Guía del usuario

AWS Site-to-Site VPN

AWS Site-to-Site VPN: Guía del usuario

Table of Contents

¿Qué es AWS Site-to-Site VPN?

De forma predeterminada, las instancias que se lanzan en una VPC de Amazon no pueden comunicarse con su propia red (remota). Puede habilitar el acceso a la red remota desde la VPC mediante la creación de una conexión de AWS Site-to-Site VPN (Site-to-Site VPN) y la configuración del enrutamiento para que el tráfico pase a través de la conexión.

Aunque el término conexión de VPN es un término general, en esta documentación, hace referencia a la conexión entre su VPC y su propia red local. VPN de sitio a sitio admite conexiones de VPN con cifrado Internet Protocol Security (IPsec).

Contenido

Conceptos

A continuación, se incluyen los conceptos clave de Site-to-Site VPN:

- Conexión de VPN: conexión segura entre el equipo que se encuentra en las instalaciones y sus VPC.
- Túnel de VPN: enlace cifrado donde los datos pueden pasar desde la red del cliente hasta AWS o salir de allí.

  Cada conexión de VPN incluye dos túneles de VPN que puede utilizar simultáneamente para conseguir alta disponibilidad.
- Gateway de cliente: recurso de AWS que proporciona información a AWS sobre su dispositivo de gateway de cliente.
- Dispositivo de gateway de cliente: dispositivo físico o aplicación de software que se encuentra en su extremo de la conexión de Site-to-Site VPN.
- Puerta de enlace de destino: término genérico para el punto de conexión VPN en el lado de Amazon de la conexión Site-to-Site VPN.

- Puerta de enlace privada virtual: es el punto de conexión VPN en el lado de Amazon de la conexión Site-to-Site VPN que se puede adjuntar a una única VPC.
- Puerta de enlace de tránsito: un hub de tránsito que se puede utilizar para interconectar varias VPC y redes en las instalaciones y como punto de conexión VPN para el lado de Amazon de la conexión Site-to-Site VPN.

Características de Site-to-Site VPN

Se admiten las siguientes características en las conexiones de VPN AWS Site-to-Site VPN:

- Internet Key Exchange versión 2 (IKEv2)
- Recorrido de NAT
- ASN de 4 bytes comprendidos entre 1 y 2147483647 para la configuración de gateway privada virtual (VGW). Para obtener más información, consulte Opciones de la gateway de cliente para su conexión de Site-to-Site VPN.
- ASN de 2 bytes para gateway de cliente (CGW) comprendidos entre 1 y 65535. Para obtener más información, consulte Opciones de la gateway de cliente para su conexión de Site-to-Site VPN.
- Métricas de CloudWatch
- Direcciones IP reutilizables para sus gateways de cliente
- Opciones de cifrado adicionales; incluido el cifrado AES de 256 bits, hash SHA-2 y grupos adicionales Diffie-Hellman
- Opciones de túnel configurables
- ASN privado personalizado para el lado de Amazon de una sesión BGP
- Certificado privado de una CA subordinada de AWS Private Certificate Authority
- Compatibilidad con el tráfico IPv6 para conexiones VPN en una gateway de tránsito

Limitaciones de Site-to-Site VPN

Las conexiones de Site-to-Site VPN tienen las siguientes limitaciones.

- El tráfico IPv6 no es compatible con las conexiones VPN en una gateway privada virtual.
- Una conexión de AWS VPN no es compatible con la detección de la MTU de la ruta.

Además, debe tener en cuenta lo siguiente cuando utilice Site-to-Site VPN:

- Al conectar las VPC a una red en las instalaciones común, se recomienda utilizar bloques de CIDR no superpuestos para las redes.

Uso de Site-to-Site VPN

Puede crear los recursos de Site-to-Site VPN, acceder a ellos y administrarlos desde cualquiera de las siguientes interfaces:

- AWS Management Console: proporciona una interfaz web que se puede utilizar para acceder a los recursos de Site-to-Site VPN.
- AWS Command Line Interface (AWS CLI): proporciona comandos para numerosos servicios de AWS, como Amazon VPC, y es compatible con Windows, macOS y Linux. Para obtener más información, consulte AWS Command Line Interface.
- SDK de AWS: proporcionan API específicas de cada lenguaje y se encargan de muchos de los detalles de la conexión, como el cálculo de firmas, el control de reintentos de solicitud y el control de errores. Para obtener más información, consulte SDK de AWS.
- Query API (API de consulta): proporciona acciones de la API de nivel bajo a las que se llama mediante solicitudes HTTPS. La API de consulta es la forma más directa de acceder a Amazon VPC, pero requiere que la aplicación controle niveles de detalle de bajo nivel, como la generación de hash para firmar la solicitud y el control de errores. Para obtener más información, consulte la referencia de las API de Amazon EC2.

Precios

Se le cobra por cada hora de conexión VPN que aprovisione su conexión VPN y esté disponible. Para obtener más información, consulte los Precios de AWS Site-to-Site VPN y Accelerated Site-to-Site VPN Connection.

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

Cuando usted crea una conexión de VPN acelerada, nosotros creamos y administramos dos aceleradores en su nombre. Se le cobrará una tarifa por hora y los costos de transferencia de datos para cada acelerador. Para obtener más información, consulte Precios de AWS Global Accelerator.

Cómo funciona AWS Site-to-Site VPN

Las conexiones de Site-to-Site VPN constan de lo siguiente:

- Una puerta de enlace privada virtual o una puerta de enlace de tránsito
- Un dispositivo de puerta de enlace de cliente
- Una puerta de enlace de cliente

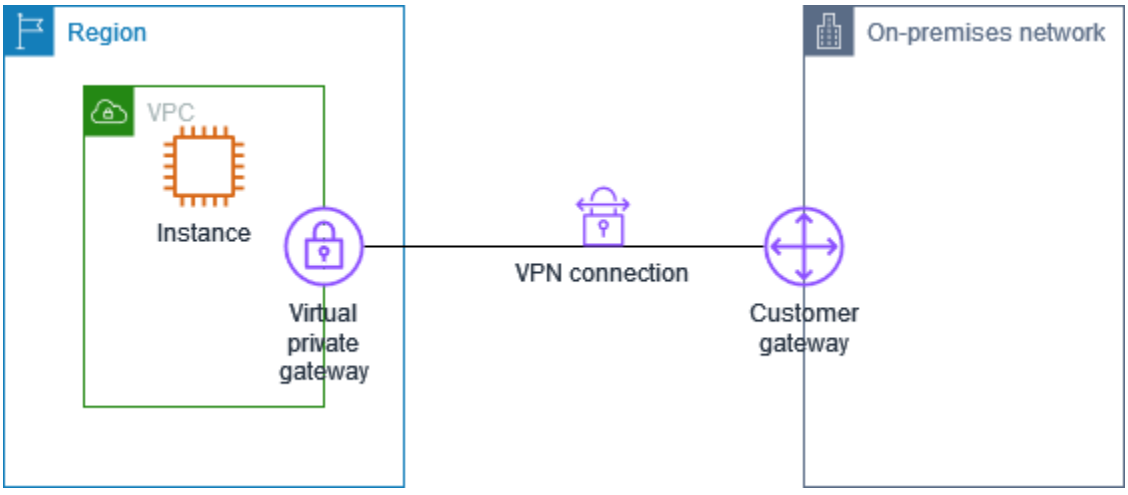
Una conexión de VPN ofrece dos túneles de VPN entre una puerta de enlace privada virtual o una puerta de enlace de tránsito en el lado de AWS y una puerta de enlace de cliente en las instalaciones.

Para obtener más información sobre las cuotas de Site-to-Site VPN, consulte Cuotas de Site-to-Site VPN.

Gateway privada virtual

La gateway privada virtual es el concentrador VPN que se encuentra en el extremo de Amazon de la conexión de Site-to-Site VPN. Debe crear una puerta de enlace privada virtual y conectarla a una nube privada virtual (VPC) con recursos que deben acceder a la conexión de Site-to-Site VPN.

El siguiente diagrama muestra una conexión de VPN entre una VPC y la red en las instalaciones mediante una puerta de enlace privada virtual.



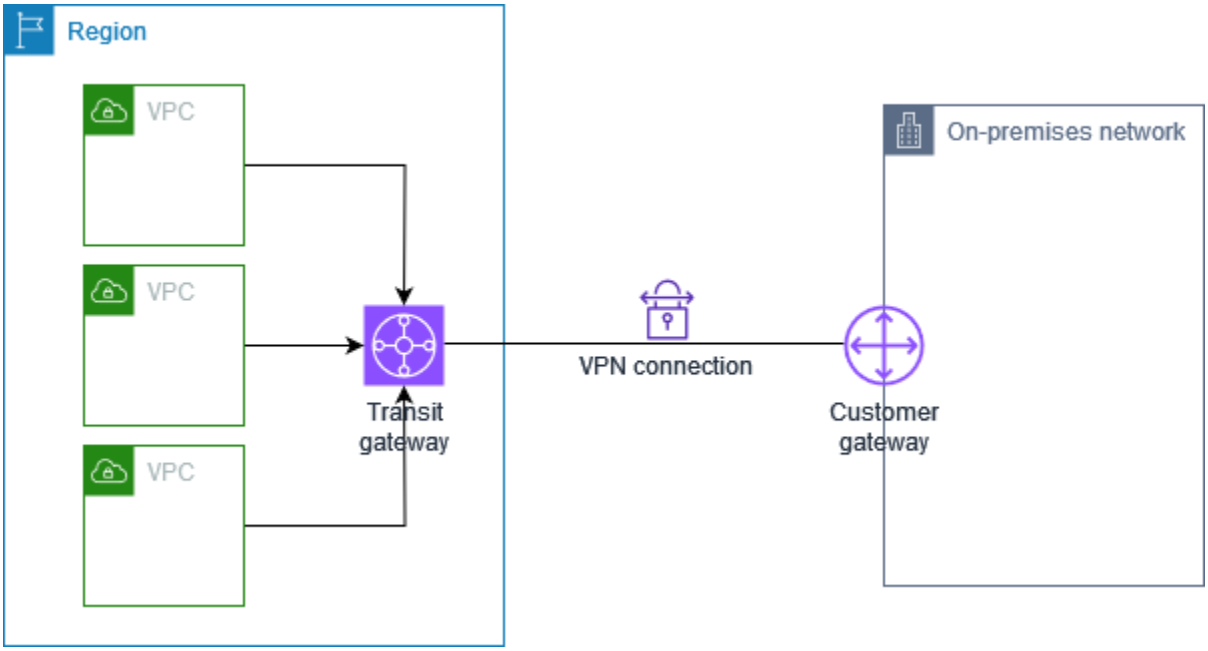
Al crear una gateway privada virtual, puede especificar el número de sistema autónomo (ASN) privado en el lado de Amazon de la gateway. Si no especifica un ASN, la gateway privada virtual se

crea con el ASN predeterminado (64 512). No se puede cambiar el ASN una vez que ha creado la gateway privada virtual. Para comprobar el ASN de su puerta de enlace privada virtual, consulte sus detalles en la página Puertas de enlace privadas virtuales de la consola de Amazon VPC o utilice el comando de AWS CLI describe-vpn-gateways.

Puerta de enlace de tránsito

Un puerta de enlace de tránsito es un hub de tránsito que puede utilizar para interconectar sus VPC y redes en las instalaciones. Para obtener más información, consulte Gateways de tránsito de Amazon VPC. Puede crear una conexión de Site-to-Site VPN como una asociación de la gateway de tránsito.

El siguiente diagrama muestra una conexión de VPN entre varias VPC y su red en las instalaciones utilizando una puerta de enlace de tránsito. La puerta de enlace de tránsito tiene tres conexiones de VPC y una conexión de VPN.



La conexión de Site-to-Site VPN de una gateway de tránsito puede admitir el tráfico IPv4 o IPv6 dentro de los túneles de VPN. Para obtener más información, consulte Tráfico IPv4 e IPv6.

Puede modificar la gateway de destino de una conexión de Site-to-Site VPN entre una gateway privada virtual y una gateway de tránsito. Para obtener más información, consulte the section called “Modificación de la puerta de enlace de destino de una conexión de VPN”.

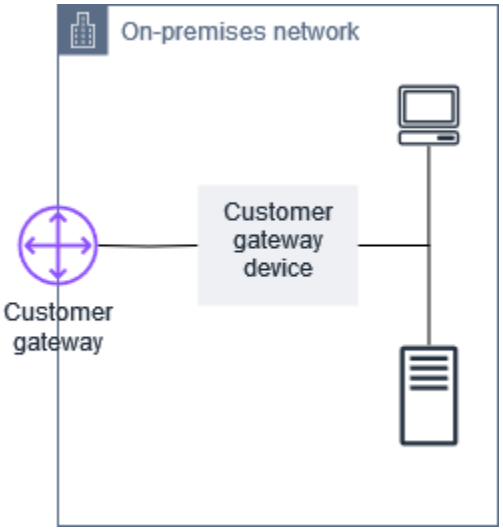
Dispositivo de gateway de cliente

Un dispositivo de gateway de cliente es un dispositivo físico o una aplicación de software que se encuentra en su extremo de la conexión de Site-to-Site VPN. Puede configurar el dispositivo para que funcione con la conexión de Site-to-Site VPN. Para obtener más información, consulte Su dispositivo de gateway de cliente.

De forma predeterminada, el dispositivo de gateway de cliente debe mostrar los túneles de la conexión de Site-to-Site VPN generando tráfico e iniciando el proceso de negociación de Intercambio de claves de Internet (IKE). Puede configurar la conexión de Site-to-Site VPN para especificar que AWS debe iniciar el proceso de negociación de IKE en su lugar. Para obtener más información, consulte Opciones de inicio del túnel de Site-to-Site VPN.

Gateway de cliente

Una gateway del cliente es un recurso que se crea en AWS y que representa el dispositivo de la gateway del cliente en la red local. Cuando crea una gateway del cliente, proporciona información sobre el dispositivo a AWS. Para obtener más información, consulte the section called “Opciones de gateway de cliente”.

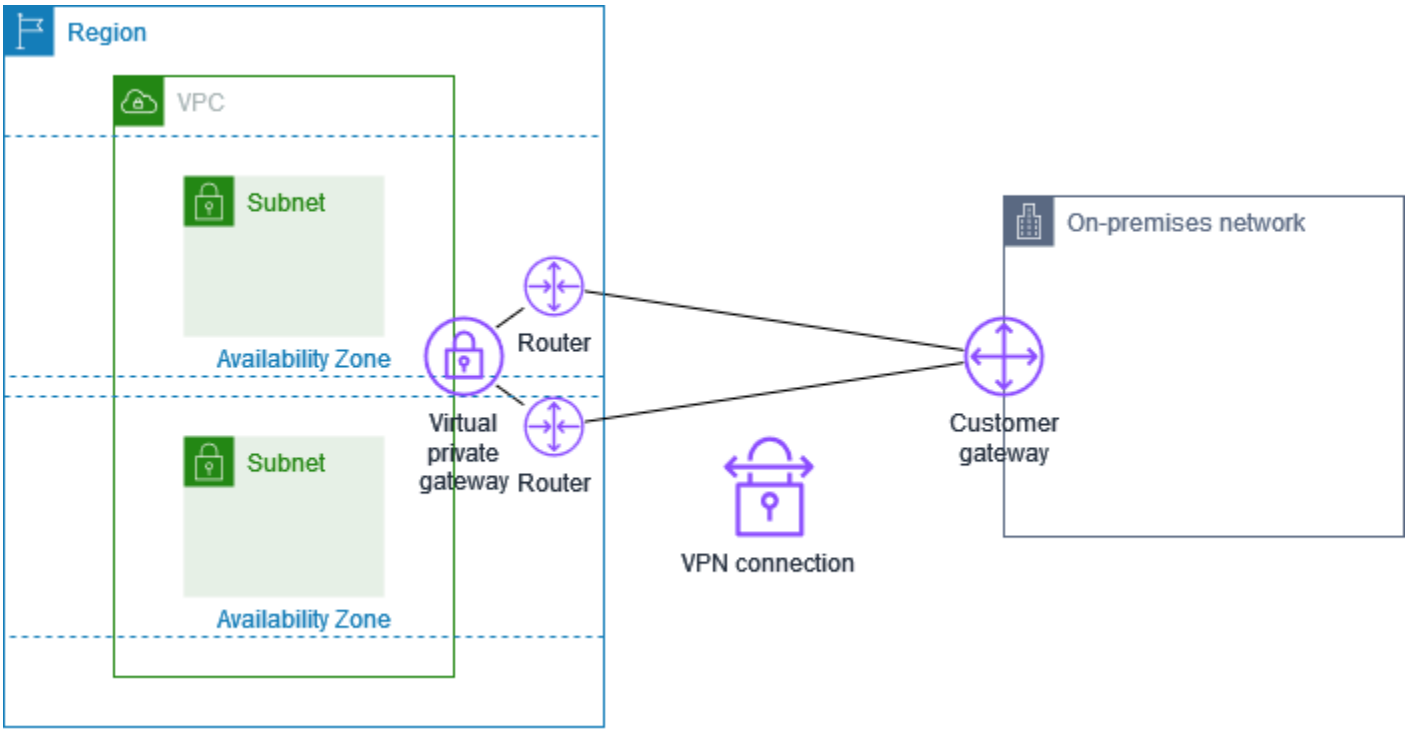


Para utilizar Amazon VPC con una conexión de Site-to-Site VPN, usted o su administrador de red también deberán configurar la aplicación o el dispositivo de gateway de cliente en la red remota. Cuando crea la conexión de Site-to-Site VPN, la información de configuración necesaria se la proporcionamos nosotros, mientras que es el administrador de red el que normalmente lleva a cabo esta configuración. Para obtener información sobre los requisitos y la configuración de la gateway de cliente, consulte Su dispositivo de gateway de cliente.

Opciones del túnel de una conexión de Site-to-Site VPN

Utilice una conexión de Site-to-Site VPN para conectar la red remota a una VPC. Cada conexión Site-to-Site VPN tiene dos túneles y cada uno utiliza una dirección IP pública única. Es importante configurar ambos túneles para la redundancia. Cuando un túnel deja de estar disponible (por ejemplo, por tareas de mantenimiento), el tráfico de red se direcciona automáticamente al túnel disponible de esa conexión de Site-to-Site VPN específica.

El siguiente diagrama muestra los dos túneles de la conexión de VPN. Cada túnel termina en una zona de disponibilidad diferente para aumentar la disponibilidad. El tráfico que sale desde la red de las instalaciones a AWS utiliza ambos túneles. El tráfico que sale desde AWS a la red en las instalaciones prefiere uno de los túneles, pero puede conmutarse por error automáticamente al otro túnel si se produce un error en el lado de AWS.



Cuando cree una conexión de Site-to-Site VPN, tendrá que descargar un archivo de configuración específico para su dispositivo de gateway de cliente, que contendrá información para configurar el dispositivo y también cada túnel. Si lo desea, puede especificar usted mismo algunas de las opciones del túnel al crear la conexión de Site-to-Site VPN. De lo contrario, AWS proporciona los valores predeterminados.

> **Note**
>
> Los puntos de enlace de túnel de Site-to-Site VPN evalúan las propuestas de la gateway del cliente comenzando por el valor configurado más bajo de la siguiente lista, independientemente del orden de la propuesta de la gateway del cliente. Puede utilizar el comando `modify-vpn-connection-options` para restringir la lista de opciones que aceptarán los puntos de enlace de AWS. Para obtener más información, consulte lasopciones de modify-vpn-connection en la Referencia de la línea de comandos de Amazon EC2.

A continuación, se muestran las opciones de túnel que puede configurar.

Tiempo de espera de detección de pares muertos (DPD)

El número de segundos después del cual se produce un tiempo de espera de DPD. Un tiempo de espera de DPD de 40 segundos significa que el punto de conexión de la VPN considerará que el par está muerto 30 segundos después del primer keep-alive erróneo. Puede especificar 30 o un valor superior.

Predeterminado: 40

Acción de tiempo de espera de DPD

La acción que se debe realizar después de que se agote el tiempo de espera de detección de pares muertos (DPD). Puede especificar lo siguiente:

- `Clear`: finalice la sesión de IKE cuando se cumpla el tiempo de espera de DPD (detenga el túnel y borre las rutas)
- `None`: no realice ninguna acción cuando se cumpla el tiempo de espera de DPD
- `Restart`: reinicie la sesión de IKE cuando se cumpla el tiempo de espera de DPD

Para obtener más información, consulte Opciones de inicio del túnel de Site-to-Site VPN.

Valor predeterminado: `Clear`

Opciones de registro de VPN

Con los registros de Site-to-Site VPN, puede obtener acceso a detalles sobre el establecimiento del túnel de seguridad IP (IPsec), las negociaciones de intercambio de claves de Internet (IKE) y los mensajes del protocolo de detección de pares muertos (DPD).

Para obtener más información, consulte AWS Site-to-Site VPN registros.

Formatos de registro disponibles: `json`, `text`

Versiones de IKE

Las versiones de IKE permitidas para el túnel de VPN. Puede especificar uno o varios valores predeterminados.

Predeterminado: `ikev1`, `ikev2`

Túnel interior de CIDR IPv4

Intervalo de direcciones IPv4 internas (internas) para el túnel VPN. Pude especificar un bloque de CIDR de tamaño /30 desde el rango `169.254.0.0/16`. El bloque de CIDR debe ser único en todas las conexiones de Site-to-Site VPN que utilicen la misma gateway privada virtual.

> **Note**
>
> El bloque de CIDR no tiene por qué ser único en todas las conexiones de una puerta de enlace de tránsito. En caso de no ser único, puede crear un conflicto en la puerta de enlace de cliente. Tenga cuidado cuando vuelva a utilizar el mismo bloque de CIDR en varias conexiones de Site-to-Site VPN de una puerta de enlace de tránsito.

Los siguientes bloques de CIDR están reservados y no se pueden utilizar:

- `169.254.0.0/30`
- `169.254.1.0/30`
- `169.254.2.0/30`
- `169.254.3.0/30`
- `169.254.4.0/30`
- `169.254.5.0/30`
- `169.254.169.252/30`

Predeterminado: un bloque de CIDR IPv4 de tamaño /30 del intervalo `169.254.0.0/16`.

Túnel interior de CIDR IPv6

(Sólo conexiones VPN IPv6) Intervalo de direcciones IPv6 internas (internas) para el túnel VPN. Puede especificar un bloque CIDR de tamaño /126 desde el rango local `fd00::/8`. El bloque de

CIDR debe ser único en todas las conexiones de Site-to-Site VPN que utilicen la misma gateway de tránsito.

Predeterminado: un bloque de CIDR IPv6 de tamaño /126 del intervalo local `fd00::/8`.

CIDR de red IPv4 local

(Sólo conexión VPN IPv4) Intervalo CIDR IPv4 en el lado de la gateway del cliente (en las instalaciones) que puede comunicarse a través de los túneles VPN.

Valor predeterminado: 0.0.0.0/0

CIDR de red IPv4 remota

(Solo conexión de VPN IPv4) El rango CIDR IPv4 en el lado de AWS que puede comunicarse a través de los túneles de VPN.

Valor predeterminado: 0.0.0.0/0

CIDR de red IPv6 local

(Sólo conexión VPN IPv6) Intervalo CIDR IPv6 en el lado de la gateway del cliente (local) que puede comunicarse a través de los túneles VPN.

Predeterminado:: :/0

CIDR de red IPv6 remota

(Solo conexión de VPN IPv6) El rango CIDR IPv6 en el lado de AWS que puede comunicarse a través de los túneles de VPN.

Predeterminado:: :/0

Números de grupo Diffie-Hellman (DH) de fase 1

Los números del grupo DH permitidos para el túnel de VPN para las negociaciones IKE de la fase 1. Puede especificar uno o varios valores predeterminados.

Predeterminado: 2, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24

Números de grupo Diffie-Hellman (DH) de fase 2

Los números del grupo DH permitidos para el túnel de VPN para las negociaciones IKE de la fase 2. Puede especificar uno o varios valores predeterminados.

Predeterminado: 2, 5, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24

Algoritmos de cifrado de la fase 1

Los algoritmos de cifrado permitidos para el túnel VPN para las negociaciones IKE de fase 1. Puede especificar uno o varios valores predeterminados.

Predeterminado: AES128, AES256, AES128-GCM-16, AES256-GCM-16

Algoritmos de cifrado de la fase 2

Los algoritmos de cifrado permitidos para el túnel VPN para las negociaciones IKE de fase 2. Puede especificar uno o varios valores predeterminados.

Predeterminado: AES128, AES256, AES128-GCM-16, AES256-GCM-16

Algoritmos de integridad de la fase 1

Los algoritmos de integridad permitidos para el túnel VPN para las negociaciones IKE de fase 1. Puede especificar uno o varios valores predeterminados.

Predeterminado: SHA-1, SHA2-256, SHA2-384, SHA2-512

Algoritmos de integridad de la fase 2

Los algoritmos de integridad permitidos para el túnel VPN para las negociaciones IKE de fase 2. Puede especificar uno o varios valores predeterminados.

Predeterminado: SHA-1, SHA2-256, SHA2-384, SHA2-512

Vida útil de la fase 1

> **Note**
>
> AWS inicia los cambios de clave con los valores de tiempo establecidos en los campos de vida útil de la fase 1 y 2. Si tales campos de vida útil son diferentes a los valores de protocolo de enlace negociados, esto puede interrumpir la conectividad del túnel.

La duración en segundos de la fase 1 de las negociaciones IKE. Puede especificar un número comprendido entre 900 y 28 800.

Predeterminado: 28 800 (8 horas)

Vida útil de la fase 2

> **Note**
>
> AWS inicia los cambios de clave con los valores de tiempo establecidos en los campos de vida útil de la fase 1 y 2. Si tales campos de vida útil son diferentes a los valores de protocolo de enlace negociados, esto puede interrumpir la conectividad del túnel.

La duración en segundos de la fase 2 de las negociaciones IKE. Puede especificar un número comprendido entre 900 y 3600. El número que especifique debe ser inferior al número de segundos para la duración de la fase 1.

Predeterminado: 3600 (1 hora)

Clave previamente compartida (PSK)

La clave previamente compartida (PSK) para establecer la asociación de seguridad de intercambio de claves de Internet (IKE) inicial entre la puerta de enlace de destino y la puerta de enlace de cliente.

La PSK debe tener un mínimo de 8 caracteres y un máximo de 64 y no puede comenzar por cero (0). Se permiten caracteres alfanuméricos, puntos (.) y guiones bajos (_).

Predeterminado: una cadena alfanumérica de 32 caracteres.

Difusión de cambio de clave

El porcentaje de la ventana de cambio de clave (determinado por el tiempo del margen de cambio de clave) dentro del cual se selecciona aleatoriamente el tiempo de cambio de clave.

Puede especificar un valor porcentual entre 0 y 100.

Predeterminado: 100

Tiempo de margen de cambio de clave

El tiempo de margen en segundos antes de que venza la duración de la fase 1 y 2, durante el cual el lado de AWS de la conexión VPN realiza un cambio de clave de IKE.

Puede especificar un número comprendido entre 60 y la mitad del valor de la duración de la fase 2.

El tiempo exacto de cambio de clave se selecciona aleatoriamente en función del valor de la difusión del cambio de clave.

Predeterminado: 270 (4,5 minutos)

Tamaño de paquetes del período de reproducción

El número de paquetes de un período de reproducción de IKE.

Puede especificar un valor comprendido entre 64 y 2048.

Predeterminado: 1024

Acción de inicio

La acción que se debe realizar al establecer el túnel para una conexión de VPN. Puede especificar lo siguiente:

- `Start`: AWS inicia la negociación de IKE para mostrar el túnel. Solo se admite si la gateway del cliente está configurada con una dirección IP.
- `Add`: su dispositivo de gateway de cliente debe iniciar la negociación de IKE para mostrar el túnel.

Para obtener más información, consulte Opciones de inicio del túnel de Site-to-Site VPN.

Valor predeterminado: `Add`

Control del ciclo de vida del punto de conexión del túnel

El control del ciclo de vida del punto de conexión del túnel permite controlar el programa de sustituciones de los puntos de conexión.

Para obtener más información, consulte Control del ciclo de vida del punto de conexión del túnel.

Valor predeterminado: `Off`

Puede especificar las opciones del túnel al crear una conexión de Site-to-Site VPN. También puede o modificar las opciones de túnel de una conexión de VPN existente. Para obtener más información, consulte los siguientes temas:

- Paso 5: Crear una conexión de VPN
- Modificar las opciones del túnel de Site-to-Site VPN

Opciones de autenticación de un túnel de Site-to-Site VPN

Puede utilizar claves compartidas previamente o certificados para autenticar los puntos de enlace del túnel de Site-to-Site VPN.

Claves previamente compartidas

Una clave previamente compartida es la opción de autenticación predeterminada.

Una clave previamente compartida es una opción que puede especificar al crear un túnel de Site-to-Site VPN.

Una clave previamente compartida es una cadena que se escribe al configurar el dispositivo de gateway de cliente. Si no especifica una cadena, generaremos una automáticamente para usted. Para obtener más información, consulte Su dispositivo de gateway de cliente.

Certificado privado de AWS Private Certificate Authority

Si no quiere utilizar claves previamente compartidas, puede utilizar un certificado privado de AWS Private Certificate Authority para autenticar la VPN.

Tiene que crear un certificado privado de una entidad emisora de certificados subordinada que use AWS Private Certificate Authority (Autoridad de certificación privada de AWS). Para firmar la CA subordinada de ACM, puede utilizar una CA raíz de ACM o una CA externa. Para obtener información sobre cómo crear un certificado privado, consulte la sección sobre Creación y administración de una CA privada en la Guía del usuario de AWS Private Certificate Authority .

Debe crear un rol vinculado al servicio para poder generar y utilizar el certificado en el lado de AWS del punto de conexión del túnel de Site-to-Site VPN. Para obtener más información, consulte the section called “Roles vinculados al servicio”.

Después de generar el certificado privado, especifique el certificado al crear la gateway de cliente y luego aplíquelo al dispositivo de gateway de cliente.

Si no especifica la dirección IP de su dispositivo de gateway de cliente, no verificaremos la dirección IP. Esta operación le permite trasladar el dispositivo de gateway de cliente a otra dirección IP sin tener que volver a configurar la conexión de VPN.

Opciones de inicio del túnel de Site-to-Site VPN

De forma predeterminada, el dispositivo de gateway de cliente debe mostrar los túneles de la conexión de Site-to-Site VPN generando tráfico e iniciando el proceso de negociación de Intercambio de claves de Internet (IKE). Puede configurar sus túneles VPN para especificar si, en su lugar, AWS debe iniciar o reiniciar el proceso de negociación de IKE.

Opciones de iniciación de IKE de túnel de VPN

Las siguientes opciones de iniciación de IKE están disponibles. Puede implementar una o ambas opciones en uno o ambos túneles de la conexión de Site-to-Site VPN. Consulte Opciones de túnel de VPN para obtener más información sobre estas y otras opciones de configuración del túnel.

- Acción de inicio: acción que se debe realizar al establecer el túnel de VPN para una conexión de VPN nueva o modificada. De forma predeterminada, el dispositivo de gateway de cliente inicia el proceso de negociación de IKE para mostrar el túnel. Puede AWS especificar que, en su lugar, se inicie el proceso de negociación de IKE.
- Acción de tiempo de espera de DPD: la acción que se debe realizar después de que se cumpla el tiempo de espera de detección de pares muertos (DPD). De forma predeterminada, la sesión de IKE se detiene, el túnel se desactiva y se eliminan las rutas. Puede especificar que AWS debe reiniciarse la sesión de IKE cuando se agote el tiempo de espera de DPD, o puede especificar que no se AWS debe realizar ninguna acción cuando se agote el tiempo de espera de DPD.

Reglas y limitaciones

Se aplican las siguientes reglas y limitaciones:

- Para iniciar la negociación del IKE, AWS necesita la dirección IP pública del dispositivo de puerta de enlace del cliente. Si configuró la autenticación basada en certificados para su conexión VPN y no especificó una dirección IP al crear el recurso de puerta de enlace de cliente AWS, debe crear una nueva puerta de enlace de cliente y especificar la dirección IP. A continuación, modifique la conexión de VPN y especifique la nueva gateway de cliente. Para obtener más información, consulte Cambio de la puerta de enlace de cliente para una conexión de Site-to-Site VPN.
- La iniciación por IKE (acción de inicio) desde el AWS lado de la conexión VPN solo se admite con IKEv2.
- Si se utiliza la iniciación IKE desde el AWS lado de la conexión VPN, no se incluye una configuración de tiempo de espera. Intentará establecer una conexión continuamente hasta que se

establezca una. Además, el AWS lado de la conexión VPN reiniciará la negociación de IKE cuando reciba un mensaje de eliminación de SA desde la pasarela del cliente.

- Si el dispositivo de gateway del cliente está detrás de un firewall u otro dispositivo que utilice la traducción de direcciones de red (NAT), debe tener una identidad (IDr) configurada. Para obtener más información acerca de IDr, consulte RFC 7296.

Si no configuras el inicio de IKE desde un AWS lado para tu túnel VPN y la conexión VPN pasa por un período de inactividad (normalmente 10 segundos, según la configuración), es posible que el túnel deje de funcionar. Para evitar este problema, utilice una herramienta de monitoreo de red para generar pings keepalive.

Uso de opciones de iniciación de túnel de VPN

Para obtener más información sobre cómo trabajar con las opciones de iniciación de túnel de VPN, consulte los temas siguientes:

- Para crear una nueva conexión de VPN y especificar las opciones de iniciación del túnel de VPN: Paso 5: Crear una conexión de VPN
- Para modificar las opciones de iniciación del túnel de VPN en una conexión de VPN existente: Modificar las opciones del túnel de Site-to-Site VPN

Sustitución de los puntos de enlace de un túnel de Site-to-Site VPN

Por motivos de redundancia, las conexiones de Site-to-Site VPN tienen dos túneles de VPN.
A veces, uno o ambos puntos de enlace del túnel de VPN se sustituyen cuando AWS realiza actualizaciones del túnel o cuando usted modifica la conexión de VPN. Durante la sustitución de un punto de enlace del túnel, la conectividad a través del túnel podría verse interrumpida mientras se aprovisiona el nuevo punto de enlace.

Temas

- Sustituciones de puntos de conexión iniciadas por el cliente
- Sustituciones de puntos de conexión administrados por AWS
- Control del ciclo de vida del punto de conexión del túnel

Sustituciones de puntos de conexión iniciadas por el cliente

Cuando se modifican los siguientes componentes de una conexión de VPN, se reemplazan uno o ambos puntos de enlace del túnel.

Modificación	Acción de la API	Impacto en el túnel
Modificación de la gateway de destino de la conexión de VPN	ModifyVpnConnection	Los dos túneles dejan de estar disponibles mientras se aprovisionan los nuevos puntos de enlace del túnel.
Cambio de la gateway de cliente de la conexión de VPN	ModifyVpnConnection	Los dos túneles dejan de estar disponibles mientras se aprovisionan los nuevos puntos de enlace del túnel.
Modificación de las opciones de la conexión de VPN	ModifyVpnConnectionOptions	Los dos túneles dejan de estar disponibles mientras se aprovisionan los nuevos puntos de enlace del túnel.
Modificación de las opciones del túnel de VPN	ModifyVpnTunnelOptions	El túnel modificado no está disponible durante la actualización.

Sustituciones de puntos de conexión administrados por AWS

AWS Site-to-Site VPN es un servicio administrado que aplica actualizaciones periódicas a los puntos de enlace del túnel de VPN. Estas actualizaciones se producen por una variedad de razones, entre las que se incluyen las siguientes:

- Al aplicar actualizaciones generales, como parches, mejoras de resiliencia y otras mejoras
- Al retirar el hardware subyacente
- Cuando las tareas de monitoreo automatizadas determinan que un punto de enlace del túnel de VPN no está en buen estado

AWS aplica las actualizaciones de punto de conexión de túnel a un túnel de la conexión VPN a la vez. Durante una actualización del punto de conexión del túnel, es posible que la conexión de VPN experimente una breve pérdida de redundancia. Por tanto, es importante configurar los dos túneles de la conexión de VPN para que ofrezcan una alta disponibilidad.

Control del ciclo de vida del punto de conexión del túnel

El control del ciclo de vida del punto de conexión del túnel permite controlar el programa de sustituciones de los puntos de conexión y puede ayudar a minimizar las interrupciones de conectividad durante las sustituciones del punto de conexión del túnel administradas por AWS. Con esta característica, tiene la opción de elegir aceptar las actualizaciones administradas por AWS de los puntos de conexión del túnel en el momento que mejor le convenga a su empresa. Utilice esta característica si tiene necesidades empresariales a corto plazo o si solo puede admitir un único túnel por conexión VPN.

> **Note**
>
> En raras circunstancias, AWS podría aplicar actualizaciones críticas a los puntos de conexión del túnel de forma inmediata, aunque la característica de control del ciclo de vida del punto de conexión del túnel esté habilitada.

Temas

Cómo funciona el control del ciclo de vida del punto de conexión del túnel

Active la característica de control del ciclo de vida del punto de conexión del túnel para túneles individuales dentro de una conexión VPN. Se puede habilitar en el momento de la creación de la VPN o modificando las opciones de túnel para una conexión VPN existente.

Una vez activado el control del ciclo de vida del punto de conexión del túnel, obtendrá una visibilidad adicional de los próximos eventos de mantenimiento del túnel de dos maneras:

- Recibirá notificaciones de AWS Health sobre las próximas sustituciones de los puntos de conexión del túnel.
- El estado del mantenimiento pendiente, junto con las marcas temporales Mantenimiento automático aplicado después y Último mantenimiento aplicado, se pueden ver en la AWS Management Console o mediante el comando get-vpn-tunnel-replacement-status de la AWS CLI.

Cuando esté disponible el mantenimiento de un punto de conexión de túnel, tendrá la oportunidad de aceptar la actualización en el momento que más le convenga, antes de la marca temporal Mantenimiento automático aplicado después proporcionada.

Si no aplica las actualizaciones antes de la fecha de Mantenimiento automático aplicado después, AWS realizará automáticamente la sustitución del punto de conexión del túnel poco después, como parte del ciclo de actualización de mantenimiento normal.

Habilitar el control del ciclo de vida del punto de conexión del túnel

Puede habilitar esta característica mediante AWS Management Console o AWS CLI.

> **Note**
>
> De forma predeterminada, al activar la característica para una conexión VPN existente, se iniciará la sustitución del punto de conexión del túnel al mismo tiempo. Si desea activar la característica, pero no iniciar inmediatamente la sustitución del punto de conexión del túnel, puede utilizar la opción omitir la sustitución del túnel.

Existing VPN connection

Los siguientes pasos demuestran cómo habilitar el control del ciclo de vida del punto de conexión del túnel en una conexión VPN existente.

Para habilitar el control del ciclo de vida del punto de conexión del túnel con la AWS Management Console

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.

2. En el panel de navegación izquierdo, elija Conexiones de Site-to-Site VPN.
3. Seleccione la conexión adecuada en Conexiones de VPN.
4. Elija Acciones y, a continuación, Modificar opciones de túnel de VPN.
5. Seleccione el túnel específico que desea modificar; para ello, elija la dirección IP fuera del túnel de VPN adecuada.
6. En Control del ciclo de vida del punto de conexión del túnel, seleccione la casilla Habilitar.
7. (Opcional) Seleccione Omitir la sustitución del túnel.
8. Elija Guardar cambios.

Para habilitar el control del ciclo de vida del punto de conexión del túnel con la AWS CLI

Utilice el comando modify-vpn-tunnel-options para activar el control del ciclo de vida del punto de conexión del túnel.

New VPN connection

Los siguientes pasos demuestran cómo habilitar el control del ciclo de vida del punto de conexión del túnel durante la creación de una nueva conexión de VPN.

Para habilitar el control del ciclo de vida del punto de conexión del túnel durante la creación de una nueva conexión de VPN con la AWS Management Console

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Site-to-Site VPN Connections (Conexiones de Site-to-Site VPN).
3. Elija Create VPN Connection (Crear conexión VPN).
4. En las secciones de opciones del Túnel 1 y opciones del Túnel 2, en Control del ciclo de vida del punto de conexión del túnel, seleccione Habilitar.
5. Elija Create VPN Connection (Crear conexión de VPN).

Para habilitar el control del ciclo de vida del punto de conexión del túnel durante la creación de una nueva conexión de VPN con la AWS CLI

Utilice el comando create-vpn-connection para activar el control del ciclo de vida del punto de conexión del túnel.

Comprobar si el control del ciclo de vida del punto de conexión del túnel está activado

Puede comprobar si el control del ciclo de vida del punto de conexión del túnel está habilitado en un túnel de VPN existente mediante la AWS Management Console o la CLI.

Para comprobar si el control del ciclo de vida del punto de conexión del túnel está habilitado con la AWS Management Console

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación izquierdo, elija Conexiones de Site-to-Site VPN.
3. Seleccione la conexión adecuada en Conexiones de VPN.
4. Seleccione la pestaña Detalles del túnel.
5. En los detalles del túnel, busque Control del ciclo de vida del punto de conexión del túnel, que indicará si la característica está Habilitada o Desactivada.

Para comprobar si el control del ciclo de vida del punto de conexión del túnel está habilitado con la AWS CLI

Utilice el comando describe-vpn-connections para comprobar si el control del ciclo de vida del punto de conexión del túnel está activado.

Comprobar si hay actualizaciones disponibles

Tras habilitar la característica de control del ciclo de vida del punto de conexión del túnel, puede consultar si una actualización de mantenimiento está disponible para la conexión de VPN con la AWS Management Console o la CLI.

Para comprobar si hay actualizaciones disponibles mediante la AWS Management Console

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación izquierdo, elija Conexiones de Site-to-Site VPN.
3. Seleccione la conexión adecuada en Conexiones de VPN.
4. Seleccione la pestaña Detalles del túnel.
5. Compruebe la columna Mantenimiento pendiente. El estado será Disponible o Ninguno.

Para comprobar si hay actualizaciones disponibles mediante la AWS CLI

Utilice el comando get-vpn-tunnel-replacement-status para comprobar si hay actualizaciones disponibles.

Aceptar una actualización de mantenimiento

Cuando haya una actualización de mantenimiento disponible, puede aceptarla mediante la AWS Management Console o la CLI.

Para aceptar una actualización de mantenimiento disponible con la AWS Management Console

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación izquierdo, elija Conexiones de Site-to-Site VPN.
3. Seleccione la conexión adecuada en Conexiones de VPN.
4. Elija Acciones y, a continuación, Sustituir túnel de VPN.
5. Seleccione el túnel específico que desea sustituir; para ello, elija la dirección IP fuera del túnel de VPN adecuada.
6. Elija Replace (Reemplazar).

Para aceptar una actualización de mantenimiento disponible con la AWS CLI

Utilice el comando replace-vpn-tunnel para aceptar una actualización de mantenimiento disponible.

Desactivar el control del ciclo de vida del punto de conexión del túnel

Si ya no desea utilizar la característica de control del ciclo de vida del punto de conexión del túnel, puede desactivarla mediante la AWS Management Console o la AWS CLI. Cuando desactive esta característica, AWS implementará automáticamente actualizaciones de mantenimiento de forma periódica y es posible que estas actualizaciones se realicen durante el horario laboral. Para evitar el impacto empresarial, le recomendamos encarecidamente que configure los túneles de la conexión de VPN para una disponibilidad alta.

> **Note**
>
> Mientras haya un mantenimiento pendiente disponible, no puede especificar la opción Omitir la sustitución del túnel mientras se desactiva la característica. Siempre puede desactivar la característica sin utilizar la opción Omitir la sustitución del túnel, pero AWS implementará automáticamente las actualizaciones de mantenimiento pendientes disponibles al iniciar inmediatamente una sustitución del punto de conexión del túnel.

Para desactivar el control del ciclo de vida del punto de conexión del túnel con la AWS Management Console

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación izquierdo, elija Conexiones de Site-to-Site VPN.
3. Seleccione la conexión adecuada en Conexiones de VPN.
4. Elija Acciones y, a continuación, Modificar opciones de túnel de VPN.
5. Seleccione el túnel específico que desea modificar; para ello, elija la dirección IP fuera del túnel de VPN adecuada.
6. Para desactivar el control del ciclo de vida del punto de conexión del túnel, en Control del ciclo de vida del punto de conexión del túnel, desactive la casilla Habilitar.
7. (Opcional) Seleccione Omitir la sustitución del túnel.
8. Elija Guardar cambios.

Para desactivar el control del ciclo de vida del punto de conexión del túnel con la AWS CLI

Utilice el comando modify-vpn-tunnel-options para desactivar el control del ciclo de vida del punto de conexión del túnel.

Opciones de la gateway de cliente para su conexión de Site-to-Site VPN

La siguiente tabla describe la información que necesitará para crear un recurso de gateway de cliente en AWS.

Elemento	Descripción
(Opcional) Etiqueta de nombre.	Crea una etiqueta con una clave de "Nombre" y un valor que especifique.
(Solo direccionamiento dinámico) Número de sistema autónomo (ASN) para protocolo de gateway fronteriza (BGP) de la gateway de cliente.	Se admiten ASN en el rango de 1 a 4,294,967 ,295. Puede utilizar un ASN público existente asignado a su red, con excepción de lo siguiente: • 7224: reservado en todas las regiones

Elemento	Descripción
	• 9059: reservado en la región `eu-west-1` • 10124: reservado en la región `ap-northeast-1` • 17943: reservado en la región `ap-southeast-1` Si no tienes un ASN público, puedes usar un ASN privado entre 64 512 y 65 534 o entre 4 200 000 000 y 4 294 967 294. El ASN predeterminado es 65000. Consulte Opciones de direccionamiento de Site-to-Site VPN para obtener más información sobre el enrutamiento.
(Opcional) La dirección IP de la interfaz externa del dispositivo de puerta de enlace de cliente.	La dirección IP debe ser estática. Si su dispositivo de puerta de enlace de cliente está detrás de un dispositivo de traducción de direcciones de red (NAT), utilice la dirección IP de su dispositivo NAT. Además, asegúrese de que los paquetes UDP del puerto 500 (y del puerto 4500, si se utiliza NAT Traversal) puedan pasar entre la red y los puntos finales. AWS Site-to-Site VPN Consulte Reglas de firewall para obtener más información. No se requiere una dirección IP cuando se utiliza un certificado privado AWS Private Certificate Authority y una VPN pública.

Elemento	Descripción
(Opcional) Certificado privado de una CA subordinada que utilice AWS Certificate Manager (ACM).	Si quiere utilizar la autenticación basada en certificados, proporcione el ARN de un certifica do privado ACM para usarlo en el dispositivo de gateway de cliente. Cuando crea una gateway de cliente, puede configurarla para que utilice certificados privados de AWS Private Certificate Authority para autenticar Site-to-Site VPN. Si elige usar esta opción, crea una autoridad de certificación (CA) privada totalmente AWS alojada para uso interno de su organizac ión. Tanto el certificado de CA raíz como los certificados de CA subordinados los almacena y administra. Autoridad de certificación privada de AWS Antes de crear la pasarela de cliente, debe crear un certificado privado de una CA subordinada utilizando y AWS Private Certifica te Authority, a continuación, especificar el certificado al configurar la pasarela de cliente. Para obtener información sobre la creación de un certificado privado, consulte la sección de creación y administración de una CA privada en la Guía del usuario de AWS Private Certifica te Authority .
(Opcional) Dispositivo.	Un nombre para el dispositivo de puerta de enlace de cliente asociado con esta puerta de enlace de cliente.

Conexiones de Site-to-Site VPN aceleradas

Si lo desea, puede acelerar la conexión de Site-to-Site VPN. Una conexión VPN Site-to-Site acelerada (conexión VPN acelerada) se utiliza AWS Global Accelerator para enrutar el tráfico desde la red local a la ubicación AWS perimetral más cercana al dispositivo de puerta de enlace del cliente. AWS Global Accelerator optimiza la ruta de la red, utilizando la red AWS global libre de congestión para dirigir el tráfico al punto final que proporciona el mejor rendimiento de las aplicaciones (para obtener más información, consulte). AWS Global Accelerator Puede utilizar una conexión de VPN acelerada para evitar las interrupciones en la red que podrían producirse cuando el tráfico se direcciona a través del Internet público.

Cuando usted crea una conexión de VPN acelerada, nosotros creamos y administramos dos aceleradores en su nombre, uno para cada túnel de VPN. No puede ver ni administrar estos aceleradores usted mismo mediante la consola o las AWS Global Accelerator API.

Para obtener información sobre las AWS regiones que admiten conexiones VPN aceleradas, consulte las preguntas frecuentes sobre VPN AWS aceleradas de Site-to-Site.

Habilitación de la aceleración

De forma predeterminada, cuando se crea una conexión de Site-to-Site VPN, la aceleración está desactivada. Si lo desea, puede activarla al realizar una nueva conexión de Site-to-Site VPN en una gateway de tránsito. Para obtener más información y ver los pasos, consulte Creación de una asociación de VPN de puerta de enlace de tránsito.

Las conexiones de VPN aceleradas utilizan un grupo independiente de direcciones IP para las direcciones IP del punto de enlace del túnel. Las direcciones IP de los dos túneles de VPN se seleccionan en dos zonas de red distintas.

Reglas y restricciones

Para utilizar una conexión de VPN acelerada, se aplican las siguientes reglas:

- La aceleración solo se admite en las conexiones de Site-to-Site VPN que están asociadas a una gateway de tránsito. Las gateway privadas virtuales no admiten conexiones de VPN aceleradas.
- No se puede usar una conexión VPN acelerada de sitio a sitio con una AWS Direct Connect interfaz virtual pública.
- No se puede activar ni desactivar la aceleración para una conexión VPN de sitio a sitio existente. En su lugar, puede crear una nueva conexión VPN de sitio a sitio con aceleración activada o

desactivada según sea necesario. A continuación, puede configurar el dispositivo de gateway de cliente para que utilice la nueva conexión de Site-to-Site VPN y elimine la anterior.

