COLOMBIA POTENCIA DE LA VIDA

TIC

Lección 2

Conexión a la red remota con AWS Site-to-Site VPN

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

UTP Universidad Tecnológica de Pereira

AWS Site-to-Site VPN

AWS
Site-to-Site VPN

AWS Site-to-Site es la solución de alta disponibilidad que le permite conectar de forma segura a la red en las instalaciones o el sitio de su sucursal a la VPC.

- Utiliza comunicaciones de seguridad de protocolo de Internet (IPSec) para crear túneles de red virtual privada (VPN) cifrados.
- Proporciona dos túneles cifrados por conexión de VPN.
- Se paga por hora de conexión de VPN.

De forma predeterminada, las instancias que lanzan en una nube virtual privada (VPC) en AWS no pueden comunicarse con la red en las instalaciones.

Puede utilizar AWS Site-to-Site Virtual Private Network (AWS Site-to-Site VPN) para conectar de forma segura la red en las instalaciones o el sitio de su sucursal a la VPC. Cada conexión de AWS Site-to-Site VPN utiliza comunicaciones de seguridad del protocolo de Internet (IPSec) para crear túneles de VPN cifrados entre dos ubicaciones. Un túnel de VPN es un enlace cifrado por el que los datos pueden viajar entre la red del cliente y AWS.

El lado de AWS de la conexión es la gateway privada virtual. (Tenga en cuenta que, en lugar de una gateway privada virtual, también puede crear una conexión de Site-to-Site VPN como una asociación en una gateway de tránsito. Más adelante en este módulo, podrá obtener más información sobre AWS Transit Gateway). El lado en las instalaciones de la conexión es la gateway de cliente.

AWS Site-to-Site VPN proporciona dos túneles de VPN entre varias zonas de disponibilidad que puede utilizar simultáneamente y así obtener una alta disponibilidad. Puede transmitir el tráfico principal a través del primer túnel y utilizar el segundo para lograr redundancia. Si un túnel deja de funcionar, el tráfico llegará igualmente a su VPC.

Si crea una conexión de Site-to-Site VPN con su VPC, se le cobrará por cada hora de conexión
de VPN en la que dicha conexión esté aprovisionada y disponible. Para obtener más información sobre precios, consulte Precios de AWS Site-to-Site VPN y conexiones de Site-to- Site VPN aceleradas.

COLOMBIA POTENCIA DE LA VIDA

TIC

Direccionamiento estático y dinámico

Cuando crea una conexión de Site-to-Site VPN, debe especificar el tipo de direccionamiento que planea utilizar y debe actualizar la tabla de enrutamiento de su subred.

