera.

Visualización de la duración máxima de la sesión de VPN para un punto de conexión de Client VPN (AWS CLI)

Utilice el comando describe-client-vpn-endpoints.

Modificar la duración máxima de la AWS Client VPN sesión y el comportamiento del tiempo de espera

Siga estos pasos para modificar la duración máxima de una sesión de VPN existente de Client VPN y cambiar el comportamiento de desconexión al finalizar el tiempo de espera de la sesión.

Modificar la duración máxima de una sesión VPN existente para un punto de conexión de Client VPN (consola)

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN endpoints (Puntos de conexión de Client VPN).
3. Seleccione el punto de conexión de Client VPN que desee modificar, elija Actions (Acciones) y, a continuación, elija Modify Client VPN Endpoint (Modificar punto de conexión de Client VPN).
4. Para el Session timeout hours (Tiempo de espera de la sesión), elija el tiempo máximo de duración de la sesión VPN deseado en horas.
5. En Desconectarse al finalizar el tiempo de espera de la sesión, elija si desea desconectar una sesión cuando termine el tiempo máximo de sesión. De forma predeterminada, este ajuste está desactivado la primera vez que se modifica un punto de conexión.
6. Elija Modify Client VPN endpoint (Modificar punto de conexión de Client VPN).

Modificar la duración máxima de una sesión VPN existente para un punto de conexión de Client VPN (AWS CLI)

Utilice el comando modify-client-vpn-endpoint.

Integración de Transit Gateway con Client VPN

Puede conectar un punto final Client VPN de forma nativa a una Transit Gateway para un acceso remoto seguro a varias VPCs redes locales y otros recursos conectados a la Transit Gateway. Esto elimina la necesidad de crear puntos de conexión VPN independientes para cada VPC o gestionar el enrutamiento complejo a través de un intermedio. VPCs

Temas

- Descripción general de
- Ventajas

Descripción general de

Al asociar un Transit Gateway a un punto final Client VPN, los clientes VPN conectados pueden acceder a todos los recursos conectados al Transit Gateway si se configuran las rutas y reglas de autorización adecuadas en el punto final Client VPN.

Los puntos finales asociados a Transit Gateway conservan la dirección IP de origen del cliente. No se aplica la traducción de direcciones de red de origen (SNAT), lo que proporciona una mayor visibilidad del tráfico de clientes.

> **Important**
>
> No se pueden mezclar asociaciones de subredes de VPC y asociaciones de Transit Gateway en un único punto final Client VPN. Elija un tipo de asociación al crear el punto final.

Ventajas

La integración de Transit Gateway con Client VPN ofrece las siguientes ventajas:

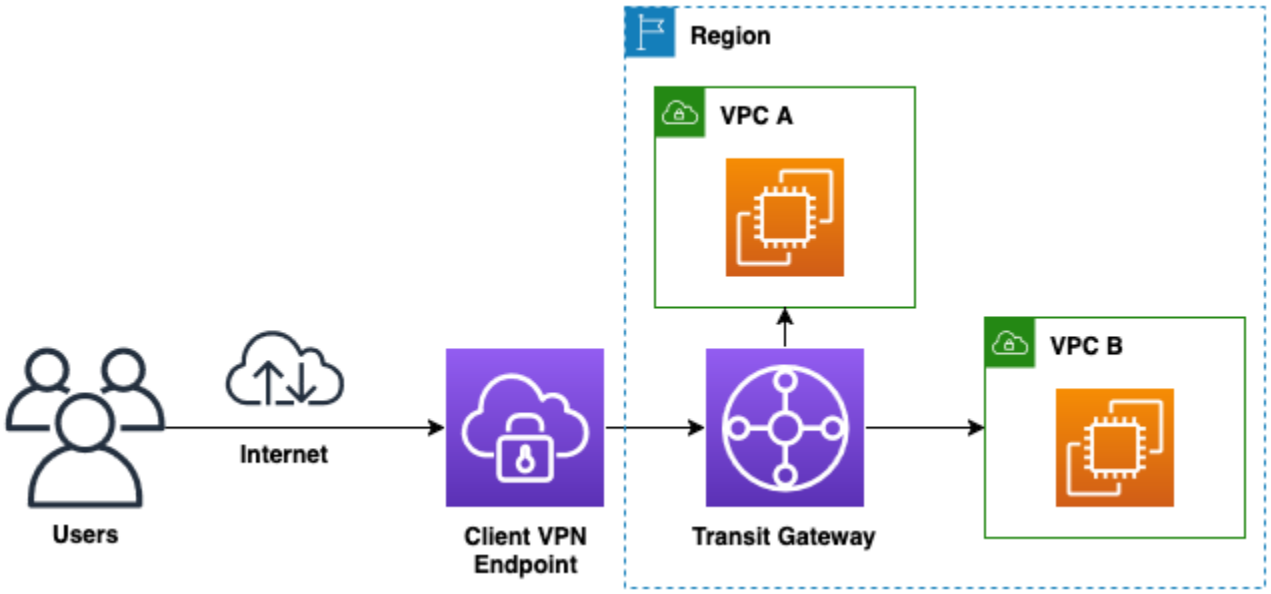
- Administración simplificada: elimine la necesidad de puntos finales de VPN separados por VPC. No es necesario crear un intermedio VPCs únicamente para la terminación de la VPN.
- Enrutamiento centralizado: aproveche Transit Gateway como centro de enrutamiento central. Simplifique la administración de rutas en toda su red.
- Visibilidad mejorada: conserve las direcciones IP de origen del cliente (sin SNAT). Proporciona compatibilidad con registros de flujo para Client VPN.

- Escalabilidad: añada fácilmente nuevos elementos VPCs a su Transit Gateway, a los que puede acceder a través de Client VPN. Amplíe para dar soporte a grandes fuerzas de trabajo y unidades de negocio remotas.
- Seguridad centralizada: implemente políticas de seguridad coherentes en todas las redes conectadas. Mantenga registros de auditoría completos.

Cómo funciona la integración de Transit Gateway

A continuación se describe cómo funciona Client VPN con Transit Gateway:

1. Creación del punto final: se crea un punto final de Client VPN y se especifica el ID de Transit Gateway.
2. Creación de adjuntos: crea AWS automáticamente un adjunto del tipo Transit Gateway `client-vpn` para el punto final.
3. Selección de zona de disponibilidad: usted especifica qué zonas de disponibilidad desea utilizar o AWS selecciona 2 zonas de disponibilidad automáticamente.
4. Configuración de rutas: agrega rutas a la tabla de rutas de puntos finales de Client VPN para dirigir el tráfico de los clientes a las redes de destino a través de Transit Gateway.
5. Flujo de conexión del cliente: cuando un cliente se conecta, el tráfico fluye desde el cliente a través del punto final de Client VPN hasta la Transit Gateway y, después, hasta la red de destino según las tablas de rutas de Transit Gateway.



Requisitos previos

Antes de crear un punto final Client VPN asociado a Transit Gateway, compruebe los siguientes requisitos.

Requisitos de Transit Gateway

- Una Transit Gateway existente en la misma región que el punto final Client VPN.
- Para el acceso entre cuentas, la Transit Gateway debe compartirse con su cuenta a través AWS Resource Access Manager de.
- La Transit Gateway debe tener asignado un bloque IPv4 CIDR. Si planea usar IPv6 una configuración de doble pila, asigne también un bloque IPv6 CIDR.

Requisitos de red

- El rango CIDR del cliente no debe superponerse con los rangos CIDR VPCs conectados a Transit Gateway.
- Las zonas de disponibilidad que seleccione deben ser compatibles con Transit Gateway.
- Las rutas de retorno deben configurarse en las tablas de enrutamiento de la VPC para dirigir el tráfico destinado al rango CIDR del cliente a Transit Gateway.

Requisitos del certificado

- Un certificado de servidor aprovisionado en AWS Certificate Manager (ACM) en la misma región que el punto final Client VPN.
- Si utiliza la autenticación mutua, un certificado de cliente aprovisionado en ACM.

Cree un terminal VPN Client de Transit Gateway

Puede crear un punto final Client VPN asociado a una Transit Gateway mediante la consola o el AWS CLI.

Para crear un punto final VPN Client de Transit Gateway (consola)

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN Endpoints (Puntos de enlace de Client VPN) y Create Client VPN Endpoint (Crear punto de enlace de Client VPN).
3. (Opcional) En Etiqueta de nombre y Descripción, introduzca un nombre y una descripción para el punto de conexión.

4. Para el tipo de dirección IP de tráfico, elija una de las siguientes opciones:
   - IPv4— Especifique un rango de IPv4 CIDR del cliente (por ejemplo,`10.0.0.0/22`).
   - IPv6— asigna AWS automáticamente el rango IPv6 CIDR del cliente.
   - Pila doble: especifique un rango de IPv4 CIDR del cliente. AWS asigna automáticamente el rango IPv6 CIDR del cliente.
5. Para el ARN del certificado de servidor, especifique el ARN del certificado TLS aprovisionado en ACM.
6. Elija un método de autenticación. Para obtener más información, consulte Autenticación de cliente en AWS Client VPN.
7. (Opcional) Para el registro de conexiones, active Habilitar los detalles del registro en las conexiones de los clientes y especifique el grupo de registros y el flujo de CloudWatch registros.
8. Para Infraestructura de red, elija Transit Gateway.
9. Para el ID de Transit Gateway, selecciona Transit Gateway en la lista desplegable.
10. (Opcional) Para las zonas de disponibilidad, selecciona hasta 5 zonas de disponibilidad. Si no selecciona zonas de disponibilidad, selecciona 2 AWS automáticamente.
11. (Opcional) Configure ajustes adicionales, como los servidores DNS, el protocolo de transporte, el túnel dividido, el puerto VPN, el tiempo de espera de la sesión y el banner de inicio de sesión.
12. Elija Create Client VPN endpoint (Crear punto de conexión de Client VPN).

> **Note**
>
> Tras la creación, el estado del punto final es. `pending-associate` El adjunto de Transit Gateway se crea automáticamente. Los clientes pueden conectarse una vez que el archivo adjunto esté disponible.

Para crear un punto de conexión VPN Client de Transit Gateway (AWS CLI)

Utilice el comando create-client-vpn-endpoint con el parámetro `--transit-gateway-id`.

El siguiente ejemplo crea un punto final Client VPN con zonas de disponibilidad específicas:

```
aws ec2 create-client-vpn-endpoint \
    --client-cidr-block 10.0.0.0/22 \
```

```
    --server-certificate-arn arn:aws:acm:us-east-1:123456789012:certificate/
a1b2c3d4-5678-90ab-cdef-11111EXAMPLE \
    --authentication-options Type=certificate-
authentication,MutualAuthentication={ClientRootCertificateChainArn=arn:aws:acm:us-
east-1:123456789012:certificate/a1b2c3d4-5678-90ab-cdef-22222EXAMPLE} \
    --connection-log-options Enabled=false \
    --transit-gateway-id tgw-0a1b2c3d4e5f6EXAMPLE \
    --availability-zone-list us-east-1a us-east-1b us-east-1c
```

Ejemplo de código de salida:

```
{
    "ClientVpnEndpointId": "cvpn-endpoint-0a1b2c3d4e5f6EXAMPLE",
    "Status": {
        "Code": "pending-associate"
    },
    "DnsName": "cvpn-endpoint-0a1b2c3d4e5f6EXAMPLE.prod.clientvpn.us-
east-1.amazonaws.com"
}
```

Para permitir la selección AWS automática de 2 zonas de disponibilidad, omita el `--availability-zone-list` parámetro:

```
aws ec2 create-client-vpn-endpoint \
    --client-cidr-block 10.0.0.0/22 \
    --server-certificate-arn arn:aws:acm:us-east-1:123456789012:certificate/
a1b2c3d4-5678-90ab-cdef-11111EXAMPLE \
    --authentication-options Type=certificate-
authentication,MutualAuthentication={ClientRootCertificateChainArn=arn:aws:acm:us-
east-1:123456789012:certificate/a1b2c3d4-5678-90ab-cdef-22222EXAMPLE} \
    --connection-log-options Enabled=false \
    --transit-gateway-id tgw-0a1b2c3d4e5f6EXAMPLE
```

Verifique el archivo adjunto de Transit Gateway

Tras crear el punto final, compruebe que se haya creado el adjunto de Transit Gateway.

Para verificar el adjunto de Transit Gateway (consola)

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Transit Gateways Attachments (Conexiones de gateway de tránsito).

3. Localice el archivo adjunto con el tipo de recurso = `client-vpn` y el ID de recurso que coincidan con su ID de punto final de Client VPN.
4. Compruebe que el estado es`available`.

Para verificar el archivo adjunto de Transit Gateway (AWS CLI)

Utilice el comando describe-transit-gateway-attachments.

```
aws ec2 describe-transit-gateway-attachments \
    --filters Name=transit-gateway-id,Values=tgw-0a1b2c3d4e5f6EXAMPLE Name=resource-
type,Values=client-vpn
```

Para ver la configuración de Transit Gateway para el punto final, utilice el describe-client-vpn-endpointscomando:

```
aws ec2 describe-client-vpn-endpoints \
    --client-vpn-endpoint-ids cvpn-endpoint-0a1b2c3d4e5f6EXAMPLE
```

La salida incluye un `TransitGatewayConfiguration` objeto con el ID de Transit Gateway y las zonas de disponibilidad asociadas.

Administre las rutas

> **Important**
>
> En el caso de los puntos finales asociados a Transit Gateway, no se especifica un ID de subred de destino al crear rutas. El tráfico se dirige automáticamente a través del adjunto Transit Gateway.