- Se requiere NAT-Traversal (NAT-T) para una conexión de VPN acelerada y está habilitado de forma predeterminada. Si ha descargado un archivo de configuración de la consola de Amazon VPC, compruebe la configuración de NAT-T y ajústela si es necesario.
- La negociación de IKE para los túneles VPN acelerados debe iniciarse desde el dispositivo de puerta de enlace del cliente. Las dos opciones de túnel que afectan a este comportamiento son `Startup Action` y `DPD Timeout Action`. Para obtener más información, consulte Opciones de túnel de VPN y Opciones de iniciación de túnel de VPN.
- Es posible que las conexiones VPN de sitio a sitio que utilizan la autenticación basada en certificados no sean compatibles AWS Global Accelerator, debido a la limitada compatibilidad con la fragmentación de paquetes en Global Accelerator. Para obtener más información, consulte Cómo funciona AWS Global Accelerator. Si necesita una conexión de VPN acelerada que utilice autenticación basada en certificados, el dispositivo de la gateway del cliente debe admitir la fragmentación de IKE. De lo contrario, no habilite su VPN para la aceleración.

Opciones de direccionamiento de Site-to-Site VPN

Cuando cree una conexión de Site-to-Site VPN, debe hacer lo siguiente:

- Especifique el tipo de direccionamiento que va a usar (estático o dinámico)
- Actualice la tabla de enrutamiento de la subred

No hay ninguna cuota en el número de rutas que puede agregar a una tabla de enrutamiento. Para obtener más información, consulte la sección Tablas de ruteo del artículo Cuotas de Amazon VPC en la Guía del usuario de Amazon VPC.

Temas

- Direccionamiento estático y dinámico
- Tablas de enrutamiento y prioridad de rutas de VPN
- Enrutamiento durante las actualizaciones de punto de enlace del túnel de VPN
- Tráfico IPv4 e IPv6

Direccionamiento estático y dinámico

El tipo de enrutamiento seleccionado puede depender del fabricante y el modelo de su dispositivo de gateway de cliente. Si el dispositivo de gateway de cliente admite el protocolo de Número de sistema autónomo (ASN), especifique el direccionamiento dinámico al configurar la conexión de Site-to-Site VPN. Si el dispositivo de gateway de cliente no admite BGP, especifique un enrutamiento estático.

Si utiliza un dispositivo que admite publicidad de ASN, no será necesario especificar ninguna ruta estática en la conexión de Site-to-Site VPN, ya que el dispositivo utiliza ASN para anunciar sus rutas a la gateway privada virtual. Si utiliza un dispositivo que no admite publicidad BGP, debe seleccionar el enrutamiento estático y escribir las rutas (prefijos IP) de su red que deben comunicarse a la gateway privada virtual.

Se recomienda utilizar dispositivos que admitan BGP, siempre que estén disponibles, ya que el protocolo BGP ofrece comprobaciones de detección de conexión que pueden ayudar en la conmutación por error al segundo túnel de VPN en caso de error en el primero. Los dispositivos que no admiten BGP también pueden realizar comprobaciones de estado para ayudar en la conmutación por error al segundo túnel siempre que sea necesario.

Debe configurar el dispositivo de gateway de cliente para enrutar el tráfico desde la red local a la conexión de Site-to-Site VPN. La configuración depende del fabricante y el modelo del dispositivo. Para obtener más información, consulte Su dispositivo de gateway de cliente.

Tablas de enrutamiento y prioridad de rutas de VPN

Las tablas de enrutamiento determinan dónde se dirige el tráfico de red de la VPC. En la tabla de enrutamiento de la VPC, tiene que agregar una ruta para su red remota y especificar la gateway privada virtual como destino. Esto permite que el tráfico desde su VPC que está dirigido a su red remota se enrute a través de la gateway privada virtual y a través de uno de los túneles de VPN. Puede habilitar la propagación de rutas para que su tabla de ruteo propague automáticamente las rutas de red a la tabla.

Para determinar cómo dirigir tráfico, se utiliza la ruta más específica de su tabla de ruteo que coincida con el tráfico en cuestión (coincidencia del prefijo más largo). Si la tabla de enrutamiento tiene rutas superpuestas o coincidentes, se aplican las siguientes reglas:

- Si las rutas propagadas de una conexión Site-to-Site VPN o de una conexión AWS Direct Connect se solapan con la ruta local para su VPC, la ruta local es la más preferida aunque las rutas propagadas sean más específicas.

- Si las rutas propagadas desde una conexión de Site-to-Site VPN o AWS Direct Connect tienen el mismo bloque de CIDR de destino que otras rutas estáticas (cuando no sea posible aplicar la coincidencia de prefijo más largo), se dará prioridad a las rutas estáticas cuyos objetivos sean puertas de enlace de Internet, puertas de enlace privadas virtuales, interfaces de red, ID de instancia, una conexión de emparejamiento de VPC, puertas de enlace NAT, transit gateway o puntos de conexión de VPC de una puerta de enlace.

Por ejemplo, la siguiente tabla de enrutamiento tiene una ruta estática a una gateway de Internet y una ruta propagada a una gateway privada virtual. Ambas rutas tienen el destino `172.31.0.0/24`. En este caso, todo el tráfico con destino `172.31.0.0/24` se dirige a la gateway de Internet, ya que se trata de una ruta estática con prioridad sobre la ruta propagada.

Destino	Objetivo
10.0.0.0/16	Local
172.31.0.0/24	vgw-11223344556677889 (propagada)
172.31.0.0/24	igw-12345678901234567 (estática)

Solo los prefijos IP que la gateway privada virtual conozca, ya sea mediante anuncios de BGP o por introducción de una ruta estática, podrán recibir tráfico de su VPC. La gateway privada virtual no direcciona el tráfico cuyo destino no sea el mencionado en los anuncios de BGP recibidos, las entradas de ruta estática o los CIDR de VPC asociados. Las puerta de enlaces privadas virtuales no admiten el tráfico IPv6.

Cuando una gateway privada virtual recibe información de direccionamiento, usa la selección de rutas para determinar cómo debe dirigir el tráfico de las rutas. Se aplica la coincidencia de prefijos más larga si todos los puntos de conexión están en buen estado. El estado de un punto de conexión de túnel tiene prioridad sobre otros atributos de enrutamiento. Esta prioridad se aplica a las VPN en puertas de enlace privadas virtuales y puertas de enlace de tránsito. Si los prefijos son los mismos, la gateway privada virtual da prioridad a las rutas de la siguiente manera, desde la más preferida a la menos preferida:

- Rutas propagadas de BGP desde una conexión de AWS Direct Connect
- Rutas estáticas agregadas manualmente para una conexión de Site-to-Site VPN
- Rutas propagadas por ASN desde una conexión de Site-to-Site VPN

- En los prefijos que coinciden donde cada conexión de Site-to-Site VPN utiliza ASN, se compara la ruta AS PATH y se elige el prefijo con la ruta AS PATH más corta.

> **Note**
>
> AWS recomienda encarecidamente utilizar dispositivos de puerta de enlace de clientes que admiten enrutamiento asimétrico.
> Para los dispositivos de puerta de enlace de clientes que admiten enrutamiento asimétrico, no recomiendamos usar la ruta AS PATH prepending para asegurar que ambos túneles tengan la misma ruta AS PATH. De esta forma, podrá asegurarse de que el valor multi-exit discriminator (MED) que establecemos en un túnel durante las actualizaciones de puntos de enlace del túnel VPN se utilice para determinar la prioridad del túnel.
> En el caso de los dispositivos de puerta de enlace de cliente que no admiten enrutamiento asimétrico, puede utilizar AS PATH antepuesto y la preferencia local para dar prioridad a un túnel sobre el otro. Sin embargo, cuando la ruta de salida cambia, esto puede provocar una caída del tráfico.

- Cuando las rutas AS PATH tengan la misma longitud y si el primer AS de AS_SEQUENCE es el mismo en varias rutas, se comparan los multi-exit discriminators (MED). Se prefiere la ruta con el valor de MED más bajo.

La prioridad de ruta se ve afectada durante las actualizaciones del punto de enlace del túnel de la VPN.

En una conexión de Site-to-Site VPN, AWS selecciona uno de los dos túneles redundantes como ruta de salida principal. Esta selección puede cambiar en algún momento, por lo que le recomendamos que configure ambos túneles para una alta disponibilidad y que permita el enrutamiento asimétrico. El estado de un punto de conexión de túnel tiene prioridad sobre otros atributos de enrutamiento. Esta prioridad se aplica a las VPN en puertas de enlace privadas virtuales y puertas de enlace de tránsito.

En una gateway privada virtual, se seleccionará un solo túnel entre todas las conexiones de Site-to-Site VPN de la gateway. Para utilizar varios túneles, le recomendamos que considere las rutas múltiples de igual costo (ECMP), que se admiten en conexiones de Site-to-Site VPN de las gateways de tránsito. Para obtener más información, consulte Gateways de tránsito en Gateways de tránsito de Amazon VPC. ECMP no es puede utilizarse con las conexiones de Site-to-Site VPN de una gateway privada virtual.

En las conexiones de Site-to-Site VPN que utilizan ASN, el túnel principal se puede identificar mediante el valor multi-exit discriminator (MED). Recomendamos anunciar rutas ASN más específicas para influir en las decisiones de enrutamiento.

En las conexiones de Site-to-Site VPN que utilizan un direccionamiento estático, el túnel principal se puede identificar a través de estadísticas de tráfico o métricas.

Enrutamiento durante las actualizaciones de punto de enlace del túnel de VPN

Una conexión de Site-to-Site VPN consta de dos túneles de VPN entre un dispositivo de gateway de cliente y una gateway privada virtual o una gateway de tránsito. Recomendamos configurar ambos túneles para la redundancia. Cada cierto tiempo, AWS también lleva a cabo un mantenimiento rutinario en la conexión VPN, lo que podría desactivar uno de los dos túneles de la conexión VPN durante un breve periodo. Para obtener más información, consulte Notificaciones de sustitución de puntos de enlace de un túnel.

Cuando realizamos actualizaciones en un túnel de VPN, establecemos un valor más bajo de multi-exit discriminator (MED) saliente en el otro túnel. Si ha configurado su dispositivo de gateway de cliente para que utilice ambos túneles, la conexión de VPN utilizará el otro túnel (activo) durante el proceso de actualización del punto de enlace del túnel.

> **Note**
>
> Para asegurarse de que se prefiere el túnel activo con el MED inferior, asegúrese de que su dispositivo de gateway de cliente utilice los mismos valores de peso y preferencia local para ambos túneles (el peso y la preferencia local tienen mayor prioridad que el MED).

Tráfico IPv4 e IPv6

La conexión de Site-to-Site VPN de una gateway de tránsito puede admitir el tráfico IPv4 o IPv6 dentro de los túneles de VPN. De forma predeterminada, las conexiones de Site-to-Site VPN permiten el tráfico IPv4 dentro de los túneles de VPN. Puede configurar una nueva conexión de Site-to-Site VPN para admitir el tráfico IPv6 dentro de los túneles de VPN. A continuación, si la VPC y la red local están configuradas para el direccionamiento IPv6, puede enviar tráfico IPv6 a través de la conexión VPN.

Si activa IPv6 en los túneles de VPN de la conexión de Site-to-Site VPN, cada túnel tendrá dos bloques de CIDR. Uno es un bloque CIDR IPv4 de tamaño /30 y el otro es un bloque CIDR IPv6 de tamaño /126.

Se aplican las siguientes reglas:

- Las direcciones IPv6 solo son compatibles con las direcciones IP internas de los túneles de VPN. Las direcciones IP del túnel externo de los puntos de enlace de AWS son direcciones IPv4 y la dirección IP pública de la puerta de enlace de cliente debe ser una dirección IPv4.
- Las conexiones de Site-to-Site VPN de una gateway privada virtual no admiten IPv6.
- La compatibilidad con IPv6 no se puede activar en una conexión de Site-to-Site VPN existente.
- Las conexiones de Site-to-Site VPN no pueden admitir el tráfico IPv4 e IPv6 a la vez.

Para obtener más información acerca de cómo crear una conexión de VPN, consulte Paso 5: Crear una conexión de VPN.

Empezar con AWS Site-to-Site VPN

Utilice el siguiente procedimiento para configurar una AWS Site-to-Site VPN conexión. Durante la creación, especificará una puerta de enlace privada virtual, una puerta de enlace de tránsito o “No asociada” como tipo de puerta de enlace de destino. Si especificas «No asociada», puedes elegir el tipo de puerta de enlace de destino más adelante o puedes usarla como un adjunto de VPN para AWS Cloud WAN. Este tutorial le ayuda a crear una conexión de VPN mediante una puerta de enlace privada virtual. Supone que dispone de una VPC existente con una o varias subredes.

Para establecer una conexión de VPN mediante una puerta de enlace privada virtual, siga estos pasos:

Tareas

- Requisitos previos
- Paso 1: Crear una puerta de enlace de cliente
- Paso 2: Crear una puerta de enlace de destino
- Paso 3: Configuración del enrutamiento
- Paso 4: Actualizar el grupo de seguridad
- Paso 5: Crear una conexión de VPN
- Paso 6: Descargar el archivo de configuración
- Paso 7: Configurar el dispositivo de puerta de enlace de cliente

Tareas relacionadas

- Para crear una conexión VPN para AWS Cloud WAN, consultaCrea un adjunto de VPN para Cloud WAN AWS .
- Para crear una conexión de VPN en una puerta de enlace de tránsito, consulte Creación de una asociación de VPN de puerta de enlace de tránsito.

Requisitos previos

Necesita la siguiente información para establecer y configurar los componentes de una conexión de VPN.

Elemento	Información
Dispositivo de gateway de cliente	El dispositivo físico o de software del lado de la conexión de VPN. Necesita el proveedor (por ejemplo, Cisco Systems), la plataforma (por ejemplo, ISR Series Routers) y la versión de software (por ejemplo, IOS 12.4).
Puerta de enlace de cliente	Para crear el recurso de pasarela de clientes en AWS, necesita la siguiente información: • La dirección IP direccionable de Internet para la interfaz externa del dispositivo • El tipo de direccionamiento: estático o dinámico • Para el direccionamiento dinámico: el número de sistema autónomo (ASN) para protocolo de gateway fronteriza (BGP) • (Opcional) Certificado privado de AWS Private Certificate Authority para autenticar su VPN Para obtener más información, consulte Opciones de gateway de cliente.
(Opcional) El ASN del AWS lado de la sesión de BGP	Debe especificarse al crear una gateway privada virtual o una gateway de tránsito. Si no especifica un valor, se aplica el ASN predeterminado. Para obtener más información, consulte Gateway privada virtual.
conexión de VPN	Para crear una conexión de VPN, necesita la siguiente información: • Para el enrutamiento estático, los prefijos IP para la red privada.

Elemento	Información
	• (Opcional) Opciones de túnel para cada túnel VPN. Para obtener más información, consulte Opciones del túnel de una conexión de Site-to-Site VPN.

Paso 1: Crear una puerta de enlace de cliente

Una pasarela de cliente proporciona información AWS sobre su dispositivo o aplicación de software de pasarela de cliente. Para obtener más información, consulte Gateway de cliente.

Si planea usar un certificado privado para autenticar su VPN, cree un certificado privado de una CA subordinada utilizando. AWS Private Certificate Authority Para obtener información sobre la creación de un certificado privado, consulte la sección de creación y administración de una CA privada en la Guía del usuario de AWS Private Certificate Authority .

> **Note**
>
> Tiene que especificar una dirección IP o el nombre de recurso de Amazon del certificado privado.

Para crear una gateway de cliente con la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Puertas de enlace de cliente.
3. Elija Crear puerta de enlace de cliente.
4. (Opcional) En Name tag (Etiqueta de nombre), ingrese un nombre para la puerta de enlace de cliente. Esta acción creará una etiqueta con una clave de `Name` y el valor que especifique.
5. En BGP ASN, ingrese un número de sistema autónomo (ASN) para protocolo de puerta de enlace fronteriza (BGP) de la puerta de enlace de cliente.
6. (Opcional) En IP Address (Dirección IP), ingrese la dirección IP direccionable de Internet estática del dispositivo de puerta de enlace de cliente. Si el dispositivo de la puerta de enlace de cliente se encuentra detrás de un dispositivo NAT habilitado para NAT-T, utilice la dirección IP pública del dispositivo NAT.

7. (Opcional) Si desea utilizar un certificado privado, para Certificate ARN (ARN de certificado), elija el nombre de recurso de Amazon del certificado privado.
8. (Opcional) En Dispositivo, introduzca un nombre para el dispositivo de puerta de enlace de cliente asociado a esta puerta de enlace de cliente.
9. Elija Crear puerta de enlace de cliente.

Para crear una gateway de cliente mediante la línea de comando o API

- CreateCustomerGateway (API de consultas de Amazon EC2)
- create-customer-gateway (AWS CLI)
- New-EC2CustomerGateway (AWS Tools for Windows PowerShell)

Paso 2: Crear una puerta de enlace de destino

Para establecer una conexión VPN entre la VPC y la red local, debe crear una puerta de enlace de destino en el AWS lateral de la conexión. La gateway de destino puede ser una gateway privada virtual o una gateway de tránsito.

Creación de una gateway privada virtual

Al crear una puerta de enlace privada virtual, puede especificar un número de sistema autónomo (ASN) privado personalizado en el lado de Amazon de la puerta de enlace o usar el ASN predeterminado de Amazon. Este ASN tiene que ser distinto del ASN especificado para la puerta de enlace de cliente.

Después de crear una gateway privada virtual, debe adjuntarla a su VPC.

Para crear una gateway privada virtual y adjuntarla a su VPC.

1. En el panel de navegación, elija Puertas de enlace privadas virtuales.
2. Elija Create virtual private gateway (Crear puerta de enlace privada virtual).
3. (Opcional) En Etiqueta de nombre, introduzca un nombre para su puerta de enlace privada virtual. Esta acción creará una etiqueta con una clave de `Name` y el valor que especifique.
4. En Número de Sistema Autónomo (ASN), mantenga la selección predeterminada, ASN predeterminado de Amazon, para utilizar el ASN predeterminado de Amazon. De lo contrario, elija Custom ASN (ASN personalizado) y escriba un valor. Para un ASN de 16 bits ASN, el valor

debe estar dentro del rango de 64 512 a 65 534. Para un ASN de 32 bits ASN, el valor debe estar dentro del rango de 4 200 000 000 a 4 294 967 294.

5. Elija Create virtual private gateway (Crear puerta de enlace privada virtual).
6. Seleccione la puerta de enlace privada virtual que ha creado y, a continuación, elija Actions (Acciones), Attach to VPC (Adjuntar a VPC).
7. En VPC disponibles, elija su VPC y después elija Asociar a la VPC.

Para crear una gateway privada virtual mediante la línea de comando o API

- CreateVpnGateway (API de consultas de Amazon EC2)
- create-vpn-gateway (AWS CLI)
- New-EC2VpnGateway (AWS Tools for Windows PowerShell)

Para adjuntar una gateway privada virtual a una VPC mediante la línea de comando o API

- AttachVpnGateway (API de consultas de Amazon EC2)
- attach-vpn-gateway (AWS CLI)
- Add-EC2VpnGateway (AWS Tools for Windows PowerShell)

Crear una puerta de enlace de tránsito

Para obtener más información acerca de cómo crear una gateway de tránsito, consulte Gateways de tránsito en Gateways de tránsito de Amazon VPC.

Paso 3: Configuración del enrutamiento

Para permitir que las instancias de su VPC lleguen a la puerta de enlace de cliente, debe configurar la tabla de enrutamiento para incluir las rutas que utiliza la conexión de VPN y dirigirlas a la puerta de enlace privada virtual o a la puerta de enlace de tránsito.

(Gateway privada virtual) Habilitar la propagación de rutas en la tabla de enrutamiento

Puede desactivar la propagación de rutas para que la tabla de enrutamiento propague automáticamente las rutas de Site-to-Site VPN.

Para el direccionamiento estático, los prefijos de IP estática que especifique en la configuración de su VPN se propagarán a la tabla de ruteo cuando el estado de la conexión de VPN sea UP. Del mismo modo, para el direccionamiento dinámico, las rutas anunciadas mediante GBP de su gateway de cliente se propagarán a la tabla de ruteo cuando el estado de la conexión de VPN sea UP.

> **Note**
>
> Si la conexión se interrumpe pero la conexión de VPN permanece ACTIVA, las rutas propagadas que se encuentren en la tabla de enrutamiento no se eliminarán automáticamente. Téngalo en cuenta si, por ejemplo, desea que el tráfico se conmute por error a una ruta estática. En dicho caso, es posible que tenga que deshabilitar la propagación de rutas para eliminar las rutas propagadas.

Para habilitar la propagación de rutas utilizando la consola

1. En el panel de navegación, elija Tablas de enrutamiento.
2. Seleccione la tabla de enrutamiento asociada a la subred.
3. En la pestaña Propagación de rutas, elija Editar propagación de rutas. Seleccione la puerta de enlace privada virtual que creó en el procedimiento anterior y, a continuación, elija Guardar.

> **Note**
>
> Si no activa la propagación de rutas, deberá introducir manualmente las rutas estáticas que utiliza su conexión de VPN. Para ello, seleccione su tabla de ruteo, elija Routes, Edit. En Destination (Destino), agregue la ruta estática que se utiliza en la conexión de Site-to-Site VPN. Para Target, seleccione el ID de gateway privada virtual y elija Save.

Para deshabilitar la propagación de rutas utilizando la consola

1. En el panel de navegación, elija Tablas de enrutamiento.
2. Seleccione la tabla de enrutamiento asociada a la subred.
3. En la pestaña Propagación de rutas, elija Editar propagación de rutas. Desactive la casilla Propagar correspondiente a la puerta de enlace privada virtual.
4. Seleccione Guardar.

Para habilitar la propagación de rutas mediante la línea de comando o un API

- EnableVgwRoutePropagation(API de consultas de Amazon EC2)
- enable-vgw-route-propagation (AWS CLI)
- Enable-EC2VgwRoutePropagation (AWS Tools for Windows PowerShell)

Para deshabilitar la propagación de rutas mediante la línea de comando o un API

- DisableVgwRoutePropagation(API de consultas de Amazon EC2)
- disable-vgw-route-propagation (AWS CLI)
- Disable-EC2VgwRoutePropagation (AWS Tools for Windows PowerShell)

(Gateway de tránsito) Agregar una ruta a la tabla de enrutamiento

Si ha habilitado la propagación de la tabla de enrutamiento para la gateway de tránsito, las rutas de los datos adjuntos de VPN se propagarán a la tabla de rutas de la gateway de tránsito. Para obtener más información, consulte Direccionamiento en Gateways de tránsito de Amazon VPC.

Si asocia una VPC a la gateway de tránsito y desea habilitar recursos de la VPC para llegar a la gateway de cliente, tiene que agregar una ruta a la tabla de enrutamiento de subred para apuntar a la gateway de tránsito.

Para añadir una ruta a una tabla de ruteo de VPC

1. En el panel de navegación, elija Tablas de enrutamiento.
2. Elija la tabla de enrutamiento asociada a su VPC.
3. En la pestaña Rutas, elija Editar rutas.
4. Seleccione Añadir ruta.
5. En Destino, introduzca el intervalo de direcciones IP de destino. En Target (Destino), elija la gateway de tránsito.
6. Elija Guardar cambios.

Paso 4: Actualizar el grupo de seguridad

Para permitir el acceso a instancias en su VPC desde su red, debe actualizar las reglas del grupo de seguridad para habilitar acceso SSH, RDP e ICMP entrante.

Para agregar reglas a su grupo de seguridad con el fin de permitir el acceso

1. En el panel de navegación, elija Grupos de seguridad.
2. Seleccione el grupo de seguridad de las instancias de la VPC a las que quiere permitir el acceso.
3. En la pestaña Reglas de entrada, seleccione Editar reglas de entrada.
4. Agregue reglas que permitan el acceso SSH, RDP e ICMP entrante desde su red y, a continuación, elija Guardar reglas. Para obtener más información, consulte Trabajar con reglas de grupos de seguridad en la Guía del usuario de Amazon VPC.

Paso 5: Crear una conexión de VPN

Cree la conexión de VPN mediante la puerta de enlace de cliente en combinación con la puerta de enlace privada virtual o la puerta de enlace de tránsito que creó anteriormente.

Para crear una conexión de VPN

1. En el panel de navegación, elija Conexiones de Site-to-Site VPN.
2. Elija Create VPN Connection (Crear conexión VPN).
3. (Opcional) En Etiqueta de nombre, escriba el nombre de la conexión de VPN. Esta acción creará una etiqueta con una clave de `Name` y el valor que especifique.
4. En Target gateway type (Tipo de puerta de enlace de destino), elija Virtual private gateway (Puerta de enlace privada virtual) o Transit Gateway (Puerta de enlace de tránsito). A continuación, elija la gateway privada virtual o la gateway de tránsito que ha creado anteriormente.
5. En Puerta de enlace de cliente, seleccione Existente y, a continuación, elija la puerta de enlace de cliente que creó anteriormente en ID de puerta de enlace de cliente.
6. Seleccione una de las opciones de direccionamiento en función de si el dispositivo de gateway de cliente da soporte al protocolo de gateway fronteriza (BGP):

   - Si el dispositivo de gateway de cliente da soporte a BGP, elija Dynamic (requires BGP) (Dinámico [requiere BGP]).
   - Si el dispositivo de gateway de cliente no da soporte a BGP, elija Static (Estático). En Static IP Prefixes (Prefijos de IP estática), especifique cada prefijo de IP para la red privada de su conexión de VPN.

7. Si la puerta de enlace de destino es la puerta de enlace de tránsito, en Túnel dentro de la versión IP, especifique si los túneles de la VPN admiten tráfico IPv4 o IPv6. El tráfico IPv6 solo es compatible con conexiones VPN en una gateway de tránsito.
8. Si especificó IPv4 para la versión Túnel dentro de IP, si lo desea, puede especificar los rangos de CIDR de IPv4 para la puerta de enlace del cliente y los AWS lados que pueden comunicarse a través de los túneles de la VPN. El valor predeterminado es `0.0.0.0/0`.

   Si especificó IPv6 para la versión Túnel dentro de IP, si lo desea, puede especificar los rangos de CIDR de IPv6 para la puerta de enlace del cliente y los AWS lados que pueden comunicarse a través de los túneles VPN. El valor predeterminado para ambos rangos es `::/0`.
9. Para el tipo de dirección IP externa, mantenga la opción predeterminada, 4. PublicIpv
10. (Opcional) En Opciones de túnel, puede especificar la siguiente información para cada túnel:

    - Un bloque CIDR IPv4 de tamaño /30 desde el rango `169.254.0.0/16` para las direcciones IPv4 de túnel interior.
    - Si especificó IPv6 en Túnel dentro de la versión IP, un bloque de CIDR IPv6 /126 del intervalo `fd00::/8` para las direcciones IPv6 del túnel interior.
    - La clave previamente compartida de IKE (PSK). Las siguientes versiones son compatibles: IKEv1 o IKEv2.
    - Para editar las opciones avanzadas del túnel, seleccione Editar opciones de túnel. Para obtener más información, consulte Opciones de túnel de VPN.
11. Elija Create VPN Connection (Crear conexión VPN). Es posible que la conexión de VPN tarde unos minutos en crearse.

Para crear una conexión de VPN mediante la línea de comandos o la API

- CreateVpnConexión (API de consultas de Amazon EC2)
- create-vpn-connection (AWS CLI)
- New-EC2VpnConnection (AWS Tools for Windows PowerShell)

Paso 6: Descargar el archivo de configuración

Después de crear la conexión de VPN, podrá descargar un archivo de configuración de muestra que podrá utilizar para configurar el dispositivo de puerta de enlace de cliente.

> **Important**
>
> El archivo de configuración es solo un ejemplo y es posible que no coincida con la configuración de conexión de VPN prevista en su totalidad. Especifica los requisitos mínimos para una conexión VPN de AES128, SHA1 y Diffie-Hellman del grupo 2 en la mayoría de las regiones, y de AES128, SHA2 y Diffie-Hellman del grupo 14 en AWS las regiones. AWS GovCloud También especifica claves previamente compartidas para la autenticación. Debe modificar el archivo de configuración de ejemplo para aprovecharse de los algoritmos de seguridad adicionales, los grupos Diffie-Hellman, los certificados privados y el tráfico IPv6. Hemos agregado la compatibilidad con IKEv2 en los archivos de configuración para muchos dispositivos populares de gateway de cliente y continuaremos agregando archivos adicionales con el tiempo. Para obtener una lista de archivos de configuración con compatibilidad con IKEv2, consulte Su dispositivo de gateway de cliente.

Permisos

Para cargar correctamente la pantalla de configuración de descargas desde AWS Management Console, debe asegurarse de que su rol o usuario de IAM tenga permiso para las siguientes API `GetVpnConnectionDeviceTypes` de Amazon EC2: y. `GetVpnConnectionDeviceSampleConfiguration`

Para descargar el archivo de configuración mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Conexiones de Site-to-Site VPN.
3. Seleccione su conexión de VPN y elija Descargar configuración.
4. Seleccione el Proveedor, la Plataforma , el Software y la Versión de IKE que corresponda al dispositivo de puerta de enlace de cliente. Si su dispositivo no aparece en la lista, seleccione Generic (Genérico).
5. Elija Download (Descargar).

Para descargar un archivo de configuración de ejemplo mediante la línea de comandos o API

- GetVpnConnectionDeviceTipos (API Amazon EC2)
- GetVpnConnectionDeviceSampleConfiguration(API de consultas de Amazon EC2)
- get-vpn-connection-device-types (AWS CLI)

- get-vpn-connection-device-sample-configuration (AWS CLI)

Paso 7: Configurar el dispositivo de puerta de enlace de cliente

Utilice el archivo de configuración de ejemplo para configurar su dispositivo de gateway de cliente. El dispositivo de puerta de enlace de cliente es un dispositivo físico o de software en su lado de la conexión de VPN. Para obtener más información, consulte Su dispositivo de gateway de cliente.

Arquitecturas de Site-to-Site VPN

A continuación se muestran algunas arquitecturas comunes de Site-to-Site VPN:

- the section called “Conexiones de VPN únicas y múltiples”
- the section called “Conexiones de VPN redundantes”
- the section called “AWS VPN CloudHub”

Ejemplos de una conexión única y una conexión múltiple de VPN

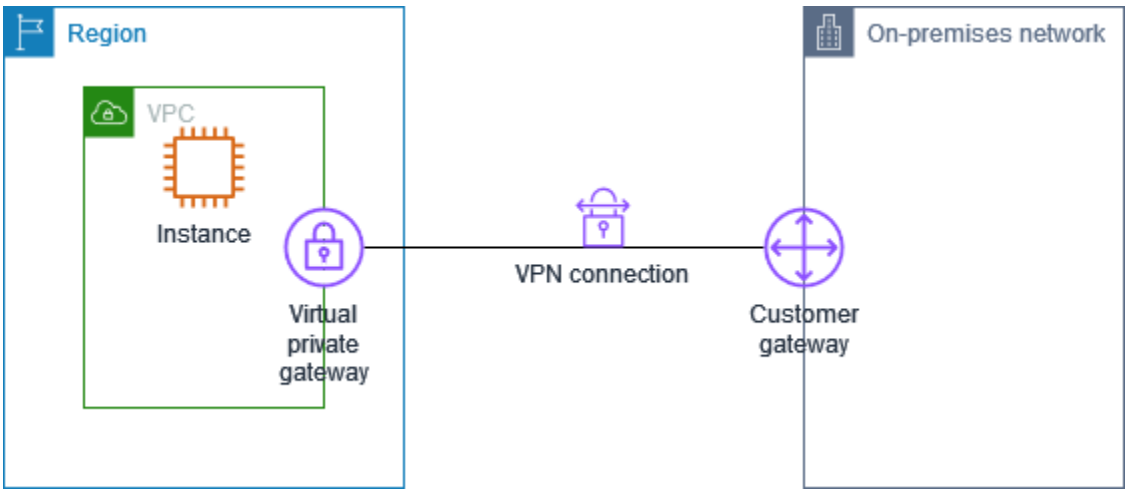
En los diagramas siguientes, se muestra una conexión única de Site-to-Site VPN y otra múltiple.

Ejemplos

- Conexión única de Site-to-Site VPN
- Conexión de Site-to-Site VPN con una gateway de tránsito
- Conexiones múltiples de Site-to-Site VPN
- Conexiones múltiples de Site-to-Site VPN con una gateway de tránsito
- Conexión de Site-to-Site VPN con AWS Direct Connect
- Conexión de Site-to-Site VPN de IP privada con AWS Direct Connect

Conexión única de Site-to-Site VPN

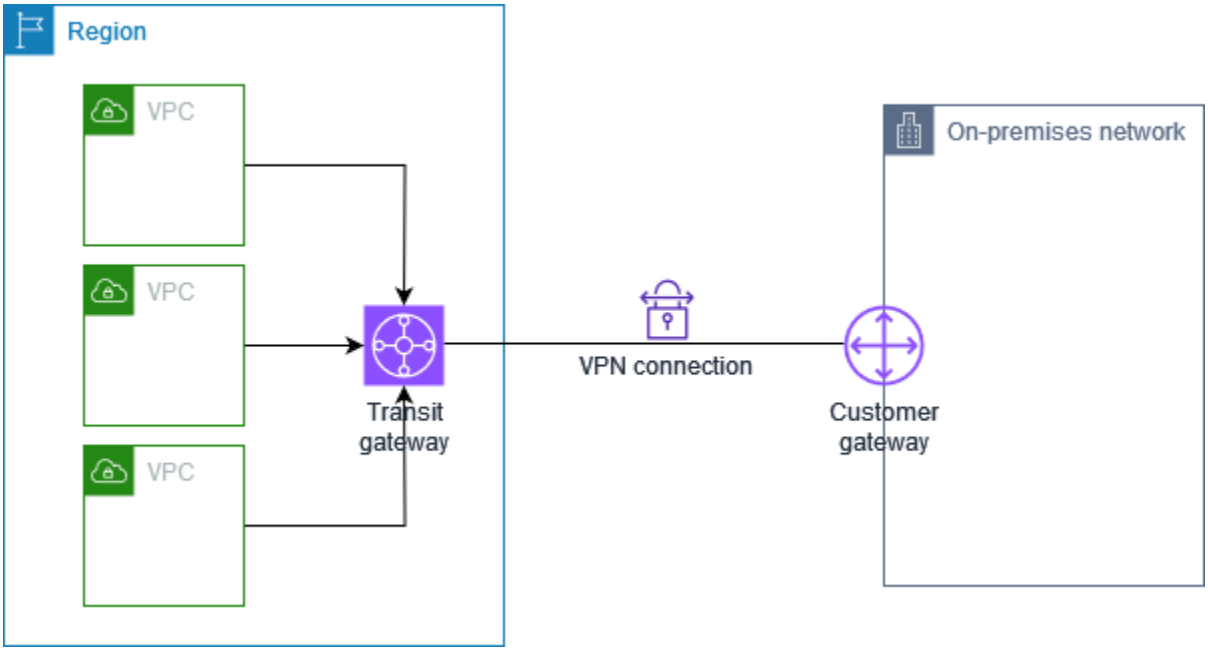
La VPC dispone de una puerta de enlace privada virtual asociada y su red en las instalaciones (remota) incluye un dispositivo de puerta de enlace de cliente que deberá configurar para habilitar la conexión VPN. Debe configurar tablas de enrutamiento de VPC para que el tráfico procedente de la VPC vinculada a su red vaya a la puerta de enlace privada virtual.



Si desea ver los pasos necesarios para configurar este escenario, consulte Empezar con AWS Site-to-Site VPN.

Conexión de Site-to-Site VPN con una gateway de tránsito

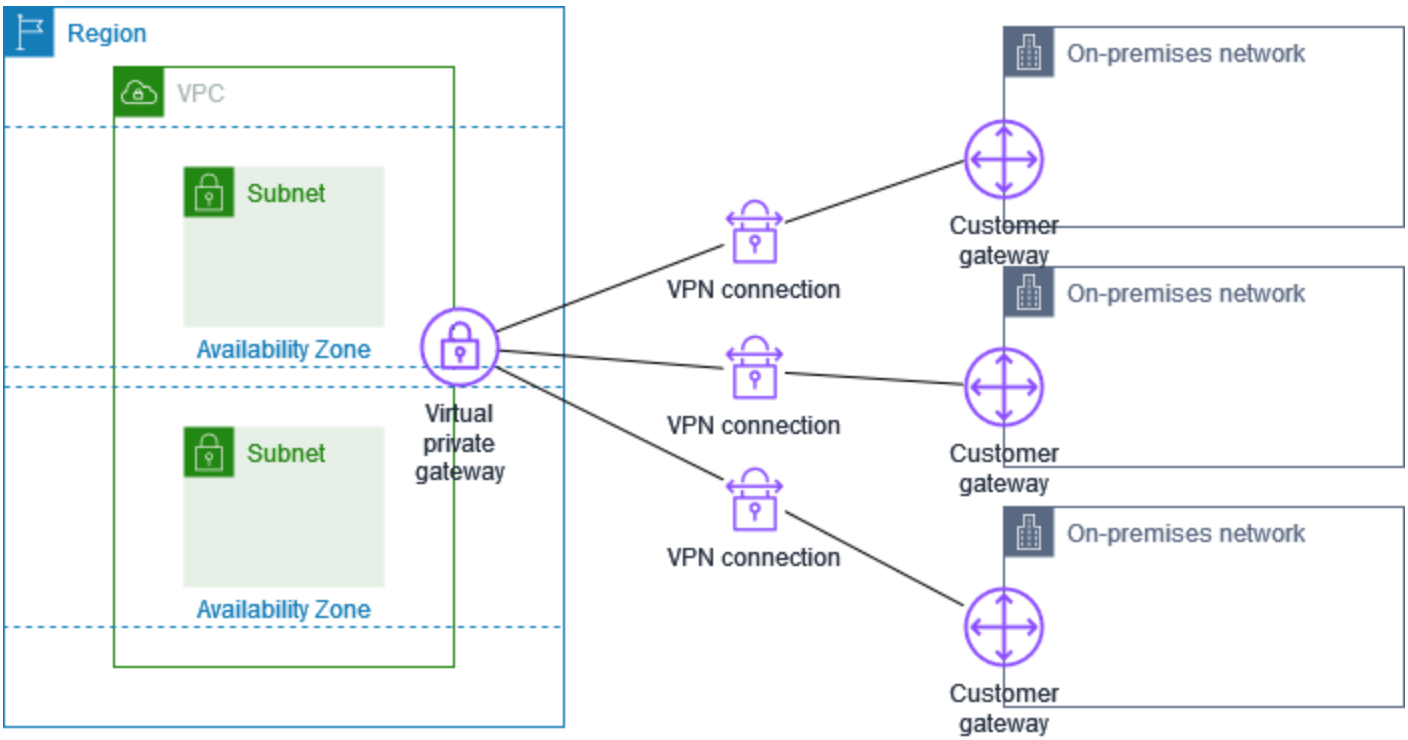
La VPC dispone de una puerta de enlace de tránsito asociada y la red en las instalaciones (remota) contiene un dispositivo de puerta de enlace de cliente que deberá configurar para habilitar la conexión de VPN. Debe configurar tablas de enrutamiento de VPC para que el tráfico procedente de la VPC vinculada a su red vaya a la puerta de enlace de tránsito.



Si desea ver los pasos necesarios para configurar este escenario, consulte Empezar con AWS Site-to-Site VPN.

Conexiones múltiples de Site-to-Site VPN

La VPC tiene asociada una gateway privada virtual y hay varias conexiones de Site-to-Site VPN con distintas ubicaciones locales. Configure el direccionamiento para que el tráfico procedente de la VPC vinculada a su red se dirija a la gateway privada virtual.

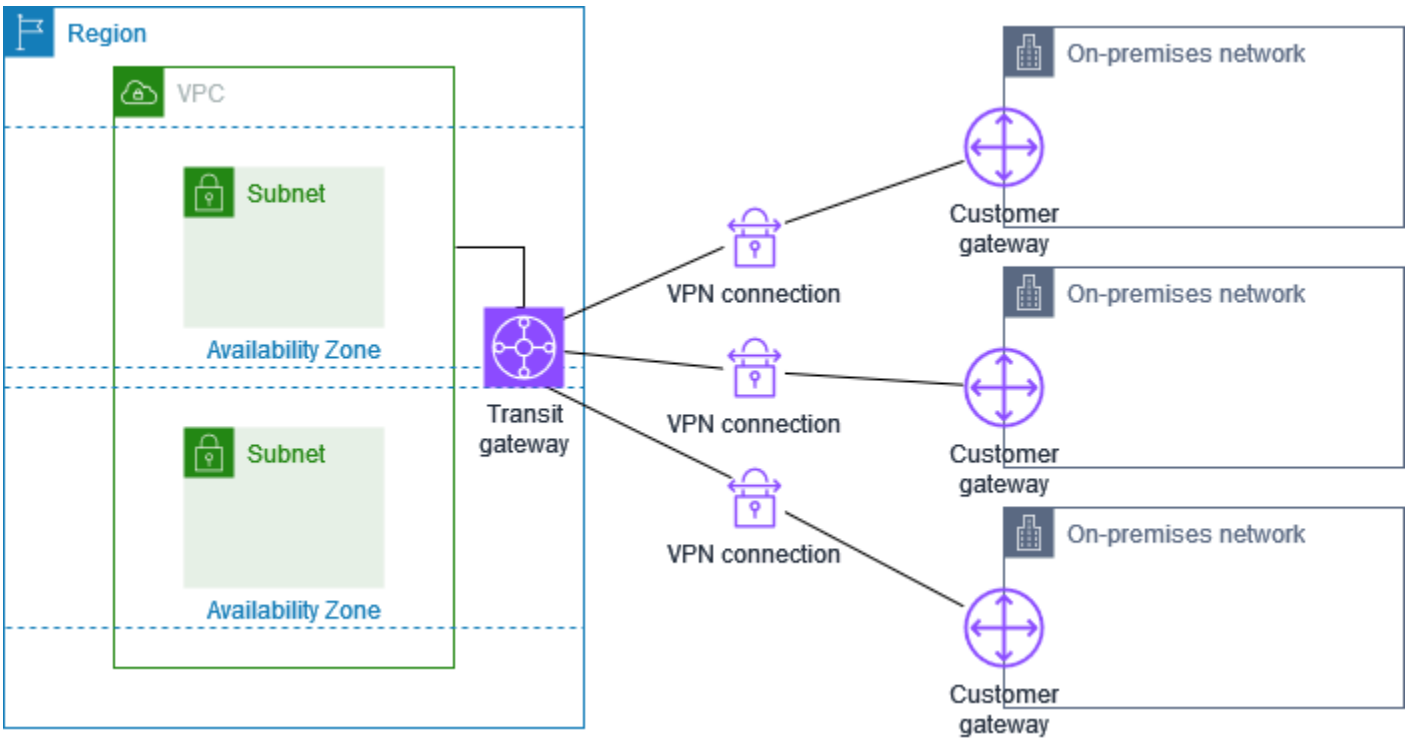


Si crea varias conexiones de Site-to-Site VPN con una única VPC, puede configurar una segunda gateway de cliente para crear una conexión redundante con la misma ubicación externa. Para obtener más información, consulte Uso de conexiones redundantes de Site-to-Site VPN para realizar la conmutación por error.

También puede utilizar esta situación para crear conexiones de Site-to-Site VPN con varias ubicaciones geográficas y proporcionar una comunicación segura entre sitios. Para obtener más información, consulte Comunicaciones seguras entre sitios mediante VPN CloudHub.

Conexiones múltiples de Site-to-Site VPN con una gateway de tránsito

La VPC tiene una gateway de tránsito conectada y hay varias conexiones de Site-to-Site VPN con diversas ubicaciones locales. Tiene que configurar el direccionamiento para que el tráfico procedente de la VPC vinculada a la red se direccione a la gateway de tránsito.

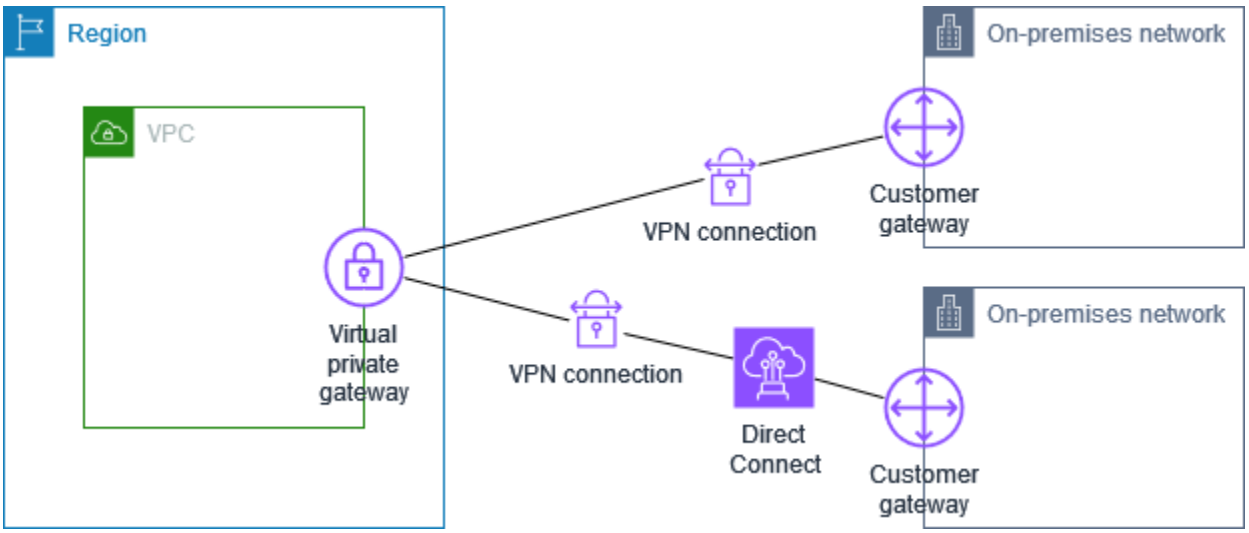


Si crea varias conexiones de Site-to-Site VPN con una única gateway de tránsito, puede configurar una segunda gateway de cliente para crear una conexión redundante con la misma ubicación externa.

También puede utilizar esta situación para crear conexiones de Site-to-Site VPN con varias ubicaciones geográficas y proporcionar una comunicación segura entre sitios.

Conexión de Site-to-Site VPN con AWS Direct Connect

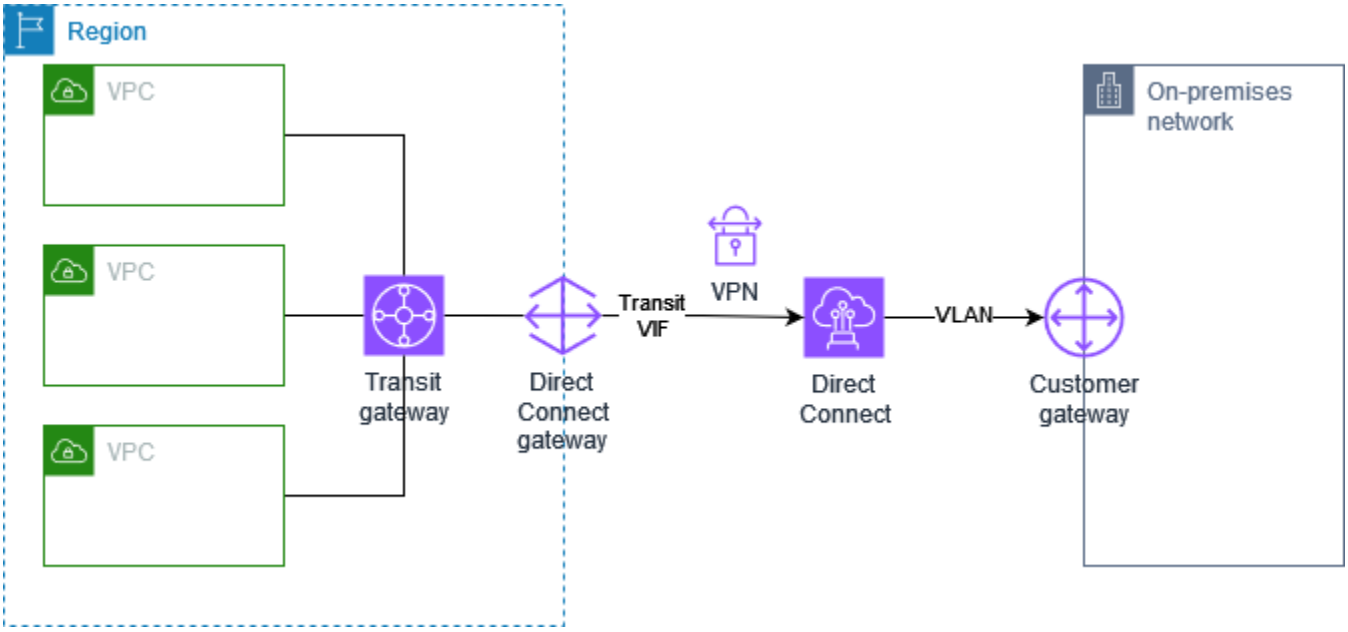
La VPC tiene una gateway privada virtual conectada y se conecta a su red en las instalaciones (remota) a través de AWS Direct Connect. Puede configurar una interfaz virtual pública de AWS Direct Connect para establecer una conexión de red dedicada entre la red y los recursos públicos de AWS a través de una gateway privada virtual. Configure el enrutamiento para que cualquier tráfico de la VPC vinculada a la red se dirija a la gateway privada virtual y a la conexión de AWS Direct Connect.



Cuando tanto AWS Direct Connect como la conexión de VPN están configurados en la misma gateway privada virtual, agregar o quitar objetos podría provocar que la gateway privada virtual entre en el estado "conectando". Esto indica que se está realizando un cambio en el enrutamiento interno que cambiará entre AWS Direct Connect y la conexión de VPN para minimizar las interrupciones y la pérdida de paquetes. Cuando esto se completa, la gateway privada virtual vuelve al estado “adjunto”.