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

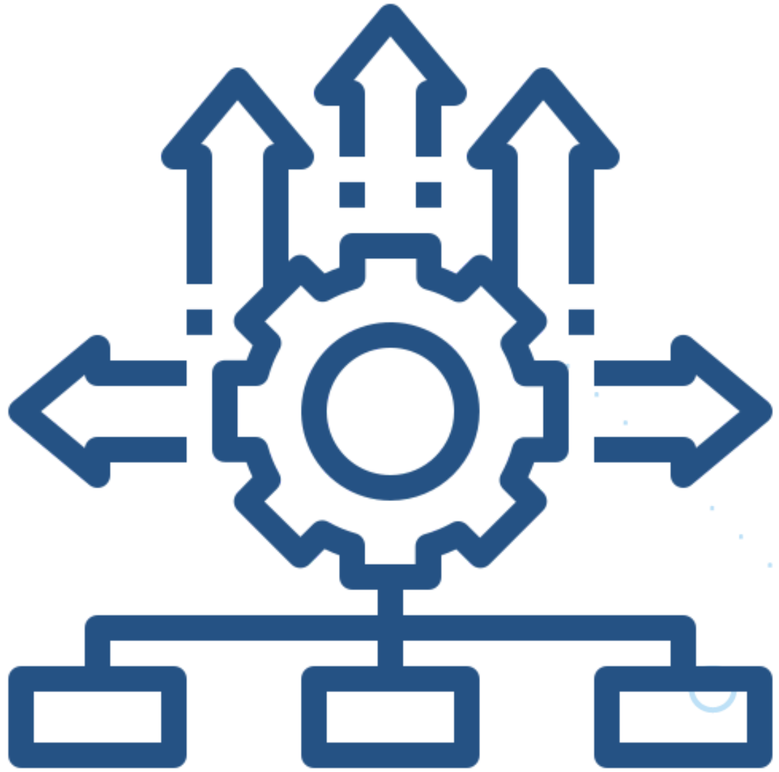
UTP Universidad Tecnológica de Pereira

- Si el dispositivo de VPN admite el protocolo de gateway fronteriza (BGP), especifique direccionamiento dinámico al configurar la conexión de Site-to-Site VPN. El direccionamiento dinámico utiliza el BGP para anunciar rutas a la gateway privada virtual. Además, admite un máximo de 100 rutas propagadas por tabla de enrutamiento. (Para conocer los límites actuales, consulte Límites de AWS Site-to-Site VPN).
- Si el dispositivo de VPN no admite BGP, especifique el direccionamiento estático. El direccionamiento estático requiere que especifique las rutas (es decir, los prefijos de IP) para la red que deberían comunicarse con la gateway privada virtual. Además, admite 50 rutas no propagadas por tabla de enrutamiento de forma predeterminada, hasta un máximo de 1000 rutas no propagadas. (Para conocer los límites actuales, consulte Límites de AWS Site-to-Site VPN).

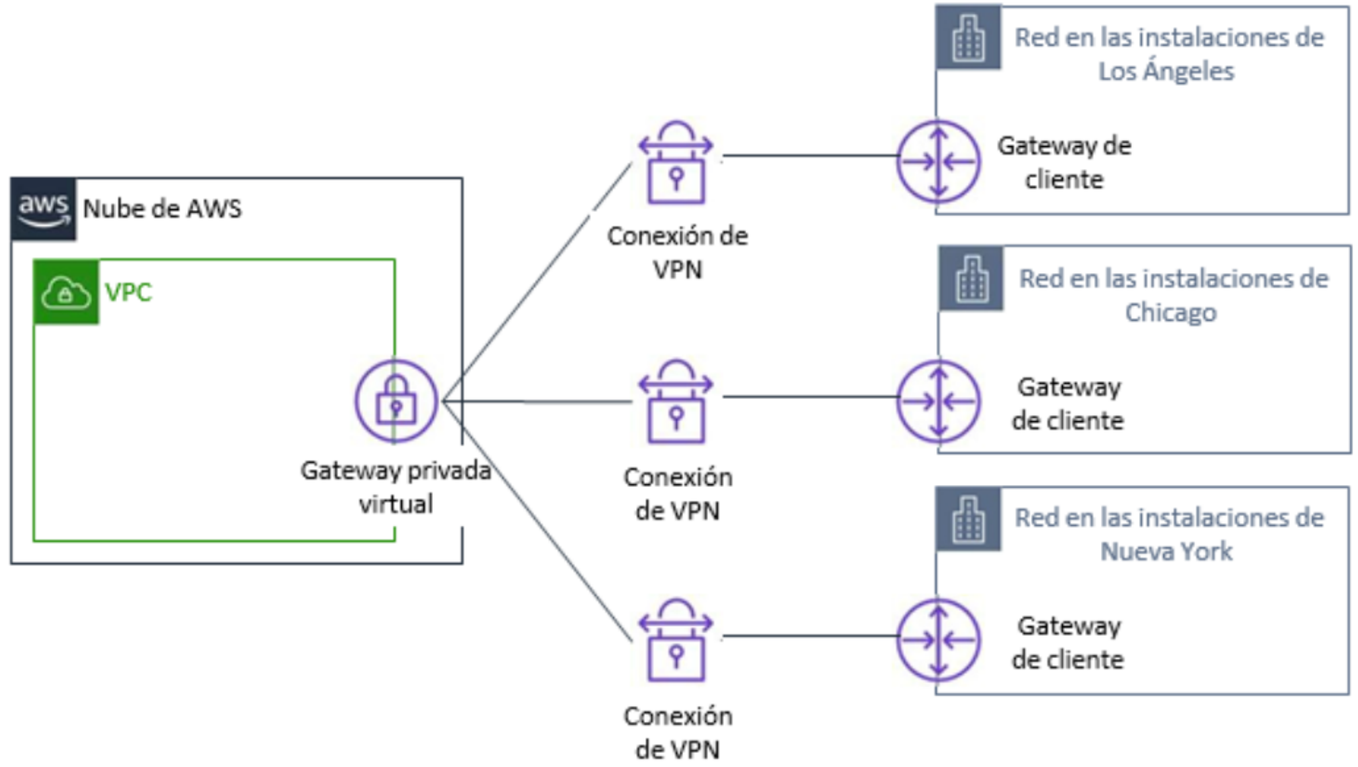
Se recomienda utilizar dispositivos que admitan BGP, ya que dicho protocolo ofrece comprobaciones de detección de conexión sólidas que pueden ayudar en la conmutación por error al segundo túnel de VPN en caso de una falla en el primero. Los dispositivos que no admiten BGP también pueden realizar comprobaciones de estado para asistir en la conmutación por error al segundo túnel cuando se necesite.