Para agregar una ruta (consola)

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN Endpoints (Puntos de enlace de Client VPN).
3. Seleccione el punto final Client VPN, elija la tabla de rutas y, a continuación, elija Crear ruta.
4. En Destino de ruta, introduzca el rango CIDR de destino (por ejemplo, `10.1.0.0/16` para una VPC `0.0.0.0/0` o para todo el tráfico).
5. (Opcional) En Descripción, introduzca una descripción para la ruta.

6. Elija Create route (Crear ruta).

Para añadir una ruta (AWS CLI)

Utilice el create-client-vpn-routecomando sin el `--target-vpc-subnet-id` parámetro.

```
aws ec2 create-client-vpn-route \
    --client-vpn-endpoint-id cvpn-endpoint-0a1b2c3d4e5f6EXAMPLE \
    --destination-cidr-block 10.1.0.0/16
```

Para añadir varias rutas, ejecute el comando para cada rango CIDR de destino:

```
# Route to VPC 1
aws ec2 create-client-vpn-route \
    --client-vpn-endpoint-id cvpn-endpoint-0a1b2c3d4e5f6EXAMPLE \
    --destination-cidr-block 10.1.0.0/16

# Route to VPC 2
aws ec2 create-client-vpn-route \
    --client-vpn-endpoint-id cvpn-endpoint-0a1b2c3d4e5f6EXAMPLE \
    --destination-cidr-block 10.2.0.0/16

# Route to on-premises network
aws ec2 create-client-vpn-route \
    --client-vpn-endpoint-id cvpn-endpoint-0a1b2c3d4e5f6EXAMPLE \
    --destination-cidr-block 192.168.0.0/16
```

Para eliminar una ruta (consola)

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN Endpoints (Puntos de enlace de Client VPN).
3. Seleccione el punto final Client VPN, elija la tabla de rutas, seleccione la ruta y, a continuación, elija Eliminar ruta.
4. Elija Eliminar ruta para confirmar.

Para eliminar una ruta (AWS CLI)

Utilice el comando delete-client-vpn-route.

```
aws ec2 delete-client-vpn-route \
```

```
    --client-vpn-endpoint-id cvpn-endpoint-0a1b2c3d4e5f6EXAMPLE \
    --destination-cidr-block 10.1.0.0/16
```

Configuración de la autorización

> **Important**
>
> La autorización basada en grupos de seguridad no es compatible con los puntos finales Client VPN asociados a Transit Gateway. Debe usar reglas de autorización basadas en la red para controlar el acceso de los clientes.

Para añadir una regla de autorización (consola)

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Client VPN Endpoints (Puntos de enlace de Client VPN).
3. Seleccione el punto final Client VPN, elija Reglas de autorización y, a continuación, elija Agregar regla de autorización.
4. Para que la red de destino permita el acceso, introduzca el rango CIDR de destino (por ejemplo,`10.1.0.0/16`).
5. En Otorgar acceso a, elija una de las siguientes opciones:
   - Permitir el acceso a todos los usuarios: todos los clientes autenticados pueden acceder a la red de destino.
   - Permitir el acceso a los usuarios de un grupo de acceso específico: introduzca el SID del grupo de Active Directory o el nombre del grupo de IdP en el ID del grupo de acceso.
6. Seleccione Add authorization rule (Añadir regla de autorización).

Para agregar una regla de autorización ()AWS CLI

Utilice el comando authorize-client-vpn-ingress.

El siguiente ejemplo autoriza a todos los usuarios a acceder a la `10.1.0.0/16` red:

```
aws ec2 authorize-client-vpn-ingress \
    --client-vpn-endpoint-id cvpn-endpoint-0a1b2c3d4e5f6EXAMPLE \
    --target-network-cidr 10.1.0.0/16 \
```

```
    --authorize-all-groups
```

El siguiente ejemplo autoriza un grupo específico de Active Directory:

```
aws ec2 authorize-client-vpn-ingress \
    --client-vpn-endpoint-id cvpn-endpoint-0a1b2c3d4e5f6EXAMPLE \
    --target-network-cidr 10.1.0.0/16 \
    --access-group-id S-1-2-34-1234567890-1234567890-1234567890-1234
```

Administre las zonas de disponibilidad

Puede modificar las zonas de disponibilidad de un punto final Client VPN asociado a Transit Gateway tras su creación.

Para añadir una única zona de disponibilidad ()AWS CLI

Utilice el comando associate-client-vpn-target-network con el `--availability-zone` parámetro.

```
aws ec2 associate-client-vpn-target-network \
    --client-vpn-endpoint-id cvpn-endpoint-0a1b2c3d4e5f6EXAMPLE \
    --availability-zone us-east-1c
```

Para eliminar una única zona de disponibilidad ()AWS CLI

En primer lugar, utilice el comando describe-client-vpn-target-networks para buscar el ID de asociación de la zona de disponibilidad.

```
aws ec2 describe-client-vpn-target-networks \
    --client-vpn-endpoint-id cvpn-endpoint-0a1b2c3d4e5f6EXAMPLE
```

A continuación, utilice el comando disassociate-client-vpn-target-network con el ID de asociación.

```
aws ec2 disassociate-client-vpn-target-network \
    --client-vpn-endpoint-id cvpn-endpoint-0a1b2c3d4e5f6EXAMPLE \
    --association-id cvpn-assoc-0a1b2c3d4e5f6EXAMPLE
```

Acceso multicuenta a Transit Gateway

Puede crear un punto final Client VPN asociado a una Transit Gateway que sea propiedad de una AWS cuenta diferente. Para ello, el propietario de la Transit Gateway debe compartir la Transit Gateway con tu cuenta a través de AWS Resource Access Manager.

Requisitos previos

- Cuenta de propietario de Transit Gateway: una Transit Gateway existente y permisos para crear recursos compartidos en ella AWS Resource Access Manager.
- Cuenta de punto final Client VPN: permisos para crear puntos finales Client VPN y aceptar AWS Resource Access Manager recursos compartidos.

En la cuenta de punto final de Client VPN, acepte el recurso compartido en la AWS Resource Access Manager consola o mediante el accept-resource-share-invitationcomando. Tras aceptar el uso compartido, la Transit Gateway aparece en el menú desplegable Transit Gateway ID al crear un punto de conexión Client VPN.

Consideraciones y limitaciones

Tenga en cuenta lo siguiente cuando utilice la integración de Transit Gateway con Client VPN:

- Restricciones de asociación
  - No se pueden mezclar asociaciones de subredes de VPC y asociaciones de Transit Gateway en un único punto final.
  - Cada punto final debe usar exclusivamente un tipo de asociación.
- Grupos de seguridad
  - Los puntos finales de Transit Gateway no admiten la autorización basada en grupos de seguridad.
  - Utilice únicamente reglas de autorización basadas en la red.
- Administración de rutas
  - No se admite la propagación automática de rutas desde Transit Gateway.
  - Debe definir manualmente las rutas para las redes de destino.
- Superposición de CIDR
  - El bloque CIDR de VPN de cliente no debe superponerse con otros archivos adjuntos de Transit Gateway o bloques CIDR de Transit Gateway.
  - Transit Gateway no admite la superposición de rangos de CIDR entre los dispositivos conectados VPCs.
- Limitación regional
  - El punto final Client VPN y Transit Gateway deben estar en la misma AWS región.
  - Client VPN no admite el emparejamiento entre regiones de Transit Gateway.

- Zonas de disponibilidad
  - Puede especificar hasta 5 zonas de disponibilidad por punto final.
  - Si no se especifica, asigna AWS automáticamente 2 zonas de disponibilidad.
  - Client VPN y Transit Gateway deben admitir todas las zonas de disponibilidad especificadas.
- Enrutamiento de retorno
  - VPCs los conectados a la Transit Gateway deben tener las rutas de retorno configuradas para enrutar el tráfico destinado al CIDR de la VPN del cliente de vuelta a la Transit Gateway.
  - Sin el enrutamiento de retorno adecuado, los clientes VPN no pueden acceder a los recursos del VPCs.
    - Para IPv4: El CIDR de Client VPN se conoce en el momento de la creación del punto final.
    - Para IPv6: Debe describir la tabla de rutas de Transit Gateway para determinar el rango de IPv6 CIDR asignado al punto final de la VPN del cliente (el rango de CIDR más grande de la tabla de enrutamiento de Transit Gateway asociada al punto final de la VPN del cliente), ya que los rangos de CIDR del IPv6 cliente los asigna automáticamente. AWS Client VPN
- Registros de conexión y flujo
  - Los registros de flujo de Transit Gateway se pueden habilitar para capturar información sobre el tráfico IP que entra y sale de sus Transit Gateways. Los registros de conexión de Client VPN se pueden habilitar para capturar información sobre los eventos de conexión de Client VPN.
  - Puede correlacionar un evento de registro de flujo de Transit Gateway con una conexión de Client VPN comparando una IP de cliente y una marca de tiempo en un evento de registro de flujo de Transit Gateway con la misma IP de cliente y período de tiempo en los registros de conexión de Client VPN.
- Conectividad a Internet
  - Para acceder a Internet a través de Client VPN con Transit Gateway, sin túnel dividido, una VPC conectada debe tener NAT configurada.
    - Para IPv4: Configure una puerta de enlace NAT para reemplazar el cliente Client IPs VPN por una dirección IP pública.
    - Para IPv6: Consulte Tráfico saliente de Internet centralizado con IPv6.

Seguridad en AWS Client VPN

La seguridad en AWS es la principal prioridad. Como cliente de AWS, se beneficiará de una arquitectura de red y de centros de datos diseñados para satisfacer los requisitos de seguridad de las organizaciones más exigentes.

La seguridad es una responsabilidad compartida entre AWS y usted. El modelo de responsabilidad compartida aborda tanto la seguridad de la nube como la seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta los servicios de AWS en la nube de AWS. AWS también proporciona servicios que puede utilizar de forma segura. Los auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los Programas de conformidad de AWS . Para obtener información sobre los programas de conformidad que se aplican a AWS Client VPN, consulte AWS Services in Scope by Compliance Program.
- Seguridad en la nube: su responsabilidad viene determinada por el servicio de AWS que utilice. También eres responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y la normativa aplicables.

AWS Client VPN forma parte del servicio Amazon VPC. Para obtener más información sobre la seguridad en Amazon VPC, consulte Seguridad en la Guía del usuario de Amazon VPC.

Esta documentación le ayuda a comprender cómo puede aplicar el modelo de responsabilidad compartida al utilizar Client VPN. En los siguientes temas, aprenderá a configurar Client VPN para satisfacer sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros servicios de AWS que le ayudarán a monitorear y proteger los recursos de Client VPN.

Temas

Protección de datos en AWS Client VPN

El modelo de se aplica a la protección de datos en AWS Client VPN. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global en la que se ejecutan todos los Nube de AWS. Eres responsable de mantener el control sobre el contenido alojado en esta infraestructura. También eres responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulte las Preguntas frecuentes sobre privacidad de datos y los . Para obtener más información sobre la protección de datos en Europa, consulte el Centro del Reglamento General de Protección de Datos (RGPD).

Para fines de protección de datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure usuarios individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utiliza la autenticación multifactor (MFA) en cada cuenta.
- Se utiliza SSL/TLS para comunicarse con AWS los recursos. Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con AWS CloudTrail. Para obtener información sobre el uso de CloudTrail senderos para capturar AWS actividades, consulte Cómo trabajar con CloudTrail senderos en la Guía del AWS CloudTrail usuario.
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utiliza servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger la información confidencial almacenada en Amazon S3.
- Si necesita módulos criptográficos validados por FIPS 140-3 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulte Estándar de procesamiento de la información federal (FIPS) 140-3.

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabaja con Client VPN u otro tipo de servicio Servicios de AWS mediante la consola, la API o AWS los SDK. AWS CLI Cualquier dato que introduzca

en etiquetas o campos de formato libre utilizados para los nombres se pueden emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya información de credenciales en la URL a fin de validar la solicitud para ese servidor.

Cifrado en tránsito

AWS Client VPN proporciona conexiones seguras desde cualquier ubicación mediante Transport Layer Security (TLS) 1.2 o una versión posterior.

Privacidad del tráfico entre redes

Activación del acceso entre redes

Puede permitir que los clientes se conecten a la VPC y a otras redes a través de un punto de enlace de Client VPN. Para obtener más información y ejemplos, consulte Escenarios y ejemplos para Client VPN.

Restringir el acceso a las redes

Puede configurar el punto de enlace de Client VPN para restringir el acceso a recursos específicos de la VPC. En la autenticación basada en usuarios, también puede restringir el acceso a partes de la red en función del grupo de usuarios que accede al punto de enlace de Client VPN. Para obtener más información, consulte Restricción del acceso a su red mediante Client VPN.

Autenticación de clientes

La autenticación es lo primero que se implementa en la nube de AWS . Se utiliza para determinar si los clientes tienen permiso para conectarse al punto de enlace de Client VPN. Si la autenticación se realiza correctamente, los clientes se conectan al punto de enlace de Client VPN y establecen una sesión de VPN. Si la autenticación falla, se deniega la conexión y el cliente no podrá establecer una sesión de VPN.

Client VPN permite utilizar los siguientes tipos de autenticación de cliente:

- Autenticación con Active Directory (basada en el usuario)
- Autenticación mutua (basada en certificados)
- Inicio de sesión único (autenticación SAML-based federada) (basado en el usuario)

Administración de identidad y acceso para AWS Client VPN

AWS Identity and Access Management (IAM) es una herramienta Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a AWS los recursos. Los administradores de IAM controlan quién puede estar autenticado (ha iniciado sesión) y autorizado (tiene permisos) para utilizar recursos de Client VPN. La IAM es una Servicio de AWS herramienta que puede utilizar sin coste adicional.