Conexión de Site-to-Site VPN de IP privada con AWS Direct Connect

Con una VPN de sitio a sitio de IP privada puede cifrar el tráfico de AWS Direct Connect entre su red en las instalaciones y AWS sin usar direcciones IP públicas. La VPN de IP privada a través de AWS Direct Connect garantiza que el tráfico entre AWS y las redes en las instalaciones es seguro y privado, lo que permite a los clientes cumplir los mandatos normativos y de seguridad.



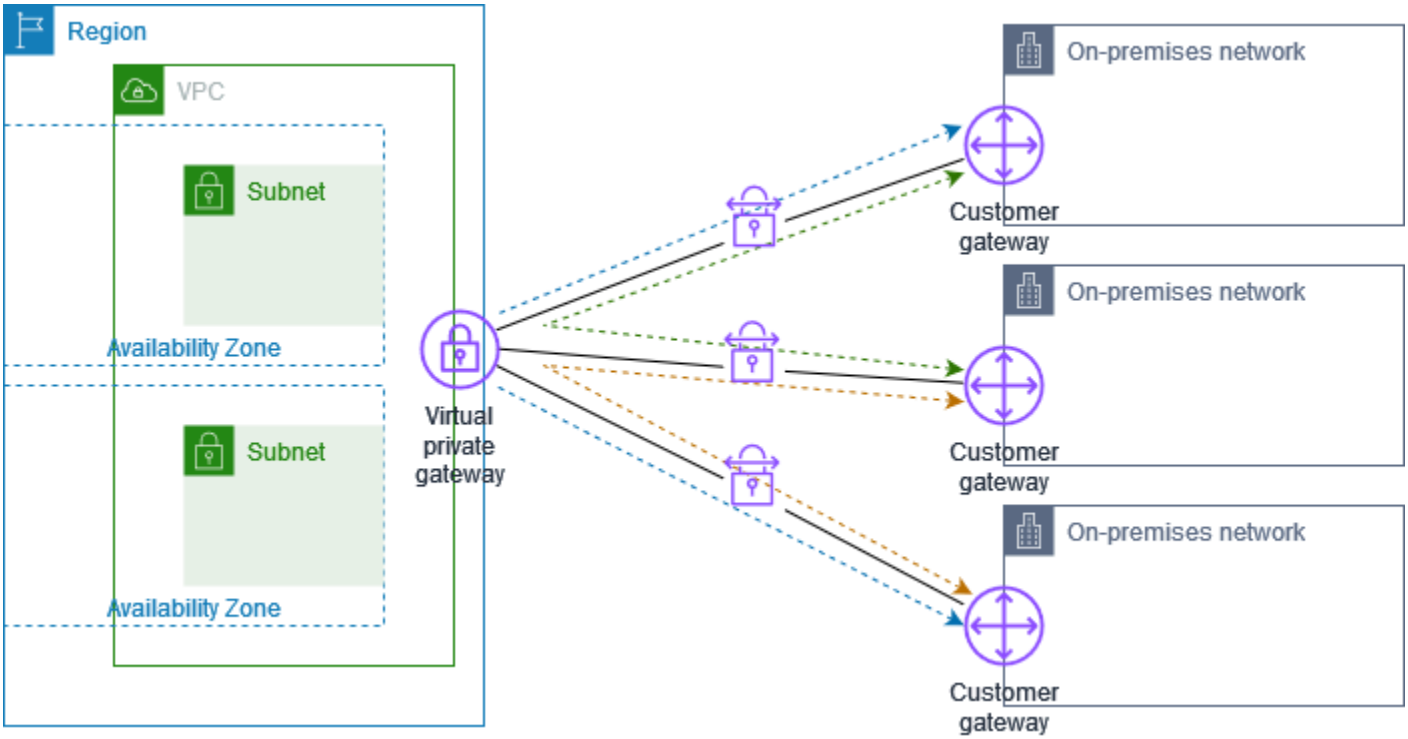
Para obtener más información, consulte la siguiente entrada de blog: Introducing AWS Site-to-Site VPN Private IP VPNs (Introducción a las VPN con IP privadas de AWS Site-to-Site VPN).

Comunicaciones seguras entre sitios mediante VPN CloudHub

Si tiene varias conexiones de AWS Site-to-Site VPN, puede proporcionar seguridad en la comunicación entre sitios gracias a AWS VPN CloudHub. Esto permite que los sitios puedan comunicarse entre sí y no solo con los recursos de la VPC. VPN CloudHub funciona con un modelo radial sencillo que puede utilizar con o sin VPC. Este diseño es perfecto si tiene varias sucursales y conexiones a Internet existentes y desea implementar un sistema radial cómodo y potencialmente de bajo coste para la conectividad principal o auxiliar entre estos sitios.

Información general

En el siguiente diagrama se muestra la arquitectura de VPN CloudHub. Las líneas discontinuas muestran el tráfico de red entre sitios remotos que se enruta a través de las conexiones VPN. Los sitios no pueden tener rangos de IP solapados.



En esta situación, haga lo siguiente:

1. Cree una única gateway privada virtual.

2. Cree varias gateway de cliente, cada una con la dirección IP pública de la gateway. Debe utilizar un Número de sistema autónomo (ASN) para protocolo de gateway fronteriza (BGP) único para cada gateway de cliente.
3. Cree una conexión de Site-to-Site VPN con direccionamiento dinámico entre cada gateway de cliente y la gateway privada virtual común.
4. Configure los dispositivos de gateway de cliente para que indiquen un prefijo específico del sitio (como 10.0.0.0/24, 10.0.1.0/24) a la gateway privada virtual. Estos anuncios de direccionamiento se reciben y se vuelven a anunciar a cada parte de BGP, lo que permite que cada sitio pueda enviar y recibir datos de otros sitios. Esto se realiza utilizando las instrucciones de red de los archivos de configuración de VPN de la conexión de Site-to-Site VPN. Las instrucciones de red varían en función del tipo de router que utilice.
5. Configure las rutas en las tablas de enrutamiento de subred para permitir que las instancias de la VPC se comuniquen con los sitios. Para obtener más información, consulte (Gateway privada virtual) Habilitar la propagación de rutas en la tabla de enrutamiento. Puede configurar una ruta agregada en la tabla de enrutamiento (por ejemplo, 10.0.0.0/16). Utilice prefijos más específicos entre los dispositivos de gateway de cliente y la gateway privada virtual.

Los sitios que utilizan las conexiones de AWS Direct Connect a la gateway privada virtual también pueden ser parte de AWS VPN CloudHub. Por ejemplo, su sede corporativa de Nueva York puede tener una conexión de AWS Direct Connect a la VPC y sus sucursales pueden utilizar las conexiones de Site-to-Site VPN a la VPC. De este modo, las sucursales de Los Ángeles y Miami podrán enviar y recibir datos a la sede corporativa y entre ellas mismas gracias a AWS VPN CloudHub.

Precios

Para utilizar AWS VPN CloudHub, debe pagar las tarifas de conexión habituales de Site-to-Site VPN para Amazon VPC. De este modo, se le facturará las tasas de conexión por cada hora que cada VPN permanezca conectada a la gateway privada virtual. Al enviar datos de un sitio a otro mediante AWS VPN CloudHub, no incurrirá en ningún costo para el envío de datos desde su sitio a la gateway privada virtual. Solo pagará tasas de transferencia de datos de AWS estándar de los datos que se reenvíen desde la gateway privada virtual al punto de enlace.

Por ejemplo, si tiene un sitio en Los Ángeles y otro sitio en Nueva York y ambos sitios tienen una conexión de Site-to-Site VPN con la gateway privada virtual, se le aplicará la tarifa por hora por cada conexión de Site-to-Site VPN (por tanto, si la tarifa fuera de 0,05 USD por hora, equivaldría a un total de 0,10 USD por hora). También se le aplicarán las tarifas estándar de transferencia de datos de AWS para todos los datos que envíe de Los Ángeles a Nueva York (y viceversa) y que atraviesen

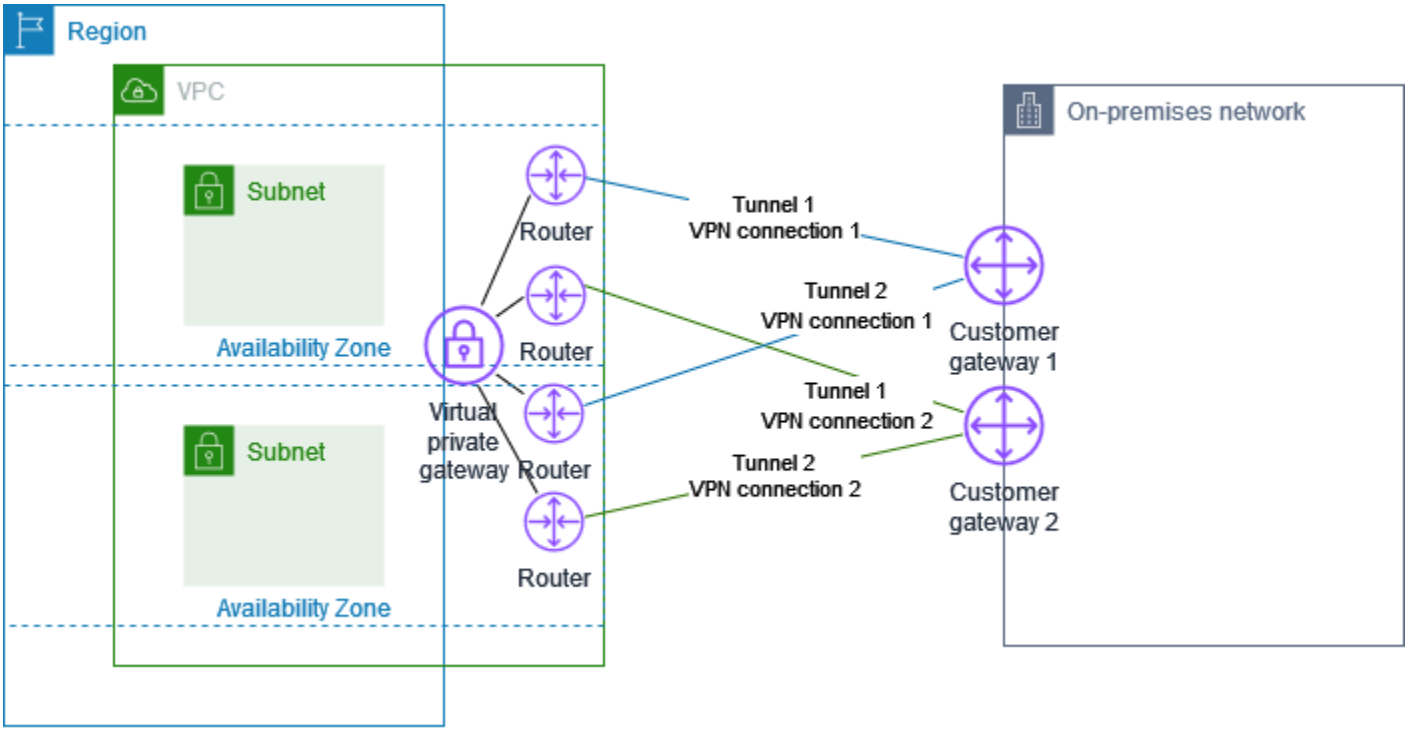
cada conexión de Site-to-Site VPN. El tráfico de red que se envía a través de la conexión de Site-to-Site VPN a la gateway privada virtual es gratuito, pero el tráfico de red que se envía a través de la conexión de Site-to-Site VPN desde la gateway privada virtual al punto de enlace se factura según la tarifa de transferencia de datos estándar de AWS.

Para obtener más información, consulte los precios de las conexiones de Site-to-Site VPN.

Uso de conexiones redundantes de Site-to-Site VPN para realizar la conmutación por error

Para protegerse frente a la pérdida de conectividad que se produciría si su dispositivo de puerta de enlace de cliente dejara de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN con la VPC y la puerta de enlace privada virtual utilizando otro dispositivo de puerta de enlace de cliente. El uso de dispositivos de puerta de enlace de cliente y conexiones de VPN redundantes permite realizar tareas de mantenimiento en uno de los dispositivos y, a la vez, mantener el flujo de tráfico a través de la segunda conexión de VPN.

En el siguiente diagrama se muestran dos conexiones de VPN. Cada conexión de VPN tiene sus propios túneles y su propia puerta de enlace de cliente.



En esta situación, haga lo siguiente:

- Configure otra conexión de Site-to-Site VPN utilizando la misma gateway privada virtual y creando una nueva gateway de cliente. La dirección IP de la gateway de cliente de la segunda conexión de Site-to-Site VPN debe estar disponible públicamente.
- Configure el otro dispositivo de gateway de cliente. Ambos dispositivos deben anunciar los mismos rangos de IP a la gateway privada virtual. Utilizamos el direccionamiento de BGP para determinar la ruta del tráfico. Si se produce un error en un dispositivo de gateway de cliente, la gateway privada virtual dirigirá todo el tráfico al dispositivo de gateway de cliente que sí funciona.

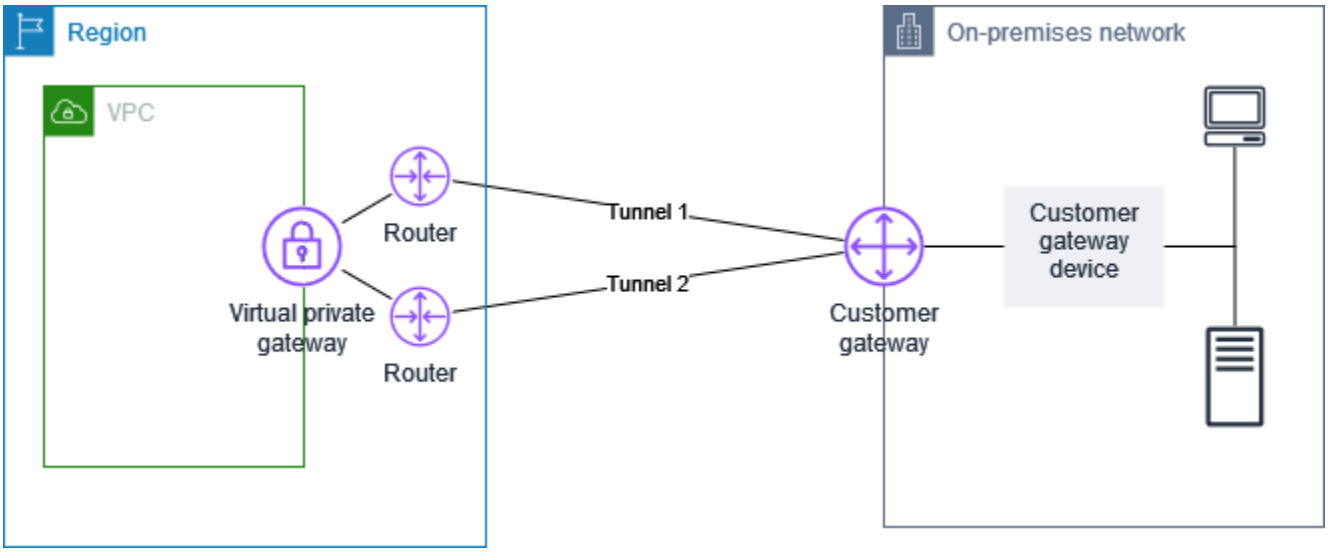
Las conexiones de Site-to-Site VPN de direccionamiento dinámico utilizan el protocolo de Número de sistema autónomo (ASN) para intercambiar la información de direccionamiento entre las gateways de cliente y las gateways privadas virtuales. En las conexiones de Site-to-Site VPN con direccionamiento estático, es necesario que las rutas estáticas de la red remota se escriban en su lado de la gateway de cliente. La información acerca de las rutas que se especifica manualmente y que anuncia mediante BGP permite a las gateways de ambos extremos determinar qué túneles están disponibles para, de este modo, redireccionar el tráfico en caso de error. Por lo tanto, se recomienda configurar su red para que utilice la información de direccionamiento que proporciona BGP (si está disponible) y seleccionar una ruta alternativa. La configuración exacta dependerá de la arquitectura de su red.

Para obtener más información acerca de cómo crear y configurar una gateway de cliente y una conexión de Site-to-Site VPN, consulte Empezar con AWS Site-to-Site VPN.

Su dispositivo de gateway de cliente

Un dispositivo de gateway de cliente es un dispositivo físico o de software que usted posee o administra en la red local (en su extremo de una conexión de Site-to-Site VPN). Usted o el administrador de red tienen que configurar el dispositivo para que funcione con la conexión de Site-to-Site VPN.

En el siguiente diagrama se muestra su red, el dispositivo de puerta de enlace de cliente y la conexión de VPN que va a una puerta de enlace privada virtual que está asociada a su VPC. Las dos líneas entre la puerta de enlace de cliente y la puerta de enlace privada virtual representan los túneles para la conexión de VPN. Si hay una falla en el dispositivo AWS, tu conexión VPN pasa automáticamente al segundo túnel para que tu acceso no se interrumpa. De vez en cuando, AWS también realiza un mantenimiento rutinario de la conexión VPN, lo que podría deshabilitar brevemente uno de los dos túneles de la conexión VPN. Para obtener más información, consulte Sustitución de los puntos de enlace de un túnel de Site-to-Site VPN. Por lo tanto, es importante que configure el dispositivo de puerta de enlace de cliente para utilizar ambos túneles.



Si desea ver los pasos necesarios para configurar una conexión de VPN, consulte Empezar con AWS Site-to-Site VPN. Durante este proceso, se crea un recurso de pasarela de clientes en AWS el que se proporciona información AWS sobre el dispositivo, por ejemplo, su dirección IP pública. Para obtener más información, consulte Opciones de la gateway de cliente para su conexión de Site-to-Site VPN. El recurso de puerta de enlace de cliente AWS no configura ni crea el dispositivo de puerta de enlace de cliente. Debe configurar el dispositivo usted mismo.

También puede encontrar dispositivos de VPN por software en AWS Marketplace.

Temas

Archivos de configuración de ejemplo

Después de crear la conexión de VPN, también tiene la opción de descargar un proporcionado por AWS el archivo de configuración de ejemplo desde la consola de Amazon VPC o mediante la API de EC2. Para obtener más información, consulte Paso 6: Descargar el archivo de configuración. También puede descargar archivos .zip de configuraciones de ejemplo específicamente para enrutamiento estático frente a dinámico:

Descargar archivos .zip

- Configuración estática: the section called “Archivos de configuración de ejemplo”
- Configuración dinámica: the section called “Archivos de configuración de ejemplo”

El archivo AWS de configuración de ejemplo proporcionado contiene información específica sobre su conexión VPN que puede utilizar para configurar el dispositivo de puerta de enlace del cliente. Estos archivos de configuración específicos del dispositivo sólo están disponibles para los dispositivos que han sido probados por AWS. Si su dispositivo específico gateway de cliente no aparece en la lista, puede descargar un archivo de configuración genérico para empezar.

Important

El archivo de configuración es solo un ejemplo y es posible que no coincida con la configuración de conexión de Site-to-Site VPN completamente. Especifica los requisitos mínimos para una conexión VPN de sitio a sitio de AES128, SHA1 y Diffie-Hellman del grupo 2 en la mayoría de las regiones, y de AES128, SHA2 y Diffie-Hellman del grupo 14 en AWS las regiones. AWS GovCloud También especifica claves previamente compartidas para la autenticación. Debe modificar el archivo de configuración de ejemplo para aprovecharse de los algoritmos de seguridad adicionales, los grupos Diffie-Hellman, los certificados privados y el tráfico IPv6.

Note

Estos AWS archivos de configuración específicos del dispositivo se proporcionan con el máximo esfuerzo. Si bien han sido probados por AWS, estas pruebas son limitadas. Si experimenta un problema con los archivos de configuración, es posible que deba contactar al proveedor específico para obtener asistencia adicional.

La tabla siguiente contiene una lista de dispositivos que tienen un archivo de configuración de ejemplo disponible para descargar que se ha actualizado para ser compatible con IKEv2. Hemos agregado la compatibilidad con IKEv2 en los archivos de configuración para muchos dispositivos populares de gateway de cliente y continuaremos agregando archivos adicionales con el tiempo. Esta lista se actualizará a medida que se agreguen más archivos de configuración de ejemplo.

Proveedor	Plataforma	Software
Punto de comprobación	Gaia	R80.10+
Cisco Meraki	Serie MX	15.12+ (WebUI)
Cisco Systems, Inc.	Serie ASA 5500	ASA 9.7+ VTI
Cisco Systems, Inc.	AMI CSrV	IOS 12.4+
Fortinet	Serie Fortigate 40+	ForTIOS 6.4.4+ (GUI)

Proveedor	Plataforma	Software
Juniper Networks, Inc.	Routers Serie J	JunOS 9.5+
Juniper Networks, Inc.	Routers SRX	JunOS 11.0+
Mikrotik	RouterOS	6.44.3
Palo Alto Networks	Serie PA	PANOS 7.0+
SonicWall	NSA, TZ	OS 6.5
Sophos	Sophos Firewall	v19+
Strongswan	Ubuntu 16.04	Strongswan 5.5.1+
Yamaha	Routers RTX	Rev.10.01.16+

Requisitos para el dispositivo de gateway del cliente

Si tiene un dispositivo que no está en la lista de ejemplos anterior, en esta sección se describen los requisitos que debe cumplir para que pueda utilizarse con una conexión de Site-to-Site VPN.

Hay cuatro puntos principales para la configuración del dispositivo de gateway de cliente. Los siguientes símbolos representan cada parte de la configuración.

	Asociación de seguridad de intercambio de claves de Internet (IKE). Necesaria para intercambiar claves utilizadas para establecer la asociación de seguridad de IPsec.
	Asociación de seguridad IPsec. Gestiona el cifrado del túnel, la autenticación, etc.
	Interfaz de túnel. Recibe el tráfico entrante y saliente del túnel.
	(Opcional) Asociación entre pares con protocolo de gateway fronterizo (BGP) Para dispositivos que usan BGP, intercambia rutas entre el dispositivo de gateway de cliente y la gateway privada virtual.

En la siguiente tabla se indican los requisitos que debe cumplir el dispositivo de gateway de cliente, el RFC relacionado (a modo de referencia) y comentarios acerca de los requisitos.

Cada conexión de VPN consta de dos túneles independientes. Cada túnel contiene una asociación de seguridad de IKE, una asociación de seguridad de IPsec y un intercambio de tráfico BGP. La limitación es de una única pareja de asociación de seguridad (SA) por túnel (un entrante y uno saliente) y, por lo tanto, dos únicas parejas de SA en total para los dos túneles (cuatro SA). Algunos dispositivos utilizan una VPN basada en políticas y crean tantas SA como entradas de ACL. Por lo tanto, es posible que necesite consolidar sus reglas y luego filtrar para no permitir el tráfico no deseado.

De forma predeterminada, el túnel de VPN aparece cuando se genera tráfico y se inicia la negociación de IKE desde el lado de la conexión de VPN. En su lugar, puede configurar la conexión VPN para iniciar la negociación del IKE desde el AWS lado de la conexión. Para obtener más información, consulte Opciones de inicio del túnel de Site-to-Site VPN.

Los puntos de enlace de VPN dan soporte al cambio de clave y comienzan las nuevas negociaciones cuando la primera fase está a punto de caducar si el dispositivo de gateway de cliente no ha enviado tráfico de renegociación.

Requisito	RFC	Comentarios
Establecimiento de una asociación de seguridad de IKE IKE	RFC 2409 RFC 7296	La asociación de seguridad IKE se establece primero entre la puerta de enlace privada virtual y el dispositivo de puerta de enlace del cliente mediante una clave previamente compartida o un certificado privado que se utiliza AWS Private Certificate Authority como autenticador. Cuando se establece, IKE negocia una clave efímera para proteger los mensajes futuros de IKE. Tiene que haber un acuerdo completo entre los parámetros, incluidos los parámetros de cifrado y autenticación. Al crear una conexión VPN en AWS, puede especificar su propia clave previamente compartida para cada túnel o puede dejar que AWS genere una por usted. Como alternativa, puede especificar el certificado privado que se utilizará AWS Private Certificate

Requisito	RFC	Comentarios
		Authority para el dispositivo de pasarela de su cliente. Para obtener más información sobre la configuración de túneles de VPN, consulte Opciones del túnel de una conexión de Site-to-Site VPN. Las siguientes versiones son compatibles: IKEv1 e IKEv2. El modo principal solo se admite con IKEv1. El servicio Site-to-Site VPN es una solución basada en rutas. Si utiliza una configuración basada en políticas , debe limitar su configuración a una asociación de seguridad (SA) única.
Establecimiento de asociaciones de seguridad de IPsec en modo de túnel IPsec	RFC 4301	Mediante la clave efímera de IKE, se establecen las claves entre la gateway privada virtual y el dispositivo de gateway de cliente para crear una asociación de seguridad (SA) de IPsec. El tráfico entre las gateways se cifra y se descifra mediante esta SA. IKE cambia automáticamente las claves efímeras utilizadas para cifrar el tráfico dentro de la SA de IPsec de forma periódica para garantizar la confidencialidad de las comunicaciones.
Uso del cifrado AES de 128 bits o la función de cifrado AES de 256 bits	RFC 3602	La función de cifrado se utiliza para garantizar la privacidad entre las asociaciones de seguridad de IKE y de IPsec.
Uso de la función de hash SHA-1 o SHA-2 (256)	RFC 2404	Esta función de hash se utiliza para autenticar asociaciones de seguridad de IKE y de IPsec.

Requisito	RFC	Comentarios
Uso de la confidencialidad directa total Diffie-Hellman	RFC 2409	IKE utiliza Diffie-Hellman para establecer claves efímeras para proteger todas las comunicaciones entre los dispositivos de gateway de cliente y las gateways privadas virtuales. Se admiten los siguientes grupos: • Grupos de fase 1: 2, 14-24 • Grupos de fase 2: 2, 5, 14-24
(Conexiones de VPN enrutadas dinámicamente) Uso de la detección de pares muertos de IPsec	RFC 3706	La detección de pares muertos permite a los dispositivos de VPN identificar rápidamente cuándo una condición de red impide la entrega de paquetes a través de Internet. Cuando esto sucede, las gateways eliminan las asociaciones de seguridad e intentan crear nuevas asociaciones. Durante este proceso, se utiliza el túnel IPsec alternativo, si es posible.
(Conexiones de VPN enrutadas dinámicamente) Vincular el túnel a la interfaz lógica (VPN basada en rutas) Tunnel	Ninguna	El dispositivo debe poder vincular el túnel IPSec a una interfaz lógica. La interfaz lógica contiene una dirección IP utilizada para establecer el intercambio de tráfico BGP con la gateway privada virtual. Esta interfaz lógica no debería realizar ninguna encapsulación adicional (por ejemplo, GRE o IP en IP). Su interfaz debería configurarse en una unidad de transmisión máxima (MTU) de 1399 bytes.
(Conexiones de VPN enrutadas dinámicamente) Establecimiento de intercambio de tráfico BGP BGP	RFC 4271	BGP se utiliza para intercambiar rutas entre el dispositivo de gateway de cliente y la gateway privada virtual para dispositivos que utilizan BGP. Todo el tráfico BGP se cifra y se transmite mediante la asociación de seguridad de IPsec. BGP es necesario para que ambas gateways intercambien los prefijos IP, a los que se obtiene acceso mediante la SA de IPsec.

Una conexión AWS VPN no admite Path MTU Discovery (RFC 1191).

Si tiene un firewall entre el dispositivo de gateway de cliente e Internet, consulte Configuración de un firewall entre Internet y el dispositivo de gateway de cliente.

Prácticas recomendadas para su dispositivo de puerta de enlace de cliente

Utilice IKEv2

Recomendamos encarecidamente utilizar IKEv2 para la conexión VPN de Site-to-Site. IKEv2 es un protocolo más simple, robusto y seguro que IKEv1. Solo debe utilizar el IKEv1 si el dispositivo de puerta de enlace del cliente no es compatible con el IKEv2. Para obtener más información sobre las diferencias entre el IKEv1 y el IKEv2, consulte el apéndice A del RFC7296.

Restablecimiento de la marca “Don't Fragment (DF)” en los paquetes

Algunos paquetes llevan una marca, conocida como la marca "Don't Fragment" (DF), que indica que el paquete no debe fragmentarse. Si los paquetes llevan la marca, las gateways generan un mensaje "ICMP Path MTU Exceeded". En algunos casos, las aplicaciones no contienen los mecanismos suficientes para procesar estos mensajes ICMP y reducir la cantidad de datos transmitidos en cada paquete. Algunos dispositivos VPN pueden anular la marca DF y fragmentar los paquetes de forma incondicional según sea necesario. Si el dispositivo de gateway de cliente tiene esta capacidad, recomendamos que la utilice según corresponda. Consulte RFC 791 para obtener más información.

Fragmentación de paquetes IP antes del cifrado

Si los paquetes que se envían a través de la conexión VPN de Site-to-Site superan el tamaño de la MTU, deben estar fragmentados. Para evitar una disminución del rendimiento, le recomendamos que configure el dispositivo de puerta de enlace del cliente para fragmentar los paquetes antes de cifrarlos. Luego, la VPN Site-to-Site volverá a ensamblar los paquetes fragmentados antes de reenviarlos al siguiente destino, a fin de lograr un mayor flujo a través de la red. packet-per-second AWS Consulte RFC 4459 para obtener más información.

Asegúrese de que el tamaño del paquete no supere la MTU para las redes de destino

Dado que la VPN Site-to-Site volverá a ensamblar todos los paquetes fragmentados recibidos desde el dispositivo de puerta de enlace del cliente antes de reenviarlos al siguiente destino, tenga en

cuenta que es posible que haya que tener en cuenta el tamaño del paquete o la MTU en las redes de destino a las que estos paquetes se reenvíen a continuación, por ejemplo, a través de AWS Direct Connect

Ajuste los tamaños de MTU y MSS de acuerdo con los algoritmos en uso

Los paquetes TCP suelen ser el tipo más común de paquetes en los túneles IPsec. Site-to-Site VPN admite una unidad máxima de transmisión (MTU) de 1446 bytes y un tamaño máximo de segmento (MSS) correspondiente de 1406 bytes. Sin embargo, los algoritmos de cifrado tienen distintos tamaños de encabezado y pueden impedir la capacidad de alcanzar estos valores máximos. Para obtener un rendimiento óptimo evitando la fragmentación, le recomendamos que configure la MTU y el MSS basándose específicamente en los algoritmos que se utilizan.

Utilice la siguiente tabla para configurar su MTU o MSS a fin de evitar la fragmentación y lograr un rendimiento óptimo:

Algoritmo de cifrado	Algoritmo hash	NAT transversal	MTU	MSS (IPv4)	MSS (IPv6 en IPv4)
AES-GCM-16	N/A	disabled	1446	1406	1386
AES-GCM-16	N/A	enabled	1438	1398	1378
AES-CBC	SHA1, SHA2-256	disabled	1438	1398	1378
AES-CBC	SHA1, SHA2-256	enabled	1422	1382	1362
AES-CBC	SHA2-384	disabled	1422	1382	1362
AES-CBC	SHA2-384	enabled	1422	1382	1362
AES-CBC	SHA2-512	disabled	1422	1382	1362
AES-CBC	SHA2-512	enabled	1406	1366	1346

> **Note**
>
> Los algoritmos AES-GCM cubren tanto el cifrado como la autenticación, por lo que no existe una opción distinta de algoritmo de autenticación que afecte a la MTU.

Desactivar los ID únicos de IKE

Algunos dispositivos de puerta de enlace de clientes admiten una configuración que garantiza que, como máximo, exista una asociación de seguridad de fase 1 por configuración de túnel. Esta configuración puede provocar estados de fase 2 incoherentes entre los pares de VPN. Si el dispositivo de puerta de enlace de su cliente admite esta configuración, le recomendamos que la desactive.

Configuración de un firewall entre Internet y el dispositivo de gateway de cliente

Debe tener una dirección IP estática para utilizarla como punto final para los túneles IPsec que conectan el dispositivo de puerta de enlace del cliente con los puntos finales. AWS Site-to-Site VPN Si hay un firewall entre AWS y el dispositivo de puerta de enlace del cliente, deben existir las reglas de las siguientes tablas para establecer los túneles IPSec. Las direcciones IP del AWS lado -estarán en el archivo de configuración.

Entrante (de Internet)

Regla de entrada I1	
IP de origen	IP externa de Tunnel1
IP destino	Gateway de cliente
Protocolo	UDP
Puerto de origen	500
Destino	500
Regla de entrada I2	
IP de origen	IP externa de Tunnel2

IP destino	Gateway de cliente
Protocolo	UDP
Puerto de origen	500
Puerto de destino	500
Regla de entrada I3	
IP de origen	IP externa de Tunnel1
IP destino	Gateway de cliente
Protocolo	IP 50 (ESP)
Regla de entrada I4	
IP de origen	IP externa de Tunnel2
IP destino	Gateway de cliente
Protocolo	IP 50 (ESP)

Saliente (a Internet)

Regla de salida O1	
IP de origen	Gateway de cliente
IP destino	IP externa de Tunnel1
Protocolo	UDP
Puerto de origen	500
Puerto de destino	500
Regla de salida O2	
IP de origen	Gateway de cliente

IP destino	IP externa de Tunnel2
Protocolo	UDP
Puerto de origen	500
Puerto de destino	500
Regla de salida O3	
IP de origen	Gateway de cliente
IP destino	IP externa de Tunnel1
Protocolo	IP 50 (ESP)
Regla de salida O4	
IP de origen	Gateway de cliente
IP destino	IP externa de Tunnel2
Protocolo	IP 50 (ESP)

Las reglas I1, I2, O1 y O2 permiten la transmisión de paquetes IKE. Las reglas I3, I4, O3 y O4 permiten la transmisión de paquetes IPsec que contienen el tráfico de red cifrado.

> **Note**
>
> Si utiliza el cruce de NAT (NAT-T) en su dispositivo, asegúrese de que el tráfico UDP del puerto 4500 también pueda pasar entre la red y los puntos finales. AWS Site-to-Site VPN Compruebe si su dispositivo anuncia NAT-T.

Múltiples escenarios de conexión de VPN

A continuación, presentamos varios escenarios en los que puede crear varias conexiones de VPN con uno o varios dispositivos de gateway de cliente.

Varias conexiones de VPN que utilizan el mismo dispositivo de gateway de cliente

Puede crear conexiones de VPN adicionales desde la ubicación de las instalaciones a otras VPC con el mismo dispositivo de gateway de cliente. Puede reutilizar la misma dirección IP de gateway de cliente para cada una de estas conexiones de VPN.

Conexión de VPN redundante que usa otro dispositivo de gateway de cliente

Para protegerse contra la pérdida de conectividad en caso de que el dispositivo de gateway de cliente deje de estar disponible, puede configurar otra conexión de VPN que use otro dispositivo de gateway de cliente. Para obtener más información, consulte Uso de conexiones redundantes de Site-to-Site VPN para realizar la conmutación por error. Al establecer dispositivos de gateway de cliente redundantes en una única ubicación, ambos dispositivos deberían anunciar los mismos rangos IP.

Varios dispositivos de puerta de enlace del cliente a una única puerta de enlace privada virtual ()AWS VPN CloudHub

Puede establecer varias conexiones de VPN a una única gateway privada virtual desde varios dispositivos de gateway de cliente. Esto le permite tener varias ubicaciones conectadas a la AWS VPN CloudHub. Para obtener más información, consulte Comunicaciones seguras entre sitios mediante VPN CloudHub. Si tiene dispositivos de gateway de cliente en distintas ubicaciones geográficas, cada dispositivo debería anunciar un único conjunto de rangos IP específicos de la ubicación.

Enrutamiento para su dispositivo de gateway de cliente

AWS recomienda anunciar rutas BGP específicas para influir en las decisiones de enrutamiento en la puerta de enlace privada virtual. Compruebe la documentación de su proveedor acerca de los comandos específicos de su dispositivo.

Al crear varias conexiones de VPN, la gateway privada virtual envía el tráfico de red a la conexión de VPN apropiada utilizando las rutas asignadas estáticamente o anuncios de ruta de BGP, La ruta depende de cómo se haya configurado la conexión de VPN. Las rutas asignadas estáticamente son preferibles frente a las rutas anunciadas de BGP en los casos en los que existen rutas idénticas en la gateway privada virtual. Si selecciona la opción de utilizar el anuncio de BGP, no podrá especificar rutas estáticas.

Para obtener más información sobre la prioridad de una ruta, consulte Tablas de enrutamiento y prioridad de rutas de VPN.

Ejemplos de configuraciones de dispositivos de gateway de cliente para el direccionamiento estático

Temas

Archivos de configuración de ejemplo

Para descargar un archivo de configuración de muestra con valores específicos para la configuración de conexión de la VPN de sitio a sitio, utilice la consola de Amazon VPC, la línea de comandos AWS o la API de Amazon EC2. Para obtener más información, consulte Paso 6: Descargar el archivo de configuración.

También puede descargar archivos de configuración de ejemplo genéricos para enrutamiento estático que no incluyan valores específicos de la configuración de conexión Site-to-Site VPN: static-routing-examples.zip

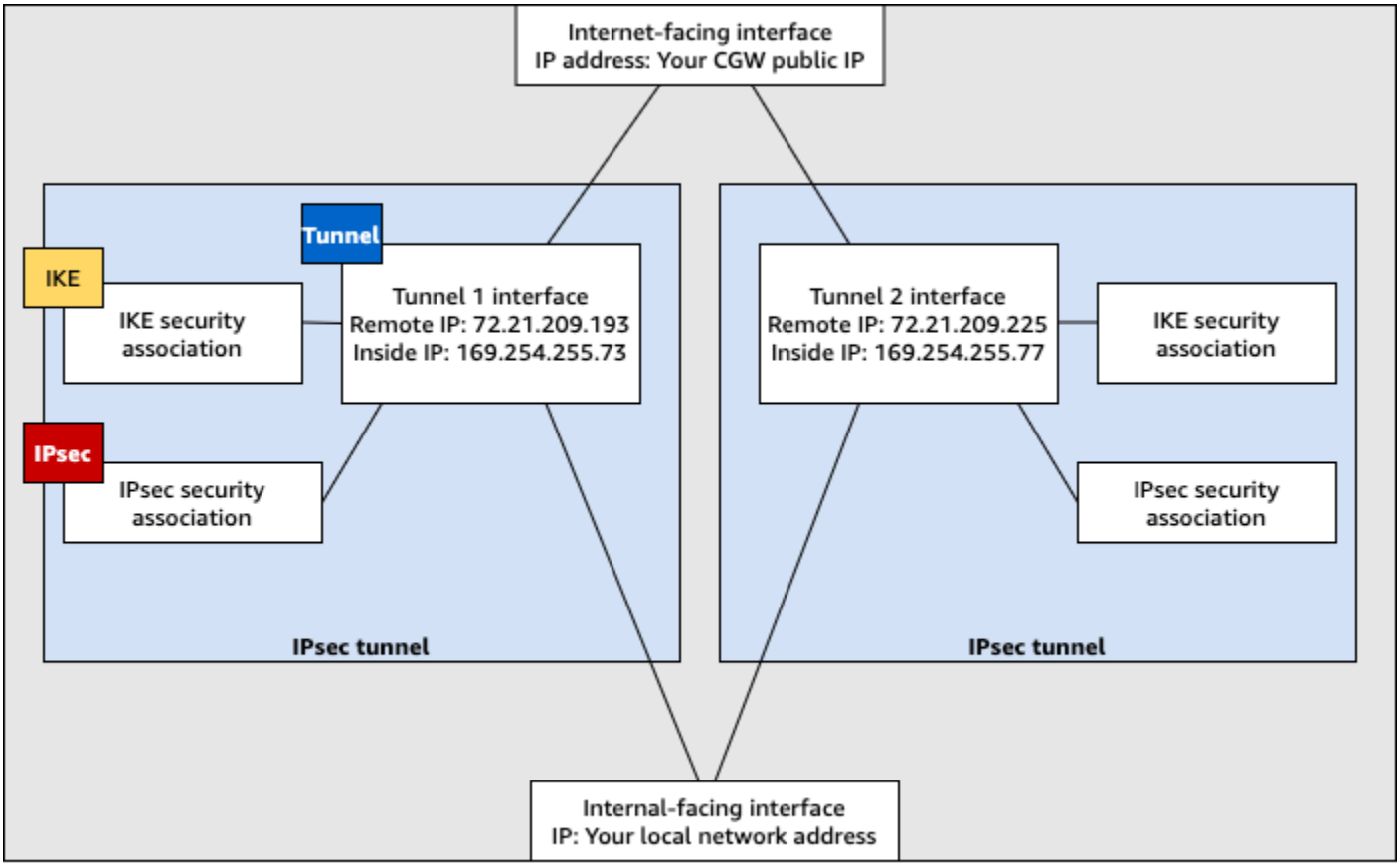
Los archivos utilizan valores de marcadores de posición para algunos componentes. Por ejemplo, usan:

- Valores de ejemplo para el ID de conexión de VPN, el ID de gateway de cliente y el ID de gateway privada virtual
- *Marcadores de posición para los puntos finales de la dirección IP remota (externa) (AWS_ENDPOINT_1 y AWS AWS_ENDPOINT_2)*
- Un marcador de posición de posición para la dirección IP de la interfaz externa direccionable a Internet en el dispositivo de gateway de cliente (*su-dirección-ip-cgw*).
- Un marcador de posición para el valor de clave previamente compartida (clave previamente compartida)
- Valores de ejemplo de direcciones IP interiores para el túnel.
- Valores de muestra para la configuración de MTU.

> **Note**
>
> La configuración de MTU proporcionada en los archivos de configuración de muestra son solo ejemplos. Consulte Prácticas recomendadas para su dispositivo de puerta de enlace de cliente para obtener información sobre cómo establecer el valor de MTU óptimo para su situación.

Además de proporcionar valores de marcador de posición, los archivos especifican los requisitos mínimos para una conexión VPN de sitio a sitio de AES128, SHA1 y Diffie-Hellman del grupo 2 en la AWS mayoría de las regiones, y de AES128, SHA2 y Diffie-Hellman del grupo 14 en las regiones. AWS GovCloud También se especifican claves previamente compartidas para la autenticación. Debe modificar el archivo de configuración de ejemplo para aprovecharse de los algoritmos de seguridad adicionales, los grupos Diffie-Hellman, los certificados privados y el tráfico IPv6.

En el siguiente diagrama se ofrece una descripción general de los diferentes componentes que se configuran en el dispositivo de gateway de cliente. Incluye valores de ejemplo para las direcciones IP de la interfaz del túnel.



Procedimientos de interfaz de usuario para el direccionamiento estático

A continuación, se presentan algunos procedimientos de ejemplo para configurar un dispositivo de gateway de cliente a través de su interfaz de usuario (si está disponible).

Check Point

Los siguientes son los pasos para configurar su dispositivo de puerta de enlace de cliente si su dispositivo es un dispositivo Check Point Security Gateway con R77.10 o superior, que utiliza el sistema operativo Gaia y Check Point SmartDashboard. También puede consultar el artículo Check Point Security Gateway IPsec VPN to Amazon Web Services VPC en el centro de soporte técnico de Check Point.

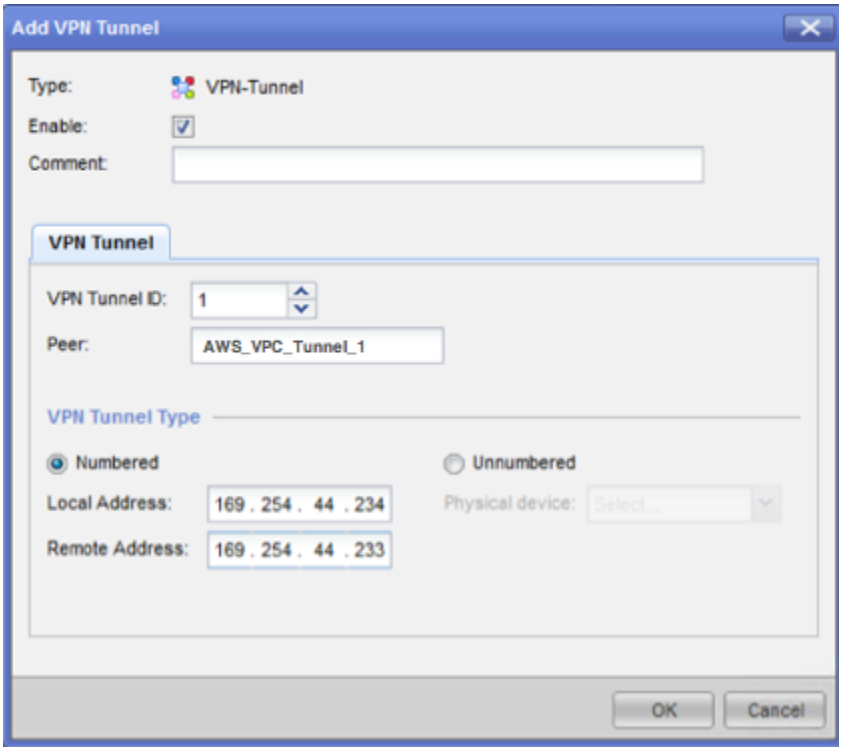
Para configurar la interfaz de túnel

El primer paso es crear los túneles de VPN y proporcionar las direcciones IP privadas (internas) de la gateway de cliente y la gateway privada virtual de cada túnel. Para crear el primer túnel, utilice la información proporcionada en la sección `IPSec Tunnel #1` del archivo de

configuración. Para crear el segundo túnel, utilice los valores proporcionados en la sección `IPSec Tunnel #2` del archivo de configuración.

1. Abra el portal de Gaia de su dispositivo Check Point Security Gateway.
2. Elija Network Interfaces, Add, VPN tunnel.
3. En el cuadro de diálogo, configure los ajustes tal como se muestra y elija OK cuando haya terminado:

   - Para VPN Tunnel ID, escriba cualquier valor único, como 1.
   - Para Peer, escriba un nombre único para cada túnel, como `AWS_VPC_Tunnel_1` o `AWS_VPC_Tunnel_2`.
   - Asegúrese de que la opción Numbered (Numerado) esté seleccionada y, en Local Address (Dirección local), escriba la dirección IP especificada para `CGW Tunnel IP` en el archivo de configuración; por ejemplo: `169.254.44.234`.
   - Para Remote Address, escriba la dirección IP especificada para `VGW Tunnel IP` en el archivo de configuración; por ejemplo: `169.254.44.233`.



4. Conéctese a su gateway de seguridad a través de SSH. Si va a utilizar el shell no predeterminado, cambie a clish ejecutando el siguiente comando: `clish`.

5. Para el túnel 1, ejecute el siguiente comando:

```
set interface vpnt1 mtu 1436
```

   Para el túnel 2, ejecute el siguiente comando:

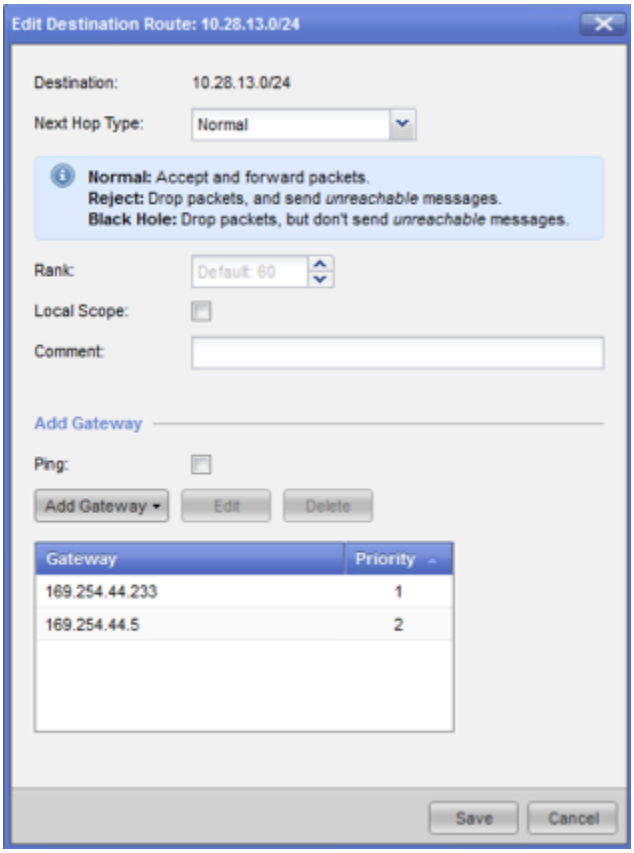
```
set interface vpnt2 mtu 1436
```

6. Repita estos pasos para crear un segundo túnel, utilizando la información de la sección `IPSec Tunnel #2` del archivo de configuración.

Para configurar las rutas estáticas

En este paso, debe especificar la ruta estática de la subred en la VPC para que cada túnel le permita enviar tráfico a través de las interfaces del túnel. El segundo túnel permite la conmutación por error en caso de que haya un problema con el primer túnel. Si se detecta un problema, la ruta estática basada en políticas se quitará de la tabla de ruteo y se activará la segunda ruta. También debe habilitar la gateway de Check Point para hacer ping al otro extremo del túnel y comprobar si el túnel está activo.

1. En el portal de Gaia, elija IPv4 Static Routes, Add.
2. Especifique el CIDR de su subred; por ejemplo: `10.28.13.0/24`.
3. Elija Add Gateway, IP Address.
4. Escriba la dirección IP especificada para `VGW Tunnel IP` en el archivo de configuración (por ejemplo: `169.254.44.233`) y especifique una prioridad de 1.
5. Seleccione Ping.
6. Repita los pasos 3 y 4 para el segundo túnel, utilizando el valor `VGW Tunnel IP` de la sección `IPSec Tunnel #2` del archivo de configuración. Especifique una prioridad de 2.



7. Seleccione Guardar.

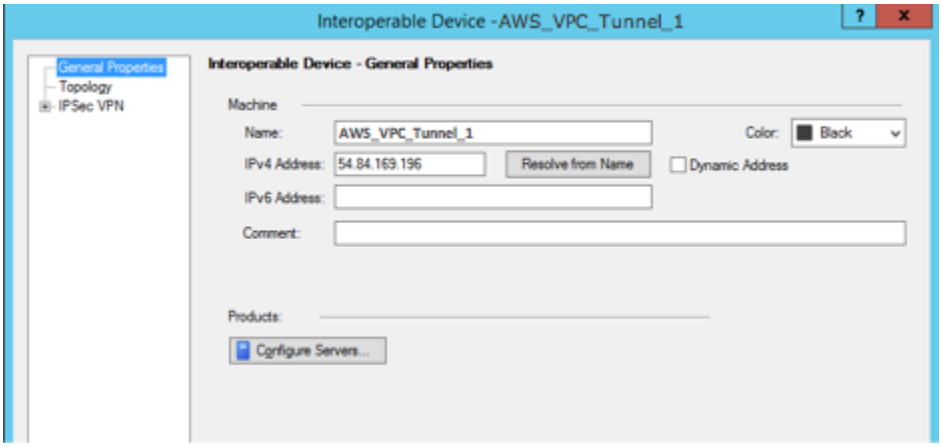
Si va a utilizar un clúster, repita los pasos anteriores para los demás miembros del clúster.

Para definir un nuevo objeto de red

En este paso, creará un objeto de red para cada túnel de VPN, especificando las direcciones IP públicas (externas) de la gateway privada virtual. Más tarde añadirá estos objetos de red como gateways satélite para su comunidad de VPN. También debe crear un grupo vacío para que actúe como marcador de posición para el dominio de VPN.

1. Abra el punto de control. SmartDashboard
2. Para Groups, abra el menú contextual y elija Groups, Simple Group. Puede utilizar el mismo grupo para cada objeto de red.
3. Para Network Objects, abra el menú contextual (clic con el botón derecho) y elija New, Interoperable Device.
4. Para Name (Nombre), escriba el nombre que ha proporcionado para cada túnel, por ejemplo: `AWS_VPC_Tunnel_1` o `AWS_VPC_Tunnel_2`.

5. Para IPv4 Address, escriba la dirección IP externa de la gateway privada virtual proporcionada en el archivo de configuración; por ejemplo: `54.84.169.196`. Guarde la configuración y cierre el cuadro de diálogo.



6. En SmartDashboard, abra las propiedades de la puerta de enlace y, en el panel de categorías, elija Topología.
7. Para recuperar la configuración de la interfaz, elija Get Topology.
8. En la sección VPN Domain (Dominio de VPN), elija Manually defined (Definido manualmente), desplácese hasta el grupo sencillo vacío que creó en el paso 2 y selecciónelo. Seleccione Aceptar.

> **Note**
>
> Puede conservar cualquier dominio de VPN existente que haya configurado. No obstante, asegúrese de que los hosts y las redes utilizados o servidos por la nueva conexión de VPN no estén declarados en ese dominio de VPN, especialmente si el dominio de VPN se obtiene automáticamente.

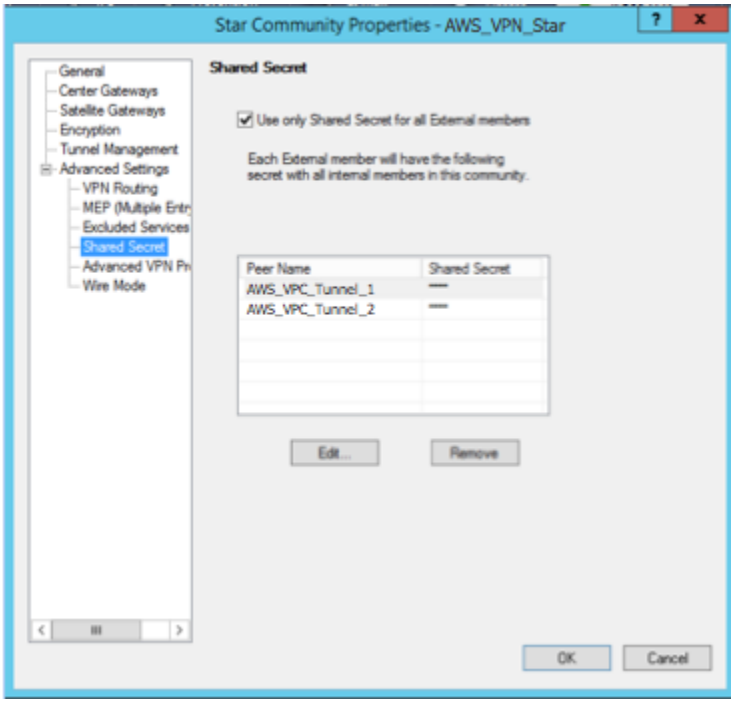
9. Repita estos pasos para crear un segundo objeto de red, utilizando la información de la sección `IPSec Tunnel #2` del archivo de configuración.

> **Note**
>
> Si va a utilizar clústeres, edite la topología y defina las interfaces como interfaces de clúster. Utilice las direcciones IP especificadas en el archivo de configuración.

Para crear y configurar los ajustes de comunidad de VPN, IKE e IPsec

En este paso, creará una comunidad de VPN en su gateway de Check Point, a la que agregará los objetos de red (dispositivos interoperables) para cada túnel. También configurará los ajustes de intercambio de claves por Internet (IKE) y de IPsec.

1. En las propiedades de su gateway, elija IPSec VPN en el panel Category.
2. Elija Communities, New, Star Community.
3. Proporcione un nombre para su comunidad (por ejemplo, `AWS_VPN_Star`) y, a continuación, elija Center Gateways en el panel Category.
4. Elija Add y agregue su gateway o clúster a la lista de gateways participantes.
5. En el panel Category (Categoría), elija Satellite Gateways (Gateways satélite), Add (Agregar), y luego agregue los dispositivos interoperables que creó anteriormente (`AWS_VPC_Tunnel_1` y `AWS_VPC_Tunnel_2`) a la lista de gateways participantes.
6. En el panel Category, elija Encryption. En la sección Encryption Method, elija IKEv1 only. En la sección Encryption Suite, elija Custom, Custom Encryption.
7. En el cuadro de diálogo, configure las propiedades de cifrado tal como se muestra y elija OK cuando haya terminado:
   - Propiedades de asociación de seguridad de IKE (fase 1):
     - Perform key exchange encryption with: AES-128
     - Perform data integrity with: SHA-1
   - Propiedades de asociación de seguridad de IPsec (fase 2):
     - Perform IPsec data encryption with: AES-128
     - Perform data integrity with: SHA-1
8. En el panel Category, elija Tunnel Management. Elija Set Permanent Tunnels, On all tunnels in the community. En la sección VPN Tunnel Sharing, elija One VPN tunnel per Gateway pair.
9. En el panel Category, expanda Advanced Settings y elija Shared Secret.
10. Seleccione el nombre homólogo para el primer túnel, elija Edit (Editar) y escriba la clave previamente compartida según lo especificado en la sección `IPSec Tunnel #1` del archivo de configuración.
11. Seleccione el nombre homólogo para el segundo túnel, elija Edit (Editar) y escriba la clave previamente compartida según lo especificado en la sección `IPSec Tunnel #2` del archivo de configuración.



12. Aún en la categoría Advanced Settings (Configuración avanzada), elija Advanced VPN Properties (Propiedades avanzadas de VPN), configure las propiedades según se indica y elija OK (Aceptar) cuando haya terminado:

    - IKE (fase 1):
        - Use Diffie-Hellman group (Usar el grupo Diffie-Hellman): `Group 2`
        - Renegotiate IKE security associations every `480` minutes
    - IPsec (fase 2):
        - Elija Use Perfect Forward Secrecy
        - Use Diffie-Hellman group (Usar el grupo Diffie-Hellman): `Group 2`
        - Renegotiate IPsec security associations every `3600` seconds

Para crear reglas de firewall

En este paso, configurará una política con reglas de firewall y reglas de coincidencia direccional que permitan la comunicación entre la VPC y la red local. Luego instalará la política en su gateway.

1. En el SmartDashboard, elija Propiedades globales para su puerta de enlace. En el panel Category, expanda VPN y elija Advanced.
2. Elija Enable VPN Directional Match in VPN Column y guarde los cambios.

3. En el SmartDashboard, elija Firewall y cree una política con las siguientes reglas:
   - Permitir que la subred de VPC se comunique con la red local a través de los protocolos necesarios.
   - Permitir que la red local se comunique con la subred de VPC a través de los protocolos necesarios.
4. Abra el menú contextual para la celda de la columna de VPN, y elija Edit Cell.
5. En el cuadro de diálogo VPN Match Conditions, elija Match traffic in this direction only. Cree las siguientes reglas de coincidencia direccional; para ello, elija Add para cada una, y seleccione OK cuando haya terminado:
   - `internal_clear` > VPN community (Comunidad VPN) (la comunidad Star de VPN que creó antes; por ejemplo: `AWS_VPN_Star`)
   - VPN community > VPN community
   - Comunidad VPN > `internal_clear`
6. En el SmartDashboard, selecciona Política e instala.
7. En el cuadro de diálogo, elija su gateway y seleccione OK para instalar la política.

Para modificar la propiedad tunnel_keepalive_method

Su gateway de Check Point puede utilizar la detección de pares muertos (DPD) para identificar cuándo se desactiva una asociación de IKE. Para configurar DPD para un túnel permanente, el túnel permanente debe configurarse en la comunidad de AWS VPN (consulte el paso 8).

De forma predeterminada, la propiedad `tunnel_keepalive_method` de una gateway de VPN está configurada como `tunnel_test`. Debe cambiar el valor a `dpd`. Cada gateway de VPN de la comunidad de VPN que requiera monitorización de DPD debe configurarse con la propiedad `tunnel_keepalive_method`, incluida cualquier gateway de VPN de terceros. No puede configurar mecanismos de monitorización distintos para la misma gateway.

Puede actualizar la propiedad `tunnel_keepalive_method` utilizando la herramienta GuiDBedit.

1. Abra el Check Point SmartDashboard y elija Security Management Server, Domain Management Server.
2. Elija File, Database Revision Control..., y cree una instantánea de revisión.

3. Cierre todas las SmartConsole ventanas, como el SmartDashboard SmartView Rastreador y el SmartView Monitor.
4. Inicie la herramienta GuiBDedit. Para obtener más información, consulte el artículo Check Point Database Tool, en el centro de soporte técnico de Check Point.
5. Elija Security Management Server, Domain Management Server.
6. En el panel superior izquierdo, elija Table, Network Objects, network_objects.
7. En el panel superior derecho, seleccione el objeto de Security Gateway, Cluster correspondiente.
8. Presione CTRL+F, o utilice el menú Search para buscar lo siguiente: `tunnel_keepalive_method`.
9. En el panel inferior, abra el menú contextual de `tunnel_keepalive_method` y seleccione Edit... (Editar...). Elija dpd y luego OK (Aceptar).
10. Repita los pasos del 7 al 9 por cada gateway que forme parte de la comunidad de AWS VPN.
11. Elija File, Save All.
12. Cierre la herramienta GuiDBedit.
13. Abra el Check Point SmartDashboard y elija Security Management Server, Domain Management Server.
14. Instale la política en el objeto Security Gateway, Cluster correspondiente.

Para obtener más información, consulte el artículo New VPN features in R77.10, en el centro de soporte técnico de Check Point.

Para habilitar el bloqueo TCP MSS

El bloqueo de TCP MSS reduce el tamaño máximo de segmento de los paquetes TCP para evitar la fragmentación de los paquetes.

1. Vaya al siguiente directorio: `C:\Program Files (x86)\CheckPoint\SmartConsole\R77.10\PROGRAM\`.
2. Abra la herramienta Check Point Database ejecutando el archivo `GuiDBEdit.exe`.
3. Elija Table, Global Properties, properties.
4. Para `fw_clamp_tcp_mss`, elija Edit. Cambie el valor a `true` y elija OK.

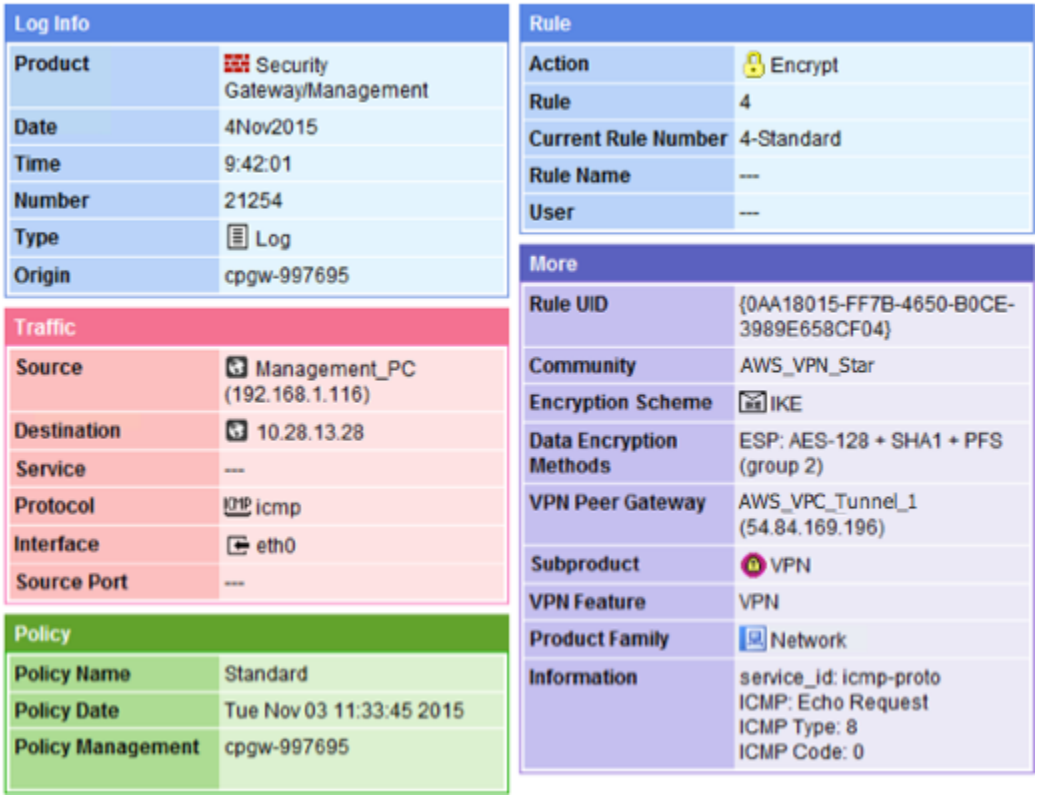
Para verificar el estado del túnel

Puede verificar el estado del túnel ejecutando el siguiente comando desde la herramienta de línea de comandos en el modo experto.

```
vpn tunnelutil
```

En las opciones que aparecen, elija 1 para verificar las asociaciones de IKE y 2 para verificar las asociaciones de IPsec.

También puede utilizar Check Point Smart Tracker Log para verificar que los paquetes de la conexión se están cifrando. Por ejemplo, el siguiente log indica que un paquete para la VPC se ha enviado a través del túnel 1 y se ha cifrado.



SonicWALL

El procedimiento siguiente muestra cómo configurar los túneles de VPN en el dispositivo SonicWALL utilizando la interfaz de gestión SonicOS.

Para configurar los túneles

1. Abra la interfaz de gestión SonicWALL SonicOS.
2. En el panel izquierdo, elija VPN, Settings. En VPN Policies, elija Add....
3. En la ventana de política de VPN de la pestaña General , complete la información siguiente:

- Policy Type (Tipo de política): seleccione Tunnel Interface (Interfaz de túnel).
- Authentication Method: elija IKE using Preshared Secret.
- Name: escriba un nombre para la política de VPN. Le recomendamos utilizar el nombre del ID de VPN tal como se indica en el archivo de configuración.
- Nombre o dirección de gateway principal de IPsec: escriba la dirección IP de la gateway privada virtual tal como se indica en el archivo de configuración (por ejemplo, `72.21.209.193`).
- IPsec Secondary Gateway Name or Address: deje el valor predeterminado.
- Shared Secret: escriba la clave previamente compartida tal como se indica en el archivo de configuración y vuelva a escribirla en Confirm Shared Secret.
- Local IKE ID: escriba la dirección IPv4 de la gateway de cliente (dispositivo SonicWALL).
- Peer IKE ID: escriba la dirección IPv4 de la gateway privada virtual.

4. En la pestaña Network, complete la información siguiente:

   - En Local Networks, elija Any address. Se recomienda utilizar esta opción para evitar problemas de conectividad en su red local.
   - En Remote Networks, elija Choose a destination network from list. Cree un objeto de dirección con el CIDR de su VPC en AWS.

5. En la pestaña Proposals (Propuestas), complete la información siguiente:

   - En IKE (Phase 1) Proposal, haga lo siguiente:
     - Exchange: elija Main Mode.
     - DH Group (Grupo de DH): escriba un valor para el grupo Diffie-Hellman (por ejemplo, 2).
     - Encryption: elija AES-128 o AES-256.
     - Authentication: elija SHA1 o SHA256.
     - Life Time: escriba `28800`.
   - En IKE (Phase 2) Proposal, haga lo siguiente:
     - Protocol: elija ESP.
     - Encryption: elija AES-128 o AES-256.
     - Authentication: elija SHA1 o SHA256.
     - Seleccione la casilla de verificación Enable Perfect Forward Secrecy y elija el grupo Diffie-Hellman.

- Life Time: escriba `3600`.

> **Important**
>
> Si creó su gateway privada virtual antes de octubre de 2015, debe especificar el grupo 2 de Diffie-Hellman, AES-128 y SHA1 para ambas fases.

6. En la pestaña Advanced, complete la información siguiente:
   - Seleccione Enable Keep Alive.
   - Seleccione Enable Phase2 Dead Peer Detection y escriba lo siguiente:
     - En Dead Peer Detection Interval, escriba `60` (este es el valor mínimo que puede aceptar el dispositivo SonicWALL).
     - En Failure Trigger Level, escriba `3`.
   - En VPN Policy bound to, seleccione Interface X1. Esta es la interfaz que suele designarse para las direcciones IP públicas.
7. Seleccione Aceptar. En la página Settings, debe seleccionar la casilla de verificación Enable para el túnel de manera predeterminada. El punto verde indica que el túnel está activo.

Información adicional para dispositivos Cisco

Algunos Cisco ASA solo admiten el modo Active/Standby. Al utilizar estos Cisco ASA, solo puede tener un túnel activo cada vez. El otro túnel en espera se activará si el primer túnel se vuelve no disponible. Con esta redundancia, siempre debería tener conectividad a su VPC a través de uno de los túneles.

Cisco ASA a partir de la versión 9.7.1 y posteriores admiten el modo Activo/Activo. Al utilizar estos Cisco ASA, puede tener ambos túneles activos al mismo tiempo. Con esta redundancia, siempre debería tener conectividad a su VPC a través de uno de los túneles.

Para los dispositivos Cisco, debe hacer lo siguiente:

- Configurar la interfaz externa.
- Asegurarse de que el número de secuencia de política de Crypto ISAKMP es único.
- Asegurarse de que el número de secuencia de política de Crypto List es único.

- Asegurarse de que Crypto IPsec Transform Set y la secuencia de política de Crypto ISAKMP son coherentes con los demás túneles IPsec que están configurados en el dispositivo.
- Asegurarse de que el número de monitorización de SLA es único.
- Configurar todo el direccionamiento interno que mueve el tráfico entre el dispositivo de gateway de cliente y su red local.

Pruebas

Para obtener más información acerca de cómo probar la conexión de Site-to-Site VPN, consulte Prueba de una conexión de Site-to-Site VPN.

Ejemplos de configuraciones de dispositivos de gateway de cliente para el direccionamiento dinámico (BGP)

Temas

Archivos de configuración de ejemplo

Para descargar un archivo de configuración de muestra con valores específicos para la configuración de conexión de la VPN de sitio a sitio, utilice la consola de Amazon VPC, la línea de comandos AWS o la API de Amazon EC2. Para obtener más información, consulte Paso 6: Descargar el archivo de configuración.

También puede descargar archivos genéricos de configuración de ejemplo para enrutamiento dinámico que no incluyen valores específicos de la configuración de conexión Site-to-Site VPN: dynamic-routing-examples.zip

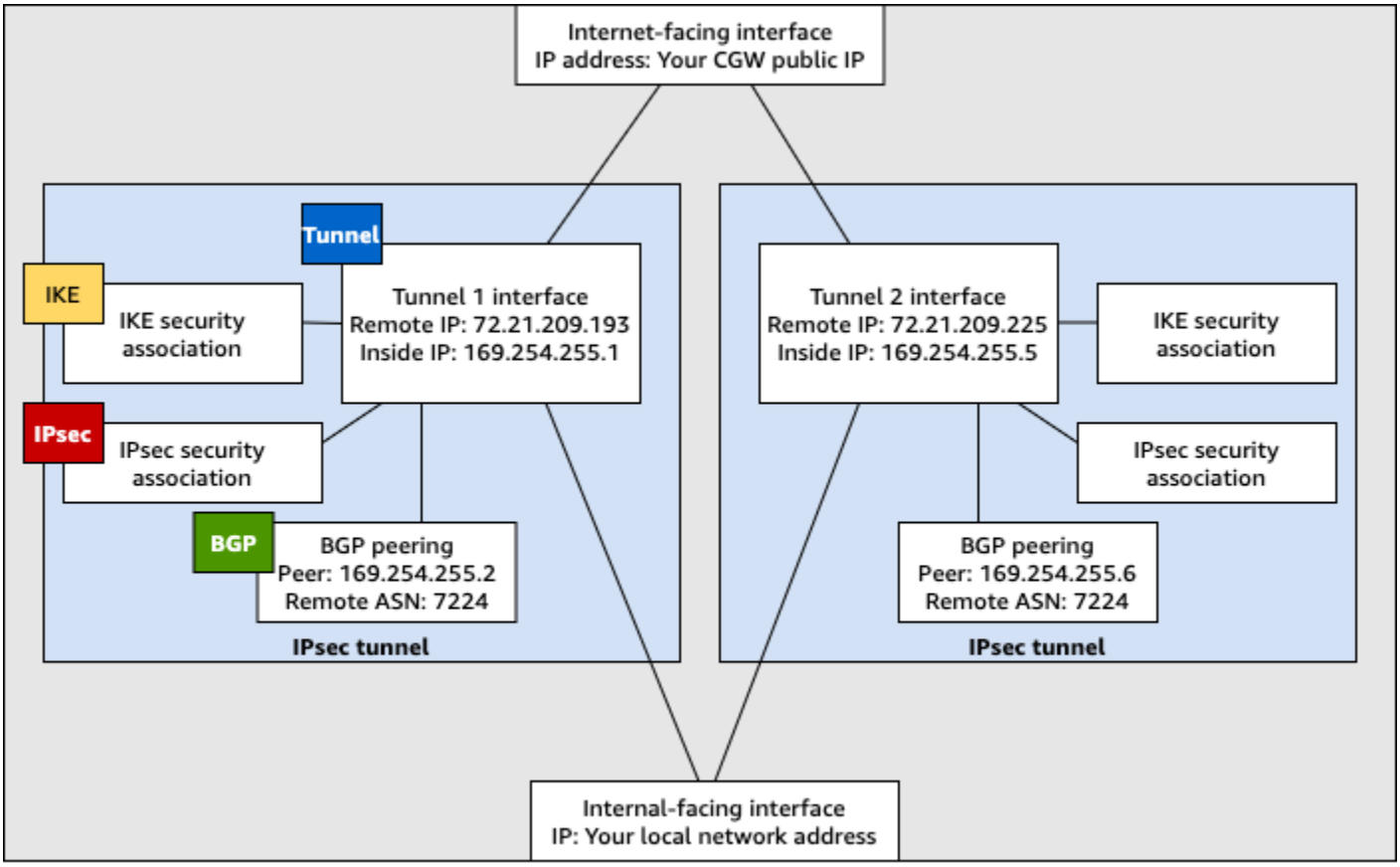
Los archivos utilizan valores de marcadores de posición para algunos componentes. Por ejemplo, usan:

- Valores de ejemplo para el ID de conexión de VPN, el ID de gateway de cliente y el ID de gateway privada virtual
- *Marcadores de posición para los puntos finales de la dirección IP remota (externa) (AWS_ENDPOINT_1 y AWS AWS_ENDPOINT_2)*
- Un marcador de posición de posición para la dirección IP de la interfaz externa direccionable a Internet en el dispositivo de gateway de cliente (*su-dirección-ip-cgw*).
- Un marcador de posición para el valor de clave previamente compartida (clave previamente compartida)
- Valores de ejemplo de direcciones IP interiores para el túnel.
- Valores de muestra para la configuración de MTU.

> **Note**
>
> La configuración de MTU proporcionada en los archivos de configuración de muestra son solo ejemplos. Consulte Prácticas recomendadas para su dispositivo de puerta de enlace de cliente para obtener información sobre cómo establecer el valor de MTU óptimo para su situación.

Además de proporcionar valores de marcador de posición, los archivos especifican los requisitos mínimos para una conexión VPN de sitio a sitio de AES128, SHA1 y Diffie-Hellman del grupo 2 en la AWS mayoría de las regiones, y de AES128, SHA2 y Diffie-Hellman del grupo 14 en las regiones. AWS GovCloud También se especifican claves previamente compartidas para la autenticación. Debe modificar el archivo de configuración de ejemplo para aprovecharse de los algoritmos de seguridad adicionales, los grupos Diffie-Hellman, los certificados privados y el tráfico IPv6.

En el siguiente diagrama se ofrece una descripción general de los diferentes componentes que se configuran en el dispositivo de gateway de cliente. Incluye valores de ejemplo para las direcciones IP de la interfaz del túnel.



Customer gateway device

Procedimientos de la interfaz de usuario para el direccionamiento dinámico

A continuación, se presentan algunos procedimientos de ejemplo para configurar un dispositivo de gateway de cliente a través de su interfaz de usuario (si está disponible).

Check Point

Los siguientes son los pasos para configurar un dispositivo Check Point Security Gateway que ejecute la versión R77.10 o superior, mediante el portal web de Gaia y Check Point. SmartDashboard También puede consultar el artículo Amazon Web Services (AWS) VPN BGP en el centro de soporte técnico de Check Point.

Para configurar la interfaz de túnel

El primer paso es crear los túneles de VPN y proporcionar las direcciones IP privadas (internas) de la gateway de cliente y la gateway privada virtual de cada túnel. Para crear el primer túnel, utilice la información proporcionada en la sección `IPSec Tunnel #1` del archivo de

configuración. Para crear el segundo túnel, utilice los valores proporcionados en la sección `IPSec Tunnel #2` del archivo de configuración.

1. Conéctese a su gateway de seguridad a través de SSH. Si va a utilizar el shell no predeterminado, cambie a clish ejecutando el siguiente comando: `clish`.
2. Configure el ASN de la puerta de enlace del cliente (el ASN que se proporcionó cuando se creó la puerta de enlace del cliente en AWS) ejecutando el siguiente comando.

```
set as 65000
```

3. Cree la interfaz del primer túnel utilizando la información que se proporciona en la sección `IPSec Tunnel #1` del archivo de configuración. Especifique un nombre exclusivo para su túnel como, por ejemplo, `AWS_VPC_Tunnel_1`.

```
add vpn tunnel 1 type numbered local 169.254.44.234 remote 169.254.44.233
 peer AWS_VPC_Tunnel_1
set interface vpnt1 state on
set interface vpnt1 mtu 1436
```

4. Repita estos comandos para crear el segundo túnel utilizando la información que se proporciona en la sección `IPSec Tunnel #2` del archivo de configuración. Especifique un nombre exclusivo para su túnel como, por ejemplo, `AWS_VPC_Tunnel_2`.

```
add vpn tunnel 1 type numbered local 169.254.44.38 remote 169.254.44.37
 peer AWS_VPC_Tunnel_2
set interface vpnt2 state on
set interface vpnt2 mtu 1436
```

5. Establezca el ASN de la gateway privada virtual.

```
set bgp external remote-as 7224 on
```

6. Configure BGP para el primer túnel utilizando la información que se proporciona en la sección `IPSec Tunnel #1` del archivo de configuración.

```
set bgp external remote-as 7224 peer 169.254.44.233 on
set bgp external remote-as 7224 peer 169.254.44.233 holdtime 30
set bgp external remote-as 7224 peer 169.254.44.233 keepalive 10
```

7. Configure BGP para el segundo túnel utilizando la información que se proporciona en la sección `IPSec Tunnel #2` del archivo de configuración.

```
set bgp external remote-as 7224 peer 169.254.44.37 on
set bgp external remote-as 7224 peer 169.254.44.37 holdtime 30
set bgp external remote-as 7224 peer 169.254.44.37 keepalive 10
```

8. Guarde la configuración.

```
save config
```

Para crear una política de BGP

A continuación, cree una política de BGP que permita importar las rutas que anuncia AWS. A continuación, configurará la gateway de cliente para anunciar estas rutas locales a AWS.

1. En Gaia WebUI, elija Advanced Routing, Inbound Route Filters. Elija Add y seleccione Add BGP Policy (Based on AS).
2. En Add BGP Policy (Añadir política de BGP), seleccione un valor entre 512 y 1024 en el primer campo y escriba el ASN de la gateway privada virtual en el segundo campo (por ejemplo, `7224`).
3. Seleccione Guardar.

Para anunciar rutas locales

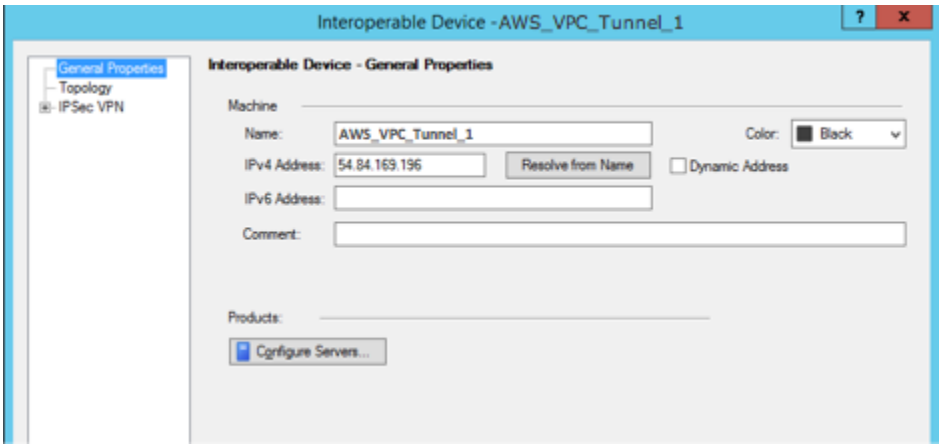
A continuación se presentan los pasos para distribuir rutas de interfaces locales. También puede redistribuir rutas desde distintos orígenes (por ejemplo, rutas estáticas o rutas obtenidas mediante protocolos de direccionamiento dinámico). Para obtener más información, consulte la Gaia Advanced Routing R77 Versions Administration Guide.

1. En Gaia WebUI, elija Advanced Routing, Routing Redistribution. Elija Add Redistribution From (Añadir redistribución desde) y luego seleccione Interface (Interfaz).
2. En To Protocol (A protocolo), seleccione el ASN de la gateway privada virtual (por ejemplo, `7224`).
3. En Interface, seleccione una interfaz interna. Seleccione Guardar.

Para definir un nuevo objeto de red

A continuación, cree un objeto de red para cada túnel de VPN, especificando las direcciones IP públicas (externas) de la gateway privada virtual. Más tarde añadirá estos objetos de red como gateways satélite para su comunidad de VPN. También debe crear un grupo vacío para que actúe como marcador de posición para el dominio de VPN.

1. Abra el punto de control. SmartDashboard
2. Para Groups, abra el menú contextual y elija Groups, Simple Group. Puede utilizar el mismo grupo para cada objeto de red.
3. Para Network Objects, abra el menú contextual (clic con el botón derecho) y elija New, Interoperable Device.
4. En Name (Nombre), escriba el nombre que ha proporcionado para el túnel en el paso 1, por ejemplo: `AWS_VPC_Tunnel_1` o `AWS_VPC_Tunnel_2`.
5. Para IPv4 Address, escriba la dirección IP externa de la gateway privada virtual proporcionada en el archivo de configuración; por ejemplo: `54.84.169.196`. Guarde la configuración y cierre el cuadro de diálogo.



6. En el panel de categorías izquierdo, elija Topology.
7. En la sección VPN Domain (Dominio de VPN), elija Manually defined (Definido manualmente), desplácese hasta el grupo sencillo vacío que creó en el paso 2 y selecciónelo. Seleccione Aceptar.
8. Repita estos pasos para crear un segundo objeto de red, utilizando la información de la sección `IPSec Tunnel #2` del archivo de configuración.
9. Vaya a su objeto de red de gateway, abra el objeto de clúster o gateway y elija Topology.

10. En la sección VPN Domain (Dominio de VPN), elija Manually defined (Definido manualmente), desplácese hasta el grupo sencillo vacío que creó en el paso 2 y selecciónelo. Seleccione Aceptar.

> **Note**
>
> Puede conservar cualquier dominio de VPN existente que haya configurado. No obstante, asegúrese de que los hosts y las redes utilizados o servidos por la nueva conexión de VPN no estén declarados en ese dominio de VPN, especialmente si el dominio de VPN se obtiene automáticamente.

> **Note**
>
> Si va a utilizar clústeres, edite la topología y defina las interfaces como interfaces de clúster. Utilice las direcciones IP especificadas en el archivo de configuración.

Para crear y configurar los ajustes de comunidad de VPN, IKE e IPsec

A continuación, cree una comunidad de VPN en su gateway de Check Point, a la que agregará los objetos de red (dispositivos interoperables) para cada túnel. También configurará los ajustes de intercambio de claves por Internet (IKE) y de IPsec.

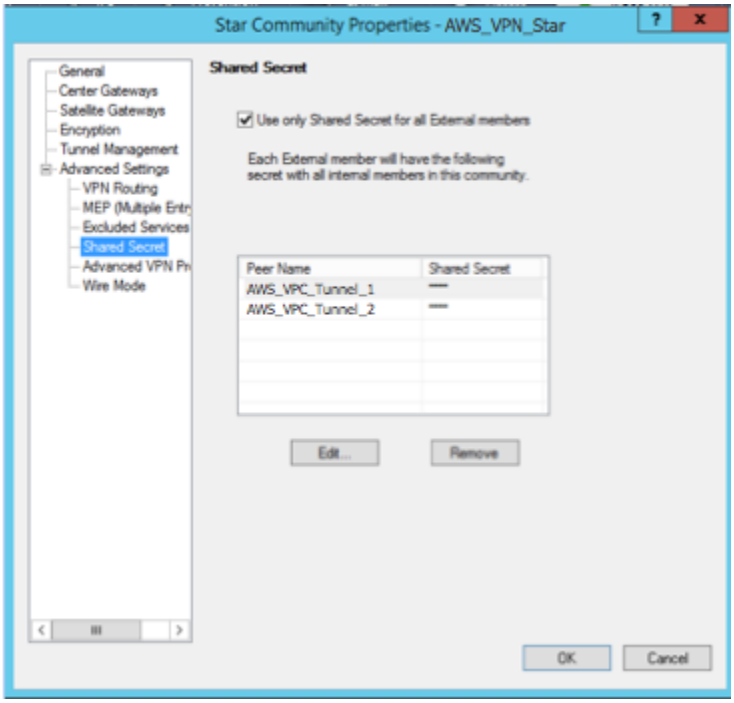
1. En las propiedades de su gateway, elija IPSec VPN en el panel Category.
2. Elija Communities, New, Star Community.
3. Proporcione un nombre para su comunidad (por ejemplo, `AWS_VPN_Star`) y, a continuación, elija Center Gateways en el panel Category.
4. Elija Add y agregue su gateway o clúster a la lista de gateways participantes.
5. En el panel Category (Categoría), elija Satellite Gateways (Gateways satélite), Add (Agregar), y agregue los dispositivos interoperables que creó anteriormente (`AWS_VPC_Tunnel_1` y `AWS_VPC_Tunnel_2`) a la lista de gateways participantes.
6. En el panel Category, elija Encryption. En la sección Encryption Method, elija IKEv1 for IPv4 and IKEv2 for IPv6. En la sección Encryption Suite, elija Custom, Custom Encryption.

> **Note**
>
> Debe seleccionar la opción IKEv1 para IPv4 e IKEv2 para IPv6 para la funcionalidad IKEv1.

7. En el cuadro de diálogo, configure las propiedades de cifrado tal como se muestra y elija OK (Aceptar) cuando haya terminado:

   - Propiedades de asociación de seguridad de IKE (fase 1):
     - Perform key exchange encryption with: AES-128
     - Perform data integrity with: SHA-1
   - Propiedades de asociación de seguridad de IPsec (fase 2):
     - Perform IPsec data encryption with: AES-128
     - Perform data integrity with: SHA-1

8. En el panel Category, elija Tunnel Management. Elija Set Permanent Tunnels, On all tunnels in the community. En la sección VPN Tunnel Sharing, elija One VPN tunnel per Gateway pair.
9. En el panel Category, expanda Advanced Settings y elija Shared Secret.
10. Seleccione el nombre homólogo para el primer túnel, elija Edit (Editar) y escriba la clave previamente compartida según lo especificado en la sección `IPSec Tunnel #1` del archivo de configuración.
11. Seleccione el nombre homólogo para el segundo túnel, elija Edit (Editar) y escriba la clave previamente compartida según lo especificado en la sección `IPSec Tunnel #2` del archivo de configuración.



12. Aún en la categoría Advanced Settings (Configuración avanzada), elija Advanced VPN Properties (Propiedades avanzadas de VPN), configure las propiedades según se indica y elija OK (Aceptar) cuando haya terminado:

    - IKE (fase 1):
        - Use Diffie-Hellman group (Usar el grupo Diffie-Hellman): `Group 2 (1024 bit)`
        - Renegotiate IKE security associations every `480` minutes
    - IPsec (fase 2):
        - Elija Use Perfect Forward Secrecy
        - Use Diffie-Hellman group (Usar el grupo Diffie-Hellman): `Group 2 (1024 bit)`
        - Renegotiate IPsec security associations every `3600` seconds

Para crear reglas de firewall

A continuación, configurará una política con reglas de firewall y reglas de coincidencia direccional que permitan la comunicación entre la VPC y la red local. Luego instalará la política en su gateway.

1. En SmartDashboard, elija Propiedades globales para su puerta de enlace. En el panel Category, expanda VPN y elija Advanced.
2. Elija Enable VPN Directional Match in VPN Column y elija OK.

3. En el SmartDashboard, elija Firewall y cree una política con las siguientes reglas:
   - Permitir que la subred de VPC se comunique con la red local a través de los protocolos necesarios.
   - Permitir que la red local se comunique con la subred de VPC a través de los protocolos necesarios.
4. Abra el menú contextual para la celda de la columna de VPN, y elija Edit Cell.
5. En el cuadro de diálogo VPN Match Conditions, elija Match traffic in this direction only. Cree las siguientes reglas de coincidencia direccional; para ello, elija Add (Agregar) para cada una y seleccione OK (Aceptar) cuando haya terminado:
   - `internal_clear` > VPN community (Comunidad VPN) (la comunidad Star de VPN que creó antes; por ejemplo: `AWS_VPN_Star`)
   - VPN community > VPN community
   - Comunidad VPN > `internal_clear`
6. En el SmartDashboard, selecciona Política e instala.
7. En el cuadro de diálogo, elija su gateway y seleccione OK para instalar la política.

Para modificar la propiedad tunnel_keepalive_method

Su gateway de Check Point puede utilizar la detección de pares muertos (DPD) para identificar cuándo se desactiva una asociación de IKE. Para configurar DPD para un túnel permanente, el túnel permanente debe configurarse en la comunidad de AWS VPN.

De forma predeterminada, la propiedad `tunnel_keepalive_method` de una gateway de VPN está configurada como `tunnel_test`. Debe cambiar el valor a `dpd`. Cada gateway de VPN de la comunidad de VPN que requiera monitorización de DPD debe configurarse con la propiedad `tunnel_keepalive_method`, incluida cualquier gateway de VPN de terceros. No puede configurar mecanismos de monitorización distintos para la misma gateway.

Puede actualizar la propiedad `tunnel_keepalive_method` utilizando la herramienta GuiDBedit.

1. Abra el Check Point SmartDashboard y elija Security Management Server, Domain Management Server.
2. Elija File, Database Revision Control..., y cree una instantánea de revisión.

3. Cierre todas las SmartConsole ventanas, como el SmartDashboard SmartView Rastreador y el SmartView Monitor.
4. Inicie la herramienta GuiBDedit. Para obtener más información, consulte el artículo Check Point Database Tool, en el centro de soporte técnico de Check Point.
5. Elija Security Management Server, Domain Management Server.
6. En el panel superior izquierdo, elija Table, Network Objects, network_objects.
7. En el panel superior derecho, seleccione el objeto de Security Gateway, Cluster correspondiente.
8. Presione CTRL+F, o utilice el menú Search para buscar lo siguiente: `tunnel_keepalive_method`.
9. En el panel inferior, abra el menú contextual de `tunnel_keepalive_method` y seleccione Edit... Elija dpd, OK (Aceptar).
10. Repita los pasos del 7 al 9 por cada gateway que forme parte de la comunidad de AWS VPN.
11. Elija File, Save All.
12. Cierre la herramienta GuiDBedit.
13. Abra el Check Point SmartDashboard y elija Security Management Server, Domain Management Server.
14. Instale la política en el objeto Security Gateway, Cluster correspondiente.

Para obtener más información, consulte el artículo New VPN features in R77.10, en el centro de soporte técnico de Check Point.

Para habilitar el bloqueo TCP MSS

El bloqueo de TCP MSS reduce el tamaño máximo de segmento de los paquetes TCP para evitar la fragmentación de los paquetes.

1. Vaya al siguiente directorio: `C:\Program Files (x86)\CheckPoint\SmartConsole\R77.10\PROGRAM\`.
2. Abra la herramienta Check Point Database ejecutando el archivo `GuiDBEdit.exe`.
3. Elija Table, Global Properties, properties.
4. Para `fw_clamp_tcp_mss`, elija Edit. Cambie el valor a `true` y luego elija OK (Aceptar).

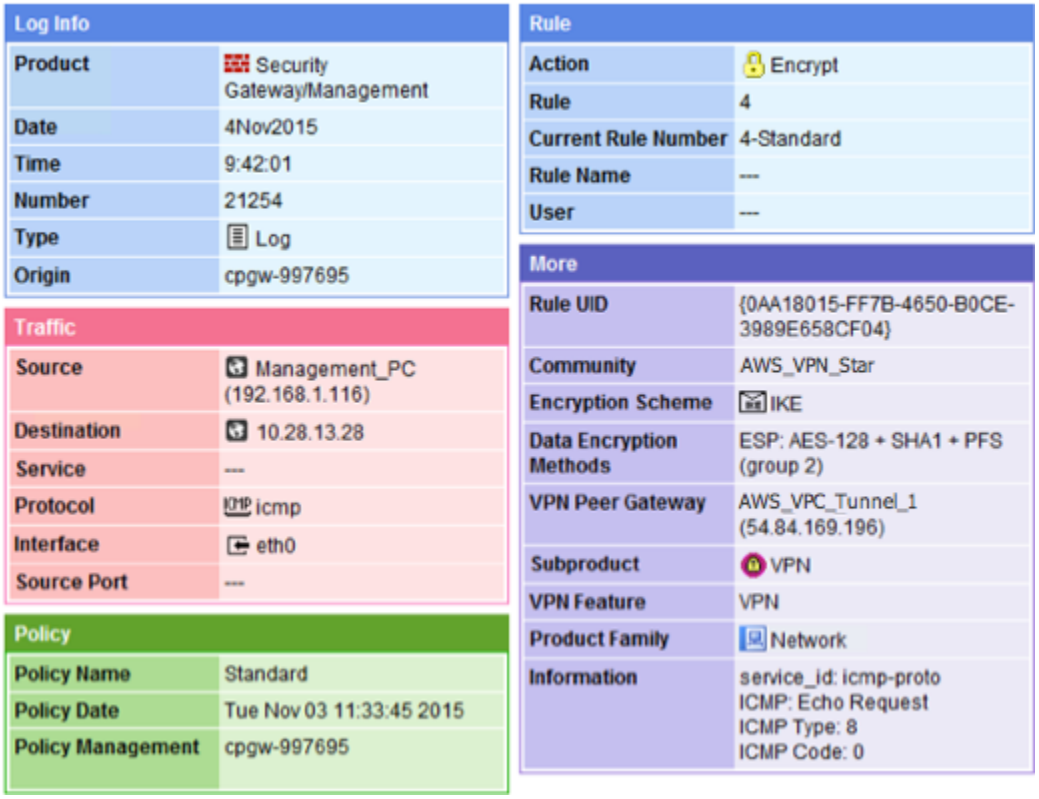
Para verificar el estado del túnel

Puede verificar el estado del túnel ejecutando el siguiente comando desde la herramienta de línea de comandos en el modo experto.

```
vpn tunnelutil
```

En las opciones que aparecen, elija 1 para verificar las asociaciones de IKE y 2 para verificar las asociaciones de IPsec.

También puede utilizar Check Point Smart Tracker Log para verificar que los paquetes de la conexión se están cifrando. Por ejemplo, el siguiente log indica que un paquete para la VPC se ha enviado a través del túnel 1 y se ha cifrado.



SonicWALL

Puede configurar el dispositivo SonicWALL mediante la interfaz de administración de SonicOS. Para obtener más información sobre la configuración de los túneles, consulte Procedimientos de interfaz de usuario para el direccionamiento estático.

Sin embargo, no es posible configurar BGP para el dispositivo utilizando la interfaz de administración. En su lugar, utilice las instrucciones de la línea de comandos que se ofrecen en el archivo de configuración de ejemplo, en la sección BGP.

Información adicional para dispositivos Cisco

Algunos Cisco ASA solo admiten el modo Active/Standby. Al utilizar estos Cisco ASA, solo puede tener un túnel activo cada vez. El otro túnel en espera se activará si el primer túnel se vuelve no disponible. Con esta redundancia, siempre debería tener conectividad a su VPC a través de uno de los túneles.

Cisco ASA a partir de la versión 9.7.1 y posteriores admiten el modo Activo/Activo. Al utilizar estos Cisco ASA, puede tener ambos túneles activos al mismo tiempo. Con esta redundancia, siempre debería tener conectividad a su VPC a través de uno de los túneles.

Para los dispositivos Cisco, debe hacer lo siguiente:

- Configurar la interfaz externa.
- Asegurarse de que el número de secuencia de política de Crypto ISAKMP es único.
- Asegurarse de que el número de secuencia de política de Crypto List es único.
- Asegurarse de que Crypto IPsec Transform Set y la secuencia de política de Crypto ISAKMP son coherentes con los demás túneles IPsec que están configurados en el dispositivo.
- Asegurarse de que el número de monitorización de SLA es único.
- Configurar todo el direccionamiento interno que mueve el tráfico entre el dispositivo de gateway de cliente y su red local.

Información adicional para dispositivos Juniper

La siguiente información se aplica a los archivos de configuración de ejemplo para dispositivos de gateway de cliente SRX y Juniper J-Series.

- La interfaz externa se conoce como *ge-0/0/0.0*.
- Los ID de la interfaz de túnel se conocen como *st0.1* y *st0.2*.
- Asegúrese de identificar la zona de seguridad para la interfaz del enlace de subida (la información de configuración utiliza la zona predeterminada "poco fiable").
- Asegúrese de identificar la zona de seguridad para la interfaz interior (la información de configuración utiliza la zona predeterminada "de confianza").

Pruebas

Para obtener más información acerca de cómo probar la conexión de Site-to-Site VPN, consulte Prueba de una conexión de Site-to-Site VPN.

Configuración de Windows Server como dispositivo de gateway de cliente

Puede configurar el servidor que ejecute Windows Server como dispositivo de gateway de cliente para la VPC. Utilice el siguiente proceso tanto si ejecuta Windows Server en una instancia de EC2 en una VPC o en su propio servidor. Los siguientes procedimientos se aplican a Windows Server 2012 R2 y versiones posteriores.

Contenido

Configuración de instancias de Windows

Si configura Windows Server en una instancia EC2 iniciada desde una AMI de Windows, haga lo siguiente:

- Deshabilite la comprobación de origen/destino para la instancia:
  1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
  2. Seleccione la instancia de Windows y elija Actions (Acciones), Networking (Redes), Change source/destination check (Cambiar comprobación de origen o destino). Elija Stop (Detener)y, a continuación, seleccione Save (Guardar).
- Actualice la configuración del adaptador para poder direccionar el tráfico procedente de otras instancias:

1. Conéctese a la instancia de Windows. Para obtener más información, consulte Conexión con la instancia de Windows.
2. Abra el Panel de control e inicie el Administrador de dispositivos.
3. Expanda el nodo Adaptadores de red.
4. Seleccione el adaptador de red (según el tipo de instancia, puede ser Amazon Elastic Network Adapter o Intel 82599 Virtual Function) y elija Action (Acción), Properties (Propiedades).
5. En la pestaña Advanced, deshabilite las propiedades IPv4 Checksum Offload, TCP Checksum Offload (IPv4) y UDP Checksum Offload (IPv4) y, a continuación, elija OK.

- Asigne una dirección IP elástica a su cuenta y asóciela a la instancia. Para obtener más información, consulte Uso de direcciones IP elásticas. Anote esta dirección, ya que la necesitará para crear la gateway de cliente en su VPC.
- Asegúrese de que las reglas del grupo de seguridad de su instancia permiten el tráfico IPsec saliente. De forma predeterminada, un grupo de seguridad permite todo el tráfico saliente. No obstante, si el estado original de las reglas salientes del grupo de seguridad se ha modificado, debe crear las siguientes reglas de protocolo personalizadas de salida para el tráfico IPsec: protocolo IP 50, protocolo IP 51 y UDP 500.