Temas

Público

La forma de usar AWS Identity and Access Management (IAM) varía según la función que desempeñes:

- Usuario del servicio: solicite permisos al administrador si no puede acceder a las características (consulte Solución de problemas de AWS Client VPN identidad y acceso).
- Administrador del servicio: determine el acceso de los usuarios y envíe las solicitudes de permiso (consulte ¿Cómo AWS Client VPN funciona con IAM).
- Administrador de IAM: escribe las políticas para administrar el acceso (consulte Ejemplos de políticas basadas en la identidad para AWS Client VPN).

Autenticación con identidades

La autenticación es la forma en que inicias sesión AWS con tus credenciales de identidad. Debe autenticarse como usuario de Usuario raíz de la cuenta de AWS IAM o asumir una función de IAM.

Puede iniciar sesión como una identidad federada con las credenciales de una fuente de identidad, como AWS IAM Identity Center (IAM Identity Center), la autenticación de inicio de sesión único o las credenciales. Google/Facebook Para obtener más información sobre el inicio de sesión, consulte Cómo iniciar sesión en la Cuenta de AWS en la Guía del usuario de AWS Sign-In .

Para el acceso programático, AWS proporciona un SDK y una CLI para firmar criptográficamente las solicitudes. Para obtener más información, consulte AWS Signature Version 4 para solicitudes de API en la Guía del usuario de IAM.

Cuenta de AWS usuario root

Al crear un Cuenta de AWS, se comienza con una identidad de inicio de sesión denominada usuario Cuenta de AWS raíz que tiene acceso completo a todos Servicios de AWS los recursos. Se recomiendaencarecidamente que no utilice el usuario raíz para las tareas diarias. Para ver las tareas que requieren credenciales de usuario raíz, consulte Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Identidad federada

Como práctica recomendada, exija a los usuarios humanos que utilicen la federación con un proveedor de identidades para acceder Servicios de AWS mediante credenciales temporales.

Una identidad federada es un usuario del directorio empresarial, del proveedor de identidades web o al Directory Service que se accede Servicios de AWS mediante credenciales de una fuente de identidad. Las identidades federadas asumen roles que proporcionan credenciales temporales.

Para una administración de acceso centralizada, se recomienda AWS IAM Identity Center. Para obtener más información, consulte ¿Qué es el Centro de identidades de IAM? en la Guía del usuario de AWS IAM Identity Center .

Usuarios y grupos de IAM

Un usuario de IAM es una identidad con permisos específicos para una sola persona o aplicación. Recomendamos el uso de credenciales temporales en lugar de usuarios de IAM con credenciales de larga duración. Para obtener más información, consulte Exigir a los usuarios humanos que utilicen la federación con un proveedor de identidad para acceder AWS mediante credenciales temporales en la Guía del usuario de IAM.

Un grupo de IAM especifica un conjunto de usuarios de IAM y facilita la administración de los permisos para grupos grandes de usuarios. Para obtener más información, consulte Casos de uso para usuarios de IAM en la Guía del usuario de IAM.

Roles de IAM

Un Rol de IAM es una identidad con permisos específicos que proporciona credenciales temporales. Puede asumir un rol cambiando de un rol de usuario a uno de IAM (consola) o llamando a una AWS CLI operación de AWS API. Para obtener más información, consulte Métodos para asumir un rol en la Guía del usuario de IAM.

Los roles de IAM son útiles para el acceso de usuario federado, los permisos de usuario de IAM temporales, el acceso entre cuentas, el acceso entre servicios y las aplicaciones que se ejecutan en Amazon EC2. Para obtener más información, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Administración del acceso con políticas

AWS Para controlar el acceso, puede crear políticas y adjuntarlas a AWS identidades o recursos. Una política define los permisos cuando están asociados a una identidad o un recurso. AWS evalúa estas políticas cuando un director hace una solicitud. La mayoría de las políticas se almacenan AWS como documentos JSON. Para obtener más información sobre los documentos de políticas de JSON, consulte Información general de políticas de JSON en la Guía del usuario de IAM.

Mediante las políticas, los administradores especifican quién tiene acceso a qué, definiendo qué entidad principal puede realizar acciones sobre qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Un administrador de IAM crea políticas de IAM y las agrega a roles, que los usuarios pueden asumir posteriormente. Las políticas de IAM definen permisos independientemente del método que se utilice para realizar la operación.

Políticas basadas en identidades

Las políticas basadas en identidad son documentos de política de permisos JSON que asocia a una identidad (usuario, grupo o rol). Estas políticas controlan qué acciones pueden realizar las identidades, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en la identidad, consulte Definición de permisos de IAM personalizados con políticas administradas por el cliente en la Guía del usuario de IAM.

Las políticas basadas en identidad pueden ser políticas insertadas (incrustadas directamente en una sola identidad) o políticas administradas (políticas independientes asociadas a varias identidades). Para obtener información sobre cómo elegir entre políticas administradas e insertadas, consulte Selección entre políticas administradas y políticas insertadas en la Guía del usuario de IAM.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de políticas JSON que se asocian a un recurso. Los ejemplos incluyen las Políticas de confianza de roles de IAM y las Políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Debe especificar una entidad principal en una política basada en recursos.

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No puedes usar políticas AWS gestionadas de IAM en una política basada en recursos.

Otros tipos de políticas

AWS admite tipos de políticas adicionales que pueden establecer los permisos máximos que conceden los tipos de políticas más comunes:

- Límites de permisos: establecen los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM. Para obtener más información, consulte Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.
- Políticas de control de servicios (SCPs): especifican los permisos máximos para una organización o unidad organizativa en AWS Organizations. Para obtener más información, consulte Políticas de control de servicios en la Guía del usuario de AWS Organizations .
- Políticas de control de recursos (RCPs): establece los permisos máximos disponibles para los recursos de tus cuentas. Para obtener más información, consulte Políticas de control de recursos (RCPs) en la Guía del AWS Organizations usuario.
- Políticas de sesión: políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal para un rol o un usuario federado. Para obtener más información, consulte Políticas de sesión en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo se AWS determina si se debe permitir una solicitud cuando se trata de varios tipos de políticas, consulte la lógica de evaluación de políticas en la Guía del usuario de IAM.

¿Cómo AWS Client VPN funciona con IAM

Antes de utilizar IAM para administrar el acceso a Client VPN, conozca qué características de IAM se pueden utilizar con Client VPN.

Funciones de IAM que puede utilizar con AWS Client VPN

Característica de IAM	Compatibilidad con Client VPN
Políticas basadas en identidades	Sí
Políticas basadas en recursos	No
Acciones de políticas	Sí
Recursos de políticas	Sí
Claves de condición de política (específicas del servicio)	Sí
ACLs	No
ABAC (etiquetas en políticas)	Sí
Credenciales temporales	Sí
Permisos de entidades principales	Sí
Roles de servicio	Sí
Roles vinculados al servicio	Sí

Políticas basadas en identidades para Client VPN

Compatibilidad con las políticas basadas en identidad: sí

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en la identidad,

consulte Definición de permisos de IAM personalizados con políticas administradas por el cliente en la Guía del usuario de IAM.

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. Para obtener más información sobre los elementos que puede utilizar en una política de JSON, consulte Referencia de los elementos de la política de JSON de IAM en la Guía del usuario de IAM.

Ejemplos de políticas basadas en identidades para Client VPN

Para ver ejemplos de políticas basadas en identidad de Client VPN, consulte Ejemplos de políticas basadas en la identidad para AWS Client VPN.

Políticas basadas en recursos dentro de Client VPN

Admite políticas basadas en recursos: no

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Los ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política basada en recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Para habilitar el acceso entre cuentas, puede especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política en función de recursos. Para obtener más información, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Acciones de políticas para Client VPN

Compatibilidad con las acciones de políticas: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Para ver una lista de las acciones de Client VPN, consulte Acciones definidas por AWS Client VPN en la Referencia de autorización del servicio.

Las acciones de políticas en Client VPN utilizan el siguiente prefijo antes de la acción:

```
ec2
```

Para especificar varias acciones en una única instrucción, sepárelas con comas.

```
"Action": [
      "ec2:action1",
      "ec2:action2"
         ]
```

Para ver ejemplos de políticas basadas en identidad de Client VPN, consulte Ejemplos de políticas basadas en la identidad para AWS Client VPN.

Recursos de políticas para Client VPN

Compatibilidad con los recursos de políticas: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). En el caso de las acciones que no admiten permisos por recurso, utilice un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

```
"Resource": "*"
```

Para ver una lista de los tipos de recursos de Client VPN y sus tipos ARNs, consulte Recursos definidos por AWS Client VPN en la Referencia de autorización del servicio. Para saber con qué acciones puede especificar el ARN de cada recurso, consulte Acciones definidas por AWS Client VPN.

Para ver ejemplos de políticas basadas en identidad de Client VPN, consulte Ejemplos de políticas basadas en la identidad para AWS Client VPN.

Claves de condición de política para Client VPN

Compatibilidad con claves de condición de políticas específicas del servicio: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` especifica cuándo se ejecutan las instrucciones en función de criterios definidos. Puede crear expresiones condicionales que utilizan operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud. Para ver todas las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del usuario de IAM.

Para ver una lista de las claves de condición de Client VPN, consulte Claves de condición de AWS Client VPN en la Referencia de autorización del servicio. Para saber con qué acciones y recursos puede usar una clave de condición, consulte Acciones definidas por AWS Client VPN.

Para ver ejemplos de políticas basadas en identidad de Client VPN, consulte Ejemplos de políticas basadas en la identidad para AWS Client VPN.

ACLs en Client VPN

Soporta ACLs: No

Las listas de control de acceso (ACLs) controlan qué directores (miembros de la cuenta, usuarios o roles) tienen permisos para acceder a un recurso. ACLs son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

ABAC con Client VPN

Admite ABAC (etiquetas en las políticas): sí

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos en función de atributos denominados etiquetas. Puede adjuntar etiquetas a las entidades y AWS los recursos de IAM y, a continuación, diseñar políticas de ABAC para permitir las operaciones cuando la etiqueta del director coincida con la etiqueta del recurso.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información sobre ABAC, consulte Definición de permisos con la autorización de ABAC en la Guía del usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulte Uso del control de acceso basado en atributos (ABAC) en la Guía del usuario de IAM.

Uso de credenciales temporales con Client VPN

Compatibilidad con credenciales temporales: sí

Las credenciales temporales proporcionan acceso a AWS los recursos a corto plazo y se crean automáticamente cuando se utiliza la federación o se cambia de rol. AWS recomienda generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para obtener más información, consulte Credenciales de seguridad temporales en IAM y Servicios de AWS que funcionan con IAM en la Guía del usuario de IAM.

Permisos de entidades principales entre servicios para Client VPN

Admite sesiones de acceso directo (FAS): sí

Las sesiones de acceso directo (FAS) utilizan los permisos del principal que llama y los que solicitan Servicio de AWS para realizar solicitudes a los servicios descendentes. Servicio de AWS Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Sesiones de acceso directo.

Roles de servicio para Client VPN

Compatible con roles de servicio: sí

Un rol de servicio es un rol de IAM que asume un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Crear un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

Uso de roles vinculados a servicios en Client VPN

Compatible con roles vinculados al servicio: sí

Un rol vinculado a un servicio es un tipo de rol de servicio que está vinculado a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio

aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

Ejemplos de políticas basadas en la identidad para AWS Client VPN

De forma predeterminada, los usuarios y roles no tienen permiso para crear, ver ni modificar recursos de Client VPN. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan.

Para obtener información acerca de cómo crear una política basada en identidades de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte Creación de políticas de IAM (consola) en la Guía del usuario de IAM.

Para obtener más información sobre las acciones y los tipos de recursos definidos por Client VPN, incluido el ARNs formato de cada uno de los tipos de recursos, consulte Acciones, recursos y claves de condición de AWS Client VPN en la Referencia de autorización del servicio.

Temas

Prácticas recomendadas sobre las políticas

Las políticas basadas en identidades determinan si alguien puede crear, acceder o eliminar los recursos de Client VPN de la cuenta. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su. Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Con el fin de obtener más información, consulte las políticas administradas por AWS o las políticas administradas por AWS para funciones de tarea en la Guía de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos

como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulte Políticas y permisos en IAM en la Guía del usuario de IAM.

- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo CloudFormation. Para obtener más información, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utiliza el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte Validación de políticas con el Analizador de acceso de IAM en la Guía del usuario de IAM.
- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para exigir la MFA cuando se invoquen las operaciones de la API, añada condiciones de MFA a sus políticas. Para más información, consulte Acceso seguro a la API con MFA en la Guía del usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.

Cómo permitir a los usuarios consultar sus propios permisos

En este ejemplo, se muestra cómo podría crear una política que permita a los usuarios de IAM ver las políticas administradas e insertadas que se asocian a la identidad de sus usuarios. Esta política incluye permisos para completar esta acción en la consola o mediante programación mediante la API o. AWS CLI AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
```

```
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Solución de problemas de AWS Client VPN identidad y acceso

Utilice la siguiente información para diagnosticar y solucionar los problemas comunes que puedan surgir cuando trabaje con Client VPN e IAM.

Temas

- No tengo autorización para realizar una acción en Client VPN
- No estoy autorizado a realizar tareas como: PassRole
- Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis recursos de Client VPN

No tengo autorización para realizar una acción en Client VPN

Si recibe un error que indica que no tiene autorización para realizar una acción, las políticas se deben actualizar para permitirle realizar la acción.