Tome nota del intervalo CIDR de la red en la que se encuentra la instancia de Windows, por ejemplo, `172.31.0.0/16`.

Paso 1: Crear una conexión de VPN y configurar la VPC

Para crear una conexión VPN desde la VPC, haga lo siguiente:

1. Cree una gateway privada virtual y conéctela a su VPC. Para obtener más información, consulte Creación de una gateway privada virtual.
2. A continuación, cree una conexión de VPN y una nueva gateway para cliente. Para la gateway de cliente, especifique la dirección IP pública del servidor de Windows. Para la conexión de VPN, elija el direccionamiento estático y, a continuación, escriba el intervalo de CIDR de la red en la que se encuentra el servidor de Windows, por ejemplo, `172.31.0.0/16`. Para obtener más información, consulte Paso 5: Crear una conexión de VPN.

Después de crear la conexión VPN, configure la VPC para habilitar la comunicación a través de la conexión VPN.

Para configurar la VPC

- Cree una subred privada en la VPC (en caso de que no disponga de ninguna) para lanzar instancias que se comunicarán con el servidor de Windows. Para obtener más información, consulte Creación de una subred en la VPC.

  > **Note**
  >
  > La subred privada es una subred que no dispone de una ruta a ninguna gateway de Internet. El direccionamiento de esta subred se describe en la sección siguiente.

- Actualice las tablas de ruteo de la conexión de VPN:
  - Agregue una ruta a la tabla de rutas de la subred privada con la gateway privada virtual como destino y la red del servidor de Windows (intervalo CIDR) como destino. Para obtener más información, consulte Agregar y eliminar rutas de una tabla de rutas en la Guía del usuario de Amazon VPC.
  - Habilite la propagación de rutas para la gateway privada virtual. Para obtener más información, consulte (Gateway privada virtual) Habilitar la propagación de rutas en la tabla de enrutamiento.
- Cree un grupo de seguridad para las instancias que permita la comunicación entre la VPC y la red:
  - Añada reglas que permitan el acceso a SSH o RDP entrante desde su red. Esto le permitirá conectarse a instancias de su VPC desde la red. Por ejemplo, para permitir a los equipos de la red obtener acceso a instancias de Linux de su VPC, cree una regla entrante del tipo SSH y establezca el origine en el rango de CIDR de su red (por ejemplo, `172.31.0.0/16`). Para obtener más información, consulte Grupos de seguridad de su VPC en la Guía del usuario de Amazon VPC.
  - Añada una regla que permita el acceso a ICMP entrante desde su red. Esto permite probar la conexión VPN al hacer ping a una instancia de la VPC desde el servidor de Windows.

Paso 2: Descargar el archivo de configuración de la conexión de VPN

Puede utilizar la consola de Amazon VPC a fin de descargar un archivo de configuración de servidor de Windows para la conexión de VPN.

Para descargar el archivo de configuración

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Site-to-Site VPN Connections (Conexiones de Site-to-Site VPN).

3. Seleccione su conexión de VPN y elija Download Configuration (Descargar configuración).
4. Seleccione Microsoft como proveedor, Windows Server como plataforma y 2012 R2 como software. Elija Descargar. Puede abrir el archivo o guardarlo.

El archivo de configuración contiene una sección de información similar a la del siguiente ejemplo. Verá esta información presentada dos veces, una vez para cada túnel.

```
vgw-1a2b3c4d Tunnel1
-----------------------------------------------------------------
Local Tunnel Endpoint:       203.0.113.1
Remote Tunnel Endpoint:      203.83.222.237
Endpoint 1:                  [Your_Static_Route_IP_Prefix]
Endpoint 2:                  [Your_VPC_CIDR_Block]
Preshared key:               xCjNLsLoCmKsakwcdoR9yX6GsEXAMPLE
```

`Local Tunnel Endpoint`

La dirección IP que especificó para la gateway del cliente al crear la conexión de VPN.

`Remote Tunnel Endpoint`

Una de las dos direcciones IP de la puerta de enlace privada virtual que termina la conexión VPN en el AWS lado de la conexión.

`Endpoint 1`

El prefijo de IP que especificó como ruta estática al crear la conexión de VPN. Estas son las direcciones IP de su red que pueden utilizar la conexión de VPN para obtener acceso a su VPC.

`Endpoint 2`

Rango de direcciones IP (bloque de CIDR) de la VPC asociada a la gateway privada virtual (por ejemplo 10.0.0.0/16).

`Preshared key`

Clave previamente compartida que se utiliza para establecer la conexión de VPN IPsec entre el `Local Tunnel Endpoint` y el `Remote Tunnel Endpoint`.

Le sugerimos que configure ambos túneles como parte de la conexión VPN. Cada túnel se conecta a un concentrador de VPN independiente en el lado de Amazon de la conexión VPN. Aunque solo hay un túnel activo a la vez, el segundo túnel se establece automáticamente si el primero cae. Disponer

de túneles redundantes garantiza una disponibilidad continua en caso de fallo del dispositivo. Puesto que solo hay disponible un túnel cada vez, la consola de Amazon VPC indica que hay un túnel inactivo. Este es el comportamiento esperado, de modo que no necesita realizar ninguna acción.

Con dos túneles configurados, si se produce un fallo en un dispositivo interno AWS, la conexión VPN pasa automáticamente al segundo túnel de la puerta de enlace privada virtual en cuestión de minutos. Al configurar su dispositivo de gateway de cliente, es importante que configure ambos túneles.

> **Note**
>
> De vez en cuando, AWS realiza tareas de mantenimiento rutinarias en la puerta de enlace privada virtual. Este mantenimiento podría deshabilitar uno de los dos túneles de su conexión de VPN durante un breve periodo. Cuando esto ocurra, su conexión de VPN cambiará automáticamente al segundo túnel mientras duren las tareas de mantenimiento.

La información adicional acerca del intercambio de claves por Internet (IKE) y las asociaciones de seguridad de IPsec (SA) se muestran en el archivo de configuración descargado.

```
MainModeSecMethods:         DHGroup2-AES128-SHA1
MainModeKeyLifetime:        480min,0sess
QuickModeSecMethods:        ESP:SHA1-AES128+60min+100000kb
QuickModePFS:               DHGroup2
```

`MainModeSecMethods`

Algoritmos de cifrado y autenticación para IKE SA. Estas son las configuraciones sugeridas destinadas a la conexión VPN y la configuración predeterminada para las conexiones VPN IPsec del servidor de Windows.

`MainModeKeyLifetime`

Vida útil de la clave de IKE SA. Esta es la configuración sugerida para la conexión de VPN y la configuración predeterminada para las conexiones de VPN IPsec del servidor de Windows.

`QuickModeSecMethods`

Algoritmos de cifrado y autenticación para IPsec SA. Estas son las configuraciones sugeridas destinadas a la conexión VPN y la configuración predeterminada para las conexiones VPN IPsec del servidor de Windows.

`QuickModePFS`

Se recomienda utilizar la confidencialidad directa total (PFS) de clave maestra para las sesiones de IPsec.

Paso 3: Configuración de Windows Server

Antes de configurar el túnel VPN, debe instalar y configurar los servicios de direccionamiento y acceso remoto en el servidor de Windows. De esta forma, los usuarios remotos podrán obtener acceso a los recursos de su red.

Para instalar servicios de direccionamiento y acceso remoto

1. Inicie sesión en su servidor de Windows.
2. Vaya al menú Inicio y elija Administrador del servidor.
3. Instale los servicios de acceso remoto y direccionamiento:
    a. Desde el menú Administrar, elija Agregar roles y características.
    b. En la página Antes de comenzar, asegúrese de que su servidor cumple todos los requisitos previos. A continuación, elija Siguiente.
    c. Elija Instalación basada en características o en roles y, a continuación, elija Siguiente.
    d. Elija Select a server from the server pool (Seleccionar un servidor del grupo de servidores), seleccione el servidor de Windows y, a continuación, elija Next (Siguiente).
    e. Seleccione Servicios de acceso y directivas de redes en la lista. En el cuadro de diálogo que aparecerá, elija Agregar características para confirmar las características necesarias para esta función.
    f. En la misma lista, elija Acceso remoto y elija Siguiente.
    g. En la página Seleccionar características, elija Siguiente.
    h. En la página Servicios de acceso y directivas de redes, elija Siguiente.
    i. En la página Acceso remoto, elija Siguiente. En la página siguiente, seleccione DirectAccess una VPN (RAS). En el cuadro de diálogo que aparecerá, elija Agregar características para confirmar las características necesarias para este servicio de función. En la misma lista, elija Enrutamiento y, a continuación, elija Siguiente.
    j. En la página Rol de servidor web (IIS), elija Siguiente. Deje la selección predeterminada y elija Siguiente.

k. Elija Instalar. Cuando finalice la instalación, elija Cerrar.

Para configurar y habilitar el servidor de enrutamiento y acceso remoto

1. En el panel, elija Notificaciones (icono con la marca). Debería haber una tarea para completar la configuración posterior a la implementación. Elija el enlace Abrir el Asistente para introducción.
2. Elija Implementar solo VPN.
3. En el cuadro de diálogo Enrutamiento y acceso remoto, elija el nombre del servidor, elija Acción y luego seleccione Configurar y habilitar Enrutamiento y acceso remoto.
4. En el Asistente para instalación del servidor de enrutamiento y acceso remoto, en la primera página, elija Siguiente.
5. En la página Configuración, elija Configuración personalizada y Siguiente.
6. Elija Enrutamiento LAN, Siguiente y Finalizar.
7. Cuando lo solicite el cuadro de diálogo Enrutamiento y acceso remoto, elija Iniciar servicio.

Paso 4: Configurar el túnel de VPN

Puede configurar el túnel VPN al ejecutar los scripts netsh incluidos en el archivo de configuración descargado o mediante la interfaz de usuario del servidor de Windows.

> **Important**
>
> Le sugerimos que utilice la clave maestra Perfect Forward Secret (PFS) para sus sesiones de IPSec. Si decide ejecutar el script netsh, incluye un parámetro para habilitar PFS (). `qmpfs=dhgroup2` No puede habilitar PFS mediante la interfaz de usuario de Windows; debe hacerlo mediante la línea de comandos.

Opciones

- Opción 1: ejecutar el script netsh
- Opción 2: utilizar la interfaz de usuario del servidor de Windows

Opción 1: ejecutar el script netsh

Copie el script netsh del archivo de configuración descargado y reemplace las variables. A continuación se muestra un ejemplo de script.

```
netsh advfirewall consec add rule Name="vgw-1a2b3c4d Tunnel 1" ^
Enable=Yes Profile=any Type=Static Mode=Tunnel ^
LocalTunnelEndpoint=Windows_Server_Private_IP_address ^
RemoteTunnelEndpoint=203.83.222.236 Endpoint1=Your_Static_Route_IP_Prefix ^
Endpoint2=Your_VPC_CIDR_Block Protocol=Any Action=RequireInClearOut ^
Auth1=ComputerPSK Auth1PSK=xCjNLsLoCmKsakwcdoR9yX6GsEXAMPLE ^
QMSecMethods=ESP:SHA1-AES128+60min+100000kb ^
ExemptIPsecProtectedConnections=No ApplyAuthz=No QMPFS=dhgroup2
```

Name: puede sustituir el nombre recomendado (`vgw-1a2b3c4d Tunnel 1`) por el nombre que prefiera.

LocalTunnelPunto final: introduzca la dirección IP privada del servidor Windows de la red.

Endpoint1: el bloque de CIDR de la red en la que reside el servidor de Windows. Por ejemplo, `172.31.0.0/16`. Rodee este valor con comillas dobles (“).

Endpoint2: bloque de CIDR de su VPC o subred de su VPC. Por ejemplo, `10.0.0.0/16`. Rodee este valor con comillas dobles (“).

Ejecute el script actualizado en una ventana de símbolo del sistema en el servidor de Windows. (El signo ^ le permite cortar y pegar texto incluido en la línea de comandos). Para configurar el segundo túnel de VPN para esta conexión de VPN, repita el proceso utilizando el script netsh en el archivo de configuración.

Cuando haya terminado, vaya a Configurar el firewall de Windows.

Para obtener más información acerca de los parámetros netsh, consulte Comandos Netsh AdvFirewall Consec en la biblioteca de Microsoft. TechNet

Opción 2: utilizar la interfaz de usuario del servidor de Windows

También puede utilizar la interfaz de usuario del servidor de Windows para configurar el túnel de VPN.

> **Important**
>
> No puede habilitar la confidencialidad directa total (PFS) de clave maestra desde la interfaz de usuario del servidor de Windows. PFS debe habilitarse con la línea de comandos, tal como se describe en Habilitación de la confidencialidad directa total (PFS) de clave maestra.

Tareas

- Configurar una regla de seguridad para un túnel VPN
- Confirmar la configuración del túnel
- Habilitación de la confidencialidad directa total (PFS) de clave maestra
- Configurar el firewall de Windows

Configurar una regla de seguridad para un túnel VPN

En esta sección, configure una regla de seguridad en el servidor de Windows para crear un túnel VPN.

Para configurar una regla de seguridad para un túnel de VPN

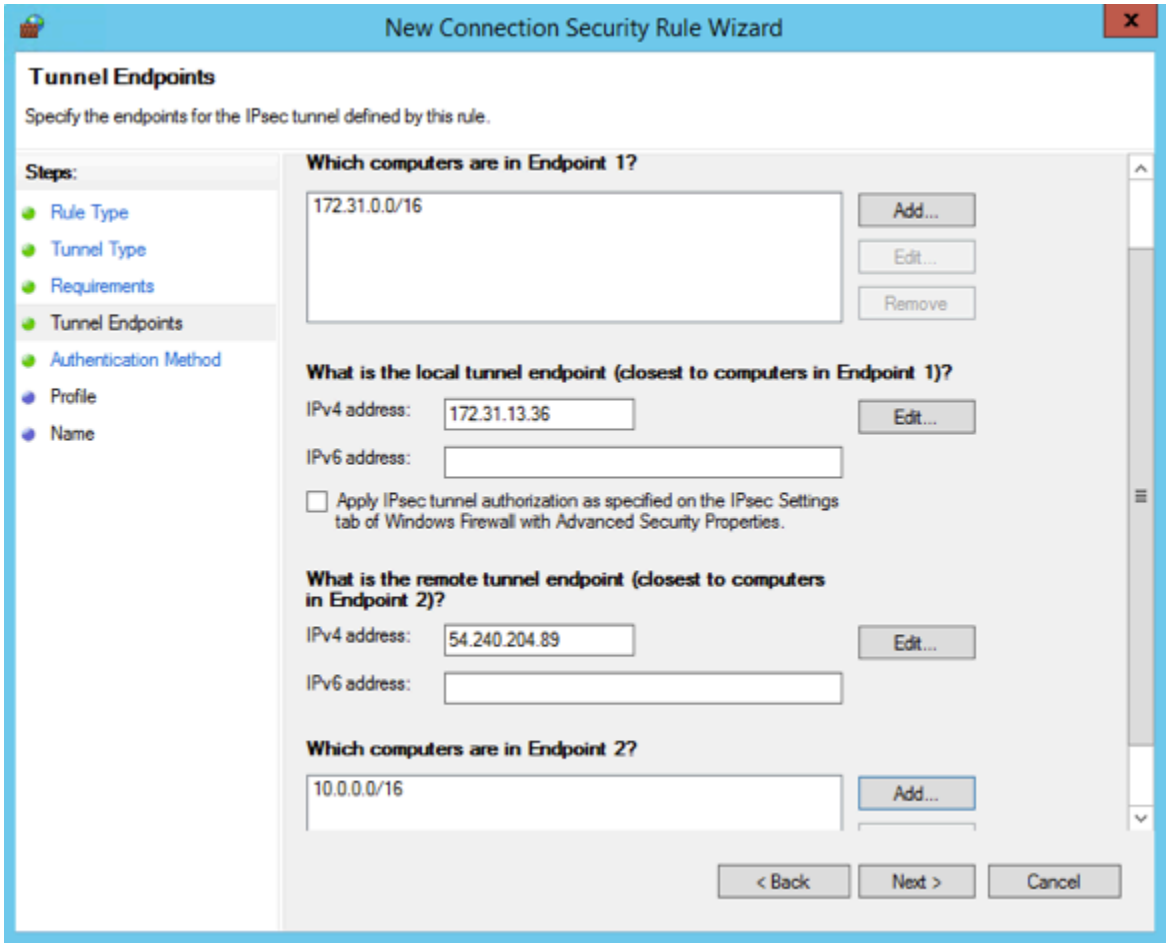
1. Abra el administrador del servidor, elija Tools (Herramientas)y, a continuación, seleccione Windows Defender Firewall with Advanced Security (Firewall de Windows Defender con seguridad avanzada).
2. Seleccione Reglas de seguridad de conexión, elija Acción y, a continuación, Nueva regla.
3. En el Asistente para nueva regla de seguridad de conexión, en la página Tipo de regla, elija Túnel y, a continuación, elija Siguiente.
4. En la página Tipo de túnel, en ¿Qué tipo de túnel desea crear?, elija Configuración personalizada. En ¿Desea eximir las conexiones protegidas por IPsec de este túnel?, deje el valor predeterminado activado (No. Enviar todo el tráfico de red que coincida con esta regla de seguridad de la conexión por el túnel.) y, a continuación, elija Siguiente.
5. En la página Requisitos, seleccione Requerir autenticación para las conexiones entrantes. No establezca túneles para las conexiones salientes y, a continuación, seleccione Siguiente.
6. En la página Extremos de túnel, en ¿Qué equipos están en el Extremo 1?, elija Agregar. Escriba el intervalo de CIDR de la red (detrás del dispositivo de gateway de cliente del servidor de Windows, por ejemplo `172.31.0.0/16`) y, a continuación, seleccione OK (Aceptar). El intervalo puede incluir la dirección IP de su dispositivo de gateway de cliente.

7. En ¿Cuál es el extremo de túnel local (más cercano a los equipos del Extremo 1)?, elija Editar. En el campo IPv4 address (Dirección IPv4), escriba la dirección IP privada del servidor de Windows y, a continuación, elija OK (Aceptar).
8. En ¿Cuál es el extremo de túnel remoto (más cercano a los equipos del Extremo 2)?, elija Editar. En el campo Dirección IPv4, escriba la dirección IP de la gateway privada virtual del Túnel 1 del archivo de configuración (consulte `Remote Tunnel Endpoint`) y, a continuación, elija Aceptar.

   > **Important**
   >
   > Si va a repetir este procedimiento para el Túnel 2, asegúrese de seleccionar el punto de conexión para el Túnel 2.

9. En ¿Qué equipos están en el Extremo 2?, elija Agregar. En el campo Esta dirección IP o subred:, escriba el bloque de CIDR de su VPC y, a continuación, elija Aceptar.

   > **Important**
   >
   > Debe desplazarse por el cuadro de diálogo hasta encontrar ¿Qué equipos están en el Extremo 2?. No elija Siguiente hasta que no haya completado este paso, ya que, de lo contrario, no podrá conectarse a su servidor.



10. Asegúrese de que todos los parámetros especificados son correctos. A continuación, elija Siguiente.
11. En la página Método de autenticación, seleccione Avanzado y elija Personalizar.
12. En Métodos de primera autenticación, elija Agregar.
13. Seleccione Clave previamente compartida, escriba el valor de la clave previamente compartida del archivo de configuración y luego elija Aceptar.

> **Important**
>
> Si va a repetir este procedimiento para el Túnel 2, asegúrese de seleccionar la clave previamente compartida para el Túnel 2.

14. Asegúrese de que la opción La primera autenticación es opcional no esté seleccionada y, a continuación, elija Aceptar.
15. Elija Siguiente.

16. En la página Perfil, active las tres casillas de verificación: Dominio, Privado y Público. Elija Siguiente.
17. En la página Nombre, escriba un nombre para la regla de conexión, por ejemplo, `VPN to Tunnel 1` y, a continuación, elija Finalizar.

Repita el procedimiento anterior, especificando los datos para el túnel 2 de su archivo de configuración.

Una vez que haya terminado, tendrá dos túneles configurados para su conexión de VPN.

Confirmar la configuración del túnel

Para confirmar la configuración del túnel

1. Abra Administrador del servidor, elija Herramientas, seleccione Firewall de Windows con seguridad avanzada y, a continuación, seleccione Reglas de seguridad de conexión.
2. Realice las comprobaciones siguientes para ambos túneles:
   - Habilitado está configurado con el valor `Yes`.
   - Extremo 1 corresponde con el bloque de CIDR de su red.
   - Extremo 2 corresponde con el bloque de CIDR de su VPC.
   - El modo de autenticación está configurado con el valor `Require inbound and clear outbound`.
   - Método de autenticación está configurado como `Custom`.
   - Puerto de extremo 1 es `Any`.
   - Puerto de extremo 2 es `Any`.
   - Protocolo es `Any`.
3. Seleccione la primera regla y elija Propiedades.
4. En la pestaña Autenticación, en Método, elija Personalizar. Compruebe que el campo Métodos de primera autenticación contiene la clave previamente compartida correcta del archivo de configuración para el túnel y, a continuación, elija Aceptar.
5. En la pestaña Avanzado, asegúrese de que las opciones Dominio, Privado y Público estén seleccionadas.

6. En Túnel IPsec, elija Personalizar. Compruebe los siguientes parámetros de túnel IPsec y, a continuación, elija Aceptar. A continuación, vuelva a seleccionar Aceptar para cerrar el cuadro de diálogo.

   - La opción Usar túnel IPsec está seleccionada.
   - El punto de enlace del túnel local (más cercano al punto de enlace 1) contiene la dirección IP del servidor de Windows. Si su dispositivo de gateway de cliente es una instancia EC2, deberá indicar la dirección IP privada de la instancia.
   - Extremo de túnel remoto (más cercano al Extremo 2) contiene la dirección IP de la gateway privada virtual de este túnel.

7. Abra las propiedades del segundo túnel. Repita los pasos del 4 al 7 para este túnel.

Habilitación de la confidencialidad directa total (PFS) de clave maestra

La confidencialidad directa total (PFS) de clave maestra se puede habilitar mediante la línea de comandos. Esta característica no puede habilitarse desde la interfaz de usuario.

Para habilitar la confidencialidad directa total de clave maestra

1. En el servidor de Windows, abra una nueva ventana del símbolo del sistema.
2. Introduzca el comando siguiente sustituyendo `rule_name` por el nombre que asignó en la primera regla de conexión.

   ```
   netsh advfirewall consec set rule name="rule_name" new QMPFS=dhgroup2
    QMSecMethods=ESP:SHA1-AES128+60min+100000kb
   ```

3. Repta el paso 2 para el segundo túnel. Esta vez, sustituya `rule_name` por el nombre que asignó a la segunda regla de conexión.

Configurar el firewall de Windows

Tras configurar sus reglas de seguridad en el servidor, configure algunos ajustes básicos de IPsec para trabajar con la gateway privada virtual.

Para configurar el firewall de Windows

1. Abra el administrador del servidor, elija Tools (Herramientas), seleccione Windows Defender Firewall with Advanced Security (Firewall de Windows Defender con seguridad avanzada)y, a continuación, elija Properties (Propiedades).
2. En la pestaña Configuración IPsec, en Exenciones IPsec, asegúrese de que la opción ICMP está exento de IPsec está configurada con el valor No (predeterminado). Asegúrese de que la opción Autorización de túnel IPsec está configurada con la opción Ninguno.
3. En Predeterminados de IPsec, elija Personalizar.
4. En Intercambio de claves (modo principal), seleccione Avanzado y, a continuación, elija Personalizar.
5. En Personalizar configuración avanzada de intercambio de claves, en Métodos de seguridad, asegúrese de que se utilizan los siguientes valores predeterminados para la primera entrada:

   - Integridad: SHA-1
   - Cifrado: AES-CBC 128
   - Algoritmo de intercambio de claves: Grupo Diffie-Hellman 2
   - En Duración de la clave, asegúrese de que Minutos tenga el valor `480` y de que Sesiones tenga el valor `0`.

   Estos valores corresponden a estas entradas en el archivo de configuración.

   ```
   MainModeSecMethods: DHGroup2-AES128-SHA1,DHGroup2-3DES-SHA1
   MainModeKeyLifetime: 480min,0sec
   ```
6. En Opciones de intercambio de claves, seleccione Usar Diffie-Hellman para mayor seguridad y, a continuación, elija Aceptar.
7. En Protección de datos (modo rápido), seleccione Avanzado y, a continuación, elija Personalizar.
8. Seleccione Requerir cifrado para todas las reglas de seguridad de conexión que usan esta configuración.
9. En Integridad y cifrado de datos, deje los valores predeterminados:

   - Protocolo: ESP
   - Integridad: SHA-1

- Cifrado: AES-CBC 128
- Vigencia: 60 minutos

Estos valores corresponden a la entrada del archivo de configuración que se muestra a continuación.

```
QuickModeSecMethods:
ESP:SHA1-AES128+60min+100000kb
```

10. Elija Aceptar para volver al cuadro de diálogo Personalizar configuración IPsec y elija Aceptar de nuevo para guardar la configuración.

Paso 5: Habilitar la detección de gateways inactivas

A continuación, configure TCP para detectar cuándo una gateway deja de estar disponible. Para ello, modifique la siguiente clave de registro: `HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters`. No realice este paso hasta no haber completado las secciones anteriores. Después de cambiar la clave de registro, deberá reiniciar el servidor.

Para habilitar la detección de gateways inactivas

1. Desde su servidor Windows, inicie la línea de comandos o una PowerShell sesión e introduzca regedit para iniciar el Editor del Registro.
2. Expanda HKEY_LOCAL_MACHINE, expanda SYSTEM, expanda CurrentControlSet, expanda Servicios, expanda Tcpip y, por último, expanda Parámetros.
3. Desde el menú Editar, seleccione Nuevo y seleccione Valor de DWORD (32 bits).
4. Introduzca EnableDeadel nombre GWDetect.
5. Seleccione EnableDeadGWDetect y elija Editar, Modificar.
6. En Información del valor, escriba 1 y, a continuación, elija Aceptar.
7. Cierre el Editor del Registro y reinicie el servidor.

Para obtener más información, consulte EnableDeadGWDetect en la TechNetbiblioteca de Microsoft.

Paso 6: Comprobar la conexión de VPN

Para comprobar que la conexión de VPN está funcionando correctamente, lance una instancia en su VPC y asegúrese de que no tiene conexión a Internet. Después de lanzar la instancia, haga ping a la dirección IP privada desde el servidor de Windows. El túnel VPN aparece cuando se genera tráfico desde el dispositivo de gateway de cliente. Por lo tanto, el comando ping también inicia la conexión de VPN.

Si desea ver los pasos para probar la conexión de VPN, consulte Prueba de una conexión de Site-to-Site VPN.

En caso de error en el comando `ping`, compruebe la información siguiente:

- Asegúrese de haber configurado las reglas de su grupo de seguridad para que permitan ICMP en la instancia de su VPC. Si el servidor de Windows es una instancia EC2, asegúrese de que las reglas salientes de su grupo de seguridad permiten el tráfico IPsec. Para obtener más información, consulte Configuración de instancias de Windows.
- Asegúrese de que el sistema operativo de la instancia en la que está haciendo ping esté configurado para responder a ICMP. Le recomendamos que utilice una de las AMI de Amazon Linux.
- Si la instancia a la que va a hacer ping es una instancia de Windows, conéctese a la instancia y habilite ICMPv4 entrante en el firewall de Windows.
- Asegúrese de haber configurado las tablas de ruteo correctamente para su VPC o su subred. Para obtener más información, consulte Paso 1: Crear una conexión de VPN y configurar la VPC.
- Si el dispositivo de gateway del cliente es una instancia EC2, asegúrese de que ha deshabilitado la comprobación de origen o destino de la instancia. Para obtener más información, consulte Configuración de instancias de Windows.

En la consola de Amazon VPC, en la página VPN Connections, seleccione su conexión de VPN. El primer túnel está en estado activo. El segundo túnel debería configurarse, pero no se utiliza a menos que se desactive el primer túnel. Puede que los túneles cifrados tarden unos minutos en establecerse.

Solución de problemas del dispositivo de gateway de cliente

Los siguientes temas pueden ayudarle a solucionar problemas de conectividad en los dispositivos de puerta de enlace de cliente.

Si desea ver instrucciones generales sobre las comprobaciones, consulte Prueba de una conexión de Site-to-Site VPN.

Además de los temas de esta sección, también puede utilizar AWS Site-to-Site VPN registros para solucionar problemas de conectividad de VPN.

Temas

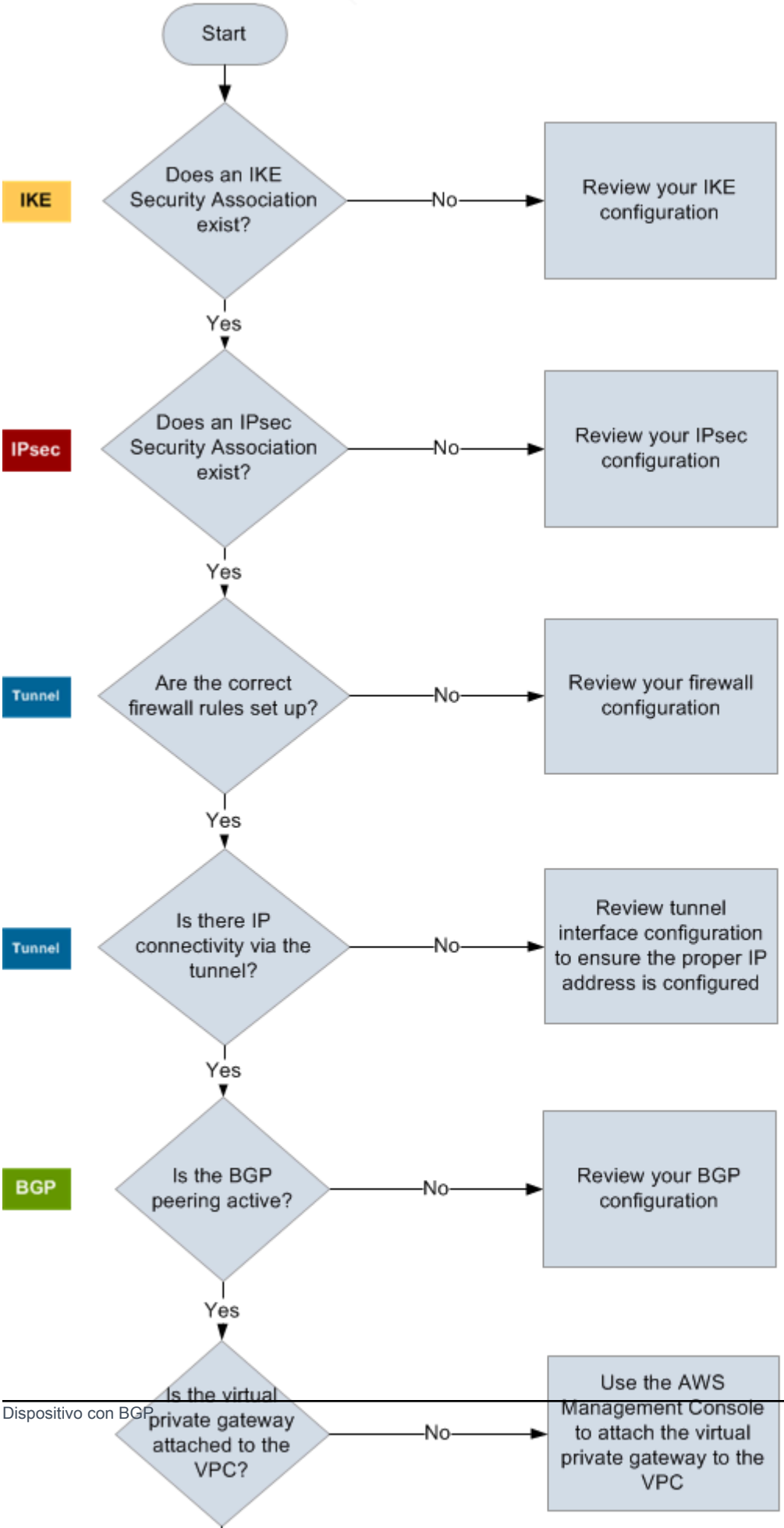
- Solución de problemas de conectividad al usar el protocolo de gateway fronteriza
- Solución de problemas de conectividad sin protocolo de gateway fronteriza
- Solución de problemas de conectividad de dispositivos de gateway de cliente de Cisco ASA
- Solución de problemas de conectividad de dispositivos de gateway de cliente de Cisco IOS
- Solución de problemas del dispositivo de gateway de cliente de Cisco IOS sin conectividad del protocolo de gateway fronteriza
- Solución de problemas de conectividad de dispositivos de gateway de cliente de Juniper JunOS
- Solución de problemas de conectividad de dispositivos de gateway de cliente de Juniper ScreenOS
- Solución de problemas de conectividad de dispositivos de gateway de cliente de Yamaha

Recursos adicionales de

- Foro de Amazon VPC
- ¿Cómo soluciono los problemas de conectividad del túnel de VPN con mi Amazon VPC?

Solución de problemas de conectividad al usar el protocolo de gateway fronteriza

El siguiente diagrama y la siguiente tabla proporcionan instrucciones generales para solucionar problemas de un dispositivo de gateway de cliente que utiliza el protocolo de gateway fronteriza (BGP). También recomendamos que habilite las características de depuración de su dispositivo. Consulte al proveedor de su dispositivo de gateway para obtener detalles.

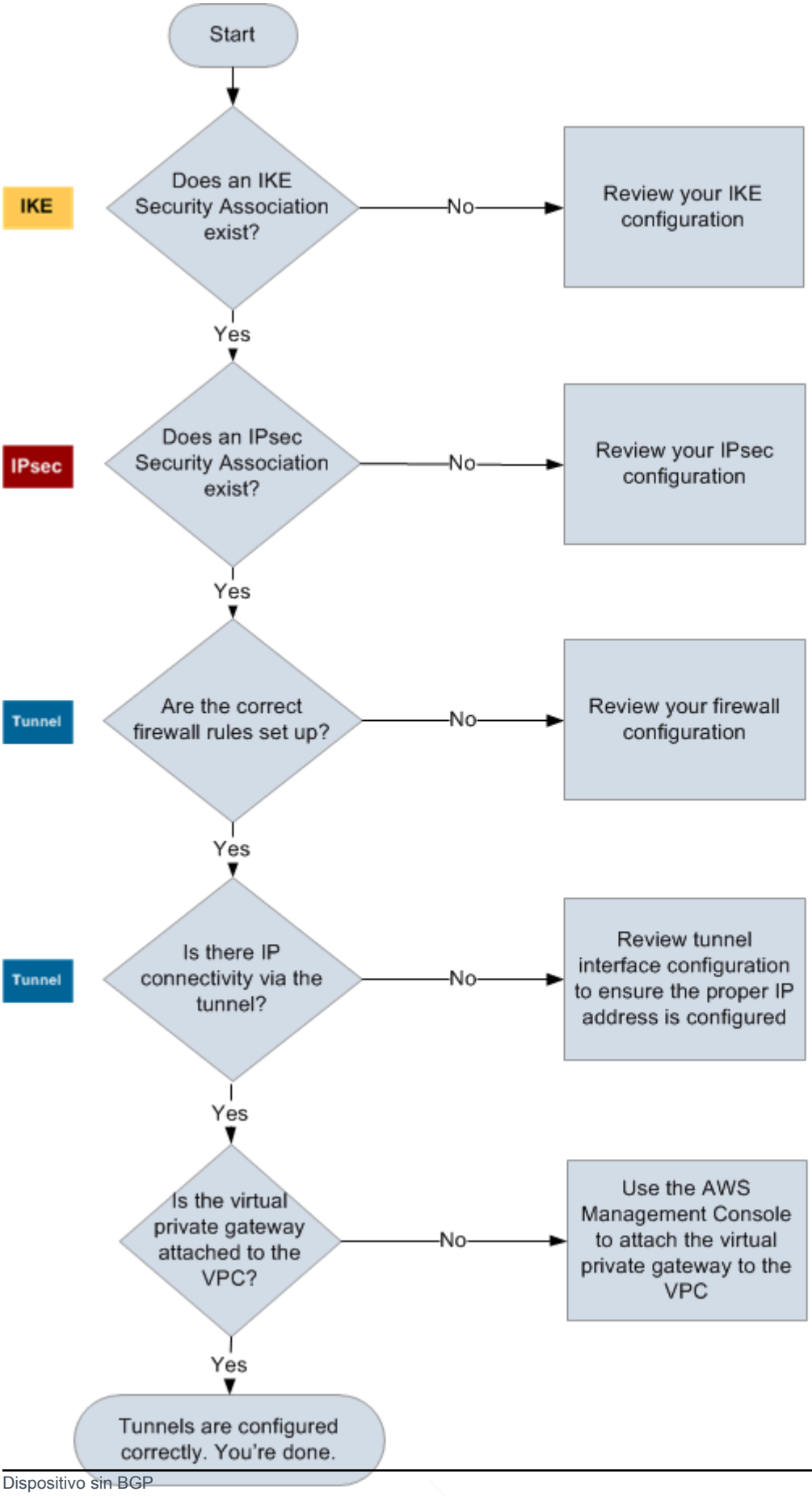

Start
IKE
Does an IKE Security Association exist?
No
Review your IKE configuration
Yes
IPsec
Does an IPsec Security Association exist?
No
Review your IPsec configuration
Yes
Tunnel
Are the correct firewall rules set up?
No
Review your firewall configuration
Yes
Tunnel
Is there IP connectivity via the tunnel?
No
Review tunnel interface configuration to ensure the proper IP address is configured
Yes
BGP
Is the BGP peering active?
No
Review your BGP configuration
Yes
Is the virtual private gateway attached to the VPC?
No
Use the AWS Management Console to attach the virtual private gateway to the VPC

IKE	Determine si existe una asociación de seguridad de IKE. Es necesario tener una asociación de seguridad de IKE para intercambiar las claves que se utilizan para establecer la asociación de seguridad de IPsec. Si no existe ninguna asociación de seguridad de IKE, revise sus opciones de configuración de IKE. Debe configurar los parámetros de cifrado, autenticación, confidencialidad directa total y modo según lo que se indica en el archivo de configuración. Si existe una asociación de seguridad de IKE, continúe hasta “IPsec”.
IPsec	Determine si existe una asociación de seguridad (SA) de IPsec. Una SA de IPSec es el propio túnel. Consulte el dispositivo de gateway de cliente para determinar si hay activa una SA de IPSec. Asegúrese de configurar los parámetros de cifrado, autenticación, confidencialidad directa total y modo según lo mostrado en el archivo de configuración. Si no existe una SA de IPSec, revise la configuración de IPSec. Si existe una SA de IPSec, vaya a la sección “Túnel”.
Túnel	Asegúrese de que se han configurado las reglas de firewall necesarias (para ver una lista de las reglas, consulte Configuración de un firewall entre Internet y el dispositivo de gateway de cliente). Si están correctamente configuradas, continúe. Determine si hay conectividad IP a través del túnel. Cada lado del túnel tiene una dirección IP según lo especificado en el archivo de configuración. La dirección de gateway privada virtual es la dirección utilizada como la dirección vecina de BGP. Desde su dispositivo de gateway de cliente, haga ping a esta dirección para determinar si el tráfico IP se está cifrando y descifrando correctamente. Si el ping no se realiza correctamente, revise la configuración de la interfaz del túnel para asegurarse de que se ha configurado la dirección IP adecuada. Si el ping es correcto, vaya a “BGP”.

BGP	Determine si la sesión de intercambio de tráfico BGP está activa. Para cada túnel, haga lo siguiente: • En su dispositivo de gateway de cliente, determine si el estado de BGP es `Active` o `Established` . El intercambio de tráfico BGP puede tardar aproximadamente 30 segundos en activarse. • Asegúrese de que el dispositivo de gateway de cliente indica la ruta predeterm inada (0.0.0.0/0) hacia la gateway privada virtual. Si los túneles no se encuentran en este estado, revise su configuración de BGP. Si se establece el intercambio de tráfico BGP, recibe un prefijo y se indica un prefijo, el túnel estará configurado correctamente. Asegúrese de que los dos túneles tienen este estado.

Solución de problemas de conectividad sin protocolo de gateway fronteriza

El siguiente diagrama y la siguiente tabla proporcionan instrucciones generales para solucionar problemas en un dispositivo de gateway de cliente que no utiliza el protocolo de gateway fronteriza (BGP). También recomendamos que habilite las características de depuración de su dispositivo. Consulte al proveedor de su dispositivo de gateway para obtener detalles.


Start
IKE
Does an IKE Security Association exist?
No
Review your IKE configuration
Yes
IPsec
Does an IPsec Security Association exist?
No
Review your IPsec configuration
Yes
Tunnel
Are the correct firewall rules set up?
No
Review your firewall configuration
Yes
Tunnel
Is there IP connectivity via the tunnel?
No
Review tunnel interface configuration to ensure the proper IP address is configured
Yes
Is the virtual private gateway attached to the VPC?
No
Use the AWS Management Console to attach the virtual private gateway to the VPC
Yes
Tunnels are configured correctly. You're done.

IKE	Determine si existe una asociación de seguridad de IKE. Es necesario tener una asociación de seguridad de IKE para intercambiar las claves que se utilizan para establecer la asociación de seguridad de IPsec. Si no existe ninguna asociación de seguridad de IKE, revise sus opciones de configuración de IKE. Debe configurar los parámetros de cifrado, autenticación, confidencialidad directa total y modo según lo que se indica en el archivo de configuración. Si existe una asociación de seguridad de IKE, continúe hasta “IPsec”.
IPsec	Determine si existe una asociación de seguridad (SA) de IPsec. Una SA de IPSec es el propio túnel. Consulte el dispositivo de gateway de cliente para determinar si hay activa una SA de IPSec. Asegúrese de configurar los parámetros de cifrado, autenticación, confidencialidad directa total y modo según lo mostrado en el archivo de configuración. Si no existe una SA de IPSec, revise la configuración de IPSec. Si existe una SA de IPSec, vaya a la sección “Túnel”.
Túnel	Asegúrese de que se han configurado las reglas de firewall necesarias (para ver una lista de las reglas, consulte Configuración de un firewall entre Internet y el dispositivo de gateway de cliente). Si están correctamente configuradas, continúe. Determine si hay conectividad IP a través del túnel. Cada lado del túnel tiene una dirección IP según lo especificado en el archivo de configuración. La dirección de gateway privada virtual es la dirección utilizada como la dirección vecina de BGP. Desde su dispositivo de gateway de cliente, haga ping a esta dirección para determinar si el tráfico IP se está cifrando y descifrando correctamente. Si el ping no se realiza correctamente, revise la configuración de la interfaz del túnel para asegurarse de que se ha configurado la dirección IP adecuada. Si el ping se realiza correctamente, vaya a “Rutas estáticas”.

Rutas estáticas	Para cada túnel, haga lo siguiente: • Compruebe que ha añadido una ruta estática a su CIDR de VPC con los túneles como el siguiente salto. • Asegúrese de que ha agregado una ruta estática en la consola de Amazon VPC para indicar a la gateway privada virtual que direccione el tráfico de vuelta a sus redes internas. Si los túneles no se encuentran en este estado, revise la configuración de su dispositivo. Asegúrese de que los dos túneles tienen este estado, y ya habrá terminado.

Solución de problemas de conectividad de dispositivos de gateway de cliente de Cisco ASA

Al solucionar problemas de conectividad de un dispositivo de gateway de cliente de Cisco, tenga en cuenta el IKE, el IPsec y el direccionamiento. Puede solucionar problemas en estas áreas en cualquier orden, pero recomendamos empezar por IKE (en la parte inferior de stack de red) y continuar de forma ascendente.

> **Important**
>
> Algunos Cisco ASA solo admiten el modo Active/Standby. Al utilizar estos Cisco ASA, solo puede tener un túnel activo cada vez. El otro túnel en espera se activará solo si el primer túnel se vuelve no disponible. El túnel en espera puede producir el siguiente error en sus archivos de registro, que puede ignorarse: `Rejecting IPSec tunnel: no matching crypto map entry for remote proxy 0.0.0.0/0.0.0.0/0/0 local proxy 0.0.0.0/0.0.0.0/0/0 on interface outside`.

IKE

Use el siguiente comando. La respuesta mostrará un dispositivo de gateway de cliente con el IKE configurado correctamente.

```
ciscoasa# show crypto isakmp sa
```

```
   Active SA: 2
   Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 2

1   IKE Peer: AWS_ENDPOINT_1
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_ACTIVE
```

Debería ver una o varias líneas con el valor de `src` para la gateway remota que se especifica en los túneles. El valor `state` debería ser `MM_ACTIVE` y el `status` debería ser `ACTIVE`. La ausencia de entradas o la aparición de una entrada con otro estado indican que IKE no se ha configurado correctamente.

Para realizar una solución de problemas más profunda, ejecute los siguientes comandos para permitir que los mensajes de log proporcionen información de diagnóstico.

```
router# term mon
router# debug crypto isakmp
```

Para deshabilitar la depuración, utilice el siguiente comando.

```
router# no debug crypto isakmp
```

IPsec

Use el siguiente comando. La respuesta mostrará un dispositivo de gateway de cliente con IPsec configurado correctamente.

```
ciscoasa# show crypto ipsec sa
```

```
interface: outside
    Crypto map tag: VPN_crypto_map_name, seq num: 2, local addr: 172.25.50.101

      access-list integ-ppe-loopback extended permit ip any vpc_subnet subnet_mask
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (vpc_subnet/subnet_mask/0/0)
      current_peer: integ-ppe1
```

```
      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.25.50.101, remote crypto endpt.: AWS_ENDPOINT_1

      path mtu 1500, ipsec overhead 74, media mtu 1500
      current outbound spi: 6D9F8D3B
      current inbound spi : 48B456A6

    inbound esp sas:
      spi: 0x48B456A6 (1219778214)
         transform: esp-aes esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, PFS Group 2, }
         slot: 0, conn_id: 4710400, crypto-map: VPN_cry_map_1
         sa timing: remaining key lifetime (kB/sec): (4374000/3593)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
    outbound esp sas:
      spi: 0x6D9F8D3B (1839172923)
         transform: esp-aes esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, PFS Group 2, }
         slot: 0, conn_id: 4710400, crypto-map: VPN_cry_map_1
         sa timing: remaining key lifetime (kB/sec): (4374000/3593)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
         0x00000000 0x00000001
```

Por cada interfaz del túnel, debería ver tanto `inbound esp sas` como `outbound esp sas`. Esto indica que aparece una SA (por ejemplo, `spi: 0x48B456A6`) y que IPsec se ha configurado correctamente.

En Cisco ASA, IPsec solo aparece después de enviar tráfico interesante (tráfico que debe cifrarse). Para mantener IPsec siempre activo, recomendamos configurar una monitorización de SLA. La monitorización de SLA sigue enviando tráfico interesante, lo que mantendrá el IPsec activo.

También puede utilizar el siguiente comando ping para obligar a su IPsec a comenzar la negociación y continuar.

```
ping ec2_instance_ip_address
```

```
Pinging ec2_instance_ip_address with 32 bytes of data:

Reply from ec2_instance_ip_address: bytes=32 time<1ms TTL=128
Reply from ec2_instance_ip_address: bytes=32 time<1ms TTL=128
Reply from ec2_instance_ip_address: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.4:
Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),

Approximate round trip times in milliseconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Para una solución de problemas más profunda, utilice el siguiente comando para permitir la depuración.

```
router# debug crypto ipsec
```

Para deshabilitar la depuración, utilice el siguiente comando.

```
router# no debug crypto ipsec
```

Enrutamiento

Haga ping al otro extremo del túnel. Si funciona, se debe establecer el IPSec. En caso contrario, compruebe sus listas de acceso y consulte la sección anterior de IPsec.

Si no puede obtener acceso a sus instancias, compruebe la siguiente información:

1. Verifique que la lista de acceso esté configurada para permitir el tráfico asociado al mapa criptográfico.

   Puede hacerlo con el siguiente comando.

   ```
   ciscoasa# show run crypto
   ```

```
crypto ipsec transform-set transform-amzn esp-aes esp-sha-hmac
crypto map VPN_crypto_map_name 1 match address access-list-name
crypto map VPN_crypto_map_name 1 set pfs
crypto map VPN_crypto_map_name 1 set peer AWS_ENDPOINT_1 AWS_ENDPOINT_2
crypto map VPN_crypto_map_name 1 set transform-set transform-amzn
crypto map VPN_crypto_map_name 1 set security-association lifetime seconds 3600
```

2. Compruebe la lista de acceso mediante el siguiente comando.

```
ciscoasa# show run access-list access-list-name
```

```
access-list access-list-name extended permit ip any vpc_subnet subnet_mask
```

3. Verifique si la lista de acceso es correcta. La siguiente lista de acceso de ejemplo permite todo el tráfico interno a la subred de VPC 10.0.0.0/16.

```
access-list access-list-name extended permit ip any 10.0.0.0 255.255.0.0
```

4. Ejecute un comando traceroute desde el dispositivo Cisco ASA para ver si llega a los routers de Amazon (por ejemplo, *AWS_ENDPOINT_1*/*AWS_ENDPOINT_2*).

   Si llega al enrutador de Amazon, compruebe las rutas estáticas que agregó en la consola de Amazon VPC, así como los grupos de seguridad de las instancias particulares.

5. Para una solución de problemas más profunda, revise la configuración.

Solución de problemas de conectividad de dispositivos de gateway de cliente de Cisco IOS

Al solucionar problemas de conectividad de un dispositivo de gateway de cliente de Cisco, tenga en cuenta cuatro elementos: IKE, IPsec, el túnel y BGP. Puede solucionar problemas en estas áreas en cualquier orden, pero recomendamos empezar por IKE (en la parte inferior de stack de red) y continuar de forma ascendente.

IKE

Use el siguiente comando. La respuesta mostrará un dispositivo de gateway de cliente con el IKE configurado correctamente.