En el siguiente ejemplo, el error se produce cuando el usuario de IAM `mateojackson` intenta utilizar la consola para consultar los detalles acerca de un recurso ficticio *`my-example-widget`*, pero no tiene los permisos ficticios `ec2:`*`GetWidget`*.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 ec2:GetWidget on resource: my-example-widget
```

En este caso, la política del usuario `mateojackson` debe actualizarse para permitir el acceso al recurso *`my-example-widget`* mediante la acción `ec2:`*`GetWidget`*.

Si necesita ayuda, póngase en contacto con su AWS administrador. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

No estoy autorizado a realizar tareas como: PassRole

Si recibe un error que indica que no tiene autorización para realizar la acción `iam:PassRole`, las políticas deberán actualizarse a fin de permitirle pasar un rol a Client VPN.

Algunas Servicios de AWS permiten transferir una función existente a ese servicio en lugar de crear una nueva función de servicio o una función vinculada a un servicio. Para ello, debe tener permisos para transferir la función al servicio.

En el siguiente ejemplo, el error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para realizar una acción en Client VPN. Sin embargo, la acción requiere que el servicio cuente con permisos que otorguen un rol de servicio. Mary no tiene permisos para transferir el rol al servicio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

En este caso, las políticas de Mary se deben actualizar para permitirle realizar la acción `iam:PassRole`.

Si necesita ayuda, póngase en contacto con su AWS administrador. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis recursos de Client VPN

Se puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Se puede especificar una persona de confianza para

que asuma el rol. En el caso de los servicios que admiten políticas basadas en recursos o listas de control de acceso (ACLs), puedes usar esas políticas para permitir que las personas accedan a tus recursos.

Para obtener más información, consulte lo siguiente:

- Para obtener información acerca de si Client VPN admite estas características, consulte ¿Cómo AWS Client VPN funciona con IAM.
- Para obtener información sobre cómo proporcionar acceso a los recursos de su Cuentas de AWS propiedad, consulte Proporcionar acceso a un usuario de IAM en otro de su propiedad en la Cuenta de AWS Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta Cómo proporcionar acceso a recursos que Cuentas de AWS son propiedad de terceros en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante una federación de identidades, consulte Proporcionar acceso a usuarios autenticados externamente (identidad federada) en la Guía del usuario de IAM.
- Para conocer sobre la diferencia entre las políticas basadas en roles y en recursos para el acceso entre cuentas, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Uso de roles vinculados a servicios para AWS Client VPN

AWS Client VPN utiliza roles vinculados al AWS Identity and Access Management servicio (IAM). Un rol vinculado a un servicio es un tipo único de rol de IAM que está vinculado directamente a Client VPN. Client VPN predefine las funciones vinculadas al servicio e incluyen todos los permisos que el servicio requiere para llamar a otros AWS servicios en su nombre.

Temas

- Uso de roles para AWS Client VPN
- Uso de roles para la autorización de conexiones en Client VPN;

Uso de roles para AWS Client VPN

AWS Client VPN utiliza funciones AWS Identity and Access Management vinculadas al servicio (IAM). Un rol vinculado a un servicio es un tipo único de rol de IAM que está vinculado directamente

a Client VPN. Client VPN predefine las funciones vinculadas al servicio e incluyen todos los permisos que el servicio requiere para llamar a otros AWS servicios en su nombre.

Un rol vinculado a un servicio simplifica la configuración de Client VPN porque ya no tendrá que agregar manualmente los permisos necesarios. Client VPN define los permisos de sus roles vinculados a servicios y, a menos que esté definido de otra manera, solo Client VPN puede asumir sus roles. Los permisos definidos incluyen las políticas de confianza y de permisos, y que la política de permisos no se pueda adjuntar a ninguna otra entidad de IAM.

Solo es posible eliminar un rol vinculado a un servicio después de eliminar sus recursos relacionados. De esta forma, se protegen los recursos de Client VPN, ya que se evita que se puedan eliminar accidentalmente permisos de acceso a los recursos.

Permisos de roles vinculados a servicios en Client VPN

Client VPN usa el rol vinculado al servicio denominado AWSServiceRoleForClientVPN: permite que Client VPN cree y administre recursos relacionados con sus conexiones VPN.

El rol vinculado al servicio de AWSServiceRoleForClientVPN confía en que el siguiente servicio asuma el rol:

- `clientvpn.amazonaws.com`

Esta función vinculada al servicio utiliza la política gestionada Client. VPNService RolePolicy Para ver los permisos de esta política, consulte Cliente VPNService RolePolicy en la Referencia de políticas AWS administradas.

Creación de roles vinculados a servicios en Client VPN

No necesita crear manualmente un rol vinculado a servicios. Cuando crea el primer punto de conexión Client VPN en su cuenta con la Consola de administración de AWS AWS CLI, la o la AWS API, Client VPN crea el rol vinculado al servicio por usted.

Si elimina este rol vinculado a servicios y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Cuando se crea el primer punto de conexión de Client VPN en la cuenta, Client VPN crea el rol vinculado a servicios para usted de nuevo.

Edición de roles vinculados a servicios en Client VPN

Client VPN no le permite editar el rol vinculado al servicio de AWSService RoleForClient VPN. Después de crear un rol vinculado al servicio, no podrá cambiar el nombre del rol, ya que varias

entidades podrían hacer referencia al rol. Sin embargo, sí puede editar la descripción del rol con IAM. Para obtener más información, consulte la Descripción sobre cómo editar un rol vinculado al servicio en la Guía del usuario de IAM.

Eliminación de roles vinculados a servicios en Client VPN

Si ya no necesita usar Client VPN, le recomendamos que elimine el rol vinculado al servicio de AWSServiceRoleForClientVPN.

Primero debe eliminar los recursos de Client VPN relacionados. Esto garantiza que no pueda eliminar accidentalmente el permiso para obtener acceso a los recursos.

Utilice la consola de IAM, la CLI de IAM o la API de IAM para eliminar los roles vinculados a servicios. Para obtener más información, consulte Eliminación de un rol vinculado a servicios en la Guía del usuario de IAM.

Uso de roles para la autorización de conexiones en Client VPN;

AWS Client VPN usa roles vinculados al AWS Identity and Access Management servicio (IAM). Un rol vinculado a un servicio es un tipo único de rol de IAM que está vinculado directamente a Client VPN. Client VPN predefine las funciones vinculadas al servicio e incluyen todos los permisos que el servicio requiere para llamar a otros AWS servicios en su nombre.

Un rol vinculado a un servicio simplifica la configuración de Client VPN porque ya no tendrá que agregar manualmente los permisos necesarios. Client VPN define los permisos de sus roles vinculados a servicios y, a menos que esté definido de otra manera, solo Client VPN puede asumir sus roles. Los permisos definidos incluyen las políticas de confianza y de permisos, y que la política de permisos no se pueda adjuntar a ninguna otra entidad de IAM.

Solo es posible eliminar un rol vinculado a un servicio después de eliminar sus recursos relacionados. De esta forma, se protegen los recursos de Client VPN, ya que se evita que se puedan eliminar accidentalmente permisos de acceso a los recursos.

Permisos de roles vinculados a servicios en Client VPN

Client VPN usa el rol vinculado al servicio denominado AWSServiceRoleForClientVPNConnectionsRol vinculado al servicio para las conexiones de Client VPN.

El rol AWSService RoleForClient VPNConnections vinculado al servicio confía en los siguientes servicios para asumir el rol:

- `clientvpn-connections.amazonaws.com`

La política de permisos de roles denominada Client VPNService ConnectionsRolePolicy permite a Client VPN realizar las siguientes acciones en los recursos especificados:

- Acción: `lambda:InvokeFunction` en `arn:aws:lambda:*:*:function:AWSClientVPN-*`

Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

Creación de roles vinculados a servicios en Client VPN

No necesita crear manualmente un rol vinculado a servicios. Cuando crea el primer punto de conexión Client VPN en su cuenta con la Consola de administración de AWS AWS CLI, la o la AWS API, Client VPN crea el rol vinculado al servicio por usted.

Si elimina este rol vinculado a servicios y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Cuando se crea el primer punto de conexión de Client VPN en la cuenta, Client VPN crea el rol vinculado a servicios para usted de nuevo.

Edición de roles vinculados a servicios en Client VPN

Client VPN no le permite editar el rol AWSService RoleForClient VPNConnections vinculado al servicio. Después de crear un rol vinculado al servicio, no podrá cambiar el nombre del rol, ya que varias entidades podrían hacer referencia al rol. Sin embargo, sí puede editar la descripción del rol con IAM. Para obtener más información, consulte la Descripción sobre cómo editar un rol vinculado al servicio en la Guía del usuario de IAM.

Eliminación de roles vinculados a servicios en Client VPN

Si ya no necesita usar Client VPN, le recomendamos que elimine el rol AWSServiceRoleForClientVPNConnectionsvinculado al servicio.

Primero debe eliminar los recursos de Client VPN relacionados. Esto garantiza que no pueda eliminar accidentalmente el permiso para obtener acceso a los recursos.

Utilice la consola de IAM, la CLI de IAM o la API de IAM para eliminar los roles vinculados a servicios. Para obtener más información, consulte Eliminación de un rol vinculado a servicios en la Guía del usuario de IAM.

Resiliencia en AWS Client VPN

La infraestructura global de AWS se compone de regiones y zonas de disponibilidad de AWS. AWS Las regiones proporcionan varias zonas de disponibilidad físicamente independientes y aisladas que se encuentran conectadas mediante redes con un alto nivel de rendimiento y redundancia, además de baja latencia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre las zonas sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de centros de datos únicos o múltiples.

Para obtener más información sobre las regiones y zonas de disponibilidad de AWS, consulte Infraestructura global de AWS.

Además de la infraestructura global de AWS, AWS Client VPN ofrece características que lo ayudan en sus necesidades de resiliencia y copia de seguridad de los datos.

Varias redes de destino para disfrutar de una alta disponibilidad

Puede asociar una red de destino con un punto de enlace de Client VPN para permitir que los clientes establezcan sesiones de VPN. Las redes de destino son subredes de la VPC. Cada una de las subredes que asocie con el punto de enlace de Client VPN debe pertenecer a una zona de disponibilidad diferente. Puede asociar varias subredes con un punto de enlace de Client VPN para disfrutar de una alta disponibilidad.

Seguridad de la infraestructura en AWS Client VPN

Como servicio gestionado,AWS Client VPN está protegido por la seguridad de la red AWS global. Para obtener información sobre los servicios AWS de seguridad y cómo se AWS protege la infraestructura, consulte Seguridad AWS en la nube. Para diseñar su AWS entorno utilizando las mejores prácticas de seguridad de la infraestructura, consulte Protección de infraestructuras en un marco de buena AWS arquitectura basado en el pilar de la seguridad.

Utiliza las llamadas a la API AWS publicadas para acceder a Client VPN a través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Conjuntos de cifrado con confidencialidad directa total (PFS) como DHE (Ephemeral Diffie-Hellman) o ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Prácticas recomendadas de seguridad para AWS Client VPN

AWS Client VPN proporciona un número de características de seguridad que debe tener en cuenta a la hora de desarrollar e implementar sus propias políticas de seguridad. Las siguientes prácticas recomendadas son directrices generales y no constituyen una solución de seguridad completa. Puesto que es posible que estas prácticas recomendadas no sean adecuadas o suficientes para el entorno, considérelas como consideraciones útiles en lugar de como normas.

Reglas de autorización

Utilice reglas de autorización para restringir los usuarios que pueden acceder a la red. Para obtener más información, consulte Reglas de autorización.

Grupos de seguridad

Utilice grupos de seguridad para controlar a qué recursos de la VPC pueden acceder los usuarios. Para obtener más información, consulte Grupos de seguridad.

Listas de revocación de certificados del cliente

Puede utilizar listas de revocación de certificados de cliente para revocar el acceso a un punto de enlace de Client VPN en certificados de cliente específicos. Por ejemplo, cuando un usuario abandona la organización. Para obtener más información, consulte Listas de revocación de certificados del cliente.

Desconexión cuando se agota el tiempo de espera de la sesión

Desconecte una sesión cuando se alcance el tiempo máximo de sesión de Client VPN para imponer una duración máxima de sesión de VPN. Para obtener más información, consulte Duración máxima de la sesión de VPN.

Herramientas de supervisión

Utilice herramientas de supervisión para realizar un seguimiento de la disponibilidad y el rendimiento de los puntos de enlace de Client VPN. Para obtener más información, consulte Monitoreo de Client VPN.

Identity and Access Management

Administre el acceso a los recursos y las API de Client VPN utilizando políticas de IAM con los usuarios y roles de IAM. Para obtener más información, consulte Administración de identidad y acceso para AWS Client VPN.

Consideraciones sobre IPv6 para AWS Client VPN

Client VPN admite ahora conectividad IPv6 nativa junto con las capacidades de IPv4 existentes. Puede crear puntos de conexión de solo IPv6, solo IPv4 o doble pila (IPv4 e IPv6) para cumplir los requisitos de red.

Componentes principales de la compatibilidad con IPv6

Hay dos parámetros de configuración clave cuando se trabaja con IPv6 en Client VPN:

Tipo de dirección IP de punto de conexión

: Este parámetro define el tipo de IP de administración de puntos de conexión, que determina el tipo de instancia de EC2 aprovisionada para el punto de conexión. Este tipo de IP se utiliza para administrar el tráfico de túnel de VPN externo (el tráfico cifrado que fluye entre el cliente y el servidor de OpenVPN a través de la Internet pública).

Tipo de dirección IP de tráfico

: Este parámetro define el tipo de tráfico que fluye a través del túnel de VPN. Este tipo de IP se usa para administrar el tráfico cifrado interno (la carga útil real), los intervalos de CIDR de los clientes, la asociación de subredes, las rutas y las reglas por punto de conexión.

Asignación de CIDR de clientes IPv6

No es necesario especificar un bloque de CIDR para el CIDR de clientes IPv6. Amazon asigna automáticamente intervalos de CIDR para clientes IPv6. Esta asignación automática habilita no-SNATing para tráfico de túnel IPv6, lo que proporciona mayor visibilidad de la dirección IPv6 del usuario conectado.

Requisitos de compatibilidad

Los puntos de conexión IPv6 y doble pila dependen de los dispositivos de usuario y de los proveedores de servicios de Internet (ISP):

- Los dispositivos de usuario que ejecutan el cliente de CVPN deben admitir la configuración de IP requerida, como se muestra en la tabla de compatibilidad que aparece a continuación.
- Los ISP deben admitir la configuración de IP requerida para que la conexión funcione correctamente.

- Para el tráfico de IPv6 o de doble pila, las subredes de VPC asociadas deben tener intervalos de CIDR de IPv6 o de doble pila.

Compatibilidad con DNS

Se admiten DNS en todos los tipos de puntos de conexión: IPv4, IPv6 y doble pila. Para los puntos de conexión IPv6, puede configurar los servidores de DNS IPv6 mediante el parámetro `--dns-server-ipv6`. Los registros de DNS AAAA son compatibles tanto en el servicio como en el cliente.

Limitaciones

A continuación, se indican las limitaciones con IPv6:

- Los clientes IPv6 no admiten la comunicación de cliente a cliente (C2C). Si un cliente IPv6 intenta comunicarse con otro cliente IPv6, se interrumpirá el tráfico.

Client Routes Enforcement para IPv6

Client VPN admite ahora Client Route Enforcement para tráfico de IPv6. Esta característica ayuda a garantizar que el tráfico de red IPv6 de los clientes conectados siga las rutas definidas por el administrador y no se envíe inadvertidamente fuera del túnel de VPN.

Aspectos clave de la compatibilidad con la aplicación de rutas de clientes IPv6:

- La marca `ClientRouteEnforcementOptions.enforced` existente habilita CRE para pilas de IPv4 e IPv6.
- IPv6 Client Route Enforcement excluye ciertos intervalos de IPv6 para mantener funcionalidades críticas de IPv6:
  - `::1/128`: reservado para bucles invertidos
  - `fe80::/10`: reservado para direcciones locales de enlace
  - `ff00::/8`: reservado para multidifusión
- IPv6 Client Route Enforcement está disponible en AWS VPN Client versión 5.3.0 y superior en Windows, macOS y Ubuntu.

Para obtener más información sobre CRE, incluido cómo configurarlo y habilitarlo, consulte the section called “Client Route Enforcement”.

Prevención de fugas de IPv6 (información antigua)

En el caso de las configuraciones antiguas que no utilizan compatibilidad nativa con IPv6, es posible que deba evitar la fuga de IPv6. Una fuga de IPv6 puede ocurrir cuando IPv4 e IPv6 están habilitados y conectados a la VPN, pero la VPN no enruta el tráfico de IPv6 a su túnel. En este caso, cuando se conecta a un destino habilitado para IPv6, todavía se está conectando con su dirección IPv6 proporcionada por su ISP. Esto filtrará su dirección IPv6 real. Las siguientes instrucciones explican cómo enrutar el tráfico IPv6 al túnel VPN.

Las siguientes directivas relacionadas con IPv6 deben agregarse al archivo de configuración de Client VPN para evitar fugas de IPv6:

```
ifconfig-ipv6 arg0 arg1
route-ipv6 arg0
```

Por ejemplo:

```
ifconfig-ipv6 fd15:53b6:dead::2 fd15:53b6:dead::1
route-ipv6 2000::/4
```

En este ejemplo, `ifconfig-ipv6 fd15:53b6:dead::2 fd15:53b6:dead::1` configurará la dirección IPv6 del dispositivo de túnel local como `fd15:53b6:dead::2` y la dirección IPv6 del punto de enlace VPN remoto como `fd15:53b6:dead::1`.

El siguiente comando, `route-ipv6 2000::/4` enrutará las direcciones IPv6 de `2000:0000:0000:0000:0000:0000:0000:0000` a `2fff:ffff:ffff:ffff:ffff:ffff:ffff:ffff` en la conexión de VPN.

> **Note**
>
> Para el enrutamiento de dispositivos “TAP” en Windows, por ejemplo, el segundo parámetro de `ifconfig-ipv6` se usará como destino de ruta para `--route-ipv6`.

Las organizaciones deben configurar los dos parámetros de `ifconfig-ipv6` ellos mismos, y pueden usar direcciones en `100::/64` (de `0100:0000:0000:0000:0000:0000:0000:0000` a `0100:0000:0000:0000:ffff:ffff:ffff:ffff`) o `fc00::/7` (de `fc00:0000:0000:0000:0000:0000:0000:0000` a

`fdff:ffff:ffff:ffff:ffff:ffff:ffff:ffff`). `100::/64` es un bloque de direcciones de descarte únicamente, y `fc00::/7` es local y único.

Otro ejemplo.

```
ifconfig-ipv6 fd15:53b6:dead::2 fd15:53b6:dead::1
route-ipv6 2000::/3
route-ipv6 fc00::/7
```

En este ejemplo, la configuración enrutará todo el tráfico IPv6 asignado actualmente a la conexión de VPN.

Verificación

Es probable que su organización tenga sus propias pruebas. Una verificación básica consiste en configurar una conexión de VPN de túnel completa y, a continuación, ejecutar ping6 en un servidor IPv6 utilizando la dirección IPv6. La dirección IPv6 del servidor debe estar en el rango especificado por el comando `route-ipv6`. Esta prueba de ping debería fallar. Sin embargo, esto puede cambiar si la compatibilidad con IPv6 se agrega al servicio de Client VPN en el futuro. Si el ping se realiza correctamente y puede acceder a sitios públicos cuando está conectado en modo túnel completo, es posible que tenga que hacer pruebas para solucionar el problema. También hay algunas herramientas disponibles públicamente.

Supervisión de AWS Client VPN

La monitorización tiene un papel importante en el mantenimiento de la fiabilidad, la disponibilidad y el desempeño de AWS Client VPN y sus demás soluciones de AWS. Puede utilizar las siguientes características para monitorear los puntos de enlace de Client VPN, analizar sus patrones de tráfico y solucionar sus problemas.

Amazon CloudWatch

Monitoriza los recursos de AWS y las aplicaciones que se ejecutan en AWS en tiempo real. Puede recopilar métricas y realizar un seguimiento de las métricas, crear paneles personalizados y definir alarmas que le advierten o que toman medidas cuando una métrica determinada alcanza el umbral que se especifique. Por ejemplo, puede hacer que CloudWatch haga un seguimiento del uso de la CPU u otras métricas de las instancias de Amazon EC2 y abrir nuevas instancias automáticamente cuando sea necesario. Para obtener más información, consulte la Guía del usuario de Amazon CloudWatch.

AWS CloudTrail

Captura llamadas a la API y eventos relacionados efectuados por su cuenta de AWS o en su nombre, y entrega los archivos de registro al bucket de Amazon S3 que se haya especificado. También puede identificar qué usuarios y cuentas llamaron a AWS, la dirección IP de origen de las llamadas y el momento en que se hicieron. Todas las acciones de Client VPN se registran en CloudTrail y están documentadas en la Referencia de las API de Amazon EC2.

Amazon CloudWatch Logs

Permite monitorizar los intentos de conexión realizados al punto de enlace de AWS Client VPN. Puede ver los intentos de conexión y los restablecimientos de conexiones de Client VPN. Para los intentos de conexión, puede ver tanto los correctos como los fallidos. Puede especificar la secuencia de registros de CloudWatch Logs que va a registrar los detalles de la conexión. Para obtener más información, consulte Registro de conexiones para un punto de conexión de AWS Client VPN y la Guía del usuario de Amazon CloudWatch Logs.

Temas

Métricas de Amazon CloudWatch para AWS Client VPN

AWS Client VPN publica las siguientes métricas en Amazon CloudWatch para los puntos de conexión de Client VPN. Las métricas se publican en Amazon CloudWatch cada cinco minutos.

Métrica	Descripción
ActiveConnectionsCount	Número de conexiones activas en el punto de enlace de Client VPN. Unidades: recuento
AuthenticationFailures	Número de errores de autenticación del punto de enlace de Client VPN. Unidades: recuento
CrlDaysToExpiry	Número de días hasta que expire la lista de revocación de certificados (CRL) configurada en el punto de enlace de Client VPN. Unidades: días
EgressBytes	Número de bytes enviados desde el punto de enlace de Client VPN. Unidades: bytes
EgressPackets	Número de paquetes enviados desde el punto de enlace de Client VPN. Unidades: recuento
IngressBytes	Número de bytes recibidos por el punto de enlace de Client VPN. Unidades: bytes
IngressPackets	Número de paquetes recibidos por el punto de enlace de Client VPN.

Métrica	Descripción
	Unidades: recuento
SelfServicePortalClientConfigurationDownloads	Número de descargas del archivo de configuración del punto de enlace de Client VPN realizadas en el portal de autoservicio. Unidad: recuento

AWS Client VPN publica las siguientes métricas de evaluación de la posición para los puntos de conexión de Client VPN.

Métrica	Descripción
ClientConnectHandlerTimeouts	Número de tiempos de espera en la invocación del controlador de conexión del cliente para las conexiones con el punto de conexión de Client VPN. Unidades: recuento
ClientConnectHandlerInvalidResponses	Número de respuestas no válidas que devuelve el controlador de conexión del cliente para las conexiones con el punto de conexión de Client VPN. Unidades: recuento
ClientConnectHandlerOtherExecutionErrors	Número de errores inesperados en la ejecución del controlador de conexión del cliente para las conexiones con el punto de conexión de Client VPN. Unidades: recuento
ClientConnectHandlerThrottlingErrors	Número de errores de limitación en la invocación del controlador de conexión del cliente para

Métrica	Descripción
	las conexiones con el punto de conexión de Client VPN. Unidades: recuento
ClientConnectHandlerDeniedConnections	Número de conexiones que deniega el controlador de conexiones con el punto de conexión de Client VPN. Unidades: recuento
ClientConnectHandlerFailedServiceErrors	Número de errores del lado del servicio en el que se ejecuta el controlador de conexión del cliente para las conexiones con el punto de conexión de Client VPN. Unidades: recuento

Puede filtrar las métricas de cada punto de enlace de Client VPN.

CloudWatch permite recuperar las estadísticas sobre estos puntos de datos como un conjunto ordenado de datos de serie temporal denominado métricas. Una métrica es una variable que hay que monitorizar y los puntos de datos son los valores de esa variable a lo largo del tiempo. Cada punto de datos tiene una marca temporal asociada y una unidad de medida opcional.

Puede utilizar estas métricas para comprobar si el sistema funciona de acuerdo con lo esperado. Por ejemplo, puede crear una alarma de CloudWatch para monitorizar una métrica determinada e iniciar una acción (por ejemplo, enviar una notificación a una dirección de correo electrónico) si la métrica no está comprendida dentro del intervalo que considera aceptable.

Para obtener más información, consulte la Guía del usuario de Amazon CloudWatch.

Tareas

- Visualización de las métricas de punto de conexión de Client VPN en Amazon CloudWatch

Visualización de las métricas de punto de conexión de Client VPN en Amazon CloudWatch

Puede ver las métricas de su punto de conexión de Client VPN de la manera siguiente.

Para ver las métricas a través de la consola de CloudWatch

Las métricas se agrupan en primer lugar por el espacio de nombres de servicio y, a continuación, por las diversas combinaciones de dimensiones dentro de cada espacio de nombres.

1. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, seleccione Métricas.
3. En All metrics (Todas las métricas), elija el espacio de nombres de métricas ClientVPN.
4. Para ver las métricas, seleccione la dimensión de métricas by endpoint (por punto de conexión).

Cómo ver métricas a través de la AWS CLI

En el símbolo del sistema, use el siguiente comando para enumerar las métricas que están disponibles para Client VPN.