```
router# show crypto isakmp sa
```

```
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
192.168.37.160  72.21.209.193   QM_IDLE           2001    0 ACTIVE
192.168.37.160  72.21.209.225   QM_IDLE           2002    0 ACTIVE
```

Debería ver una o varias líneas con el valor de `src` para la gateway remota que se especifica en los túneles. El `state` debería ser `QM_IDLE` y el `status` debería ser `ACTIVE`. La ausencia de entradas o la aparición de una entrada con otro estado indican que IKE no se ha configurado correctamente.

Para realizar una solución de problemas más profunda, ejecute los siguientes comandos para permitir que los mensajes de log proporcionen información de diagnóstico.

```
router# term mon
router# debug crypto isakmp
```

Para deshabilitar la depuración, utilice el siguiente comando.

```
router# no debug crypto isakmp
```

IPsec

Use el siguiente comando. La respuesta mostrará un dispositivo de gateway de cliente con IPsec configurado correctamente.

```
router# show crypto ipsec sa
```

```
interface: Tunnel1
    Crypto map tag: Tunnel1-head-0, local addr 192.168.37.160

    protected vrf: (none)
    local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
    remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
    current_peer 72.21.209.225 port 500
     PERMIT, flags={origin_is_acl,}
     #pkts encaps: 149, #pkts encrypt: 149, #pkts digest: 149
     #pkts decaps: 146, #pkts decrypt: 146, #pkts verify: 146
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 0, #pkts compr. failed: 0
```

```
      #pkts not decompressed: 0, #pkts decompress failed: 0
      #send errors 0, #recv errors 0

      local crypto endpt.: 174.78.144.73, remote crypto endpt.: 72.21.209.225
      path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0
      current outbound spi: 0xB8357C22(3090512930)

      inbound esp sas:
       spi: 0x6ADB173(112046451)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 1, flow_id: Motorola SEC 2.0:1, crypto map: Tunnel1-head-0
        sa timing: remaining key lifetime (k/sec): (4467148/3189)
        IV size: 16 bytes
        replay detection support: Y  replay window size: 128
        Status: ACTIVE

      inbound ah sas:

      inbound pcp sas:

      outbound esp sas:
       spi: 0xB8357C22(3090512930)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2, flow_id: Motorola SEC 2.0:2, crypto map: Tunnel1-head-0
        sa timing: remaining key lifetime (k/sec): (4467148/3189)
        IV size: 16 bytes
        replay detection support: Y  replay window size: 128
        Status: ACTIVE

      outbound ah sas:

      outbound pcp sas:

interface: Tunnel2
      Crypto map tag: Tunnel2-head-0, local addr 174.78.144.73

      protected vrf: (none)
      local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      current_peer 72.21.209.193 port 500
       PERMIT, flags={origin_is_acl,}
      #pkts encaps: 26, #pkts encrypt: 26, #pkts digest: 26
```

```
      #pkts decaps: 24, #pkts decrypt: 24, #pkts verify: 24
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts compr. failed: 0
      #pkts not decompressed: 0, #pkts decompress failed: 0
      #send errors 0, #recv errors 0

      local crypto endpt.: 174.78.144.73, remote crypto endpt.: 72.21.209.193
      path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0
      current outbound spi: 0xF59A3FF6(4120526838)

      inbound esp sas:
       spi: 0xB6720137(3060924727)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 3, flow_id: Motorola SEC 2.0:3, crypto map: Tunnel2-head-0
        sa timing: remaining key lifetime (k/sec): (4387273/3492)
        IV size: 16 bytes
        replay detection support: Y  replay window size: 128
        Status: ACTIVE

      inbound ah sas:

      inbound pcp sas:

      outbound esp sas:
       spi: 0xF59A3FF6(4120526838)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 4, flow_id: Motorola SEC 2.0:4, crypto map: Tunnel2-head-0
        sa timing: remaining key lifetime (k/sec): (4387273/3492)
        IV size: 16 bytes
        replay detection support: Y  replay window size: 128
        Status: ACTIVE

      outbound ah sas:

      outbound pcp sas:
```

Por cada interfaz del túnel, debería ver tanto `inbound esp sas` como `outbound esp sas`. Si aparece una SA (`spi: 0xF95D2F3C`, por ejemplo) y el valor de `Status` es `ACTIVE`, IPsec se ha configurado correctamente.

Para una solución de problemas más profunda, utilice el siguiente comando para permitir la depuración.

```
router# debug crypto ipsec
```

Utilice el siguiente comando para deshabilitar la depuración.

```
router# no debug crypto ipsec
```

Túnel

En primer lugar, compruebe si tiene las reglas de firewall necesarias aplicadas. Para obtener más información, consulte Configuración de un firewall entre Internet y el dispositivo de gateway de cliente.

Si sus reglas de firewall están configuradas correctamente, continúe realizando la solución de problemas con el siguiente comando.

```
router# show interfaces tun1
```

```
Tunnel1 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 169.254.255.2/30
  MTU 17867 bytes, BW 100 Kbit/sec, DLY 50000 usec,
    reliability 255/255, txload 2/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 174.78.144.73, destination 72.21.209.225
  Tunnel protocol/transport IPSEC/IP
  Tunnel TTL 255
  Tunnel transport MTU 1427 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Tunnel protection via IPSec (profile "ipsec-vpn-92df3bfb-0")
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 1 packets/sec
  5 minute output rate 1000 bits/sec, 1 packets/sec
```

```
    407 packets input, 30010 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
```

Asegúrese de que el `line protocol` está activo. Compruebe que la dirección IP de origen del túnel, la interfaz de origen y el destino coinciden respectivamente con la configuración del túnel de la dirección IP externa del dispositivo de gateway de cliente, la interfaz y la dirección IP externa de la gateway privada virtual. Asegúrese de que `Tunnel protection via IPSec` está presente. Ejecute el comando en ambas interfaces del túnel. Para resolver cualquier problema, revise la configuración y compruebe las conexiones físicas de su dispositivo de gateway de cliente.

Asimismo, utilice el siguiente comando, reemplazando `169.254.255.1` por la dirección IP interna de su gateway privada virtual.

```
router# ping 169.254.255.1 df-bit size 1410
```

```
Type escape sequence to abort.
Sending 5, 1410-byte ICMP Echos to 169.254.255.1, timeout is 2 seconds:
Packet sent with the DF bit set
!!!!!
```

Debería ver cinco signos de exclamación.

Para una solución de problemas más profunda, revise la configuración.

BGP

Use el siguiente comando.

```
router# show ip bgp summary
```

```
BGP router identifier 192.168.37.160, local AS number 65000
BGP table version is 8, main routing table version 8
2 network entries using 312 bytes of memory
2 path entries using 136 bytes of memory
3/1 BGP path/bestpath attribute entries using 444 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Bitfield cache entries: current 1 (at peak 2) using 32 bytes of memory
BGP using 948 total bytes of memory
BGP activity 4/1 prefixes, 4/1 paths, scan interval 15 secs
```

```
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
169.254.255.1   4  7224     363     323        8    0    0 00:54:21        1
169.254.255.5   4  7224     364     323        8    0    0 00:00:24        1
```

Deberían aparecer los dos vecinos. Para cada uno, debería ver un valor de `State/PfxRcd` de 1.

Si el intercambio de tráfico BGP está activado, compruebe si el dispositivo de gateway de cliente indica la ruta predeterminada (0.0.0.0/0) a la VPC.

```
router# show bgp all neighbors 169.254.255.1 advertised-routes
```

```
For address family: IPv4 Unicast
BGP table version is 3, local router ID is 174.78.144.73
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
     r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Originating default network 0.0.0.0

Network             Next Hop            Metric   LocPrf Weight Path
*> 10.120.0.0/16    169.254.255.1          100        0   7224    i

Total number of prefixes 1
```

Asimismo, asegúrese de estar recibiendo el prefijo correspondiente a su VPC desde la gateway privada virtual.

```
router# show ip route bgp
```

```
 10.0.0.0/16 is subnetted, 1 subnets
B       10.255.0.0 [20/0] via 169.254.255.1, 00:00:20
```

Para una solución de problemas más profunda, revise la configuración.

Solución de problemas del dispositivo de gateway de cliente de Cisco IOS sin conectividad del protocolo de gateway fronteriza

Al solucionar problemas de conectividad de un dispositivo de gateway de cliente de Cisco, tenga en cuenta tres elementos: IKE, IPsec y el túnel. Puede solucionar problemas en estas áreas en

cualquier orden, pero recomendamos empezar por IKE (en la parte inferior de stack de red) y continuar de forma ascendente.

IKE

Use el siguiente comando. La respuesta mostrará un dispositivo de gateway de cliente con el IKE configurado correctamente.

```
router# show crypto isakmp sa
```

```
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
174.78.144.73 205.251.233.121 QM_IDLE           2001    0 ACTIVE
174.78.144.73 205.251.233.122 QM_IDLE           2002    0 ACTIVE
```

Debería ver una o varias líneas con el valor de `src` para la gateway remota que se especifica en los túneles. El `state` debería ser `QM_IDLE` y el `status` debería ser `ACTIVE`. La ausencia de entradas o la aparición de una entrada con otro estado indican que IKE no se ha configurado correctamente.

Para realizar una solución de problemas más profunda, ejecute los siguientes comandos para permitir que los mensajes de log proporcionen información de diagnóstico.

```
router# term mon
router# debug crypto isakmp
```

Para deshabilitar la depuración, utilice el siguiente comando.

```
router# no debug crypto isakmp
```

IPsec

Use el siguiente comando. La respuesta mostrará un dispositivo de gateway de cliente con IPsec configurado correctamente.

```
router# show crypto ipsec sa
```

```
interface: Tunnel1
    Crypto map tag: Tunnel1-head-0, local addr 174.78.144.73

    protected vrf: (none)
```

```
    local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
    remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
    current_peer 72.21.209.225 port 500
     PERMIT, flags={origin_is_acl,}
     #pkts encaps: 149, #pkts encrypt: 149, #pkts digest: 149
     #pkts decaps: 146, #pkts decrypt: 146, #pkts verify: 146
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 0, #pkts compr. failed: 0
     #pkts not decompressed: 0, #pkts decompress failed: 0
     #send errors 0, #recv errors 0

     local crypto endpt.: 174.78.144.73, remote crypto endpt.:205.251.233.121
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0
     current outbound spi: 0xB8357C22(3090512930)

     inbound esp sas:
      spi: 0x6ADB173(112046451)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 1, flow_id: Motorola SEC 2.0:1, crypto map: Tunnel1-head-0
       sa timing: remaining key lifetime (k/sec): (4467148/3189)
       IV size: 16 bytes
       replay detection support: Y  replay window size: 128
       Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xB8357C22(3090512930)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 2, flow_id: Motorola SEC 2.0:2, crypto map: Tunnel1-head-0
       sa timing: remaining key lifetime (k/sec): (4467148/3189)
       IV size: 16 bytes
       replay detection support: Y  replay window size: 128
       Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:

interface: Tunnel2
```

```
Crypto map tag: Tunnel2-head-0, local addr 205.251.233.122

protected vrf: (none)
local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer 72.21.209.193 port 500
 PERMIT, flags={origin_is_acl,}
#pkts encaps: 26, #pkts encrypt: 26, #pkts digest: 26
#pkts decaps: 24, #pkts decrypt: 24, #pkts verify: 24
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 174.78.144.73, remote crypto endpt.:205.251.233.122
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0
current outbound spi: 0xF59A3FF6(4120526838)

inbound esp sas:
 spi: 0xB6720137(3060924727)
  transform: esp-aes esp-sha-hmac ,
  in use settings ={Tunnel, }
  conn id: 3, flow_id: Motorola SEC 2.0:3, crypto map: Tunnel2-head-0
  sa timing: remaining key lifetime (k/sec): (4387273/3492)
  IV size: 16 bytes
  replay detection support: Y  replay window size: 128
  Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
 spi: 0xF59A3FF6(4120526838)
  transform: esp-aes esp-sha-hmac ,
  in use settings ={Tunnel, }
  conn id: 4, flow_id: Motorola SEC 2.0:4, crypto map: Tunnel2-head-0
  sa timing: remaining key lifetime (k/sec): (4387273/3492)
  IV size: 16 bytes
  replay detection support: Y  replay window size: 128
  Status: ACTIVE

outbound ah sas:
```

```
    outbound pcp sas:
```

Por cada interfaz del túnel, debería ver tanto inbound `esp sas` como outbound `esp sas`. Esto indica que aparece una SA (por ejemplo, `spi: 0x48B456A6`), que el estado es `ACTIVE` y que IPsec se ha configurado correctamente.

Para una solución de problemas más profunda, utilice el siguiente comando para permitir la depuración.

```
router# debug crypto ipsec
```

Para deshabilitar la depuración, utilice el siguiente comando.

```
router# no debug crypto ipsec
```

Túnel

En primer lugar, compruebe si tiene las reglas de firewall necesarias aplicadas. Para obtener más información, consulte Configuración de un firewall entre Internet y el dispositivo de gateway de cliente.

Si sus reglas de firewall están configuradas correctamente, continúe realizando la solución de problemas con el siguiente comando.

```
router# show interfaces tun1
```

```
Tunnel1 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 169.254.249.18/30
  MTU 17867 bytes, BW 100 Kbit/sec, DLY 50000 usec,
    reliability 255/255, txload 2/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 174.78.144.73, destination 205.251.233.121
  Tunnel protocol/transport IPSEC/IP
  Tunnel TTL 255
  Tunnel transport MTU 1427 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Tunnel protection via IPSec (profile "ipsec-vpn-92df3bfb-0")
  Last input never, output never, output hang never
```

```
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 1 packets/sec
  5 minute output rate 1000 bits/sec, 1 packets/sec
    407 packets input, 30010 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
```

Asegúrese de que el line protocol está activo. Compruebe que la dirección IP de origen del túnel, la interfaz de origen y el destino coinciden respectivamente con la configuración del túnel de la dirección IP externa del dispositivo de gateway de cliente, la interfaz y la dirección IP externa de la gateway privada virtual. Asegúrese de que `Tunnel protection through IPSec` está presente. Ejecute el comando en ambas interfaces del túnel. Para resolver cualquier problema, revise la configuración y compruebe las conexiones físicas de su dispositivo de gateway de cliente.

También puede utilizar el siguiente comando, reemplazando `169.254.249.18` por la dirección IP interna de su gateway privada virtual.

```
router# ping 169.254.249.18 df-bit size 1410
```

```
Type escape sequence to abort.
Sending 5, 1410-byte ICMP Echos to 169.254.249.18, timeout is 2 seconds:
Packet sent with the DF bit set
!!!!!
```

Debería ver cinco signos de exclamación.

Enrutamiento

Para ver su tabla de ruteo estática, utilice el siguiente comando.

```
router# sh ip route static
```

```
     1.0.0.0/8 is variably subnetted
S       10.0.0.0/16 is directly connected, Tunnel1
is directly connected, Tunnel2
```

Debería ver que la ruta estática de CIDR de VPC a través de ambos túneles existe. Si no existe, añada las rutas estáticas tal y como se indica a continuación.

```
router# ip route 10.0.0.0 255.255.0.0 Tunnel1 track 100
router# ip route 10.0.0.0 255.255.0.0 Tunnel2 track 200
```

Comprobación de la monitorización de SLA

```
router# show ip sla statistics 100
```

```
IPSLAs Latest Operation Statistics

IPSLA operation id: 100
        Latest RTT: 128 milliseconds
Latest operation start time: *18:08:02.155 UTC Wed Jul  15 2012
Latest operation return code: OK
Number of successes: 3
Number of failures: 0
Operation time to live: Forever
```

```
router# show ip sla statistics 200
```

```
IPSLAs Latest Operation Statistics

IPSLA operation id: 200
        Latest RTT: 128 milliseconds
Latest operation start time: *18:08:02.155 UTC Wed Jul  15 2012
Latest operation return code: OK
Number of successes: 3
Number of failures: 0
Operation time to live: Forever
```

El valor de `Number of successes` indica si la monitorización de SLA se ha configurado correctamente.

Para una solución de problemas más profunda, revise la configuración.

Solución de problemas de conectividad de dispositivos de gateway de cliente de Juniper JunOS

Al solucionar problemas de conectividad de un dispositivo de gateway de cliente de Juniper, tenga en cuenta cuatro elementos: IKE, IPsec, el túnel y BGP. Puede solucionar problemas en estas áreas

en cualquier orden, pero recomendamos empezar por IKE (en la parte inferior de stack de red) y continuar de forma ascendente.

IKE

Use el siguiente comando. La respuesta mostrará un dispositivo de gateway de cliente con el IKE configurado correctamente.

```
user@router> show security ike security-associations
```

```
Index   Remote Address  State  Initiator cookie  Responder cookie  Mode
4       72.21.209.225   UP     c4cd953602568b74  0d6d194993328b02  Main
3       72.21.209.193   UP     b8c8fb7dc68d9173  ca7cb0abaedeb4bb  Main
```

Debería ver una o varias líneas que contienen una dirección remota de la gateway remota especificada en los túneles. El valor de `State` debería ser `UP`. La ausencia de entradas o la aparición de una entrada con otro estado (como `DOWN`) indican que IKE no se ha configurado correctamente.

Para realizar una solución de problemas más profunda, habilite las opciones de seguimiento de IKE, según lo recomendado en el archivo de configuración de ejemplo. A continuación, ejecute el siguiente comando para imprimir diversos mensajes de depuración en la pantalla.

```
user@router> monitor start kmd
```

Desde un host externo, puede recuperar el archivo completo de log con el siguiente comando.

```
scp username@router.hostname:/var/log/kmd
```

IPsec

Use el siguiente comando. La respuesta mostrará un dispositivo de gateway de cliente con IPsec configurado correctamente.

```
user@router> show security ipsec security-associations
```

```
Total active tunnels: 2
ID      Gateway        Port  Algorithm        SPI      Life:sec/kb Mon vsys
<131073 72.21.209.225  500   ESP:aes-128/sha1 df27aae4 326/ unlim   -   0
```

```
>131073 72.21.209.225  500   ESP:aes-128/sha1 5de29aa1 326/ unlim   -   0
<131074 72.21.209.193  500   ESP:aes-128/sha1 dd16c453 300/ unlim   -   0
>131074 72.21.209.193  500   ESP:aes-128/sha1 c1e0eb29 300/ unlim   -   0
```

En concreto, debería ver al menos dos líneas por dirección de gateway (correspondientes a la gateway remota). Los signos de intercalación al principio de cada línea (**< >**) indican la dirección del tráfico de la entrada en particular. El resultado son líneas separadas para el tráfico entrante ("**<**", tráfico de la gateway privada virtual a ese dispositivo de gateway de cliente) y el tráfico saliente ("**>**").

Para realizar una solución de problemas más profunda, habilite las opciones de seguimiento de IKE (para obtener más información, consulte la sección anterior acerca de IKE).

Túnel

En primer lugar, vuelva a comprobar si tiene las reglas de firewall necesarias aplicadas. Para obtener una lista de reglas, consulte Configuración de un firewall entre Internet y el dispositivo de gateway de cliente.

Si sus reglas de firewall están configuradas correctamente, continúe realizando la solución de problemas con el siguiente comando.

```
user@router> show interfaces st0.1
```

```
Logical interface st0.1 (Index 70) (SNMP ifIndex 126)
   Flags: Point-To-Point SNMP-Traps Encapsulation: Secure-Tunnel
   Input packets : 8719
   Output packets: 41841
   Security: Zone: Trust
   Allowed host-inbound traffic : bgp ping ssh traceroute
   Protocol inet, MTU: 9192
     Flags: None
     Addresses, Flags: Is-Preferred Is-Primary
     Destination: 169.254.255.0/30, Local: 169.254.255.2
```

Asegúrese de que el valor de `Security: Zone` es correcto y de que la dirección de `Local` coincide con el túnel del dispositivo de gateway de cliente dentro de la dirección.

A continuación, utilice el siguiente comando, reemplazando `169.254.255.1` por la dirección IP interna de su gateway privada virtual. Sus resultados deberían ser parecidos a la respuesta que se muestra aquí.

```
user@router> ping 169.254.255.1 size 1382 do-not-fragment
```

```
PING 169.254.255.1 (169.254.255.1): 1410 data bytes
64 bytes from 169.254.255.1: icmp_seq=0 ttl=64 time=71.080 ms
64 bytes from 169.254.255.1: icmp_seq=1 ttl=64 time=70.585 ms
```

Para una solución de problemas más profunda, revise la configuración.

BGP

Ejecute el siguiente comando de la .

```
user@router> show bgp summary
```

```
Groups: 1 Peers: 2 Down peers: 0
Table          Tot Paths  Act Paths Suppressed    History Damp State    Pending
inet.0                 2          1          0          0          0          0
Peer                     AS      InPkt     OutPkt    OutQ   Flaps Last Up/Dwn State|
#Active/Received/Accepted/Damped...
169.254.255.1          7224          9         10       0       0        1:00 1/1/1/0
            0/0/0/0
169.254.255.5          7224          8          9       0       0          56 0/1/1/0
            0/0/0/0
```

Para una solución de problemas más profunda, utilice el siguiente comando, reemplazando `169.254.255.1` por la dirección IP interna de su gateway privada virtual.

```
user@router> show bgp neighbor 169.254.255.1
```

```
Peer: 169.254.255.1+179 AS 7224 Local: 169.254.255.2+57175 AS 65000
  Type: External    State: Established    Flags: <ImportEval Sync>
  Last State: OpenConfirm   Last Event: RecvKeepAlive
  Last Error: None
  Export: [ EXPORT-DEFAULT ]
  Options: <Preference HoldTime PeerAS LocalAS Refresh>
  Holdtime: 30 Preference: 170 Local AS: 65000 Local System AS: 0
  Number of flaps: 0
  Peer ID: 169.254.255.1    Local ID: 10.50.0.10       Active Holdtime: 30
  Keepalive Interval: 10         Peer index: 0
```

```
  BFD: disabled, down
  Local Interface: st0.1
  NLRI for restart configured on peer: inet-unicast
  NLRI advertised by peer: inet-unicast
  NLRI for this session: inet-unicast
  Peer supports Refresh capability (2)
  Restart time configured on the peer: 120
  Stale routes from peer are kept for: 300
  Restart time requested by this peer: 120
  NLRI that peer supports restart for: inet-unicast
  NLRI that restart is negotiated for: inet-unicast
  NLRI of received end-of-rib markers: inet-unicast
  NLRI of all end-of-rib markers sent: inet-unicast
  Peer supports 4 byte AS extension (peer-as 7224)
  Table inet.0 Bit: 10000
    RIB State: BGP restart is complete
    Send state: in sync
    Active prefixes:              1
    Received prefixes:            1
    Accepted prefixes:            1
    Suppressed due to damping:    0
    Advertised prefixes:          1
Last traffic (seconds): Received 4    Sent 8    Checked 4
Input messages:  Total 24     Updates 2       Refreshes 0     Octets 505
Output messages: Total 26     Updates 1       Refreshes 0     Octets 582
Output Queue[0]: 0
```

Aquí debería ver `Received prefixes` y `Advertised prefixes` enumerados en 1 cada uno. Esto debería encontrarse en la sección `Table inet.0`.

Si el valor de `State` no es `Established`, compruebe `Last State` y `Last Error` para ver los detalles de lo que se necesita para corregir el problema.

Si el intercambio de tráfico BGP está activado, compruebe si el dispositivo de gateway de cliente indica la ruta predeterminada (0.0.0.0/0) a la VPC.

```
user@router> show route advertising-protocol bgp 169.254.255.1
```

```
inet.0: 10 destinations, 11 routes (10 active, 0 holddown, 0 hidden)
  Prefix                  Nexthop              MED     Lclpref    AS path
* 0.0.0.0/0               Self                                    I
```

Asimismo, asegúrese de estar recibiendo el prefijo correspondiente a su VPC desde la gateway privada virtual.

```
user@router> show route receive-protocol bgp 169.254.255.1
```

```
inet.0: 10 destinations, 11 routes (10 active, 0 holddown, 0 hidden)
  Prefix                  Nexthop              MED     Lclpref    AS path
* 10.110.0.0/16           169.254.255.1        100                7224 I
```

Solución de problemas de conectividad de dispositivos de gateway de cliente de Juniper ScreenOS

Al solucionar problemas de conectividad de un dispositivo de gateway de cliente basado en Juniper ScreenOS, tenga en cuenta cuatro elementos: IKE, IPsec, el túnel y BGP. Puede solucionar problemas en estas áreas en cualquier orden, pero recomendamos empezar por IKE (en la parte inferior de stack de red) y continuar de forma ascendente.

IKE e IPsec

Use el siguiente comando. La respuesta mostrará un dispositivo de gateway de cliente con el IKE configurado correctamente.

```
ssg5-serial-> get sa
```

```
total configured sa: 2
HEX ID    Gateway         Port Algorithm     SPI      Life:sec kb Sta   PID vsys
00000002<   72.21.209.225  500 esp:a128/sha1 80041ca4  3385 unlim A/-    -1 0
00000002>   72.21.209.225  500 esp:a128/sha1 8cdd274a  3385 unlim A/-    -1 0
00000001<   72.21.209.193  500 esp:a128/sha1 ecf0bec7  3580 unlim A/-    -1 0
00000001>   72.21.209.193  500 esp:a128/sha1 14bf7894  3580 unlim A/-    -1 0
```

Debería ver una o varias líneas con una dirección remota de la gateway remota que se especifica en los túneles. El valor de `Sta` debería ser `A/-`, y el valor de `SPI` debería ser un número hexadecimal distinto de `00000000`. Unas entradas con unos estados diferentes indican que IKE no se ha configurado correctamente.

Para realizar una resolución de problemas más profunda, habilite las opciones de seguimiento de IKE (según lo recomendado en la información de configuración de ejemplo).

Túnel

En primer lugar, vuelva a comprobar si tiene las reglas de firewall necesarias aplicadas. Para obtener una lista de reglas, consulte Configuración de un firewall entre Internet y el dispositivo de gateway de cliente.

Si sus reglas de firewall están configuradas correctamente, continúe realizando la solución de problemas con el siguiente comando.

```
ssg5-serial-> get interface tunnel.1
```

```
  Interface tunnel.1:
  description tunnel.1
  number 20, if_info 1768, if_index 1, mode route
  link ready
  vsys Root, zone Trust, vr trust-vr
  admin mtu 1500, operating mtu 1500, default mtu 1500
  *ip 169.254.255.2/30
  *manage ip 169.254.255.2
  route-deny disable
  bound vpn:
    IPSEC-1

  Next-Hop Tunnel Binding table
  Flag Status Next-Hop(IP)    tunnel-id  VPN

  pmtu-v4 disabled
  ping disabled, telnet disabled, SSH disabled, SNMP disabled
  web disabled, ident-reset disabled, SSL disabled

  OSPF disabled  BGP enabled  RIP disabled  RIPng disabled  mtrace disabled
  PIM: not configured  IGMP not configured
  NHRP disabled
  bandwidth: physical 0kbps, configured egress [gbw 0kbps mbw 0kbps]
             configured ingress mbw 0kbps, current bw 0kbps
             total allocated gbw 0kbps
```

Asegúrese de que puede ver `link:ready` y de que la dirección de `IP` coincide con el túnel del dispositivo de gateway de cliente dentro de la dirección.

A continuación, utilice el siguiente comando, reemplazando `169.254.255.1` por la dirección IP interna de su gateway privada virtual. Sus resultados deberían ser parecidos a la respuesta que se muestra aquí.

```
ssg5-serial-> ping 169.254.255.1
```

```
Type escape sequence to abort

Sending 5, 100-byte ICMP Echos to 169.254.255.1, timeout is 1 seconds
!!!!!
Success Rate is 100 percent (5/5), round-trip time min/avg/max=32/32/33 ms
```

Para una solución de problemas más profunda, revise la configuración.

BGP

Ejecute el siguiente comando de la .

```
ssg5-serial-> get vrouter trust-vr protocol bgp neighbor
```

```
Peer AS Remote IP       Local IP          Wt Status   State     ConnID Up/Down
------------------------------------------------------------------------------
   7224 169.254.255.1   169.254.255.2    100 Enabled  ESTABLISH     10 00:01:01
   7224 169.254.255.5   169.254.255.6    100 Enabled  ESTABLISH     11 00:00:59
```

El estado de los dos BGP del mismo nivel debería ser `ESTABLISH`, lo que significa que la conexión de BGP con la gateway privada virtual está activa.

Para una solución de problemas más profunda, utilice el siguiente comando, reemplazando `169.254.255.1` por la dirección IP interna de su gateway privada virtual.

```
ssg5-serial-> get vr trust-vr prot bgp neigh 169.254.255.1
```

```
peer: 169.254.255.1,  remote AS: 7224, admin status: enable
type: EBGP, multihop: 0(disable), MED: node default(0)
connection state: ESTABLISH, connection id: 18 retry interval: node default(120s), cur
 retry time 15s
configured hold time: node default(90s), configured keepalive: node default(30s)
configured adv-interval: default(30s)
```

```
designated local IP: n/a
local IP address/port: 169.254.255.2/13946, remote IP address/port: 169.254.255.1/179
router ID of peer: 169.254.255.1, remote AS: 7224
negotiated hold time: 30s, negotiated keepalive interval: 10s
route map in name: , route map out name:
weight: 100 (default)
self as next hop: disable
send default route to peer: disable
ignore default route from peer: disable
send community path attribute: no
reflector client: no
Neighbor Capabilities:
  Route refresh: advertised and received
  Address family IPv4 Unicast:  advertised and received
force reconnect is disable
total messages to peer: 106, from peer: 106
update messages to peer: 6, from peer: 4
Tx queue length 0, Tx queue HWM: 1
route-refresh messages to peer: 0, from peer: 0
last reset 00:05:33 ago, due to BGP send Notification(Hold Timer Expired)(code 4 :
 subcode 0)
number of total successful connections: 4
connected: 2 minutes 6 seconds
Elapsed time since last update: 2 minutes 6 seconds
```

Si el intercambio de tráfico BGP está activado, compruebe si el dispositivo de gateway de cliente indica la ruta predeterminada (0.0.0.0/0) a la VPC. Este comando se aplica a ScreenOS 6.2.0 y versiones superiores.

```
ssg5-serial-> get vr trust-vr protocol bgp  rib neighbor 169.254.255.1 advertised
```

```
i: IBGP route, e: EBGP route, >: best route, *: valid route
               Prefix         Nexthop    Wt  Pref   Med Orig    AS-Path
--------------------------------------------------------------------------------
>i          0.0.0.0/0         0.0.0.0 32768   100     0  IGP
Total IPv4 routes advertised: 1
```

Asimismo, asegúrese de estar recibiendo el prefijo correspondiente a su VPC desde la gateway privada virtual. Este comando se aplica a ScreenOS 6.2.0 y versiones superiores.

```
ssg5-serial-> get vr trust-vr protocol bgp  rib neighbor 169.254.255.1 received
```

```
i: IBGP route, e: EBGP route, >: best route, *: valid route
               Prefix         Nexthop    Wt  Pref   Med Orig    AS-Path
------------------------------------------------------------------------------
>e*     10.0.0.0/16   169.254.255.1   100   100   100  IGP   7224
Total IPv4 routes received: 1
```

Solución de problemas de conectividad de dispositivos de gateway de cliente de Yamaha

Al solucionar problemas de conectividad de un dispositivo de gateway de cliente de Yamaha, tenga en cuenta cuatro elementos: IKE, IPsec, el túnel y BGP. Puede solucionar problemas en estas áreas en cualquier orden, pero recomendamos empezar por IKE (en la parte inferior de stack de red) y continuar de forma ascendente.

> **Note**
>
> La configuración del `proxy ID` utilizada en la fase 2 de IKE está desactivada de forma predeterminada en el enrutador Yamaha. Esto puede provocar problemas para conectarse a Site-to-Site VPN. Si no `proxy ID` está configurado en su router, consulte el archivo de configuración AWS de ejemplo proporcionado para que Yamaha lo configure correctamente.

IKE

Ejecute el siguiente comando de la . La respuesta mostrará un dispositivo de gateway de cliente con el IKE configurado correctamente.

```
# show ipsec sa gateway 1
```

```
sgw  flags local-id                      remote-id        # of sa
-------------------------------------------------------------------------
1    U K   YOUR_LOCAL_NETWORK_ADDRESS     72.21.209.225    i:2 s:1 r:1
```

Debería ver una línea con el valor de `remote-id` de la gateway remota que se especifica en los túneles. Puede enumerar todas las asociaciones de seguridad (SA) omitiendo el número de túnel.

Para realizar una solución de problemas más profunda, ejecute los siguientes comandos para permitir que los mensajes de log de nivel DEBUG proporcionen información de diagnóstico.

```
# syslog debug on
# ipsec ike log message-info payload-info key-info
```

Para cancelar los elementos registrados, ejecute el siguiente comando.

```
# no ipsec ike log
# no syslog debug on
```

IPsec

Ejecute el siguiente comando de la . La respuesta mostrará un dispositivo de gateway de cliente con IPsec configurado correctamente.

```
# show ipsec sa gateway 1 detail
```

```
SA[1] Duration: 10675s
Local ID: YOUR_LOCAL_NETWORK_ADDRESS
Remote ID: 72.21.209.225
Protocol: IKE
Algorithm: AES-CBC, SHA-1, MODP 1024bit

SPI: 6b ce fd 8a d5 30 9b 02 0c f3 87 52 4a 87 6e 77
Key: ** ** ** ** **  (confidential)   ** ** ** ** **
-------------------------------------------------
SA[2] Duration: 1719s
Local ID: YOUR_LOCAL_NETWORK_ADDRESS
Remote ID: 72.21.209.225
Direction: send
Protocol: ESP (Mode: tunnel)
Algorithm: AES-CBC (for Auth.: HMAC-SHA)
SPI: a6 67 47 47
Key: ** ** ** ** **  (confidential)   ** ** ** ** **
-------------------------------------------------
SA[3] Duration: 1719s
Local ID: YOUR_LOCAL_NETWORK_ADDRESS
Remote ID: 72.21.209.225
Direction: receive
Protocol: ESP (Mode: tunnel)
Algorithm: AES-CBC (for Auth.: HMAC-SHA)
SPI: 6b 98 69 2b
Key: ** ** ** ** **  (confidential)   ** ** ** ** **
```

```
------------------------------------------------
SA[4] Duration: 10681s
Local ID: YOUR_LOCAL_NETWORK_ADDRESS
Remote ID: 72.21.209.225
Protocol: IKE
Algorithm: AES-CBC, SHA-1, MODP 1024bit
SPI: e8 45 55 38 90 45 3f 67 a8 74 ca 71 ba bb 75 ee
Key: ** ** ** ** **  (confidential)   ** ** ** ** **
------------------------------------------------
```

Por cada interfaz del túnel, debería ver tanto `receive sas` como `send sas`.

Para una solución de problemas más profunda, utilice el siguiente comando para permitir la depuración.

```
# syslog debug on
# ipsec ike log message-info payload-info key-info
```

Ejecute el siguiente comando para deshabilitar la depuración.

```
# no ipsec ike log
# no syslog debug on
```

Túnel

En primer lugar, compruebe si tiene las reglas de firewall necesarias aplicadas. Para obtener una lista de reglas, consulte Configuración de un firewall entre Internet y el dispositivo de gateway de cliente.

Si sus reglas de firewall están configuradas correctamente, continúe realizando la solución de problemas con el siguiente comando.

```
# show status tunnel 1
```

```
TUNNEL[1]:
Description:
  Interface type: IPsec
  Current status is Online.
  from 2011/08/15 18:19:45.
  5 hours 7 minutes 58 seconds  connection.
```

```
  Received:    (IPv4) 3933 packets [244941 octets]
               (IPv6) 0 packet [0 octet]
  Transmitted: (IPv4) 3933 packets [241407 octets]
               (IPv6) 0 packet [0 octet]
```

Asegúrese de que el valor `current status` esté online y que `Interface type` sea IPsec. Asegúrese de ejecutar el comando en ambas interfaces del túnel. Para resolver cualquier problema aquí, revise la configuración.

BGP

Ejecute el siguiente comando de la .

```
# show status bgp neighbor
```

```
BGP neighbor is 169.254.255.1, remote AS 7224, local AS 65000, external link
  BGP version 0, remote router ID 0.0.0.0
  BGP state = Active
  Last read 00:00:00, hold time is 0, keepalive interval is 0 seconds
  Received 0 messages, 0 notifications, 0 in queue
  Sent 0 messages, 0 notifications, 0 in queue
  Connection established 0; dropped 0
  Last reset never
Local host: unspecified
Foreign host: 169.254.255.1, Foreign port: 0

BGP neighbor is 169.254.255.5, remote AS 7224, local AS 65000, external link
  BGP version 0, remote router ID 0.0.0.0
  BGP state = Active
  Last read 00:00:00, hold time is 0, keepalive interval is 0 seconds
  Received 0 messages, 0 notifications, 0 in queue
  Sent 0 messages, 0 notifications, 0 in queue
  Connection established 0; dropped 0
  Last reset never
Local host: unspecified
Foreign host: 169.254.255.5, Foreign port:
```

Deberían aparecer los dos vecinos. Para cada uno, debería ver un valor de `BGP state` de `Active`.

Si el intercambio de tráfico BGP está activado, compruebe si el dispositivo de gateway de cliente indica la ruta predeterminada (0.0.0.0/0) a la VPC.

```
# show status bgp neighbor 169.254.255.1 advertised-routes
```

```
Total routes: 1
*: valid route
  Network            Next Hop        Metric LocPrf Path
* default            0.0.0.0              0        IGP
```

Asimismo, asegúrese de estar recibiendo el prefijo correspondiente a su VPC desde la gateway privada virtual.

```
# show ip route
```

```
Destination         Gateway          Interface       Kind  Additional Info.
default             ***.***.***.***   LAN3(DHCP)    static
10.0.0.0/16         169.254.255.1    TUNNEL[1]       BGP  path=10124
```

Uso de Site-to-Site VPN

Puede utilizar los recursos de Site-to-Site VPN a través de la consola de Amazon VPC o la AWS CLI.

Contenido

Crea un adjunto de VPN Site-to-Site para Cloud WAN AWS

Sigue el procedimiento que se indica a continuación para crear un adjunto de VPN de sitio a sitio para Cloud WAN. AWS

Para crear un adjunto de VPN para AWS Cloud WAN mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Conexiones de Site-to-Site VPN.
3. Elija Create VPN Connection (Crear conexión VPN).
4. (Opcional) En Etiqueta de nombre, escriba el nombre de la conexión. Esta acción creará una etiqueta con una clave de `Name` y el valor que especifique.
5. En Target gateway type (Tipo de puerta de enlace de destino), elija Not associated (No asociada).

6. En Customer gateway (Puerta de enlace de cliente), realice alguna de las siguientes operaciones:
   - Para utilizar una puerta de enlace de cliente existente, elija Existente y, a continuación, elija la puerta de enlace de cliente.
   - Para crear una gateway de cliente, elija New (Nuevo). En IP Address (Dirección IP), ingrese una dirección IP pública estática. En Certificate ARN (ARN de certificado), elija el ARN de su certificado privado (si utiliza autenticación basada en certificados). En BGP ASN, escriba el número de sistema autónomo (ASN) para protocolo de gateway fronteriza (BGP) de la gateway de cliente. Para obtener más información, consulte Opciones de gateway de cliente.
7. En Opciones de enrutamiento, elija Dinámico o Estático.
8. En Túnel dentro de la versión de IP, elija IPv4 o IPv6.
9. (Opcional) En Enable acceleration (Habilitar aceleración), seleccione la casilla de verificación para habilitar la aceleración. Para obtener más información, consulte Conexiones de VPN aceleradas.

   Si habilita la aceleración, creamos dos aceleradores que utilizan su conexión de VPN. Se aplican cargos adicionales de .
10. (Opcional) En Local IPv4 network CIDR (CIDR de red IPv4 local), especifique el rango CIDR de IPv4 en el lado de la puerta de enlace de cliente (en las instalaciones) que puede comunicarse a través de los túneles de VPN. El valor predeterminado es `0.0.0.0/0`.

    Para el CIDR de red IPv4 remota, especifica el rango de CIDR de IPv4 en el AWS lado que puede comunicarse a través de los túneles VPN. El valor predeterminado es `0.0.0.0/0`.

    Si especificó IPv6 para la versión Túnel dentro de IP, especifique los rangos de CIDR de IPv6 en el lado de la puerta de enlace del cliente y en el AWS lado que pueden comunicarse a través de los túneles VPN. El valor predeterminado para ambos rangos es `::/0`.
11. (Opcional) En Opciones de túnel, puede especificar la siguiente información para cada túnel:
    - Un bloque CIDR IPv4 de tamaño /30 desde el rango `169.254.0.0/16` para las direcciones IPv4 de túnel interior.
    - Si especificó IPv6 en Túnel dentro de la versión IP, un bloque de CIDR IPv6 /126 del intervalo `fd00::/8` para las direcciones IPv6 del túnel interior.
    - La clave previamente compartida de IKE (PSK). Las siguientes versiones son compatibles: IKEv1 o IKEv2.

- Para editar las opciones avanzadas del túnel, seleccione Editar opciones de túnel. Para obtener más información, consulte Opciones de túnel de VPN.

12. Elija Create VPN Connection (Crear conexión VPN).

Para crear una conexión de Site-to-Site VPN a través de la línea de comandos o la API

- CreateVpnConexión (API de consultas de Amazon EC2)
- create-vpn-connection (AWS CLI)

Creación de una asociación de VPN de puerta de enlace de tránsito

Para crear una conexión de VPN en una puerta de enlace de tránsito, debe especificar la puerta de enlace de tránsito y la puerta de enlace de cliente. Será necesario crear la puerta de enlace de tránsito antes de seguir este procedimiento. Para obtener más información acerca de cómo crear una gateway de tránsito, consulte Gateways de tránsito en Gateways de tránsito de Amazon VPC.

Para crear una conexión de VPN en una puerta de enlace de tránsito con la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Conexiones de Site-to-Site VPN.
3. Elija Create VPN Connection (Crear conexión VPN).
4. (Opcional) En Etiqueta de nombre, escriba el nombre de la conexión. Esta acción creará una etiqueta con una clave de `Name` y el valor que especifique.
5. En Tipo de puerta de enlace de destino, elija Puerta de enlace de tránsito y, a continuación, elija la puerta de enlace de tránsito.
6. En Customer gateway (Puerta de enlace de cliente), realice alguna de las siguientes operaciones:
   - Para utilizar una puerta de enlace de cliente existente, elija Existente y, a continuación, elija la puerta de enlace de cliente.

     Si su puerta de enlace de cliente se encuentra detrás de un dispositivo de conversión de direcciones de red (NAT) que admite NAT traversal (NAT-T), utilice la dirección IP pública de su dispositivo NAT y ajuste las reglas de su firewall para desbloquear el puerto UDP 4500.

- Para crear una gateway de cliente, elija New (Nuevo). EnIP Address (Dirección IP), introduzca una dirección IP pública estática. En Certificate ARN (ARN de certificado), elija el ARN de su certificado privado (si utiliza autenticación basada en certificados). En BGP ASN, escriba el número de sistema autónomo (ASN) para protocolo de gateway fronteriza (BGP) de la gateway de cliente. Para obtener más información, consulte Opciones de gateway de cliente.

7. En Opciones de enrutamiento, elija Dinámico o Estático.
8. En Túnel dentro de la versión IP, especifique si los túneles de VPN admiten tráfico IPv4 o IPv6. El tráfico IPv6 solo es compatible con conexiones VPN en una gateway de tránsito.
9. (Opcional) En Enable acceleration (Habilitar aceleración), seleccione la casilla de verificación para habilitar la aceleración. Para obtener más información, consulte Conexiones de VPN aceleradas.

   Si habilita la aceleración, creamos dos aceleradores que utilizan su conexión de VPN. Se aplican cargos adicionales.
10. (Opcional) En Local IPv4 network CIDR (CIDR de red IPv4 local), especifique el rango CIDR de IPv4 en el lado de la puerta de enlace de cliente (en las instalaciones) que puede comunicarse a través de los túneles de VPN. El valor predeterminado es `0.0.0.0/0`.

    En Remote IPv4 network CIDR (CIDR de red IPv4 remoto), especifique el rango CIDR de IPv4 en el lado de AWS que se puede comunicar a través de los túneles de VPN. El valor predeterminado es `0.0.0.0/0`.

    Si especificó IPv6 para Tunnel inside IP version (Versión IP dentro del túnel), especifique los rangos CIDR de IPv6 en el lado de la puerta de enlace de cliente y en el lado de AWS que se pueden comunicar a través de los túneles de VPN. El valor predeterminado para ambos rangos es `::/0`.
11. (Opcional) En Opciones de túnel, puede especificar la siguiente información para cada túnel:

    - Un bloque CIDR IPv4 de tamaño /30 desde el rango `169.254.0.0/16` para las direcciones IPv4 de túnel interior.
    - Si especificó IPv6 en Túnel dentro de la versión IP, un bloque de CIDR IPv6 /126 del intervalo `fd00::/8` para las direcciones IPv6 del túnel interior.
    - La clave previamente compartida de IKE (PSK). Las siguientes versiones son compatibles: IKEv1 o IKEv2.

- Para editar las opciones avanzadas del túnel, seleccione Editar opciones de túnel. Para obtener más información, consulte Opciones de túnel de VPN.

12. Elija Create VPN Connection (Crear conexión VPN).

Para crear una vinculación de VPN con la AWS CLI

Utilice el comando create-vpn-connection y especifique el ID de la gateway de tránsito en la opción `--transit-gateway-id`.

Prueba de una conexión de Site-to-Site VPN

Tras crear la AWS Site-to-Site VPN conexión y configurar la pasarela del cliente, puede lanzar una instancia y probar la conexión haciendo ping a la instancia.

Antes de comenzar, asegúrese de lo siguiente:

- Utilizar una AMI que responda a las solicitudes de ping. Le recomendamos que utilice una de las AMI de Amazon Linux.
- Configure el grupo de seguridad o la ACL de red en su VPC para filtrar el tráfico entrante de la instancia para permitir el tráfico ICMP entrante y saliente. Esto permite que la instancia reciba solicitudes `ping`.
- Si va a utilizar instancias que ejecuten Windows Server, conecte la instancia y habilite el tráfico ICMPv4 entrante en el firewall de Windows para poder hacer ping a la instancia.
- (Enrutamiento estático) Asegúrese de que el dispositivo de gateway de cliente tenga una ruta estática a la VPC, y de que su conexión VPN tenga una ruta estática, para poder redirigir el tráfico a su dispositivo de gateway de cliente.
- (Enrutamiento dinámico) Asegúrese de que el estado de BGP en su dispositivo de gateway de cliente esté establecido. Una sesión de intercambio de tráfico BGP tarda aproximadamente 30 segundos en activarse. Compruebe que las rutas se anuncien con BGP correctamente y muestren una tabla de enrutamiento de subred para que el tráfico pueda regresar al gateway de cliente. Asegúrese de que los dos túneles estén configurados con la política de direccionamiento de BGP.
- Compruebe que haya configurado el enrutamiento de las tablas de enrutamiento de subred para la conexión de VPN.

Para probar la conectividad

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel, elija Iniciar instancia.
3. (Opcional) En Nombre, introduzca un nombre descriptivo para su instancia.
4. En Imágenes de aplicación y sistema operativo (Imagen de máquina de Amazon), elija Inicio rápido y, a continuación, elija el sistema operativo correspondiente a su instancia.
5. En Nombre del par de claves, seleccione un par de claves existente o cree uno nuevo.
6. En Configuración de red, elija Seleccionar un grupo de seguridad existente y, a continuación, elija el grupo de seguridad que configuró.
7. En el panel Resumen, elija Iniciar instancia.
8. Cuando la instancia esté en ejecución, obtenga su dirección IP privada (por ejemplo, 10.0.0.4). En la consola de Amazon EC2, se muestra la dirección en los datos de la instancia.
9. Desde un equipo de su red que se encuentre detrás del dispositivo de gateway de cliente, utilice el comando ping con la dirección IP privada de la instancia.

   ```
   ping 10.0.0.4
   ```

   La respuesta correcta será similar a la que se muestra a continuación.

   ```
   Pinging 10.0.0.4 with 32 bytes of data:

   Reply from 10.0.0.4: bytes=32 time<1ms TTL=128
   Reply from 10.0.0.4: bytes=32 time<1ms TTL=128
   Reply from 10.0.0.4: bytes=32 time<1ms TTL=128

   Ping statistics for 10.0.0.4:
   Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),

   Approximate round trip times in milliseconds:
   Minimum = 0ms, Maximum = 0ms, Average = 0ms
   ```

   Para probar la conmutación por error de los túneles, puede desactivar temporalmente uno de los túneles de su dispositivo de puerta de enlace de cliente y, a continuación, repetir este paso. No se pueden deshabilitar los túneles en el lado de AWS de la conexión de VPN.
10. Para probar la conexión desde AWS la red local, puedes usar SSH o RDP para conectarte a la instancia desde la red. A continuación, puede ejecutar el comando `ping` con la dirección IP

privada de otro equipo de la red para comprobar que ambos lados de la conexión pueden iniciar y recibir solicitudes.

Para obtener más información sobre cómo conectarse a una instancia de Linux, consulte Conectarse a su instancia de Linux en la Guía del usuario de Amazon EC2. Para obtener más información sobre cómo conectarse a una instancia de Windows, consulte Conectarse a su instancia de Windows en la Guía del usuario de Amazon EC2.

Eliminación de una conexión de Site-to-Site VPN

Si ya no necesitas una AWS Site-to-Site VPN conexión, puedes eliminarla. Cuando elimina una conexión de Site-to-Site VPN, no se elimina la gateway de cliente ni la gateway privada virtual asociada a la conexión. Si ya no necesita la gateway de cliente ni la gateway privada virtual, puede eliminarlas.

> **Warning**
>
> Si elimina su conexión de Site-to-Site VPN y luego crea una nueva, deberá descargar un nuevo archivo de configuración y volver a configurar el dispositivo de puerta de enlace de cliente.

Tareas

- Eliminación de una conexión de VPN
- Eliminación de una puerta de enlace de cliente
- Desasociación y eliminación de una puerta de enlace privada virtual

Eliminación de una conexión de VPN

Cuando se elimina una conexión de Site-to-Site VPN, esta permanece visible durante un breve espacio de tiempo con el estado `deleted` y después se borra automáticamente.

Para eliminar una conexión de VPN con la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Conexiones de Site-to-Site VPN.

3. Seleccione la conexión de VPN y elija Acciones, Eliminar conexión de VPN.
4. Cuando le pidan confirmación, escriba **`delete`** y elija Eliminar.

Para eliminar una conexión de VPN mediante la línea de comandos o la API

- DeleteVpnConexión (API de consultas de Amazon EC2)
- delete-vpn-connection (AWS CLI)
- Remove-EC2VpnConnection (AWS Tools for Windows PowerShell)

Eliminación de una puerta de enlace de cliente

Si ya no necesita una gateway de cliente, puede eliminarla. No se pueden eliminar las gateways de cliente que se están utilizando en una conexión de Site-to-Site VPN.

Para eliminar una gateway de cliente con la consola

1. En el panel de navegación, elija Puertas de enlace de cliente.
2. Elija la puerta de enlace de cliente y elija Acciones, Eliminar puerta de enlace de cliente.
3. Cuando le pidan confirmación, escriba **`delete`** y elija Eliminar.

Para eliminar una gateway de cliente mediante la línea de comando o API

- DeleteCustomerGateway (API de consultas de Amazon EC2)
- delete-customer-gateway (AWS CLI)
- Remove-EC2CustomerGateway (AWS Tools for Windows PowerShell)

Desasociación y eliminación de una puerta de enlace privada virtual

Si ya no necesita una gateway privada virtual para su VPC, puede de cliente, puede separarla del VPC.

Para desasociar una gateway privada virtual con la consola

1. En el panel de navegación, elija Puertas de enlace privadas virtuales.
2. Seleccione la gateway privada virtual y elija Actions, Detach from VPC.

3. Elija Desasociar puerta de enlace privada virtual.

Si ya no necesita la gateway privada virtual separada, puede eliminarla. Tenga en cuenta que no podrá eliminar la gateway privada virtual si sigue adjunta a la VPC. Después de que borre una puerta de enlace privada virtual, esta permanece visible durante un breve periodo de tiempo con un estado de `deleted` y, a continuación, la entrada se elimina automáticamente.

Para eliminar una gateway privada virtual con la consola

1. En el panel de navegación, elija Puertas de enlace privadas virtuales.
2. Seleccione la puerta de enlace privada virtual y elija Acciones, Eliminar puerta de enlace privada virtual.
3. Cuando le pidan confirmación, escriba **`delete`** y elija Eliminar.

Para desasociar una gateway privada virtual mediante la línea de comando o API

- DetachVpnGateway (API de consultas de Amazon EC2)
- detach-vpn-gateway (AWS CLI)
- Dismount-EC2VpnGateway (AWS Tools for Windows PowerShell)

Para eliminar una gateway privada virtual mediante la línea de comando o API

- DeleteVpnGateway (API de consultas de Amazon EC2)
- delete-vpn-gateway (AWS CLI)
- Remove-EC2VpnGateway (AWS Tools for Windows PowerShell)

Modificación de la puerta de enlace de destino de una conexión de Site-to-Site VPN

Puede modificar la puerta de enlace de destino de una conexión de AWS Site-to-Site VPN. Hay disponibles las siguientes opciones de migración:

- De una gateway privada virtual existente a una gateway de tránsito
- Una gateway privada virtual existente a otra gateway privada virtual
- De una gateway de tránsito existente a otra gateway de tránsito

- De una gateway de tránsito existente a una gateway privada virtual

Después de modificar la gateway de destino, la conexión de Site-to-Site VPN no estará disponible durante un breve período de tiempo, mientras se aprovisionan los nuevos puntos de enlace.

Las siguientes tareas le ayudan a realizar la migración a una nueva gateway.

Tareas

- Paso 1: Crear la puerta de enlace de destino nueva
- Paso 2: Actualizar las rutas estáticas (condicional)
- Paso 3: Migrar a una nueva gateway
- Paso 4: Actualizar tablas de enrutamiento de VPC
- Paso 5: Actualizar el enrutamiento de la puerta de enlace de destino (condicional)
- Paso 6: Actualizar el ASN de la puerta de enlace de cliente (condicional)

Paso 1: Crear la puerta de enlace de destino nueva

Antes de realizar la migración a la nueva puerta de enlace de destino, debe configurarla. Para obtener más información acerca de cómo añadir una gateway privada virtual, consulte the section called “Creación de una gateway privada virtual”. Para obtener más información acerca de cómo agregar una gateway de tránsito, consulte Crear una gateway de tránsito en Gateways de tránsito de Amazon VPC.

Si la nueva gateway de destino es una gateway de tránsito, asocie las VPC a la gateway de tránsito. Para obtener más información sobre las conexiones de la VPC, consulte Vinculaciones de una gateway de tránsito a una VPC en Gateways de tránsito de Amazon VPC .

Cuando el destino cambia de una gateway privada virtual a una gateway de tránsito, se puede configurar el ASN de la gateway de tránsito para que tenga el mismo valor que el ASN de la gateway privada virtual. Si prefiere tener un ASN diferente, debe establecer el ASN del dispositivo de gateway de cliente en el ASN de la gateway de tránsito. Para obtener más información, consulte the section called “Paso 6: Actualizar el ASN de la puerta de enlace de cliente (condicional)”.

Paso 2: Actualizar las rutas estáticas (condicional)

Este paso es necesario cuando se pasa de una gateway privada virtual con rutas estáticas a una gateway de destino.

Debe eliminar las rutas estáticas antes de migrar a la nueva gateway.

> **Tip**
>
> Mantenga una copia de la ruta estática antes de eliminarla. Tendrá que volver a agregar estas rutas a la gateway de tránsito cuando haya terminado de migrar la conexión de VPN.

Para eliminar una ruta de una tabla de ruteo

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Route tables y, a continuación, seleccione la tabla de enrutamiento.
3. En la pestaña Rutas, elija Editar rutas.
4. Elija Eliminar para la ruta estática hacia la puerta de enlace privada virtual.
5. Elija Guardar cambios.

Paso 3: Migrar a una nueva gateway

Para cambiar la puerta de enlace de destino

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Conexiones de Site-to-Site VPN.
3. Elija la conexión de VPN y elija Acciones, Modificar conexión de VPN.
4. En Tipo de destino, elija el tipo de puerta de enlace.
   a. Si la puerta de enlace de destino nueva es una puerta de enlace privada virtual, elija la puerta de enlace de VPN.
   b. Si la puerta de enlace de destino nueva es una puerta de enlace de tránsito, elija la puerta de enlace de tránsito.
5. Elija Guardar cambios.

Para modificar una conexión de Site-to-Site VPN a través de la línea de comandos o la API

- ModifyVpnConnection (API de consulta de Amazon EC2)
- modify-vpn-connection (AWS CLI)

Paso 4: Actualizar tablas de enrutamiento de VPC

Después de migrar a la nueva gateway, es posible que tenga que modificar la tabla de ruteo de VPC. Para obtener más información, consulte Tablas de ruteo en la Guía del usuario de Amazon VPC.

En la siguiente tabla se proporciona información sobre las actualizaciones de la tabla de enrutamiento de VPC que se deben llevar a cabo después de modificar el destino de la puerta de enlace VPN.

Gateway existente	Nueva gateway	Cambio en la tabla de ruteo de VPC
Gateway privada virtual con rutas propagadas	Puerta de enlace de tránsito	Agregue una ruta que contenga el ID de la puerta de enlace de tránsito.
Gateway privada virtual con rutas propagadas	Gateway privada virtual con rutas propagadas	No se requiere ninguna acción.
Gateway privada virtual con rutas propagadas	Gateway privada virtual con ruta estática	Agregue una ruta que contenga el ID de la nueva puerta de enlace privada virtual.
Gateway privada virtual con rutas estáticas	Puerta de enlace de tránsito	Actualice la ruta que contiene el ID de la puerta de enlace privada virtual al ID de la puerta de enlace de tránsito.
Gateway privada virtual con rutas estáticas	Gateway privada virtual con rutas estáticas	Actualice la ruta que contiene el ID de la puerta de enlace virtual privada al ID de la nueva puerta de enlace virtual privada.
Gateway privada virtual con rutas estáticas	Gateway privada virtual con rutas propagadas	Elimine la ruta que contiene el ID de la puerta de enlace privada virtual.

Gateway existente	Nueva gateway	Cambio en la tabla de ruteo de VPC
Puerta de enlace de tránsito	Gateway privada virtual con rutas estáticas	Actualice la ruta que contiene el ID de la puerta de enlace de tránsito al ID de la puerta de enlace privada virtual.
Puerta de enlace de tránsito	Gateway privada virtual con rutas propagadas	Elimine la ruta que contiene el ID de la puerta de enlace de tránsito.
Puerta de enlace de tránsito	Puerta de enlace de tránsito	Actualice la ruta que contiene el ID de la puerta de enlace de tránsito por el ID de la nueva puerta de enlace de tránsito.

Paso 5: Actualizar el enrutamiento de la puerta de enlace de destino (condicional)

Si la nueva gateway es de tránsito, modifique la tabla de enrutamiento de la gateway de tránsito para que permita el tráfico entre la VPC y Site-to-Site VPN. Para obtener más información, consulte Tablas de enrutamiento de Transit Gateway en Transit Gateways de Amazon VPC.

Si eliminó las rutas estáticas de VPN, debe agregarlas en la tabla de enrutamiento de la gateway de tránsito.

A diferencia de una puerta de enlace privada virtual, una puerta de enlace de tránsito establece el mismo valor para el discriminador de salida múltiple (MED) en todos los túneles de una conexión de VPN. Si está migrando de una puerta de enlace privada virtual a una puerta de enlace de tránsito y ha confiado en el valor del MED para la selección de túnel, le recomendamos que implemente cambios de enrutamiento para evitar problemas de conexión. Por ejemplo, puede anunciar rutas más específicas en su puerta de enlace de tránsito. Para obtener más información, consulte Tablas de enrutamiento y prioridad de rutas de VPN.

Paso 6: Actualizar el ASN de la puerta de enlace de cliente (condicional)

Cuando la nueva gateway tenga un ASN diferente que la gateway antigua, debe actualizar el ASN en su dispositivo de gateway de cliente para que apunte al nuevo ASN. Para obtener más información, consulte Opciones de la gateway de cliente para su conexión de Site-to-Site VPN.

Modificación de las opciones de conexión de Site-to-Site VPN

Puede modificar las opciones de una conexión de Site-to-Site VPN. Puede modificar las siguientes opciones:

- Los rangos de CIDR IPv4 en el lado local (gateway de cliente) y en el lado remoto (AWS) de la conexión de VPN que puede comunicarse a través de los túneles de VPN. El valor predeterminado es `0.0.0.0/0` para ambos rangos.
- Los rangos de CIDR IPv6 en el lado local (gateway de cliente) y remoto (AWS) de la conexión de VPN que puede comunicarse a través de los túneles de VPN. El valor predeterminado es `::/0` para ambos rangos.

Al modificar las opciones de conexión de VPN, las direcciones IP del punto de enlace de la VPN en el lado de AWS no cambian y las opciones de túnel no cambian. Su conexión de VPN no estará disponible temporalmente durante un breve período mientras se actualiza la conexión de VPN.

Para modificar las opciones de conexión de 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 Conexiones de Site-to-Site VPN.
3. Seleccione su conexión de VPN y elija Acciones, Modificar las opciones de conexión de VPN.
4. Introduzca nuevos intervalos de CIDR según sea necesario.
5. Elija Guardar cambios.

Para modificar las opciones de conexión de VPN utilizando la línea de comandos o la API

- modify-vpn-connection-options (AWS CLI)
- ModifyVpnConnectionOptions (API de consulta de Amazon EC2)

Modificar las opciones del túnel de Site-to-Site VPN

Puede modificar las opciones de los túneles de VPN de la conexión de Site-to-Site VPN. Puede modificar un túnel de VPN al mismo tiempo.

> **Important**
>
> Al modificar un túnel de VPN, la conectividad a través del túnel se interrumpe durante varios minutos. Asegúrese de tener previsto el tiempo de inactividad esperado.

Para modificar las opciones del túnel de VPN utilizando la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Conexiones de Site-to-Site VPN.
3. Seleccione la conexión de Site-to-Site VPN y elija Acciones, Modificar las opciones de túnel de VPN.
4. En Dirección IP externa del túnel de VPN, elija la IP del punto de conexión del túnel de VPN.
5. Elija o introduzca nuevos valores para las opciones de túnel según sea necesario. Para obtener más información, consulte Opciones de túnel de VPN.
6. Elija Save changes (Guardar cambios).

Para modificar las opciones del túnel de VPN utilizando la línea de comandos o la API

- (AWS CLI) Utilice describe-vpn-connections para consultar las opciones de túnel actuales y modify-vpn-tunnel-options para modificar las opciones de túnel.
- (API de consulta de Amazon EC2) Utilice DescribeVpnConnections para consultar las opciones actuales del túnel y ModifyVpnTunnelOptions para modificarlas.

Edición de rutas estáticas en una conexión de Site-to-Site VPN

En las conexiones de Site-to-Site VPN de una puerta de enlace privada virtual configurada para un enrutamiento estático, puede agregar o eliminar rutas estáticas en la configuración de VPN.

Para agregar o eliminar una ruta estática mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Conexiones de Site-to-Site VPN.
3. Seleccione la conexión de VPN.
4. Elija Editar rutas estáticas.
5. Agregue o elimine rutas según sea necesario.
6. Elija Guardar cambios.
7. Si no ha habilitado la propagación de rutas en la tabla de ruteo, deberá actualizar manualmente las rutas de su tabla de ruteo para que reflejen los prefijos IP estáticos actualizados en su conexión de VPN. Para obtener más información, consulte (Gateway privada virtual) Habilitar la propagación de rutas en la tabla de enrutamiento.
8. Para una conexión de VPN en una puerta de enlace de tránsito, agregue, modifique o elimine las rutas estáticas de la tabla de enrutamiento de la puerta de enlace de tránsito. Para obtener más información, consulte Tablas de enrutamiento de Transit Gateway en Transit Gateways de Amazon VPC.

Para añadir una ruta estática mediante la línea de comando o un API

- CreateVpnConnectionRoute(API de consultas de Amazon EC2)
- create-vpn-connection-route (AWS CLI)
- New-EC2VpnConnectionRoute (AWS Tools for Windows PowerShell)

Para eliminar una ruta estática mediante la línea de comando o un API

- DeleteVpnConnectionRoute(API de consultas de Amazon EC2)
- delete-vpn-connection-route (AWS CLI)
- Remove-EC2VpnConnectionRoute (AWS Tools for Windows PowerShell)

Cambio de la puerta de enlace de cliente para una conexión de Site-to-Site VPN

Puede cambiar la gateway de cliente de una conexión Site-to-Site VPN utilizando la consola de Amazon VPC o una herramienta de línea de comandos.

Después de cambiar la puerta de enlace de cliente, su conexión de VPN no estará disponible temporalmente durante un breve periodo mientras aprovisionamos los nuevos puntos de conexión.

Para cambiar la gateway de cliente mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Conexiones de Site-to-Site VPN.
3. Seleccione la conexión de VPN.
4. Elija Acciones, Modificar la conexión de VPN.
5. En Tipo de destino, elija Puerta de enlace de cliente.
6. En Puerta de enlace de cliente de destino, elija la nueva puerta de enlace de cliente.
7. Elija Guardar cambios.

Para modificar la gateway de cliente mediante la línea de comando o API

- ModifyVpnConnection (API de consulta de Amazon EC2)
- modify-vpn-connection (AWS CLI)

Remplazo de credenciales comprometidas para la conexión de Site-to-Site VPN

Si cree que las credenciales del túnel de la conexión de Site-to-Site VPN se han visto comprometidas, puede cambiar la clave de IKE previamente compartida o el certificado de ACM. El método que utilice depende de la opción de autenticación que haya utilizado para los túneles de la VPN. Para obtener más información, consulte Opciones de autenticación de un túnel de Site-to-Site VPN.

Para cambiar la clave de IKE previamente compartida

Puede modificar las opciones de los túneles de la conexión de VPN y especificar una nueva clave de IKE previamente compartida para cada túnel. Para obtener más información, consulte Modificar las opciones del túnel de Site-to-Site VPN.

Si lo desea, también puede eliminar la conexión de VPN. Para obtener más información, consulte Eliminación de una conexión de VPN. No es necesario eliminar la VPC ni la gateway privada virtual. A continuación, cree una nueva conexión de VPN mediante la misma puerta de enlace privada virtual

y configure las nuevas claves en su dispositivo de puerta de enlace de cliente. Puede especificar sus propias claves previamente compartidas para los túneles o permitir a AWS generar nuevas claves previamente compartidas para usted. Para obtener más información, consulte Creación de una conexión de VPN. Las direcciones internas y externas del túnel podrían cambiar al crear de nuevo la conexión de VPN.

Para cambiar el certificado del extremo de AWS del punto de enlace del túnel

Gire el certificado. Para obtener más información, consulte Rotación de certificados de punto de conexión de túnel de VPN.

Para cambiar el certificado en el dispositivo de gateway de cliente

1. Cree un nuevo certificado. Para obtener información, consulte Emisión y administración de certificados en la Guía del usuario de AWS Certificate Manager.
2. Agregue el certificado al dispositivo de gateway de cliente.

Rotación de certificados de punto de conexión de túnel de Site-to-Site VPN

Puede rotar los certificados de los puntos de enlace de un túnel situado en el lado de AWS a través de la consola de Amazon VPC. Cuando el certificado de un punto de enlace de túnel esté a punto de caducar, AWS rota automáticamente el certificado con el rol vinculado al servicio. Para obtener más información, consulte the section called “Roles vinculados al servicio”.

Para rotar el certificado del punto de enlace de un túnel de Site-to-Site 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 Conexiones de Site-to-Site VPN.
3. Seleccione la conexión de Site-to-Site VPN y, a continuación, elija Acciones, Modificar certificado de túnel de VPN.
4. Seleccione el punto de conexión del túnel.
5. Seleccione Guardar.

Para rotar el certificado del punto de enlace de un túnel de Site-to-Site VPN a través de la AWS CLI

Utilice el comando modify-vpn-tunnel-certificate.

VPN IP privada con AWS Direct Connect

Con una VPN IP privada, puede implementar una VPN con IPsec AWS Direct Connect, cifrando el tráfico entre su red local y AWS sin el uso de direcciones IP públicas ni equipos VPN adicionales de terceros.

Uno de los principales casos de uso de la VPN con IP privada AWS Direct Connect es ayudar a los clientes de los sectores financiero, sanitario y federal a cumplir sus objetivos normativos y de cumplimiento. La conexión VPN con IP privada AWS Direct Connect garantiza que el tráfico entre las redes locales AWS y entre ellas sea seguro y privado, lo que permite a los clientes cumplir con sus requisitos normativos y de seguridad.

Contenido

Beneficios de la VPN de IP privada

- Administración y operaciones de red simplificadas: sin una VPN IP privada, los clientes tienen que implementar VPN y enrutadores de terceros para implementar VPN privadas a través AWS Direct Connect de las redes. Con la capacidad de VPN de IP privada, los clientes no tienen que implementar ni administrar su propia infraestructura de VPN. De este modo, se simplifican las operaciones de la red y se reducen los costos.
- Mejora de la seguridad: anteriormente, los clientes tenían que utilizar una interfaz AWS Direct Connect virtual pública (VIF) para cifrar el tráfico AWS Direct Connect, lo que requería direcciones IP públicas para los puntos finales de la VPN. El uso de IP públicas aumenta la probabilidad de ataques externos (DOS), lo que a su vez obliga a los clientes a implementar equipos de seguridad adicionales para la protección de la red. Además, una VIF pública abre el acceso entre todos los

servicios AWS públicos y las redes locales de los clientes, lo que aumenta la gravedad del riesgo. La función de VPN con IP privada permite el cifrado a través de VIF en AWS Direct Connect tránsito (en lugar de VIF públicas), además de la posibilidad de configurar direcciones IP privadas. Esto proporciona conectividad end-to-end privada además del cifrado, lo que mejora la seguridad general.

- Mayor escala de rutas: las conexiones VPN IP privadas ofrecen límites de ruta más altos (5000 rutas de salida y 1000 rutas de entrada) en comparación con las conexiones individuales AWS Direct Connect , que actualmente tienen un límite de 200 rutas de salida y 100 de entrada.

Cómo funciona la VPN de IP privada

La VPN Site-to-Site con IP privada funciona a través de una interfaz virtual de AWS Direct Connect tránsito (VIF). Utiliza una puerta de enlace de AWS Direct Connect y otra de tránsito para interconectar sus redes en las instalaciones con las VPC de AWS . Una conexión VPN IP privada tiene puntos de terminación en la puerta de enlace de tránsito, en el AWS lateral, y en el dispositivo de puerta de enlace del cliente, en el lado local. Debe asignar direcciones IP privadas a los extremos de los túneles IPSec de la puerta de enlace de tránsito y del dispositivo de puerta de enlace del cliente. Puede usar direcciones IP privadas de los rangos de direcciones IPv4 privadas RFC1918 o RFC6598.

Adjunta una conexión de VPN de IP privada a una puerta de enlace de tránsito. A continuación, enruta el tráfico entre la conexión de VPN y cualquier VPC (u otras redes) que también estén conectadas a la puerta de enlace de tránsito. Esto se hace asociando una tabla de enrutamiento con la conexión de VPN. En la dirección inversa, puede enrutar el tráfico de sus VPC a la conexión de VPN de IP privada mediante las tablas de enrutamiento que están asociadas a las VPC.

La tabla de enrutamiento asociada al adjunto de la VPN puede ser la misma o diferente de la asociada al adjunto subyacente. AWS Direct Connect De esta forma, podrá enrutar simultáneamente el tráfico cifrado y no cifrado entre sus VPC y sus redes en las instalaciones.

Para obtener más información sobre la ruta de tráfico que sale de la VPN, consulte las políticas de enrutamiento de la interfaz virtual privada y de la interfaz virtual de tránsito en la Guía del AWS Direct Connect usuario.

Requisitos previos

Se necesitan los siguientes recursos para completar la configuración de una VPN de IP privada sobre AWS Direct Connect:

- Una AWS Direct Connect conexión entre la red local y AWS
- Una AWS Direct Connect puerta de enlace asociada a la puerta de enlace de tránsito adecuada
- Una puerta de enlace de tránsito con un bloque de CIDR de IP privada disponible
- Un dispositivo de puerta de enlace de cliente en las instalaciones y una puerta de enlace de cliente de AWS correspondiente

Creación de la puerta de enlace de cliente

Una pasarela de clientes es un recurso que se crea en él AWS. Representa el dispositivo de puerta de enlace de cliente en las instalaciones. Cuando crea una pasarela de clientes, proporciona información sobre su dispositivo a AWS. Para obtener más información, consulte Gateway de cliente.

Para crear una gateway de cliente con la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Puertas de enlace de cliente.
3. Elija Crear puerta de enlace de cliente.
4. (Opcional) En Name tag (Etiqueta de nombre), ingrese un nombre para la puerta de enlace de cliente. Esta acción creará una etiqueta con una clave de `Name` y el valor que especifique.
5. En BGP ASN, ingrese un número de sistema autónomo (ASN) para protocolo de puerta de enlace fronteriza (BGP) de la puerta de enlace de cliente.
6. En IP address (Dirección IP), ingrese la dirección IP privada de su dispositivo de puerta de enlace de cliente.
7. (Opcional) En Device (Dispositivo), ingrese un nombre para el dispositivo que aloja esta puerta de enlace de cliente.
8. Elija Crear puerta de enlace de cliente.

Para crear una gateway de cliente mediante la línea de comando o API

- CreateCustomerGateway (API de consultas de Amazon EC2)
- create-customer-gateway (AWS CLI)

Preparación de la puerta de enlace de tránsito

Una puerta de enlace de tránsito es un hub de tránsito de red que puede utilizar para interconectar sus VPC y redes en las instalaciones. Puede crear una nueva puerta de enlace de tránsito o utilizar una ya existente para la conexión de VPN de IP privada. Al crear la puerta de enlace de tránsito, o al modificar una ya existente, se especifica un bloque de CIDR de IP privada para la conexión.

> **Note**
>
> Al especificar el bloque de CIDR de la puerta de enlace de tránsito que se va a asociar a su VPN de IP privada, asegúrese de que el bloque de CIDR no se solapa con ninguna dirección IP de ninguna otra conexión de red en la puerta de enlace de tránsito. Si algún bloque de CIDR de IP se solapa, puede provocar problemas de configuración con su dispositivo de puerta de enlace de cliente.

Para ver los pasos de AWS consola específicos para crear o modificar una pasarela de tránsito para utilizarla en la VPN con IP privada, consulte Transit Gateways en la Guía de pasarelas de tránsito de Amazon VPC.

Para crear una puerta de enlace de tránsito mediante la línea de comandos o la API

- CreateTransitGateway (API de consultas de Amazon EC2)
- create-transit-gateway (AWS CLI)

Cree la puerta de AWS Direct Connect enlace

Cree una AWS Direct Connect puerta de enlace siguiendo el procedimiento de creación de una puerta de enlace de Direct Connect de la Guía del AWS Direct Connect usuario.

Para crear una AWS Direct Connect puerta de enlace mediante la línea de comandos o la API

- CreateDirectConnectGateway(API de AWS Direct Connect consulta)
- create-direct-connect-gateway (AWS CLI)

Creación de la asociación de la puerta de enlace de tránsito

Después de crear la AWS Direct Connect puerta de enlace, cree una asociación de puerta de enlace de tránsito para la AWS Direct Connect puerta de enlace. Especifique el CIDR de IP privada para la puerta de enlace de tránsito que se identificó anteriormente en la lista de prefijos permitidos.

Para obtener más información, consulte Transit Gateway associations (Asociaciones de la puerta de enlace de tránsito) en la Guía del usuario de AWS Direct Connect .

Para crear una asociación de AWS Direct Connect puerta de enlace mediante la línea de comandos o la API

- CreateDirectConnectGatewayAsociación (API de AWS Direct Connect consulta)
- create-direct-connect-gateway-association (AWS CLI)

Creación de la conexión de VPN

Para crear una conexión de VPN mediante direcciones IP privadas

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Conexiones de Site-to-Site VPN.
3. Elija Create VPN Connection (Crear conexión VPN).
4. (Opcional) En Name tag (Etiqueta de nombre), escriba el nombre de la conexión de Site-to-Site VPN. Esta acción creará una etiqueta con una clave de `Name` y el valor que especifique.
5. En Target gateway type (Tipo de puerta de enlace de destino), elija Transit gateway (Puerta de enlace de tránsito). A continuación, elija la puerta de enlace de tránsito que identificó anteriormente.
6. En Customer gateway (Puerta de enlace de cliente), seleccione Existing (Existente). A continuación, elija la puerta de enlace de cliente que creó anteriormente.
7. Seleccione una de las opciones de direccionamiento en función de si el dispositivo de gateway de cliente da soporte al protocolo de gateway fronteriza (BGP):
   - Si el dispositivo de gateway de cliente da soporte a BGP, elija Dynamic (requires BGP) (Dinámico [requiere BGP]).
   - Si el dispositivo de gateway de cliente no da soporte a BGP, elija Static (Estático).
8. En Túnel dentro de la versión IP, especifique si los túneles de VPN admiten tráfico IPv4 o IPv6.

9. (Opcional) Si especificó IPv4 para la versión Túnel dentro de IP, también puede especificar los rangos de CIDR de IPv4 para la puerta de enlace del cliente y AWS los lados que pueden comunicarse a través de los túneles de la VPN. El valor predeterminado es `0.0.0.0/0`.

   Si especificó IPv6 para la versión Túnel dentro de IP, también puede especificar los rangos de CIDR de IPv6 para la puerta de enlace del cliente y los AWS lados que pueden comunicarse a través de los túneles VPN. El valor predeterminado para ambos rangos es `::/0`.
10. En el tipo de dirección IP externa, elija 4. PrivateIpv
11. En el campo ID del adjunto de transporte, elija el adjunto de la pasarela de tránsito correspondiente a la AWS Direct Connect pasarela correspondiente.
12. Elija Create VPN Connection (Crear conexión VPN).

> **Note**
>
> La opción Enable acceleration (Habilitar aceleración) no es aplicable a las conexiones de VPN sobre AWS Direct Connect.

Seguridad en la VPN AWS Site-to-Site

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de los centros de datos y las arquitecturas de red diseñados para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

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

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la Nube de AWS. AWS también le proporciona servicios que puede utilizar de forma segura. Los auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los AWS programas de de . Para obtener más información sobre los programas de cumplimiento que se aplican a la VPN de AWS sitio a sitio, consulte AWS Servicios dentro del alcance por programa de cumplimiento Servicios dentro del alcance por programa AWS cumplimiento.
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. Usted también es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza Site-to-Site VPN. En los siguientes temas, se le mostrará cómo configurar Site-to-Site VPN para satisfacer sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros AWS servicios que le ayudan a supervisar y proteger sus recursos de VPN de Site-to-Site.

Contenido

Protección de datos en AWS Site-to-Site VPN

El modelo de responsabilidad AWS compartida modelo se aplica a protección de datos en la VPN AWS Site-to-Site. Como se describe en este modelo, AWS es responsable de proteger la

infraestructura global en la que se ejecutan todos los. Nube de AWS Usted es responsable de mantener el control sobre el contenido alojado en esta infraestructura. Usted también es 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 la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulte la publicación de blog sobre el Modelo de responsabilidad compartida de AWS y GDPR en el Blog de seguridad de AWS .

Con fines de protección de datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure los 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:

- Utilice la autenticación multifactor (MFA) en cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos. AWS Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con. AWS CloudTrail
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utilice servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados por FIPS 140-2 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) 140-2.

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 trabajas con una VPN Site-to-Site u otra que Servicios de AWS utilice la consola, la API o los SDK. AWS CLI AWS Cualquier dato que ingrese en etiquetas o campos de formato libre utilizados para nombres se puede 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.

Privacidad del tráfico entre redes

Las conexiones de Site-to-Site VPN conectan de forma privada la VPC a la red local. Los datos que se transfieren entre su VPC y su red se direccionan a través de una conexión de VPN cifrada para ayudarlo a mantener la confidencialidad y la integridad de los datos en tránsito. Amazon da soporte a conexiones de VPN de seguridad de protocolo de Internet (IPSec). IPsec es un conjunto de protocolos que se usa para proteger las comunicaciones por protocolo de Internet (IP) mediante la autenticación y el cifrado de todos los paquetes IP de una transmisión de datos.

Cada conexión VPN Site-to-Site consta de dos túneles VPN IPsec cifrados que enlazan con su red. AWS El tráfico de cada túnel puede cifrarse con AES128 o AES256 y usar grupos Diffie-Hellman para el intercambio de claves, lo que proporciona una confidencialidad directa total. AWS autentica con funciones de hash SHA1 o SHA2.

Las instancias de la VPC no necesitan una dirección IP pública para conectarse a los recursos del otro extremo de la conexión de Site-to-Site VPN. Las instancias pueden direccionar el tráfico de Internet hacia la red de las instalaciones a través de la conexión de Site-to-Site VPN. A continuación, pueden obtener acceso a Internet a través de los puntos de tráfico salientes y de sus dispositivos de monitoreo y seguridad de la red.

Consulte los siguientes temas para obtener más información:

- Opciones del túnel de una conexión de Site-to-Site VPN: proporciona información sobre las opciones de IPsec e Intercambio de claves de Internet (IKE) disponibles para cada túnel.
- Opciones de autenticación de un túnel de Site-to-Site VPN: proporciona información sobre las opciones de autenticación de los puntos de enlace del túnel de VPN.
- Requisitos para el dispositivo de gateway del cliente: proporciona información sobre los requisitos del dispositivo de gateway de cliente en su extremo de la conexión de VPN.
- Comunicaciones seguras entre sitios mediante VPN CloudHub: Si tiene varias conexiones VPN de Site-to-Site, puede proporcionar una comunicación segura entre sus sitios locales mediante la VPN. AWS CloudHub

Gestión de identidad y acceso para la VPN AWS Site-to-Site

AWS Identity and Access Management (IAM) es una herramienta Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a los recursos. AWS Los administradores de

IAM controlan quién puede estar autenticado (ha iniciado sesión) y autorizado (tiene permisos) para utilizar recursos de Site-to-Site 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 el trabajo que se realice en la VPN Site-to-Site.

Usuario de servicio: si utiliza el servicio de Site-to-Site VPN para realizar su trabajo, su administrador le proporciona las credenciales y los permisos que necesita. A medida que utilice más características de Site-to-Site VPN para realizar su trabajo, es posible que necesite permisos adicionales. Entender cómo se administra el acceso puede ayudarlo a solicitar los permisos correctos al administrador. Si no puede acceder a una característica en Site-to-Site VPN, consulte Solución de problemas de AWS identidad y acceso a la VPN Site-to-Site.

Administrador de servicio: si está a cargo de los recursos de Site-to-Site VPN en su empresa, probablemente tenga acceso completo a Site-to-Site VPN. Su trabajo consiste en determinar a qué características y recursos de Site-to-Site VPN deben acceder los usuarios del servicio. Luego, debe enviar solicitudes a su administrador de IAM para cambiar los permisos de los usuarios de su servicio. Revise la información de esta página para conocer los conceptos básicos de IAM. Para obtener más información sobre cómo su empresa puede utilizar IAM con Site-to-Site VPN, consulte Cómo funciona la AWS VPN Site-to-Site con IAM.

Administrador de IAM: si es un administrador de IAM, es posible que quiera obtener más detalles sobre cómo escribir políticas para administrar el acceso a Site-to-Site VPN. Para consultar ejemplos de políticas basadas en la identidad de Site-to-Site VPN que puede utilizar en IAM, consulte Ejemplos de políticas basadas en la identidad para AWS la VPN Site-to-Site.

Autenticación con identidades

La autenticación es la forma en que inicias sesión para AWS usar tus credenciales de identidad. Debe estar autenticado (con quien haya iniciado sesión AWS) como usuario de IAM o asumiendo una función de IAM. Usuario raíz de la cuenta de AWS

Puede iniciar sesión AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center Los usuarios (Centro de identidades de IAM), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como una identidad federada, su administrador habrá configurado previamente la federación de identidades mediante roles de IAM. Cuando accedes AWS mediante la federación, estás asumiendo un rol de forma indirecta.

Según el tipo de usuario que sea, puede iniciar sesión en el portal AWS Management Console o en el de AWS acceso. Para obtener más información sobre cómo iniciar sesión AWS, consulte Cómo iniciar sesión Cuenta de AWS en su Guía del AWS Sign-In usuario.

Si accede AWS mediante programación, AWS proporciona un kit de desarrollo de software (SDK) y una interfaz de línea de comandos (CLI) para firmar criptográficamente sus solicitudes con sus credenciales. Si no utilizas AWS herramientas, debes firmar las solicitudes tú mismo. Para obtener más información sobre cómo usar el método recomendado para firmar las solicitudes usted mismo, consulte Firmar las solicitudes de la AWS API en la Guía del usuario de IAM.

Independientemente del método de autenticación que use, es posible que deba proporcionar información de seguridad adicional. Por ejemplo, le AWS recomienda que utilice la autenticación multifactor (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte Autenticación multifactor en la Guía del usuario de AWS IAM Identity Center y Uso de la autenticación multifactor (MFA) en AWSen la Guía del usuario de IAM.

Cuenta de AWS usuario root

Al crear una Cuenta de AWS, comienza con una identidad de inicio de sesión que tiene acceso completo a todos Servicios de AWS los recursos de la cuenta. Esta identidad se denomina usuario Cuenta de AWS raíz y se accede a ella iniciando sesión con la dirección de correo electrónico y la contraseña que utilizaste para crear la cuenta. Recomendamos encarecidamente que no utilice el usuario raíz para sus tareas diarias. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que solo el usuario raíz pueda realizar. Para ver la lista completa de las tareas que requieren que inicie sesión como 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, incluidos los que requieren acceso de administrador, 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 de usuarios empresarial, un proveedor de identidades web AWS Directory Service, el directorio del Centro de Identidad o cualquier usuario al que acceda Servicios de AWS mediante las credenciales proporcionadas a través de una fuente de identidad. Cuando las identidades federadas acceden Cuentas de AWS, asumen funciones y las funciones proporcionan credenciales temporales.

Para una administración de acceso centralizada, le recomendamos que utilice AWS IAM Identity Center. Puede crear usuarios y grupos en el Centro de identidades de IAM o puede conectarse y sincronizarse con un conjunto de usuarios y grupos de su propia fuente de identidad para usarlos en todas sus Cuentas de AWS aplicaciones. 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 propia Cuenta de AWS que tiene permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos emplear credenciales temporales, en lugar de crear usuarios de IAM que tengan credenciales de larga duración como contraseñas y claves de acceso. No obstante, si tiene casos de uso específicos que requieran credenciales de larga duración con usuarios de IAM, recomendamos rotar las claves de acceso. Para más información, consulte Rotar las claves de acceso periódicamente para casos de uso que requieran credenciales de larga duración en la Guía del usuario de IAM.

Un grupo de IAM es una identidad que especifica un conjunto de usuarios de IAM. No puede iniciar sesión como grupo. Puede usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos de grandes conjuntos de usuarios. Por ejemplo, podría tener un grupo cuyo nombre fuese IAMAdmins y conceder permisos a dicho grupo para administrar los recursos de IAM.

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales permanentes a largo plazo y los roles proporcionan credenciales temporales. Para más información, consulte Cuándo crear un usuario de IAM (en lugar de un rol) en la Guía del usuario de IAM.

Roles de IAM

Un rol de IAM es una identidad dentro de usted Cuenta de AWS que tiene permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una determinada persona. Puede asumir temporalmente una función de IAM en el AWS Management Console cambiando de función. Puede asumir un rol llamando a una operación de AWS API AWS CLI o utilizando una URL personalizada. Para más información sobre los métodos para el uso de roles, consulte Uso de roles de IAM en la Guía del usuario de IAM.

Los roles de IAM con credenciales temporales son útiles en las siguientes situaciones:

- Acceso de usuario federado: para asignar permisos a una identidad federada, puede crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener información acerca de roles para federación, consulte Creación de un rol para un proveedor de identidades de terceros en la Guía del usuario de IAM. Si utiliza IAM Identity Center, debe configurar un conjunto de permisos. IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM para controlar a qué pueden acceder las identidades después de autenticarse. Para obtener información acerca de los conjuntos de permisos, consulte Conjuntos de permisos en la Guía del usuario de AWS IAM Identity Center .
- Permisos de usuario de IAM temporales: un usuario de IAM puede asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.
- Acceso entre cuentas: puede utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, con algunas Servicios de AWS, puedes adjuntar una política directamente a un recurso (en lugar de usar un rol como proxy). Para conocer la diferencia entre las funciones y las políticas basadas en recursos para el acceso entre cuentas, consulte el tema sobre el acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.
- Acceso entre servicios: algunos utilizan funciones en otros. Servicios de AWS Servicios de AWS Por ejemplo, cuando realiza una llamada en un servicio, es común que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado al servicio.
  - Sesiones de acceso directo (FAS): cuando utilizas un usuario o un rol de IAM para realizar acciones en ellas AWS, se te considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. El FAS utiliza los permisos del principal que llama Servicio de AWS y los solicita Servicio de AWS para realizar

solicitudes a los servicios descendentes. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.

- Rol de servicio: un rol de servicio es un rol de IAM que adopta 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 Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.
- Función vinculada al servicio: una función vinculada a un servicio es un tipo de función de servicio que está vinculada 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.

- Aplicaciones que se ejecutan en Amazon EC2: puede usar un rol de IAM para administrar las credenciales temporales de las aplicaciones que se ejecutan en una instancia EC2 y realizan AWS CLI solicitudes a la API. AWS Es preferible hacerlo de este modo a almacenar claves de acceso en la instancia de EC2. Para asignar un AWS rol a una instancia EC2 y ponerlo a disposición de todas sus aplicaciones, debe crear un perfil de instancia adjunto a la instancia. Un perfil de instancia contiene el rol y permite a los programas que se ejecutan en la instancia de EC2 obtener credenciales temporales. Para más información, consulte Uso de un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias Amazon EC2 en la Guía del usuario de IAM.

Para obtener información sobre el uso de los roles de IAM, consulte Cuándo crear un rol de IAM (en lugar de un usuario) en la Guía del usuario de IAM.

Administración de acceso mediante políticas

El acceso se controla AWS creando políticas y adjuntándolas a AWS identidades o recursos. Una política es un objeto AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando un director (usuario, usuario raíz o sesión de rol) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan AWS como documentos JSON. Para obtener más información sobre la estructura y el contenido de los documentos de política JSON, consulte Información general de políticas JSON en la Guía del usuario de IAM.

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.

De forma predeterminada, los usuarios y los roles no tienen permisos. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puede añadir las políticas de IAM a roles y los usuarios pueden asumirlos.

Las políticas de IAM definen permisos para una acción independientemente del método que se utilice para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción `iam:GetRole`. Un usuario con esa política puede obtener información sobre el rol de la API AWS Management Console AWS CLI, la o la AWS API.

Políticas basadas en identidades

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 identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Las políticas basadas en identidades pueden clasificarse además como políticas insertadas o políticas administradas. Las políticas insertadas se integran directamente en un único usuario, grupo o rol. Las políticas administradas son políticas independientes que puede adjuntar a varios usuarios, grupos y roles de su Cuenta de AWS empresa. Las políticas administradas incluyen políticas AWS administradas y políticas administradas por el cliente. Para más información sobre cómo elegir una política administrada o una política insertada, consulte Elegir 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 política JSON que se asocian a un recurso. 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 en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

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.

Listas de control de acceso (ACL)

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

Amazon S3 y Amazon VPC son ejemplos de servicios que admiten las ACL. AWS WAF Para obtener más información sobre las ACL, consulte Información general de Lista de control de acceso (ACL) en la Guía para desarrolladores de Amazon Simple Storage Service.

Otros tipos de políticas

AWS admite tipos de políticas adicionales y menos comunes. Estos tipos de políticas pueden establecer el máximo de permisos que los tipos de políticas más frecuentes le conceden.

- Límites de permisos: un límite de permisos es una característica avanzada que le permite establecer los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM (usuario o rol de IAM). Puede establecer un límite de permisos para una entidad. Los permisos resultantes son la intersección de las políticas basadas en la identidad de la entidad y los límites de permisos. Las políticas basadas en recursos que especifiquen el usuario o rol en el campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites de los permisos, consulte Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.
- Políticas de control de servicios (SCP): las SCP son políticas de JSON que especifican los permisos máximos para una organización o unidad organizativa (OU). AWS Organizations AWS Organizations es un servicio para agrupar y gestionar de forma centralizada varios de los Cuentas de AWS que son propiedad de su empresa. Si habilita todas las características en una organización, entonces podrá aplicar políticas de control de servicio (SCP) a una o a todas sus cuentas. El SCP limita los permisos de las entidades en las cuentas de los miembros, incluidas las de cada una. Usuario raíz de la cuenta de AWS Para obtener más información acerca de Organizations y las SCP, consulte Funcionamiento de las SCP en la Guía del usuario de AWS Organizations .
- Políticas de sesión: las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado.

Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidades del rol y las políticas de la sesión. Los permisos también pueden proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para 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 AWS determinar 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 funciona la AWS VPN Site-to-Site con IAM

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

Funciones de IAM que puede utilizar con la VPN AWS Site-to-Site

Característica de IAM	Compatibilidad con Site-to-Site 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
ACL	No
ABAC (etiquetas en políticas)	No
Credenciales temporales	Sí
Permisos de entidades principales	Sí

Característica de IAM	Compatibilidad con Site-to-Site VPN
Roles de servicio	Sí
Roles vinculados al servicio	Sí

Para obtener una visión general de cómo funcionan la VPN Site-to-Site y otros AWS servicios con la mayoría de las funciones de IAM, consulte los AWS servicios que funcionan con IAM en la Guía del usuario de IAM.

Políticas basadas en identidad para Site-to-Site 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 identidad, consulte Creación de políticas de IAM 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. No es posible especificar la entidad principal en una política basada en identidad porque se aplica al usuario o rol al que está adjunto. Para más información sobre los elementos que puede utilizar en una política de JSON, consulte Referencia de los elementos de las políticas de JSON de IAM en la Guía del usuario de IAM.

Ejemplos de políticas basadas en identidad para Site-to-Site VPN

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

Políticas basadas en recursos dentro de Site-to-Site VPN

Compatibilidad con las políticas basadas en recursos	No

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. 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 en función de 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. Añadir a una política en función de recursos una entidad principal entre cuentas es solo una parte del establecimiento de una relación de confianza. Cuando el principal y el recurso son diferentes Cuentas de AWS, el administrador de IAM de la cuenta de confianza también debe conceder a la entidad principal (usuario o rol) permiso para acceder al recurso. Para conceder el permiso, adjunte la entidad a una política basada en identidad. Sin embargo, si la política en función de recursos concede el acceso a una entidad principal de la misma cuenta, no es necesaria una política basada en identidad adicional. Para obtener más información, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Acciones de política para Site-to-Site VPN

Admite acciones de política	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. Las acciones políticas suelen tener el mismo nombre que la operación de AWS API asociada. Hay algunas excepciones, como acciones de solo permiso que no

tienen una operación de API coincidente. También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Para ver una lista de las acciones de la VPN de sitio a sitio, consulte Acciones definidas por la VPN de sitio a sitio en la Referencia de autorización AWS del servicio.

Las acciones de políticas en Site-to-Site 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 Site-to-Site VPN, consulte Ejemplos de políticas basadas en la identidad para AWS la VPN Site-to-Site.

Recursos de políticas para Site-to-Site VPN

Admite 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. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). Puede hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, 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 VPN de sitio a sitio y sus ARN, consulte Recursos definidos por VPN de sitio a sitio en la Referencia de autorización de servicios AWS. Para saber con qué acciones puede especificar el ARN de cada recurso, consulte Acciones definidas por la VPN de AWS Site-to-Site.

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

Claves de condición de política para Site-to-Site VPN

Admite 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` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. Puede crear expresiones condicionales que utilicen operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

Si especifica varios elementos de `Condition` en una instrucción o varias claves en un único elemento de `Condition`, AWS las evalúa mediante una operación `AND` lógica. Si especifica varios valores para una única clave de condición, AWS evalúa la condición mediante una `OR` operación lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puede utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puede conceder un permiso de usuario de IAM para acceder a un recurso solo si está etiquetado con su nombre de usuario de IAM. Para más información, consulte Elementos de la política de IAM: variables y etiquetas en la Guía del usuario de IAM.

AWS admite claves de condición globales y claves de condición específicas del servicio. 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 claves de condición de la VPN de Site-to-Site, consulte Claves de condición de la VPN de sitio a sitio en la Referencia de autorización AWS del servicio. Para saber con qué acciones y recursos puede utilizar una clave de condición, consulte Acciones definidas por la VPN de AWS Site-to-Site.

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

ACL en Site-to-Site VPN

Admite las ACL	No

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

ABAC con Site-to-Site VPN

Admite ABAC (etiquetas en las políticas)	No

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos en función de atributos. En AWS, estos atributos se denominan etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a muchos AWS recursos. El etiquetado de entidades y recursos es el primer paso de ABAC. A continuación, designa las políticas de ABAC para permitir operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso al que se intenta acceder.

ABAC es útil en entornos que crecen con rapidez y ayuda en situaciones en las que la administración de las políticas resulta engorrosa.

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 ¿Qué es 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 Site-to-Site VPN

Compatible con el uso de credenciales temporales	Sí

Algunas Servicios de AWS no funcionan cuando inicias sesión con credenciales temporales. Para obtener información adicional, incluidas las que Servicios de AWS funcionan con credenciales temporales, consulta Cómo Servicios de AWS funcionan con IAM en la Guía del usuario de IAM.

Utiliza credenciales temporales si inicia sesión en ellas AWS Management Console mediante cualquier método excepto un nombre de usuario y una contraseña. Por ejemplo, cuando accedes AWS mediante el enlace de inicio de sesión único (SSO) de tu empresa, ese proceso crea automáticamente credenciales temporales. También crea credenciales temporales de forma automática cuando inicia sesión en la consola como usuario y luego cambia de rol. Para más información sobre el cambio de roles, consulte Cambio a un rol (consola) en la Guía del usuario de IAM.

Puedes crear credenciales temporales manualmente mediante la AWS CLI API o. AWS A continuación, puede utilizar esas credenciales temporales para acceder AWS. AWS recomienda generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para más información, consulte Credenciales de seguridad temporales en IAM.

Permisos de entidades principales entre servicios para Site-to-Site VPN

Admite Forward access sessions (FAS)	Sí

Cuando utilizas un usuario o un rol de IAM para realizar acciones en AWSél, se te considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza los permisos del principal que llama y los que solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Servicio de AWS Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar

ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.

Roles de servicio para Site-to-Site 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 Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

> **Warning**
>
> Cambiar los permisos de un rol de servicio podría interrumpir la funcionalidad de Site-to-Site VPN. Edite los roles de servicio solo cuando Site-to-Site VPN proporcione orientación para hacerlo.

Roles vinculados a servicios para Site-to-Site 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.

Para más información sobre cómo crear o administrar roles vinculados a servicios, consulte Servicios de AWS que funcionan con IAM. Busque un servicio en la tabla que incluya `Yes` en la columna Rol vinculado a un servicio. Seleccione el vínculo Sí para ver la documentación acerca del rol vinculado a servicios para ese servicio.

Ejemplos de políticas basadas en la identidad para AWS la VPN Site-to-Site

De forma predeterminada, los usuarios y roles no tienen permiso para crear ni modificar recursos de Site-to-Site VPN. Tampoco pueden realizar tareas mediante la AWS Management Console, AWS

Command Line Interface (AWS CLI) o la API. AWS Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puede añadir las políticas de IAM a roles y los usuarios pueden asumirlos.

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 en la Guía del usuario de IAM.

Para obtener más información sobre las acciones y los tipos de recursos definidos por la VPN de sitio a sitio, incluido el formato de los ARN de cada uno de los tipos de recursos, consulte Acciones, recursos y claves de condición de la VPN AWS de sitio a sitio en la Referencia de autorización de servicios.

Temas

- Prácticas recomendadas sobre las políticas
- Uso de la consola de Site-to-Site VPN
- Describa las conexiones VPN de Site-to-Site específicas
- Cree y describa los recursos necesarios para una conexión AWS Site-to-Site VPN

Prácticas recomendadas sobre las políticas

Las políticas basadas en identidades determinan si alguien puede crear, acceder o eliminar los recursos de Site-to-Site 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 en 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 trabajo 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 AWS CloudFormation. Para obtener más información, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utilice 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 Política de validación de Analizador de acceso de IAM en la Guía de 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 solicitar la MFA cuando se invocan las operaciones de la API, agregue las condiciones de la MFA a sus políticas. Para más información, consulte Configuración del acceso a una API protegido por MFA en la Guía de usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte las Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.

Uso de la consola de Site-to-Site VPN

Para acceder a la consola AWS de VPN de Site-to-Site, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle enumerar y ver detalles sobre los recursos de VPN de Site-to-Site que tiene en su cuenta. Cuenta de AWS Si crea una política basada en identidades que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles) que tengan esa política.

No es necesario que concedas permisos mínimos de consola a los usuarios que solo realizan llamadas a la API AWS CLI o a la AWS API. En su lugar, permite acceso únicamente a las acciones que coincidan con la operación de API que intentan realizar.

Para garantizar que los usuarios y los roles puedan seguir utilizando la consola de VPN de Site-to-Site, adjunte también la política gestionada o de VPN de sitio a las entidades. `AmazonVPCFullAccess` `AmazonVPCReadOnlyAccess` AWS Para más información, consulte Adición de permisos a un usuario en la Guía del usuario de IAM:

Describa las conexiones VPN de Site-to-Site específicas

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "ec2:DescribeVpnConnections"
         ],
         "Resource": [
         "arn:aws:ec2:us-west-2:123456789012:vpn-connection/vpn-04d5cc9b88example",
         "arn:aws:ec2:us-west-2:123456789012:vpn-connection/vpn-903004f88example"
         ]
      }
   ]
}
```