```
aws cloudwatch list-metrics --namespace "AWS/ClientVPN"
```

AWS Client VPNCuotas de

Su cuenta de AWS tiene las siguientes cuotas (anteriormente se denominaban límites) relacionadas con los puntos de enlace de Client VPN. A menos que se indique otra cosa, cada cuota es específica de la región. Puede solicitar el aumento de algunas cuotas, pero otras no se pueden aumentar.

Para solicitar un aumento de una cuota ajustable, elija Yes (Sí) en la columna Adjustable (Ajustable). Para obtener más información, consulte este tema acerca de cómo solicitar un aumento de cuota en la Guía del usuario de Service Quotas.

Cuotas de Client VPN

Nombre	Valor predeterminado	Ajustable
Reglas de autorización por punto de enlace de Client VPN	200 Para puntos de conexión de doble pila, este límite se comparte entre rutas IPv4 e IPv6.	Sí
Puntos de enlace de Client VPN por región	5	Sí
Conexiones de cliente simultáneas por punto de enlace de Client VPN	Este valor depende de la cantidad de asociaciones de subred por punto de enlace. • 1 - 7000 • 2 - 36 500 • 3 - 66 500 • 4 - 96 500 • 5 - 126 000	Sí

Nombre	Valor predeterminado	Ajustable
	Para puntos de conexión de doble pila, este límite se comparte entre conexiones IPv4 e IPv6.	
Operaciones simultáneas por punto de enlace de Client VPN †	10	No
Entradas en una lista de revocación de certificados del cliente para puntos de enlace de Client VPN	20 000	No
Asociación de redes de destino de Rutas por Client VPN	100 Para puntos de conexión de doble pila, este límite se comparte entre rutas IPv4 e IPv6.	Sí

Entre las operaciones † se incluyen:

- Asociar o desasociar subredes
- Crear o eliminar grupos de seguridad

Cuotas de usuarios y grupos

Al configurar usuarios y grupos para Active Directory o un IdP basado en SAML, se aplican las cuotas siguientes:

- Los usuarios pueden pertenecer a un máximo de 200 grupos. Se ignora cualquier grupo después de superar el límite de 200 indicado.
- La longitud máxima del ID de grupo es de 255 caracteres.

- La longitud máxima del ID de nombre es de 255 caracteres. Se trunca cualquier carácter después de superar el límite de 255 indicado.

Consideraciones generales

Tenga en cuenta lo siguiente cuando utilice los puntos de enlace de Client VPN:

- Si utiliza Active Directory para autenticar al usuario, el punto de enlace de Client VPN debe pertenecer a la misma cuenta que el recurso de AWS Directory Service utilizado para la autenticación de Active Directory.
- Si utiliza la autenticación federada basada en SAML para autenticar a un usuario, el punto de conexión de Client VPN debe pertenecer a la misma cuenta que el proveedor de identidad de IAM SAML que cree para definir la relación de confianza entre IdP y AWS. El proveedor de identidades SAML de IAM puede compartirse entre varios puntos de enlace de Client VPN de la misma cuenta de AWS.

Resolución de problemas de AWS Client VPN

Las secciones siguientes le pueden ayudar a solucionar los problemas que podrían presentarse con un punto de conexión de Client VPN.

Para obtener más información acerca de cómo solucionar los problemas del software basado en OpenVPN que utilizan los clientes para conectarse a Client VPN, consulte Solución de problemas de conexión de Client VPN en la Guía del usuario de AWS Client VPN.

Problemas comunes

- Solución de problemas AWS Client VPN: no se puede resolver el nombre DNS del punto final de Client VPN
- Solución de problemas AWS Client VPN: el tráfico no se divide entre subredes
- Solución de problemas AWS Client VPN: las reglas de autorización para los grupos de Active Directory no funcionan según lo esperado
- Solución de problemas AWS Client VPN: los clientes no pueden acceder a una VPC interconectada, a Amazon S3 ni a Internet
- Solución de problemas AWS Client VPN: el acceso a una VPC interconectada, Amazon S3 o Internet es intermitente
- Solución de problemas AWS Client VPN: el software cliente devuelve un error de TLS al intentar conectarse a Client VPN
- Solución de problemas AWS Client VPN: el software cliente devuelve errores de nombre de usuario y contraseña: autenticación de Active Directory
- Solución de problemas AWS Client VPN: el software cliente devuelve errores de nombre de usuario y contraseña: autenticación federada
- Solución de problemas AWS Client VPN: los clientes no se pueden conectar: autenticación mutua
- Solución de problemas AWS Client VPN: el cliente devuelve un error de credenciales que superan el tamaño máximo en Client VPN: autenticación federada
- Solución de problemas AWS Client VPN: el cliente no abre el navegador de un punto final: autenticación federada
- Solución de problemas AWS Client VPN: el cliente devuelve el error de no hay puertos disponibles: autenticación federada
- Solución de problemas AWS Client VPN: se interrumpe una conexión debido a una discordancia de IP

- Solución de problemas AWS Client VPN: el enrutamiento del tráfico a la LAN no funciona según lo esperado
- Solución de problemas AWS Client VPN: compruebe el límite de ancho de banda de un terminal Client VPN
- Solución de problemas de AWS Client VPN: problemas de conectividad del túnel con una VPC

Solución de problemas AWS Client VPN: no se puede resolver el nombre DNS del punto final de Client VPN

Problema

No puedo resolver el nombre de DNS del punto de enlace de Client VPN.

Causa

El archivo de configuración del punto de enlace de Client VPN contiene un parámetro llamado `remote-random-hostname`. Este parámetro obliga al cliente a prefijar una cadena aleatoria al nombre de DNS para evitar el almacenamiento en caché del DNS. Algunos clientes no reconocen este parámetro y, por lo tanto, no prefijan la cadena aleatoria requerida al nombre de DNS.

Solución

Abra el archivo de configuración del punto de enlace de Client VPN con el editor de texto que prefiera. Localice la línea que especifica el nombre DNS del punto de conexión de Client VPN y antepóngale una cadena aleatoria para que el formato sea. *`random_string.displayed_DNS_name`* Por ejemplo:

- Nombre de DNS original: `cvpn-endpoint-0102bc4c2eEXAMPLE.clientvpn.us-west-2.amazonaws.com`
- Nombre de DNS modificado: `asdfa.cvpn-endpoint-0102bc4c2eEXAMPLE.clientvpn.us-west-2.amazonaws.com`

Solución de problemas AWS Client VPN: el tráfico no se divide entre subredes

Problema

Estoy tratando de dividir el tráfico de red entre dos subredes. El tráfico privado debe direccionarse a través de una subred privada, mientras que el tráfico de Internet debe direccionarse a través de una subred pública. Sin embargo, solo se utiliza una ruta, aunque he agregado las dos a la tabla de enrutamiento del punto de enlace de Client VPN.

Causa

Puede asociar varias subredes a un punto de enlace de Client VPN, pero solo puede asociar una subred por zona de disponibilidad. La finalidad de la asociación de varias subredes es proporcionar a los clientes alta disponibilidad y redundancia de zonas de disponibilidad. Sin embargo, la VPN de cliente no permite dividir el tráfico de forma selectiva entre las subredes asociadas con el punto de enlace de la VPN del cliente.

Los clientes se conectan a un punto de enlace de VPN de cliente basado en el algoritmo rotativo de DNS. Esto significa que su tráfico se puede direccionar a través de cualquiera de las subredes asociadas cuando establecen una conexión. Por lo tanto, pueden experimentar problemas de conectividad si acaban en una subred asociada que no tiene las entradas de rutas necesarias.

Por ejemplo, supongamos que configura las siguientes asociaciones y rutas de subred:

- Asociaciones de subred
  - Asociación 1: Subred A (us-east-1a)
  - Asociación 2: Subred B (us-east-1b)
- Rutas
  - Ruta 1:10.0.0.0/16 direccionada a la Subred A
  - Ruta 2:172.31.0.0/16 direccionada a la Subred B

En este ejemplo, los clientes que acaban en la Subred A cuando se conectan no pueden acceder a la Ruta 2, mientras que los clientes que acaban en la Subred B cuando se conectan no pueden acceder a la Ruta 1.

Solución

Compruebe que el punto de enlace de VPN de cliente tiene las mismas entradas de ruta con destinos para cada red asociada. Esto garantiza que los clientes tengan acceso a todas las rutas independientemente de la subred a través de la cual se direcciona su tráfico.

Solución de problemas AWS Client VPN: las reglas de autorización para los grupos de Active Directory no funcionan según lo esperado

Problema

He configurado reglas de autorización para mis grupos de Active Directory, pero no funcionan como esperaba. He agregado una regla de autorización `0.0.0.0/0` para autorizar el tráfico en todas las redes, pero el tráfico sigue fallando en un destino específico CIDRs.

Causa

Las reglas de autorización están indexadas en la red CIDRs. Las reglas de autorización deben conceder a los grupos de Active Directory el acceso a una red CIDRs específica. Las reglas de autorización para `0.0.0.0/0` se tratan como un caso especial y, por lo tanto, se evalúan en último lugar, independientemente del orden en que se creen las reglas de autorización.

Por ejemplo, supongamos que crea cinco reglas de autorización en el siguiente orden:

- Regla 1: Acceso del grupo 1 a `10.1.0.0/16`
- Regla 2: acceso del grupo 1 a `0.0.0.0/0`
- Regla 3: acceso del grupo 2 a `0.0.0.0/0`
- Regla 4: acceso del grupo 3 a `0.0.0.0/0`
- Regla 5: acceso del grupo 2 a `172.131.0.0/16`

En este ejemplo, la regla 2, la regla 3 y la regla 4 se evalúan en último lugar. El Grupo 1 solo tiene acceso a `10.1.0.0/16` y el Grupo 2 solo tiene acceso a `172.131.0.0/16`. El Grupo 3 no tiene acceso a `10.1.0.0/16` ni `172.131.0.0/16`, pero tiene acceso a todas las demás redes. Si quita las reglas 1 y 5, los tres grupos tienen acceso a todas las redes.

Client VPN utiliza la coincidencia de prefijos más larga al evaluar las reglas de autorización. Consulte Prioridad de la ruta en la Guía del usuario de Amazon VPC para obtener más información.

Solución

Compruebe que ha creado reglas de autorización que concedan explícitamente a los grupos de Active Directory el acceso a una red específica CIDRs. Si agrega una regla de autorización para

`0.0.0.0/0`, tenga en cuenta que se evaluará en último lugar y que las reglas de autorización anteriores podrían limitar las redes a las que concede acceso.

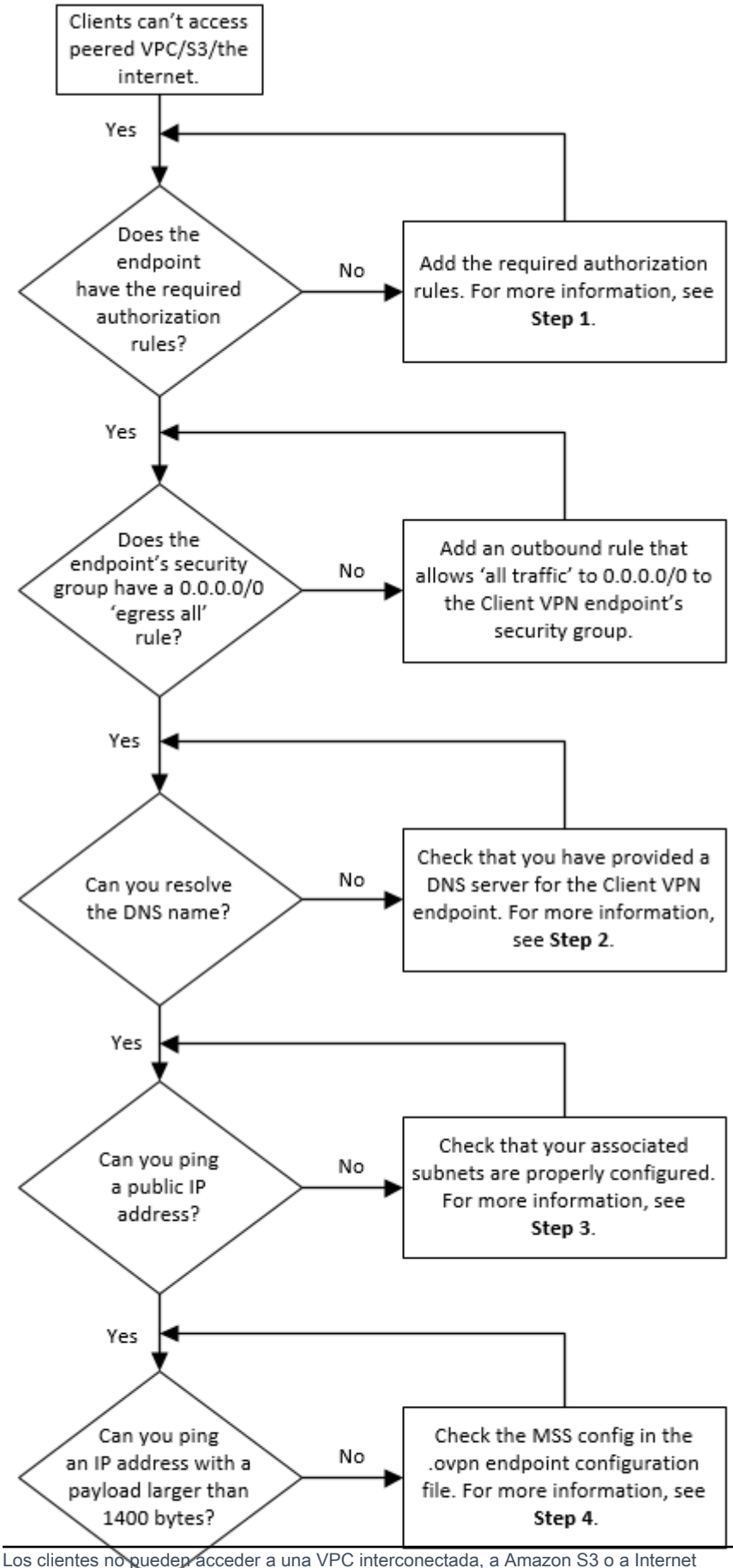
Solución de problemas AWS Client VPN: los clientes no pueden acceder a una VPC interconectada, a Amazon S3 ni a Internet

Problema

He configurado correctamente las rutas del punto de enlace de Client VPN, pero mis clientes no pueden acceder a una VPC interconectada, a Amazon S3 ni a Internet.

Solución

El siguiente diagrama de flujo contiene los pasos para diagnosticar problemas de conectividad de Internet, de las VPC interconectadas y de Amazon S3.


Clients can't access peered VPC/S3/the internet.
Yes
Does the endpoint have the required authorization rules?
No
Add the required authorization rules. For more information, see **Step 1**.
Yes
Does the endpoint's security group have a 0.0.0.0/0 'egress all' rule?
No
Add an outbound rule that allows 'all traffic' to 0.0.0.0/0 to the Client VPN endpoint's security group.
Yes
Can you resolve the DNS name?
No
Check that you have provided a DNS server for the Client VPN endpoint. For more information, see **Step 2**.
Yes
Can you ping a public IP address?
No
Check that your associated subnets are properly configured. For more information, see **Step 3**.
Yes
Can you ping an IP address with a payload larger than 1400 bytes?
No
Check the MSS config in the .ovpn endpoint configuration file. For more information, see **Step 4**.
Yes

1. Para obtener acceso a Internet, agregue una regla de autorización para `0.0.0.0/0`.

   Para acceder a una VPC interconectada, añada una regla de autorización para IPv4 el rango CIDR de la VPC.

   Para obtener acceso a S3, especifique la dirección IP del punto de enlace de Amazon S3.

2. Compruebe si puede resolver el nombre de DNS.

   Si no puede resolver el nombre de DNS, compruebe que ha especificado los servidores DNS del punto de enlace de Client VPN. Si administra su propio servidor DNS, especifique su dirección IP. Compruebe que el servidor DNS sea accesible desde la VPC.

   Si no está seguro de qué dirección IP especificar para los servidores DNS, especifique el solucionador de DNS de VPC en la dirección IP .2 de la VPC.

3. Para el acceso a Internet, compruebe si puede hacer ping a una dirección IP pública o a un sitio web público, por ejemplo, `amazon.com`. Si no obtiene respuesta, asegúrese de que la tabla de enrutamiento de las subredes asociadas tiene una ruta predeterminada que está dirigida a una gateway de Internet o a una gateway NAT. Si la ruta está en su lugar, compruebe que la subred asociada no tenga reglas de listas de control de acceso de red que bloqueen el tráfico entrante y saliente.

   Si no puede conectarse a una VPC interconectada, compruebe que la tabla de enrutamiento de la subred asociada tenga una entrada de ruta para la VPC interconectada.

   Si no puede conectarse a Amazon S3, compruebe que la tabla de enrutamiento de la subred asociada tiene una entrada de ruta para el punto de enlace de la VPC de la gateway.

4. Compruebe si puede hacer ping a una dirección IP pública con una carga superior a 1400 bytes. Utilice uno de los siguientes comandos:

   - Windows

     ```
     C:\> ping  8.8.8.8 -l 1480 -f
     ```

   - Linux

     ```
     $ ping -s 1480 8.8.8.8 -M do
     ```

Si no puede hacer ping a una dirección IP con una carga superior a 1400 bytes, abra el archivo de configuración `.ovpn` del punto de enlace de Client VPN utilizando el editor de texto que prefiera y agregue lo siguiente.