Cree y describa los recursos necesarios para una conexión AWS Site-to-Site VPN

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
         "ec2:DescribeVpnConnections",
         "ec2:DescribeVpnGateways",
         "ec2:DescribeCustomerGateways",
         "ec2:CreateCustomerGateway",
         "ec2:CreateVpnGateway",
         "ec2:CreateVpnConnection"
         ],
         "Resource": [
            "*"
         ]
      },
```

```
   {
         "Effect": "Allow",
         "Action": "iam:CreateServiceLinkedRole",
         "Resource": "arn:aws:iam::*:role/aws-service-role/s2svpn.amazonaws.com/
AWSServiceRoleForVPCS2SVPNInternal",
         "Condition": {
            "StringLike": {
               "iam:AWSServiceName":"s2svpn.amazonaws.com"
            }
         }
      }
   ]
}
```

Solución de problemas de AWS identidad y acceso a la VPN Site-to-Site

Utilice la siguiente información para diagnosticar y solucionar los problemas comunes que puedan surgir cuando trabaje con Site-to-Site VPN e IAM.

Temas

- No tengo autorización para realizar una acción en Site-to-Site VPN
- No estoy autorizado a realizar tareas como: PassRole
- Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis recursos de VPN Site-to-Site

No tengo autorización para realizar una acción en Site-to-Site 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 administrador. AWS 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 deben actualizarse a fin de permitirle pasar un rol a Site-to-Site 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 el rol 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 Site-to-Site 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 administrador. AWS 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 VPN Site-to-Site

Puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que admitan las políticas basadas en recursos o las listas de control de acceso (ACL), puede utilizar dichas políticas para conceder a las personas acceso a sus recursos.

Para más información, consulte lo siguiente:

- Para obtener información acerca de si Site-to-Site VPN admite estas características, consulte Cómo funciona la AWS VPN Site-to-Site con IAM.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a través de los Cuentas de AWS que eres propietario, consulta Cómo proporcionar acceso a un usuario de IAM en otro de tu propiedad Cuenta de AWS en la 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 la diferencia entre usar roles y políticas basadas en recursos para el acceso entre cuentas, consulte el tema Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Uso de roles vinculados a servicios para Site-to-Site VPN

AWS La VPN Site-to-Site utiliza funciones vinculadas al servicio AWS Identity and Access Management (IAM). Un rol vinculado a un servicio es un tipo único de rol de IAM que está vinculado directamente a un Site-to-Site VPN. Las funciones vinculadas al servicio están predefinidas por la VPN Site-to-Site e incluyen todos los permisos que el servicio requiere para AWS llamar a otros servicios en tu nombre.

Un rol vinculado a servicios simplifica la configuración de Site-to-Site VPN porque ya no tendrá que añadir manualmente los permisos necesarios. Site-to-Site VPN define los permisos de sus roles vinculados a servicios y, a menos que esté definido de otra manera, solo Site-to-Site 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 Site-to-Site VPN, ya que se evita que se puedan eliminar accidentalmente permisos de acceso a los recursos.

Para obtener información sobre otros servicios que admiten roles vinculados a servicios, consulte Servicios de AWS que funcionan con IAM y busque los servicios que muestran Yes (Sí) en la columna Roles vinculados a servicios. Elija una opción Sí con un enlace para ver la documentación acerca del rol vinculado al servicio en cuestión.

Rol vinculado a servicios para Site-to-Site VPN

La VPN de sitio a sitio utiliza la función vinculada al servicio denominada «Permitir que la VPN de AWSServiceRoleForVPCS2SVPNsitio a sitio cree y gestione los recursos relacionados con sus conexiones de VPN».

El rol AWSServiceRoleForVPCS2SVPN vinculado al servicio confía en los siguientes servicios para que asuman el rol:

- `AWS Certificate Manager`
- `AWS Private Certificate Authority`

La política de permisos de roles denominada AWSVPCS2SVpnServiceRolePolicy permite que la VPN de sitio a sitio complete las siguientes acciones en los recursos especificados:

- Acción: `acm:ExportCertificate` en `Resource: "*"`
- Acción: `acm:DescribeCertificate` en `Resource: "*"`
- Acción: `acm:ListCertificates` en `Resource: "*"`
- Acción: `acm-pca:DescribeCertificateAuthority` en `Resource: "*"`

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.

Crear un rol vinculado a servicios para Site-to-Site VPN

No necesita crear manualmente un rol vinculado a servicios. Cuando crea una pasarela de cliente con un certificado privado de ACM asociado en la AWS Management Console, la o la AWS API AWS CLI, la VPN Site-to-Site le crea la función vinculada al servicio.

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. Al crear una puerta de enlace de cliente con un certificado privado de ACM asociado, Site-to-Site VPN crea el rol vinculado a servicios por usted de nuevo.

Editar un rol vinculado a servicios para Site-to-Site VPN

La VPN Site-to-Site no le permite editar el rol vinculado al servicio. AWSServiceRoleForVPCS2SVPN 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 Editar un rol vinculado a servicios en la Guía del usuario de IAM.

Eliminar un rol vinculado a servicios para Site-to-Site VPN

Si ya no necesita usar una característica o servicio que requieran un rol vinculado a un servicio, le recomendamos que elimine dicho rol. Así no tendrá una entidad no utilizada que no se monitorice ni mantenga de forma activa. Sin embargo, debe limpiar los recursos de su rol vinculado al servicio antes de eliminarlo manualmente.

> **Note**
>
> Si el servicio Site-to-Site VPN está utilizando el rol cuando intenta eliminar los recursos, la eliminación podría producir un error. En tal caso, espere unos minutos e intente de nuevo la operación.

Para eliminar los recursos de VPN de Site-to-Site utilizados por AWSServiceRoleForVPCS2SVPN

Este rol vinculado a servicios solo se puede eliminar después de suprimir todas las gateways de cliente que tienen un certificado privado de ACM asociado. De esta manera, evitará eliminar por error el permiso para acceder a los certificados de ACM que se utilizan en las conexiones de Site-to-Site VPN.

Eliminación manual del rol vinculado a servicios mediante IAM

Utilice la consola de IAM AWS CLI, la o la AWS API para eliminar la función vinculada al AWSServiceRoleForVPCS2SVPN servicio. Para obtener más información, consulte Eliminación de un rol vinculado a servicios en la Guía del usuario de IAM.

Resiliencia en AWS Site-to-Site VPN

La infraestructura AWS global se basa en AWS regiones y zonas de disponibilidad. AWS Las regiones proporcionan varias zonas de disponibilidad aisladas y separadas físicamente, que están conectadas mediante redes de baja latencia, alto rendimiento y alta redundancia. 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 uno o varios centros de datos.

Para obtener más información sobre AWS las regiones y las zonas de disponibilidad, consulte Infraestructura global.AWS

Además de la infraestructura AWS global, la VPN Site-to-Site ofrece funciones que ayudan a respaldar sus necesidades de respaldo y resiliencia de datos.

Dos túneles por conexión de VPN

Una conexión de Site-to-Site VPN consta de dos túneles, cada uno de los cuales termina en una zona de disponibilidad diferente, para proporcionar una mayor disponibilidad a su VPC. Si se produce un fallo en un dispositivo interno AWS, la conexión VPN pasa automáticamente al segundo túnel para que el acceso no se interrumpa. De vez en cuando, AWS también realiza un mantenimiento rutinario de la conexión VPN, lo que puede desactivar brevemente uno de los dos túneles de la conexión VPN. Para obtener más información, consulte Sustitución de los puntos de enlace de un túnel de Site-to-Site VPN. Al configurar su gateway de cliente, por tanto es importante que configure ambos túneles.

Redundancia

Para protegerse contra una eventual pérdida de conectividad en caso de que la gateway de cliente dejara de estar disponible, puede configurar otra conexión de Site-to-Site VPN. Para obtener más información, consulte la siguiente documentación sobre :

- Uso de conexiones redundantes de Site-to-Site VPN para realizar la conmutación por error
- Opciones de conectividad de Amazon Virtual Private Cloud
- Creación de una infraestructura de red multiVPC AWS escalable y segura

Seguridad de la infraestructura en la VPN AWS Site-to-Site

Como servicio gestionado, la VPN AWS Site-to-Site está protegida por AWS la seguridad de la red 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 la VPN Site-to-Site 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.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad de seguridad de IAM principal. También puede utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Monitoreo de la conexión de Site-to-Site VPN

La supervisión es una parte importante del mantenimiento de la fiabilidad, la disponibilidad y el rendimiento de la AWS Site-to-Site VPN conexión. Debe recopilar datos de monitorización de todas las partes de su solución para que le resulte más sencillo depurar un error que se produce en distintas partes del código, en caso de que ocurra. No obstante, antes de comenzar a monitorear la conexión de Site-to-Site VPN, debe crear un plan que responda a las siguientes preguntas:

- ¿Cuáles son los objetivos de la monitorización?
- ¿Qué recursos va a supervisar?
- ¿Con qué frecuencia va a supervisar estos recursos?
- ¿Qué herramientas de monitoreo va a utilizar?
- ¿Quién se encargará de realizar las tareas de monitoreo?
- ¿Quién debería recibir una notificación cuando surjan problemas?

El siguiente paso consiste en establecer un punto de referencia del desempeño de VPN normal en su entorno. Para ello se mide el desempeño en distintos momentos y bajo distintas condiciones de carga. A medida que monitorice su VPN, almacene los datos de monitorización históricos para que pueda compararlos con los datos de desempeño actual, identificar los patrones de desempeño normal y las anomalías en el desempeño, así como desarrollar métodos para la resolución de problemas.

Para establecer un punto de referencia, debe monitorizar los elementos siguientes:

- El estado de sus túneles de VPN
- Los datos que entran en el túnel
- Los datos que salen del túnel

Contenido

Herramientas de monitoreo

AWS proporciona varias herramientas que puede utilizar para supervisar una conexión VPN de Site-to-Site. Puede configurar algunas de estas herramientas para que monitoricen por usted, pero otras herramientas requieren intervención manual. Le recomendamos que automatice las tareas de monitorización en la medida de lo posible.

Herramientas de monitoreo automatizadas

Puede utilizar las siguientes herramientas de monitoreo automatizado para vigilar las conexiones de Site-to-Site VPN e informar cuando haya algún problema:

- Amazon CloudWatch Alarms: observe una sola métrica durante un período de tiempo que especifique y realice una o más acciones en función del valor de la métrica en relación con un umbral determinado durante varios períodos de tiempo. La acción es una notificación que se envía a un tema de Amazon SNS. CloudWatch las alarmas no invocan acciones simplemente porque se encuentran en un estado determinado; el estado debe haber cambiado y se ha mantenido durante un número específico de períodos. Para obtener más información, consulte Supervisión de túneles VPN con Amazon CloudWatch.
- AWS CloudTrail Supervisión de registros: comparta archivos de registro entre cuentas, supervise los archivos de CloudTrail registro en tiempo real enviándolos a CloudWatch Logs, cree aplicaciones de procesamiento de registros en Java y valide que los archivos de registro no hayan cambiado después de la entrega. CloudTrail Para obtener más información, consulte Registro de llamadas a la API mediante AWS CloudTrail la referencia a la API de Amazon EC2 y Uso de archivos de CloudTrail registro en la Guía del AWS CloudTrail usuario.
- AWS Health eventos: reciba alertas y notificaciones relacionadas con los cambios en el estado de sus túneles de VPN Site-to-Site, las recomendaciones de configuración recomendadas o cuando se acerque a los límites de escalado. Utilice los eventos de Personal Health Dashboard para activar conmutaciones por error automatizadas, reducir el tiempo de resolución de problemas y optimizar las conexiones para disfrutar de una alta disponibilidad. Para obtener más información, consulte Supervisión de las conexiones VPN mediante AWS Health eventos.

Herramientas de monitoreo manuales

Otra parte importante de la supervisión de una conexión VPN de Site-to-Site implica la supervisión manual de los elementos que las CloudWatch alarmas no cubren. Los paneles de Amazon VPC y de CloudWatch consola ofrecen una at-a-glance visión del estado de su entorno. AWS

> **Note**
>
> En la consola de Amazon VPC, es posible que los parámetros de estado del túnel de la VPN de Site-to-Site, como «Estado» y «Último cambio de estado», no reflejen los cambios de estado transitorios ni los cambios momentáneos del túnel. Se recomienda utilizar CloudWatch métricas y registros para actualizar de forma pormenorizada los cambios en el estado del túnel.

- En el panel de control de Amazon VPC se indica:
  - El estado de los servicios en cada región
  - Las conexiones de Site-to-Site VPN
  - El estado del túnel de VPN: en el panel de navegación, elija Site-to-Site VPN Connections (Conexiones de Site-to-Site VPN), seleccione una conexión de Site-to-Site VPN y haga clic en Tunnel Details (Detalles del túnel)
- La página de CloudWatch inicio muestra:
  - Alarmas y estado actual
  - Gráficos de alarmas y recursos
  - Estado de los servicios

  Además, puede CloudWatch hacer lo siguiente:
  - Crear paneles personalizados para monitorizar los servicios que le interesan
  - Realizar un gráfico con los datos de las métricas para resolver problemas y descubrir tendencias
  - Busque y explore todas sus métricas AWS de recursos
  - Crear y editar las alarmas de notificación de problemas

AWS Site-to-Site VPN registros

AWS Site-to-Site VPN los registros le proporcionan una mayor visibilidad de sus despliegues de VPN de Site-to-Site. Con esta característica, tiene acceso a los registros de conexión de Site-to-Site VPN que proporcionan detalles sobre el establecimiento del túnel de seguridad IP (IPsec), las negociaciones de intercambio de claves de Internet (IKE) y los mensajes del protocolo de detección de pares muertos (DPD).

Los registros de VPN de Site-to-Site se pueden publicar en Amazon Logs. CloudWatch Esta característica proporciona a los clientes una única forma coherente de acceder y analizar registros detallados para todas las conexiones de Site-to-Site VPN.

Contenido

Beneficios de los registros de Site-to-Site VPN

- Solución de problemas de VPN simplificada: los registros de VPN de Site-to-Site le ayudan a identificar las discrepancias de configuración entre el dispositivo de puerta de enlace del cliente AWS y a solucionar los problemas iniciales de conectividad de la VPN. Las conexiones de VPN pueden cambiar de forma intermitente con el tiempo debido a ajustes mal configurados (como tiempos de espera mal ajustados), puede haber problemas en las redes de transporte subyacentes (como el tiempo de Internet) o los cambios de enrutamiento o los errores de ruta pueden provocar la interrupción de la conectividad a través de VPN. Esta característica le permite diagnosticar con precisión la causa de los errores de conexión intermitentes y ajustar la configuración del túnel de bajo nivel para lograr un funcionamiento fiable.
- AWS Site-to-Site VPN Visibilidad centralizada: los registros de la VPN Site-to-Site pueden proporcionar registros de la actividad de los túneles para todas las diferentes formas en que se conecta la VPN Site-to-Site: Virtual Gateway, Transit Gateway y, a través de Internet y CloudHub como medio de transporte. AWS Direct Connect Esta característica proporciona a los clientes una única forma coherente de acceder y analizar registros detallados para todas las conexiones de Site-to-Site VPN.
- Seguridad y conformidad: los registros de VPN de Site-to-Site se pueden enviar a Amazon CloudWatch Logs para un análisis retrospectivo del estado y la actividad de la conexión VPN a lo largo del tiempo. Esto puede ayudarle a cumplir con los requisitos reglamentarios y de conformidad.

Restricciones de tamaño de la política de recursos de Amazon CloudWatch Logs

CloudWatch Las políticas de recursos de Logs están limitadas a 5120 caracteres. Cuando CloudWatch Logs detecta que una política se acerca a este límite de tamaño, habilita automáticamente los grupos de registros que comiencen por. `/aws/vendedlogs/` Al habilitar el registro, la VPN Site-to-Site debe actualizar la política de recursos de CloudWatch registros con el grupo de registros que especifique. Para evitar alcanzar el límite de tamaño de la política de recursos de CloudWatch registros, añada el prefijo a los nombres de los grupos de registros. `/aws/vendedlogs/`

Contenido de los registros de Site-to-Site VPN

La siguiente información se incluye en el registro de actividad de túnel de Site-to-Site VPN.

Campo	Descripción
VpnLogCreationTimestamp	Marca temporal de creación de registros en formato legible por humanos.
VpnConnectionID	El identificador de conexión de VPN.
TunnelOutsideDirección IP	La IP externa de túnel de VPN que generó la entrada de registro.
TunnelDPDEnabled	Estado habilitado del protocolo de detección de pares muertos (verdadero/falso).
Túnel CGWnatt DetectionStatus	NAT-T detectado en el dispositivo de puerta de enlace de cliente (verdadero/falso).
TunnelIKEPhase1State	Estado del protocolo de fase 1 de IKE (Establecido | Cambio de clave | Negociación | Inactivo).
TunnelIKEPhase2State	Estado del protocolo de fase 2 de IKE (Establecido | Cambio de clave | Negociación | Inactivo).

Campo	Descripción
VpnLogDetalle	Mensajes detallados para los protocolos IPsec, IKE y DPD.

Contenido

Mensajes de error de IKEv1

Mensaje	Explicación
El par no responde: declarar muerto al par	El par no ha respondido a los mensajes de DPD, por lo que se ha impuesto la acción de tiempo de espera del DPD.
AWS El descifrado de la carga útil del túnel no se pudo realizar debido a que la clave previamente compartida no era válida	Se debe configurar la misma clave previamente compartida en ambos pares de IKE.
No se encontró ninguna propuesta que coincidiera AWS	El punto de conexión de AWS VPN no admite los atributos propuestos para la fase 1 (cifrado, hash y grupo DH), por ejemplo, 3DES
No se encontró ninguna coincidencia de propuesta. Notificación con la opción «No se ha elegido ninguna propuesta»	Los pares no intercambian ningún mensaje de error de propuesta elegida para informar de que se deben configurar las propuestas/políticas correctas para la fase 2 en pares de IKE.
AWS tunnel recibió DELETE para la SA de fase 2 con el SPI: xxxx	CGW ha enviado el mensaje Delete_SA para la fase 2
AWS tunnel recibió un DELETE para IKE_SA de CGW	CGW ha enviado el mensaje Delete_SA para la fase 1

Mensajes de error de IKEv2

Mensaje	Explicación
AWS Se agotó el tiempo de espera del DPD del túnel después de la retransmisión de {retry_count}	El par no ha respondido a los mensajes de DPD, por lo que se ha impuesto la acción de tiempo de espera del DPD.
AWS El túnel recibió el comando DELETE para IKE_SA de CGW	El par ha enviado el mensaje Delete_SA para Parent/IKE_SA
AWS tunnel recibió DELETE para la SA de fase 2 con el SPI: xxxx	El par ha enviado el mensaje Delete_SA para CHILD_SA
AWS El túnel detectó una colisión (CHILD_RE KEY) como CHILD_DELETE	CGW ha enviado el mensaje Delete_SA para la SA activa, a la que se le está cambiando la clave.
AWS La SA redundante del túnel (CHILD_SA) se está eliminando debido a una colisión detectada	Debido a una colisión, si se generan SA redundantes, los pares cerrarán la SA redundante después de hacer coincidir los valores nonce según RFC
AWS La fase 2 del túnel no se pudo establecer mientras se mantenía la fase 1	El par no pudo establecer CHILD_SA debido a un error de negociación, por ejemplo, a una propuesta incorrecta.
AWS: Selector de tráfico: TS_UNACCE PTABLE: recibido del agente de respuesta	El par ha propuesto selectores de tráfico o dominio de cifrado incorrectos. Los pares se deben configurar con CIDR idénticos y correctos.
AWS el túnel envía AUTHENTICATION_FAI LED como respuesta	El par no puede autenticar al par al verificar el contenido del mensaje IKE_AUTH
AWS tunnel detectó una falta de coincidencia de claves previamente compartidas con cgw: xxxx	Se debe configurar la misma clave previamente compartida en ambos pares de IKE.

Mensaje	Explicación
AWS Tiempo de espera del túnel: eliminar el IKE_SA de fase 1 no establecido con cgw: xxxx	La eliminación de IKE_SA semiabierto como par no ha continuado con las negociaciones
No se encontró ninguna coincidencia de propuesta. Notificación con la opción «No se ha elegido ninguna propuesta»	Los pares no intercambian ningún mensaje de error de propuesta elegida para informar que las propuestas correctas se deben configurar en pares de IKE.
No se encontró ninguna propuesta que coincidiera AWS	AWS VPN Endpoint no admite los atributos propuestos para la fase 1 (cifrado, hash y grupo DH). Por ejemplo, 3DES

Mensajes de negociación de IKEv2

Mensaje	Explicación
AWS solicitud procesada por túnel (id=xxx) para CREATE_CHILD_SA	AWS ha recibido la solicitud CREATE_CHILD_SA de CGW
AWS tunnel está enviando una respuesta (id=xxx) para CREATE_CHILD_SA	AWS está enviando la respuesta CREATE_CHILD_SA a CGW
AWS tunnel está enviando una solicitud (id=xxx) para CREATE_CHILD_SA	AWS está enviando la solicitud CREATE_CHILD_SA a CGW
AWS respuesta procesada por túnel (id=xxx) para CREATE_CHILD_SA	AWS ha recibido la respuesta CREATE_CHILD_SA de CGW

Requisitos de IAM para publicar en Logs CloudWatch

Para que la característica de registro funcione correctamente, la política de IAM asociada a la entidad principal de IAM que se está utilizando para configurar la característica debe incluir los siguientes permisos como mínimo. También puedes encontrar más información en la sección Habilitar el registro desde determinados AWS servicios de la Guía del usuario de Amazon CloudWatch Logs.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries"
      ],
      "Resource": [
        "*"
      ],
      "Effect": "Allow",
      "Sid": "S2SVPNLogging"
    },
    {
      "Sid": "S2SVPNLoggingCWL",
      "Action": [
        "logs:PutResourcePolicy",
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups"
      ],
      "Resource": [
        "*"
      ],
      "Effect": "Allow"
    }
  ]
}
```

Consultar la configuración de registros de Site-to-Site VPN

Para consultar la configuración actual de registro de túnel

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Site-to-Site VPN Connections (Conexiones de Site-to-Site VPN).
3. Seleccione la conexión de VPN que desea ver en la lista VPN connections (Conexiones de VPN).
4. Elija la pestaña Tunnel details (Detalles de túnel).

5. Amplíe las secciones Tunnel 1 options (Opciones de túnel 1) y Tunnel 2 options (Opciones de túnel 2) para ver todos los detalles de configuración de los túneles.
6. Puede ver el estado actual de la función de registro en el registro de Tunnel VPN y el grupo de CloudWatch registros actualmente configurado (si lo hay) en el grupo de CloudWatch registros.

Para ver la configuración actual del registro de túneles en una conexión VPN de Site-to-Site mediante la línea de comandos o la API AWS

- DescribeVpnConexiones (API de consultas de Amazon EC2)
- describe-vpn-connections (AWS CLI)

Habilitar registros de Site-to-Site VPN

> **Note**
>
> Cuando habilita los registros de Site-to-Site VPN para un túnel de conexión de VPN existente, la conectividad a través de ese túnel se puede interrumpir durante varios minutos. Sin embargo, cada conexión de VPN ofrece dos túneles para una alta disponibilidad, por lo que puede habilitar el registro en un túnel a la vez mientras mantiene la conectividad a través del túnel que no se modifica. Para obtener más información, consulte Sustitución de los puntos de enlace de un túnel de Site-to-Site VPN.

Para habilitar el registro de VPN durante la creación de una nueva conexión de Site-to-Site VPN

Siga el procedimiento indicado en Paso 5: Crear una conexión de VPN. En las Tunnel Options (Opciones de túnel) del Paso 9, puede especificar todas las opciones que desea usar para ambos túneles, como las opciones de VPN logging (Registro de VPN). Para obtener más información sobre estas opciones, consulte Opciones del túnel de una conexión de Site-to-Site VPN.

Para habilitar el registro de túneles en una nueva conexión VPN de Site-to-Site mediante la línea de comandos o la API AWS

- CreateVpnConexión (API de consultas de Amazon EC2)
- create-vpn-connection (AWS CLI)

Para habilitar el registro de túnel en una conexión de Site-to-Site VPN existente

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Site-to-Site VPN Connections (Conexiones de Site-to-Site VPN).
3. Seleccione la conexión de VPN que desea modificar de la lista VPN connections (Conexiones de VPN).
4. Seleccione Actions (Acciones), Modify VPN tunnel options (Modificar opciones de túnel de VPN).
5. Seleccione el túnel que desea modificar; para ello, elija la dirección IP adecuada en la lista VPN tunnel outside IP address (Túnel de VPN fuera de la dirección IP).
6. En Tunnel activity log (Registro de actividad de túnel), seleccione Enable (Habilitar).
7. En Grupo de CloudWatch registros de Amazon, selecciona el grupo de CloudWatch registros de Amazon al que quieres que se envíen los registros.
8. (Opcional) En Output format (Formato de salida), elija el formato deseado para la salida del registro, ya sea json o text (texto).
9. Seleccione Save changes (Guardar cambios).
10. (Opcional) Repita los pasos 4 a 9 para el otro túnel si lo desea.

Para habilitar el registro de túneles en una conexión VPN de Site-to-Site existente mediante la línea de comandos o la API AWS

- ModifyVpnTunnelOptions(API de consultas de Amazon EC2)
- modify-vpn-tunnel-options (AWS CLI)

Desactivar registros de Site-to-Site VPN

Para desactivar el registro de túnel en una conexión de Site-to-Site VPN

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Site-to-Site VPN Connections (Conexiones de Site-to-Site VPN).
3. Seleccione la conexión de VPN que desea modificar de la lista VPN connections (Conexiones de VPN).
4. Seleccione Actions (Acciones), Modify VPN tunnel options (Modificar opciones de túnel de VPN).
5. Seleccione el túnel que desea modificar; para ello, elija la dirección IP adecuada en la lista VPN tunnel outside IP address (Túnel de VPN fuera de la dirección IP).

6. En Tunnel activity log (Registro de actividad de túnel), desactive Enable (Habilitar).
7. Seleccione Save changes (Guardar cambios).
8. (Opcional) Repita los pasos 4 a 7 para el otro túnel si lo desea.

Para deshabilitar el registro de túneles en una conexión VPN de Site-to-Site mediante la línea de comandos o la API AWS

- ModifyVpnTunnelOptions(API de consultas de Amazon EC2)
- modify-vpn-tunnel-options (AWS CLI)

Supervisión de túneles VPN con Amazon CloudWatch

Puede monitorizar los túneles de la VPN mediante CloudWatch, que recopila y procesa los datos sin procesar del servicio de VPN para convertirlos en métricas legibles y prácticamente en tiempo real. Estas estadísticas se registran durante un periodo de 15 meses, de forma que pueda obtener acceso a información de historial y obtener una mejor perspectiva acerca del desempeño de su aplicación web o servicio. Los datos de las métricas de la VPN se envían automáticamente a CloudWatch medida que están disponibles.

Para obtener más información, consulta la Guía del CloudWatch usuario de Amazon.

Contenido

Dimensiones y métricas de VPN

Las siguientes CloudWatch métricas están disponibles para sus conexiones de VPN de Site-to-Site.

Métrica	Descripción
`TunnelState`	El estado de los túneles. Para las VPN estáticas, 0 indica DOWN y 1 indica UP. Para las VPN de BGP, 1 indica ESTABLISHED y 0

Métrica	Descripción
	se utiliza para los demás estados. Para los dos tipos de VPN, los valores entre 0 y 1 indican que al menos que un túnel no es UP. Unidades: valor fraccional entre 0 y 1
`TunnelDataIn` †	Los bytes recibidos en el AWS lateral de la conexión a través del túnel VPN desde una pasarela de cliente. Cada punto de datos de la métrica representa el número de bytes recibidos después del punto de datos anterior. Use la estadística Sum para mostrar el número total de bytes recibidos durante el periodo. Esta métrica cuenta los datos después del descifrado. Unidades: bytes
`TunnelDataOut` †	Los bytes enviados desde el AWS lado de la conexión a través del túnel VPN hasta la pasarela del cliente. Cada punto de datos de la métrica representa el número de bytes enviados después del punto de datos anterior. Use la estadística Sum para mostrar el número total de bytes enviados durante el periodo. Esta métrica cuenta los datos antes del cifrado. Unidades: bytes

† Estas métricas pueden dar información sobre el uso de la red incluso cuando el túnel no está operativo. Esto se debe a las comprobaciones periódicas de estado realizadas en el túnel y a las solicitudes de ARP y BGP en segundo plano.

Para filtrar los datos de las métricas, use las siguientes dimensiones.

Dimensión	Descripción
`VpnId`	Filtra los datos de las métricas por el ID de Site-to-Site VPN.
`TunnelIpAddress`	Filtra los datos de las métricas en función de la dirección IP del túnel de la gateway privada virtual.

Visualización de CloudWatch las métricas de VPN

Cuando creas una conexión VPN Site-to-Site, el servicio VPN envía métricas sobre tu conexión VPN a medida que están CloudWatch disponibles. Puede ver las métricas de la conexión de VPN de la siguiente manera.

Para ver las métricas mediante la consola 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 CloudWatch consola en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, seleccione Métricas.
3. En All metrics elija el espacio de nombres de métricas VPN.
4. Seleccione la dimensión de métrica para ver las métricas (por ejemplo, Métricas de túneles de VPN).

> **Note**
>
> El espacio de nombres de la VPN no aparecerá en la CloudWatch consola hasta que se haya creado una conexión VPN Site-to-Site AWS en la región que está viendo.

Para ver las métricas mediante el AWS CLI

En el símbolo del sistema, ejecute el siguiente comando:

```
aws cloudwatch list-metrics --namespace "AWS/VPN"
```

Crear CloudWatch alarmas para monitorear los túneles de VPN

Puede crear una CloudWatch alarma que envíe un mensaje de Amazon SNS cuando la alarma cambie de estado. Una alarma vigila una única métrica durante el período especificado y envía una notificación a un tema de Amazon SNS según el valor de la métrica relativo a un determinado umbral durante varios períodos de tiempo.

Por ejemplo, puede crear una alarma que monitoree el estado de un único túnel de VPN y envíe una notificación cuando el estado del túnel sea INACTIVO durante 3 puntos de datos en 15 minutos.

Para crear una alarma para el estado de un único túnel

1. Abra la CloudWatch consola en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, amplíe Alarmas y, a continuación, elija Todas las alarmas.
3. Elija Crear alarma y, a continuación, elija Seleccionar métrica.
4. Elija VPN y, a continuación, elija Métricas de túnel de VPN.
5. Seleccione la dirección IP del túnel deseado, en la misma línea que la TunnelStatemétrica. Elija Seleccionar métrica.
6. Para siempre que TunnelState sea... , seleccione Inferior y, a continuación, introduzca «1" en el campo de entrada situado debajo de... .
7. En Configuración adicional, establezca las entradas en “3 de 3” para los Puntos de datos para la alarma.
8. Elija Siguiente.
9. En Enviar una notificación al siguiente tema de SNS, seleccione una lista de notificación existente o cree una nueva.
10. Elija Siguiente.
11. Escriba un nombre para la alarma. Elija Siguiente.
12. Compruebe la configuración de la alarma y, a continuación, elija Create alarm (Crear alarma).

Puede crear una alarma que monitoree el estado de la conexión de Site-to-Site VPN. Por ejemplo, puede crear una alarma que envíe una notificación cuando el estado de uno o ambos túneles esté INACTIVO durante un período de 5 minutos.

Si desea crear una alarma para el estado de la conexión de Site-to-Site VPN

1. Abre la CloudWatch consola en https://console.aws.amazon.com/cloudwatch/.

2. En el panel de navegación, amplíe Alarmas y, a continuación, elija Todas las alarmas.
3. Elija Crear alarma y, a continuación, elija Seleccionar métrica.
4. Elija VPN y, a continuación, elija VPN Connection Metrics (Métricas de conexión VPN).
5. Selecciona tu conexión VPN de Site-to-Site y la métrica. TunnelState Elija Select metric (Seleccionar métrica).
6. En Statistic (Estadística), especifique Maximum (Máximo).

   Si ha configurado la conexión de Site-to-Site VPN de modo que ambos túneles estén activos, también puede especificar la estadística Minimum (Mínima) para que se envíe una notificación cuando haya al menos un túnel inactivo.
7. En Whenever (Siempre), elija Lower/Equal (Menor o igual) (**<=**) e ingrese 0 (o 0,5 para cuando hay al menos un túnel desactivado). Elija Siguiente.
8. En Select an SNS topic (Seleccionar un tema de SNS), seleccione una notificación existente o elija New list (Nueva lista) para crear una. Elija Siguiente.
9. Escriba un nombre y la descripción de su alarma. Elija Siguiente.
10. Compruebe la configuración de la alarma y, a continuación, elija Create alarm (Crear alarma).

También puede crear alarmas que monitoricen la cantidad de tráfico que entra o sale del túnel de VPN. Por ejemplo, la siguiente alarma monitoriza la cantidad de tráfico que entra en el túnel de VPN desde su red, y envía una notificación cuando el número de bytes alcanza un umbral de 5 000 000 durante un periodo de 15 minutos.

Para crear una alarma para el tráfico de red entrante

1. Abre la CloudWatch consola en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, amplíe Alarmas y, a continuación, elija Todas las alarmas.
3. Elija Crear alarma y, a continuación, elija Seleccionar métrica.
4. Seleccione VPN y, a continuación, elija VPN Tunnel Metrics (Métricas de túnel de VPN).
5. Seleccione la dirección IP del túnel VPN y la métrica TunnelDatade entrada. Elija Select metric (Seleccionar métrica).
6. En Statistic (Estadística), especifique Sum (Suma).
7. En Period (Periodo), seleccione 15 minutes (15 minutos).
8. En Whenever (Siempre), elija Greater/Equal (Mayor o igual)(**>=**) y escriba 5000000. Elija Siguiente.

9. En Select an SNS topic (Seleccionar un tema de SNS), seleccione una notificación existente o elija New list (Nueva lista) para crear una. Elija Siguiente.
10. Escriba un nombre y la descripción de su alarma. Elija Siguiente.
11. Compruebe la configuración de la alarma y, a continuación, elija Create alarm (Crear alarma).

La siguiente alarma monitoriza la cantidad de tráfico que sale del túnel de VPN a su red, y envía una notificación cuando el número de bytes sea inferior a 1 000 000 durante un periodo de 15 minutos.

Para crear una alarma para el tráfico de red saliente

1. Abra la CloudWatch consola en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, amplíe Alarmas y, a continuación, elija Todas las alarmas.
3. Elija Crear alarma y, a continuación, elija Seleccionar métrica.
4. Seleccione VPN y, a continuación, elija VPN Tunnel Metrics (Métricas de túnel de VPN).
5. Seleccione la dirección IP del túnel VPN y la métrica TunnelDatade salida. Elija Select metric (Seleccionar métrica).
6. En Statistic (Estadística), especifique Sum (Suma).
7. En Period (Periodo), seleccione 15 minutes (15 minutos).
8. En Whenever (Siempre que sea), elija Lower/Equal (Menor o igual)(<=) y escriba `1000000`. Elija Siguiente.
9. En Select an SNS topic (Seleccionar un tema de SNS), seleccione una notificación existente o elija New list (Nueva lista) para crear una. Elija Siguiente.
10. Escriba un nombre y la descripción de su alarma. Elija Siguiente.
11. Compruebe la configuración de la alarma y, a continuación, elija Create alarm (Crear alarma).

Para ver más ejemplos de creación de alarmas, consulta Cómo crear CloudWatch alarmas de Amazon en la Guía del CloudWatch usuario de Amazon.

Supervisión de las conexiones VPN mediante AWS Health eventos

AWS Site-to-Site VPN envía automáticamente las notificaciones al AWS AWS Health Dashboard(PHD), que funciona con la AWS Health API. Este panel no requiere configuración y está listo para ser utilizado por AWS los usuarios autenticados. Puede configurar varias acciones en respuesta a las notificaciones de eventos a través de AWS Health Dashboard.

AWS Health Dashboard Proporciona los siguientes tipos de notificaciones para sus conexiones VPN:

- Notificaciones de sustitución de puntos de enlace de un túnel
- Notificaciones de VPN con un solo túnel

Notificaciones de sustitución de puntos de enlace de un túnel

Recibirá una notificación de sustitución del punto final del túnel AWS Health Dashboard cuando se sustituya uno o ambos puntos finales del túnel VPN de su conexión VPN. El punto de enlace de un túnel se reemplaza cuando AWS realiza actualizaciones en el túnel o cuando se modifica su conexión de VPN. Para obtener más información, consulte Sustitución de los puntos de enlace de un túnel de Site-to-Site VPN.

Cuando se completa el reemplazo del punto final del túnel, AWS envía la notificación de reemplazo del punto final del túnel a través de un AWS Health Dashboard evento.

Notificaciones de VPN con un solo túnel

Por motivos de redundancia, las conexiones de Site-to-Site VPN tienen dos túneles. Se recomienda encarecidamente que configure ambos túneles para disfrutar de una alta disponibilidad. Si la conexión VPN tiene un único túnel activo y el otro se mantiene inactivo durante más de una hora al día, recibirá una notificación de túnel de VPN único mensual a través de un evento de AWS Health Dashboard . Este evento se actualizará diariamente con cualquier conexión VPN nueva detectada como túnel único, y las notificaciones se enviarán semanalmente. Cada mes se creará un nuevo evento que borrará todas las conexiones de VPN que ya no se detecten como túnel único.

Cuotas de Site-to-Site VPN

Su AWS cuenta tiene las siguientes cuotas, anteriormente denominadas límites, relacionadas con la VPN Site-to-Site. A menos que se indique lo contrario, cada cuota es específica de la región de . 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 Solicitud de un aumento de cuota en la Guía del usuario de Service Quotas.

Recursos de Site-to-Site VPN

Nombre	Valor predeterminado	Ajustable
Gateways de cliente por región	50	Sí
Gateways privadas virtuales por región	5	Sí
Conexiones de Site-to-Site VPN por región	50	Sí
Conexiones de Site-to-Site VPN por gateway privada virtual	10	Sí
Conexiones de Site-to-Site VPN aceleradas por región	10	Sí
Conexiones de Site-to-Site VPN no asociadas por región	10	Sí

> **Note**
>
> Tanto las conexiones aceleradas como las no asociadas se tienen en cuenta en la cuota total de conexiones de Site-to-Site VPN por región.

Puede asociar una gateway privada virtual a una VPC a la vez. Para establecer la misma conexión de Site-to-Site VPN con varias VPC, le recomendamos que valore la posibilidad de utilizar una

gateway de tránsito en su lugar. Para obtener más información, consulte Gateways de tránsito en Gateways de tránsito de Amazon VPC.

Las conexiones de Site-to-Site VPN en una gateway de tránsito están sujetas al límite total de las conexiones de gateway de tránsito. Para obtener más información, consulte Cuotas de gateway de tránsito.

Rutas

Las fuentes de rutas anunciadas son las rutas de VPC, otras rutas de VPN y las rutas de las interfaces virtuales de AWS Direct Connect . Las rutas anunciadas proceden de la tabla de enrutamiento vinculada a la conexión de VPN.

> **Note**
>
> Si utiliza una puerta de enlace privada virtual y la propagación de rutas está habilitada en la tabla de enrutamiento de la VPC, se agregarán automáticamente rutas dinámicas y estáticas a la conexión de VPN, hasta el límite de la tabla de enrutamiento de la VPC. Consulte las cuotas de Amazon VPC en la Guía del usuario de Amazon VPC para obtener más información.

Nombre	Valor predeterminado	Ajustable
Rutas dinámicas anunciadas entre un dispositivo de gateway de cliente y una conexión de Site-to-Site VPN de una gateway privada virtual	100	No
Rutas anunciadas entre una conexión de Site-to-Site VPN de una gateway privada virtual y un dispositivo de gateway de cliente	1 000	No
Rutas dinámicas anunciadas entre un dispositivo de gateway de cliente y una conexión de Site-to-Site VPN en una gateway de tránsito	1 000	No

Nombre	Valor predeterminado	Ajustable
Rutas anunciadas entre una conexión de Site-to-Site VPN de una gateway de tránsito y un dispositivo de gateway de cliente	5 000	No
Rutas estáticas entre un dispositivo de puerta de enlace de cliente y una conexión de Site-to-Site VPN en una puerta de enlace privada virtual	100	No

Ancho de banda y rendimiento

Hay muchos factores que pueden afectar el ancho de banda obtenido a través de una conexión Site-to-Site VPN, incluidos, entre otros, el tamaño del paquete, la mezcla de tráfico (TCP/UDP), las políticas de modelado o de limitación controlada en redes intermedias, el tiempo de Internet y los requisitos específicos de aplicaciones.

Nombre	Valor predeterminado	Ajustable
Ancho de banda máximo por túnel de VPN	Hasta 1,25 Gbps	No
Paquetes máximos por segundo (PPS) por túnel de VPN	Hasta 140 000	No

En las conexiones de Site-to-Site VPN de una gateway de tránsito, puede usar ECMP para conseguir un mayor ancho de banda de VPN agregando varios túneles de VPN. Para utilizar ECMP, la conexión de VPN debe estar configurada para el enrutamiento dinámico. ECMP no es compatible con conexiones de VPN que utilizan enrutamiento estático. Para obtener más información, consulte Gateway de tránsito.

Unidad de transmisión máxima (MTU).

Site-to-Site VPN admite una unidad máxima de transmisión (MTU) de 1446 bytes y un tamaño máximo de segmento (MSS) correspondiente de 1406 bytes. Sin embargo, ciertos algoritmos que utilizan encabezados TCP más grandes pueden reducir eficazmente ese valor máximo. Para evitar

la fragmentación, le recomendamos que configure la MTU y el MSS en función de los algoritmos seleccionados. Para obtener más información sobre MTU, MSS y los valores óptimos, consulte Prácticas recomendadas para su dispositivo de puerta de enlace de cliente.

No se admiten tramas gigantes. Para obtener más información, consulte Jumbo frames en la Guía del usuario de Amazon EC2.

Las conexiones de Site-to-Site VPN no admiten la detección de MTU de la ruta.

Recursos de cuotas adicionales

Para obtener información sobre las cuotas relacionadas con las gateways de tránsito, como el número de conexiones de una gateway de tránsito, consulte Cuotas de las gateways de tránsito en la Guía de gateways de tránsito de Amazon VPC.

Para ampliar las cuotas de VPC, consulte Cuotas de Amazon VPC en la Guía del usuario de Amazon VPC.

Historial de revisión de la Guía del usuario de Site-to-Site VPN

En la siguiente tabla se describen las actualizaciones de la Guía del usuario de AWS Site-to-Site VPN.

Cambio	Descripción	Fecha
Información de VPN clásica eliminada	Se ha eliminado la información sobre la VPN clásica de la guía.	19 de enero de 2023
Mensajes de ejemplo de registro de VPN	Se han agregado registros de ejemplo para conexiones de Site-to-Site VPN.	9 de diciembre de 2022
Utilidad de la configuración de descarga actualizada	Los clientes de Site-to-Site VPN pueden generar plantillas de configuración para dispositivos compatibles con Gateway de Cliente (CGW), lo que facilita la creación de conexiones VPN a AWS. Esta actualización agrega la compatibilidad con los parámetros de Intercambio de Clave de Internet versión 2 (IKEv2) para muchos dispositivos populares CGW e incluye dos nuevas API: GetVpnConnectionDeviceTypes y GetVpnConnectionDeviceSampleConfiguration.	21 de septiembre de 2021

Notificaciones de la conexión de VPN	Site-to-Site VPN envía automáticamente notificaciones sobre la conexión de VPN a AWS Health Dashboard.	29 de octubre de 2020
Iniciación de túnel de VPN	Puede configurar sus túneles de VPN de modo que AWS muestre los túneles.	27 de agosto de 2020
Modificar las opciones de conexión de VPN	Puede modificar las opciones de una conexión de Site-to-Site VPN.	27 de agosto de 2020
Algoritmos de seguridad adicionales	Puede aplicar algoritmos de seguridad adicionales a sus túneles VPN.	14 de agosto de 2020
Compatibilidad con IPv6	Los túneles VPN pueden admitir tráfico IPv6 dentro de los túneles.	12 de agosto de 2020
Combinar las guías de AWS Site-to-Site VPN	En esta versión, se combina el contenido de la Guía para administradores de red de AWS Site-to-Site VPN en esta guía.	31 de marzo de 2020
Conexiones de AWS Site-to-Site VPN aceleradas	Puede habilitar la aceleración para su conexión de AWS Site-to-Site VPN.	3 de diciembre de 2019
Modificar opciones de túnel de AWS Site-to-Site VPN	Puede modificar las opciones de un túnel de VPN en una conexión de AWS Site-to-Site VPN. También puede configurar opciones de túnel adicionales.	29 de agosto de 2019

Compatibilidad con certificados privados de AWS Private Certificate Authority	Puede usar un certificado privado de AWS Private Certificate Authority para autenticar la VPN.	15 de agosto de 2019
Nueva guía del usuario de Site-to-Site VPN	En esta versión, el contenido de AWS Site-to-Site VPN (anteriormente conocido como VPN administrado por AWS) está separado de la Guía del usuario de Amazon VPC.	18 de diciembre de 2018
Modificar la gateway de destino	Puede modificar la gateway de destino de la conexión de AWS Site-to-Site VPN.	18 de diciembre de 2018
ASN personalizado	Al crear una gateway privada virtual, puede especificar el número de sistema autónomo (ASN) privado en el lado de Amazon de la gateway.	10 de octubre de 2017
Opciones de túnel de VPN	Puede especificar bloques de CIDR de túnel interior y claves compartidas previamente personalizadas para sus túneles de VPN.	3 de octubre de 2017
Métricas de VPN	Puede ver las métricas de CloudWatch de las conexiones de VPN.	15 de mayo de 2017

Mejoras de VPN	La conexión de VPN ahora admite la función de cifrado AES de 256 bits, la función de hash SHA-256, NAT traversal y los grupos Diffie-Hellman adicionales durante las fases 1 y 2 de la conexión. Además, podrá utilizar la misma dirección IP de gateway de cliente para cada conexión de VPN que utilice el mismo dispositivo de gateway de cliente.	28 de octubre de 2015
Conexiones de VPN mediante configuración de direccionamiento estático	Puede crear conexiones de VPN de IPsec a Amazon VPC utilizando configuraciones de direccionamiento estático. Anteriormente, las conexiones de VPN requerían el uso del protocolo de gateway fronteriza (BGP). Ahora admitimos ambos tipos de conexiones y podrá establecer conectividad desde dispositivos que no son compatibles con BGP, incluidos Cisco ASA y Microsoft Windows Server 2008 R2.	13 de septiembre de 2012
Propagación de ruta automática	Ahora puede configurar la propagación automática de rutas desde su VPN y enlaces de AWS Direct Connect a sus tablas de enrutamiento de VPC.	13 de septiembre de 2012

AWS VPN CloudHub y conexiones de VPN redundantes	Puede comunicarse de forma segura de un sitio a otro con y sin VPC. Puede utilizar conexiones de VPN redundantes para proporcionar una conexión tolerante a errores a su VPC.	29 de septiembre de 2011

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.