```
mssfix 1328
```

Solución de problemas AWS Client VPN: el acceso a una VPC interconectada, Amazon S3 o Internet es intermitente

Problema

Tengo problemas de conectividad intermitentes cuando me conecto a una VPC interconectada, a Amazon S3 o a Internet, pero el problema no ocurre cuando me conecto a las subredes asociadas. Tengo que desconectarme y volver a conectarme para resolver los problemas de conectividad.

Causa

Los clientes se conectan a un punto de enlace de VPN de cliente basado en el algoritmo rotativo de DNS. Esto significa que su tráfico se puede direccionar a través de cualquiera de las subredes asociadas cuando establecen una conexión. Por lo tanto, pueden experimentar problemas de conectividad si acaban en una subred asociada que no tiene las entradas de rutas necesarias.

Solución

Compruebe que el punto de enlace de VPN de cliente tiene las mismas entradas de ruta con destinos para cada red asociada. Esto garantiza que los clientes tengan acceso a todas las rutas independientemente de la subred asociada a través de la cual se direcciona su tráfico.

Por ejemplo, supongamos que su punto de enlace de VPN de cliente tiene tres subredes asociadas (Subred A, B y C) y desea habilitar el acceso a Internet para sus clientes. Para ello, debe agregar tres rutas de `0.0.0.0/0` que se dirijan a cada subred asociada:

- Ruta 1: `0.0.0.0/0` para la Subred A
- Ruta 2: `0.0.0.0/0` para la Subred B
- Ruta 3: `0.0.0.0/0` para la Subred C

Solución de problemas AWS Client VPN: el software cliente devuelve un error de TLS al intentar conectarse a Client VPN

Problema

Antes podía conectar mis clientes a Client VPN sin ningún problema, pero ahora el cliente basado en OpenVPN devuelve uno de los siguientes errores cuando intenta conectarse:

```
TLS Error: TLS key negotiation failed to occur within 60 seconds (check your network
 connectivity)
TLS Error: TLS handshake failed
```

```
Connection failed because of a TLS handshake error. Contact your IT administrator.
```

Causa posible n.º 1

Si utiliza la autenticación mutua y ha importado una lista de revocación de certificados de cliente, es posible que la lista de revocación de certificados de cliente haya caducado. Durante la fase de autenticación, el punto de enlace de Client VPN comprueba el certificado de cliente en la lista de revocación de certificados de cliente que ha importado. Si esta lista ha caducado, no puede conectarse al punto de enlace de Client VPN.

Solución n.º 1

Compruebe la fecha de caducidad de su lista de revocación de certificados de cliente con la herramienta OpenSSL.

```
$ openssl crl -in path_to_crl_pem_file -noout -nextupdate
```

La salida muestra la fecha y la hora de caducidad. Si la lista de revocación de certificados de cliente ha caducado, debe crear una nueva e importarla al punto de enlace de Client VPN. Para obtener más información, consulte AWS Client VPN listas de revocación de certificados de cliente.

Causa posible n.º 2

El certificado de servidor que se utiliza para el punto de conexión de Client VPN ha caducado.

Solución n.º 2

Compruebe el estado del certificado de servidor en la AWS Certificate Manager consola o mediante la AWS CLI. Si el certificado del servidor ha caducado, cree uno nuevo y cárguelo en ACM. Para conocer los pasos detallados para generar los certificados y las claves del servidor y del cliente mediante la utilidad easy-rsa de OpenVPN e importarlos a ACM, consulte Autenticación mutua en AWS Client VPN.

También es posible que haya un problema con el software basado en OpenVPN que el cliente está utilizando para conectarse a Client VPN. Para obtener más información acerca de cómo solucionar los problemas del software basado en OpenVPN, consulte Solución de problemas de la conexión de Client VPN en la AWS Client VPN Guía del usuario.

Solución de problemas AWS Client VPN: el software cliente devuelve errores de nombre de usuario y contraseña: autenticación de Active Directory

Problema

Utilizo la autenticación de Active Directory con el punto de enlace de Client VPN y antes podía conectar los clientes a Client VPN correctamente. Pero ahora los clientes están recibiendo errores de nombre de usuario y contraseña no válidos.

Causas posibles

Si utiliza la autenticación de Active Directory y ha habilitado la autenticación multifactor (MFA) después de distribuir el archivo de configuración del cliente, el archivo no contiene la información necesaria para solicitar a los usuarios que introduzcan su código MFA. A los usuarios se les pide que introduzcan únicamente su nombre de usuario y contraseña, por lo que la autenticación falla.

Solución

Descargue un nuevo archivo de configuración de cliente y distribúyalo entre sus clientes. Compruebe que el archivo contenga la siguiente línea.

```
static-challenge "Enter MFA code " 1
```

Para obtener más información, consulte AWS Client VPN exportación de archivos de configuración de terminales. Pruebe la configuración de MFA de Active Directory sin utilizar el punto de enlace de Client VPN para comprobar que MFA funciona de la forma prevista.

Solución de problemas AWS Client VPN: el software cliente devuelve errores de nombre de usuario y contraseña: autenticación federada

Problema

Al intentar iniciar sesión con un nombre de usuario y una contraseña con autenticación federada, aparece el error “Las credenciales recibidas son incorrectas. Póngase en contacto con el administrador de TI”.

Causa

Este error puede deberse a que no se incluye al menos un atributo en la respuesta SAML del IdP.

Solución

Asegúrese de que al menos un atributo se incluye en la respuesta SAML del IdP. Para obtener más información, consulte Recursos de configuración de IdP basados en SAML.

Solución de problemas AWS Client VPN: los clientes no se pueden conectar: autenticación mutua

Problema

Utilizo la autenticación mutua con el punto de enlace de Client VPN. Los clientes están recibiendo errores de negociación de claves TLS y errores de tiempo de espera.

Causas posibles

El archivo de configuración proporcionado a los clientes no contiene el certificado del cliente y la clave privada del cliente, o el certificado y la clave son incorrectos.

Solución

Asegúrese de que el archivo de configuración contiene el certificado de cliente y la clave correctos. Si es necesario, corrija el archivo de configuración y vuelva a distribuirlo entre sus clientes. Para obtener más información, consulte AWS Client VPN exportación de archivos de configuración de terminales.

Solución de problemas AWS Client VPN: el cliente devuelve un error de credenciales que superan el tamaño máximo en Client VPN: autenticación federada

Problema

Utilizo la autenticación federada con el punto de enlace de Client VPN. Cuando los clientes escriben el nombre de usuario y la contraseña en la ventana del navegador del proveedor de identidades (IdP) basado en SAML, reciben un error que indica que las credenciales superan el tamaño máximo admitido.

Causa

La respuesta SAML que devuelve el IdP supera el tamaño máximo admitido. Para obtener más información, consulte Requisitos y consideraciones de la autenticación federada basada en SAML.

Solución

Pruebe a reducir el número de grupos a los que pertenece el usuario en el IdP e intente conectarse de nuevo.

Solución de problemas AWS Client VPN: el cliente no abre el navegador de un punto final: autenticación federada

Problema

Utilizo la autenticación federada con el punto de enlace de Client VPN. Cuando los clientes intentan conectarse al punto de enlace, el software del cliente no abre una ventana del navegador y, en su lugar, se muestra una ventana emergente para el nombre de usuario y la contraseña.

Causa

El archivo de configuración proporcionado a los clientes no contiene la marca `auth-federate`.

Solución

Exporte el archivo de configuración más reciente, impórtelo al cliente AWS proporcionado e intente conectarse de nuevo.

Solución de problemas AWS Client VPN: el cliente devuelve el error de no hay puertos disponibles: autenticación federada

Problema

Utilizo la autenticación federada con el punto de enlace de Client VPN. Cuando los clientes intentan conectarse al punto de enlace, el software de cliente devuelve el siguiente error:

```
The authentication flow could not be initiated. There are no available ports.
```

Causa

El cliente AWS proporcionado requiere el uso del puerto TCP 35001 para completar la autenticación. Para obtener más información, consulte Requisitos y consideraciones de la autenticación federada basada en SAML.

Solución

Compruebe que el dispositivo del cliente no está bloqueando el puerto TCP 35001 ni lo está utilizando para otro proceso.

Solución de problemas AWS Client VPN: se interrumpe una conexión debido a una discordancia de IP

Problema

La conexión de VPN ha finalizado y el software cliente devuelve el siguiente error: `"The VPN connection is being terminated due to a discrepancy between the IP address of the connected server and the expected VPN server IP. Please contact your network administrator for assistance in resolving this issue."`

Causa

El cliente AWS proporcionado requiere que la dirección IP a la que está conectado coincida con la IP del servidor VPN que respalda el punto final Client VPN. Para obtener más información, consulte Reglas y mejores prácticas de uso AWS Client VPN.

Solución

Compruebe que no haya ningún proxy DNS entre el cliente AWS proporcionado y el punto final Client VPN.

Solución de problemas AWS Client VPN: el enrutamiento del tráfico a la LAN no funciona según lo esperado

Problema

El intento de enrutar el tráfico a la red de área local (LAN) no funciona según lo esperado cuando los rangos de direcciones IP de la LAN no se encuentran dentro de los siguientes rangos de direcciones IP privadas estándar: `10.0.0.0/8`, `172.16.0.0/12`, `192.168.0.0/16` o `169.254.0.0/16`.

Causa

Si se detecta que el rango de direcciones LAN del cliente se encuentra fuera de los rangos estándar anteriores, el punto de conexión de Client VPN enviará automáticamente la directiva de OpenVPN “redirect-gateway block-local” al cliente, lo que forzará todo el tráfico de LAN en la VPN. Para obtener más información, consulte Reglas y mejores prácticas de uso AWS Client VPN.

Solución

Si necesita acceso de LAN durante las conexiones de VPN, se recomienda que utilice los rangos de direcciones convencionales mostrados anteriormente para la LAN.

Solución de problemas AWS Client VPN: compruebe el límite de ancho de banda de un terminal Client VPN

Problema

Tengo que comprobar el límite de ancho de banda de un punto de enlace de Client VPN.

Causa

El rendimiento depende de varios factores, como la capacidad de la conexión desde su ubicación y la latencia de red entre la aplicación de escritorio de Client VPN del equipo y el punto de enlace de la VPC. Se admite un ancho de banda mínimo de 10 Mbps por conexión de usuario.

Solución

Ejecute los siguientes comandos para verificar el ancho de banda.

```
sudo iperf3 -s -V
```

En el cliente:

```
sudo iperf -c server IP address -p port -w 512k -P 60
```

Solución de problemas de AWS Client VPN: problemas de conectividad del túnel con una VPC

Cuando tenga problemas de conectividad con su conexión de AWS Client VPN, siga este método sistemático para identificarlos y resolverlos. En esta sección se proporcionan procedimientos paso a paso para diagnosticar problemas comunes de conectividad de Client VPN entre clientes remotos y recursos de Amazon VPC.

Temas

Requisitos previos de conectividad de red

Antes de solucionar los problemas de conectividad de Client VPN, compruebe estos requisitos previos de red:

- Asegúrese de que la subred de punto de conexión de Client VPN tenga conectividad a Internet (a través de puerta de enlace de Internet o puerta de enlace NAT).
- Compruebe que el punto de conexión de Client VPN esté asociado a subredes en diferentes zonas de disponibilidad para garantizar alta disponibilidad.
- Compruebe que la VPC tenga suficiente espacio de direcciones IP y que no entre en conflicto con los bloques de CIDR del cliente.
- Confirme que las subredes de destino tengan las asociaciones de tabla de enrutamiento adecuadas.

Comprobación del estado del punto de conexión de Client VPN

En primer lugar, compruebe que el punto de conexión de Client VPN se encuentre en el estado correcto:

1. Utilice AWS CLI para comprobar el estado del punto de conexión de Client VPN:

   ```
   aws ec2 describe-client-vpn-endpoints --region your-region
   ```

2. Busque el estado del punto de conexión en la salida. El estado debería ser `available`.
3. Compruebe que el punto de conexión tenga redes de destino asociadas (subredes).
4. Si el estado no es `available`, compruebe si hay mensajes de error o estados pendientes que puedan indicar problemas de configuración.

Verificación de conexiones de clientes

Compruebe el estado de las conexiones de clientes con el punto de conexión de Client VPN:

1. Compruebe las conexiones de clientes activas:

   ```
   aws ec2 describe-client-vpn-connections --client-vpn-endpoint-id cvpn-endpoint-id
    --region your-region
   ```

2. Revise el estado de la conexión y los mensajes de error que puedan aparecer en el resultado.
3. Compruebe los registros de autenticación del cliente para ver si hay intentos de autenticación fallidos.
4. Compruebe que los clientes reciben direcciones IP del bloque de CIDR del cliente configurado.

> **Note**
>
> Si los clientes no pueden conectarse, es probable que el problema esté relacionado con la configuración de la autenticación, las reglas de autorización o la conectividad de red.

Verificación de la autenticación del cliente

Los problemas de autenticación suelen producir errores de conectividad en Client VPN:

- Para la autenticación mutua, asegúrese de que los certificados del clientes sean válidos y no hayan caducado.
- Para la autenticación de Active Directory, compruebe las credenciales de usuario y la conectividad del dominio.
- Para la autenticación federada basada en SAML, compruebe la configuración del IdP y los permisos de usuario.
- Revise los registros de autenticación en CloudWatch para obtener información detallada sobre los errores.
- Compruebe que el método de autenticación configurado en el punto de conexión coincide con la configuración del cliente.

Comprobación de reglas de autorización

Las reglas de autorización controlan a qué recursos de red pueden acceder los clientes:

1. Enumere las reglas de autorización actuales:

```
aws ec2 describe-client-vpn-authorization-rules --client-vpn-endpoint-id cvpn-endpoint-id --region your-region
```

2. Compruebe que haya reglas para las redes de destino a las que necesitan acceder los clientes.

3. Compruebe que las reglas especifican los grupos de Active Directory correctos (si utiliza la autenticación AD).
4. Asegúrese de que las reglas de autorización se encuentren en estado `active`.

Validación de rutas de Client VPN

La configuración de enrutamiento adecuada es esencial para la conectividad de Client VPN:

1. Compruebe las rutas de punto de conexión de Client VPN:

```
aws ec2 describe-client-vpn-routes --client-vpn-endpoint-id cvpn-endpoint-id --
region your-region
```

2. Compruebe que hay reglas para las redes de destino a las que deban acceder los clientes.
3. Consulte las tablas de enrutamiento de Amazon VPC para asegurarse de que el tráfico de retorno pueda llegar al punto de conexión de Client VPN:

```
aws ec2 describe-route-tables --filters "Name=vpc-id,Values=vpc-id" --region your-
region
```

4. Compruebe que las asociaciones de redes de destino estén configuradas correctamente.

Verificación de grupos de seguridad y ACL de red

Los grupos de seguridad y las ACL de red pueden bloquear el tráfico de Client VPN:

1. Compruebe los grupos de seguridad para las instancias de EC2 de destino:

```
aws ec2 describe-security-groups --group-ids sg-xxxxxxxxx --region your-region
```

2. Compruebe que las reglas de entrada permiten tráfico del bloque de CIDR de Client VPN:
   - SSH (puerto 22) desde el CIDR de Client VPN: `10.0.0.0/16`
   - HTTP (puerto 80) desde el CIDR de Client VPN: `10.0.0.0/16`
   - HTTPS (puerto 443) desde el CIDR de Client VPN: `10.0.0.0/16`
   - Puertos de aplicaciones personalizados si es necesario
3. Para el grupo de seguridad del punto de conexión de Client VPN (en su caso), asegúrese de que permita:

- Puerto UDP 443 (OpenVPN) desde 0.0.0.0/0
- Todo el tráfico de salida a bloques de CIDR de VPC

4. Compruebe que las ACL de red no bloqueen el tráfico. Las ACL de red no tienen estado, por lo que se deben configurar reglas de entrada y salida.
5. Verifique las reglas de entrada y salida para el tráfico específico que intenta enviar.

Prueba de conectividad de clientes

Pruebe la conectividad de los clientes de Client VPN a los recursos de Amazon VPC:

1. Desde un cliente de Client VPN conectado, pruebe la conectividad a recursos de Amazon VPC:

```
ping vpc-resource-ip
traceroute vpc-resource-ip
```

2. Pruebe la conectividad de aplicaciones específicas.

```
telnet vpc-resource-ip port
```

3. Verifique la resolución de DNS si utiliza nombres de DNS privados:

```
nslookup private-dns-name
```

4. Pruebe la conectividad a los recursos de Internet si está habilitada la tunelización dividida.

Diagnóstico del dispositivo cliente

Realice estas comprobaciones en el dispositivo cliente:

1. Verifique que el archivo de configuración del cliente (.ovpn) contenga los ajustes correctos:
   - URL correcta del punto de conexión del servidor
   - Certificado del cliente y clave privada válidos
   - Configuración adecuada del método de autenticación
2. Compruebe los registros del cliente para ver si hay errores de conexión:
   - Windows: Visor de eventos → Registros de aplicaciones y servicios → OpenVPN

- macOS: aplicación Consola, busque “Tunnelblick” u “OpenVPN”
- Linux: `/var/log/openvpn/` o systemd journal

3. Pruebe la conectividad de red básica desde el cliente:

```
ping 8.8.8.8
nslookup cvpn-endpoint-id.cvpn.region.amazonaws.com
```

Solución de problemas de resolución de DNS

Los problemas de DNS pueden impedir el acceso a recursos que utilizan nombres de DNS privados:

1. Compruebe si los servidores de DNS están configurados en el punto de conexión de Client VPN:

```
aws ec2 describe-client-vpn-endpoints --client-vpn-endpoint-ids cvpn-endpoint-id --
query 'ClientVpnEndpoints[0].DnsServers'
```

2. Pruebe la resolución de DNS desde el cliente:

```
nslookup private-resource.internal
dig private-resource.internal
```

3. Verifique las reglas de Route 53 Resolver si usa una resolución de DNS personalizada.
4. Compruebe que los grupos de seguridad permiten tráfico de DNS (puerto 53 UDP/TCP) desde el CIDR de Client VPN hasta los servidores de DNS.

Solución de problemas de rendimiento

Solución de problemas de rendimiento con conexiones de Client VPN:

- Supervise el uso del ancho de banda mediante métricas de CloudWatch para bytes de entrada/salida.
- Compruebe la pérdida de paquetes mediante pruebas de ping continuas desde los clientes.
- Verifique que el punto de conexión de Client VPN no alcance los límites de conexión.
- Considere la posibilidad de utilizar varios puntos de conexión de Client VPN para la distribución de la carga.

- Pruebe con diferentes ubicaciones de clientes para identificar problemas de rendimiento regionales.

Monitorización de métricas de Client VPN

Monitorización de las métricas de punto de conexión de Client VPN a través de CloudWatch:

1. Compruebe las métricas de conexión activa:

```
aws cloudwatch get-metric-statistics \
  --namespace AWS/ClientVPN \
  --metric-name ActiveConnectionsCount \
  --dimensions Name=Endpoint,Value=cvpn-endpoint-id \
  --start-time start-time \
  --end-time end-time \
  --period 300 \
  --statistics Average
```

2. Revise las métricas de error de autenticación:

```
aws cloudwatch get-metric-statistics \
  --namespace AWS/ClientVPN \
  --metric-name AuthenticationFailures \
  --dimensions Name=Endpoint,Value=cvpn-endpoint-id \
  --start-time start-time \
  --end-time end-time \
  --period 300 \
  --statistics Sum
```

3. Revise otras métricas disponibles, como los bytes y los paquetes de entrada y salida.

Comprobación de los registros de Client VPN

Los registros de conexión de Client VPN proporcionan información detallada sobre los intentos y errores de conexión:

- Habilite el registro de conexiones de Client VPN si aún no está configurado.
- Revise los registros de CloudWatch para ver si hay intentos de conexión, errores de autenticación y errores de autorización.

- Busque códigos y mensajes de error específicos que indiquen la causa raíz de los problemas de conectividad.
- Compruebe en las conexiones fallidas si hay patrones que puedan indicar problemas de configuración.

Problemas y soluciones comunes

Problemas comunes que pueden afectar a la conectividad de Client VPN:

Errores de autenticación

: Certificados de cliente que han caducado o no son válidos, o credenciales de Active Directory incorrectas. Compruebe la configuración de autenticación y la validez de las credenciales.

Ausencia de reglas de autorización

: Los clientes no pueden acceder a las redes de destino porque faltan reglas de autorización o son incorrectas. Agregue las reglas de autorización adecuadas para las redes requeridas.

Problemas de tunelización dividida

: El enrutamiento del tráfico es incorrecto debido a la configuración de túneles divididos. Revise y ajuste la configuración de tunelización dividida si es necesario.

Agotamiento del grupo de IP del cliente

: No hay direcciones IP disponibles en el bloque de CIDR del cliente. Amplíe el intervalo de CIDR del cliente o desconecte los clientes no utilizados.

Problemas de MTU

: Los paquetes grandes se descartan debido a las limitaciones de tamaño de la MTU. Configure la MTU en 1436 bytes o habilite Path MTU Discovery en los dispositivos cliente.

Problemas de resolución de DNS

: Los clientes no pueden resolver nombres de DNS privados. Compruebe la configuración del servidor de DNS y asegúrese de que el tráfico de DNS esté permitido a través de grupos de seguridad.

Solapamiento de intervalos de IP

El bloque de CIDR del cliente entra en conflicto con los intervalos de redes locales. Compruebe y resuelva cualquier intervalo de direcciones IP que se solape entre el CIDR del cliente y las redes locales.

Errores de establecimiento de comunicación de TLS

La conexión falla durante la negociación de TLS. Compruebe la validez del certificado, asegúrese de que los conjuntos de cifrado sean correctos y compruebe que los certificados de cliente y servidor estén configurados correctamente.

Retrasos de propagación de rutas

Las nuevas rutas no están disponibles de forma inmediata para los clientes. Espere de 1 a 2 minutos a la propagación de la ruta después de realizar cambios en rutas de Client VPN.

Caídas o inestabilidad de la conexión

Desconexiones frecuentes o inestables. Compruebe la congestión de la red, las interferencias del firewall o la configuración de administración de energía en los dispositivos cliente.

Historial de revisión de la Guía del usuario de Client VPN

En la siguiente tabla, se describen las actualizaciones de la Guía del administrador de AWS Client VPN.

Cambio	Descripción	Fecha
Compatibilidad con IPv	Client VPN permite ahora conectividad IPv6 completa para puntos de conexión de Client VPN y admite conexiones a recursos IPv6 en sus VPC y desde clientes en redes IPv6.	25 de agosto de 2025
Característica Client Route Enforcement	Adición de la característica client route enforcement	20 de abril de 2025
Aumento de cuota de Client VPN	Se ha aumentado la cuota de reglas de autorización por punto de conexión de Client VPN de 50 a 200.	13 de marzo de 2025
Compatibilidad con desconexión cuando se agota el tiempo de espera de la sesión	El tiempo de espera de la sesión permite ahora la desconexión cuando se alcanza la duración máxima de la sesión.	13 de enero de 2025
Aumento de las cuotas	Las cuotas de reglas de autorización por punto de conexión de Client VPN y las rutas por punto de conexión de Client VPN han aumentado de 50 y 10, respectivamente, a 100.	19 de diciembre de 2024

Ejemplos de reglas de autorización	Adición de escenarios de ejemplo para las reglas de autorización.	15 de septiembre de 2022
Duración máxima de la sesión VPN	Puede configurar una sesión VPN de duración máxima menor para cumplir con los requisitos de seguridad y conformidad.	20 de enero de 2022
Banner de inicio de sesión de cliente	Puede habilitar un banner de texto en las aplicaciones de escritorio de Client VPN proporcionadas por AWS cuando se establece una sesión de VPN para cumplir con las necesidades normativas y de conformidad.	20 de enero de 2022
Controlador de la conexión del cliente	Puede activar el controlador de la conexión del cliente en el punto de enlace de Client VPN para ejecutar una lógica personalizada que autorice nuevas conexiones.	4 de noviembre de 2020
Portal de autoservicio	Puede activar un portal de autoservicio en el punto de enlace de Client VPN para sus clientes.	29 de octubre de 2020
Acceso entre clientes	Puede permitir que los clientes utilicen un punto de enlace de Client VPN para conectarse entre sí.	29 de septiembre de 2020

Autenticación federada basada en SAML	Puede autenticar a los usuarios de Client VPN utilizando la autentica ción federada basada en SAML 2.0.	19 de mayo de 2020
Especificar grupos de seguridad durante la creación	Puede especificar una VPC y grupos de seguridad al crear el punto de enlace de AWS Client VPN.	5 de marzo de 2020
Puertos VPN configurables	Puede especificar un número de puerto VPN compatible para su punto de enlace de AWS Client VPN.	16 de enero de 2020
Compatibilidad con Multi-Fac tor Authentication (MFA)	El punto de enlace de AWS Client VPN da soporte a la MFA si está habilitado para Active Directory.	30 de septiembre de 2019
Compatibilidad con la división de túneles	Puede habilitar la división de túneles en el punto de enlace de AWS Client VPN.	24 de julio de 2019
Versión inicial	Esta versión introduce AWS Client VPN.	18 de diciembre de 2018

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.