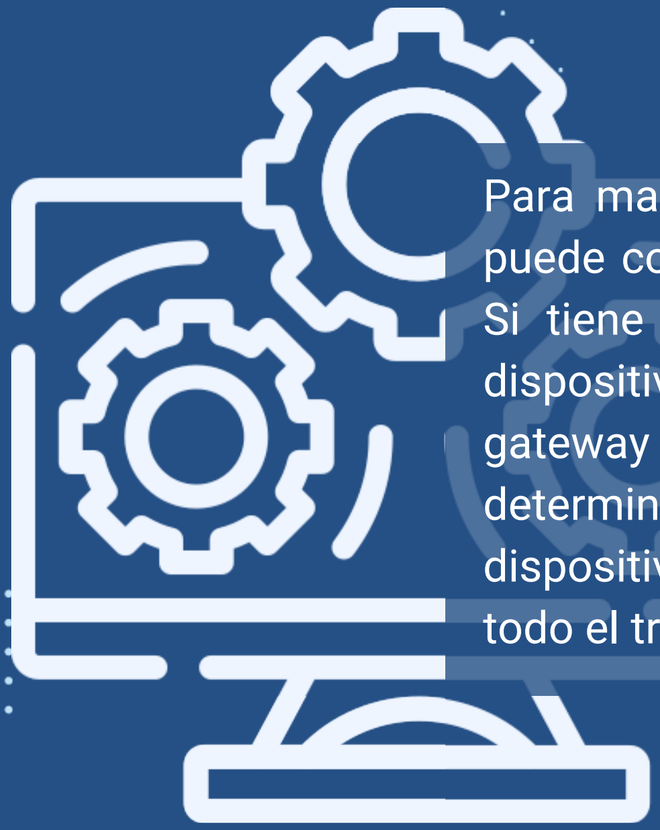
Para obtener una lista de los dispositivos de direccionamiento estático y dinámico que se han puesto a prueba con Amazon VPC, consulte Customer Gateway Devices We've Tested en la Guía del administrador de AWS Site-to-Site VPN Network.

Para obtener más información sobre las opciones de direccionamiento de Site-to-Site VPN, consulte Static and Dynamic Routing Options.



Conexión de varias VPN





Para mantener una alta disponibilidad de la gateway de cliente, puede configurar dispositivos de gateway de cliente redundantes. Si tiene dispositivos de gateway de cliente redundantes, cada dispositivo anuncia el mismo prefijo (por ejemplo, 0.0.0.0/0) a la gateway privada virtual. AWS utiliza 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.

Puede establecer varias conexiones de VPN entre múltiples dispositivos de gateway de cliente y una única gateway privada virtual mediante AWS VPN CloudHub. Esta configuración se puede utilizar de diferentes formas para implementar redundancia y conmutación por error en su lado de la conexión de VPN.

AWS VPN CloudHub funciona con un sistema radial para permitir que varios sitios accedan a su VPC o que accedan de forma segura los unos a los otros. Puede utilizarlo con o sin una VPC. Configura cada dispositivo de gateway de cliente para que anuncie un prefijo específico del sitio (como 10.0.0.0/24, 10.0.1.0/24) a la gateway privada virtual. La gateway privada virtual dirige el tráfico al sitio correcto y anuncia la accesibilidad de un sitio a todos los demás.

Para obtener más información sobre el uso de AWS Site-to-Site VPN, consulte los siguientes
recursos:

- Ejemplos de una conexión única y una conexión múltiple de Site-to-Site VPN
- Uso de conexiones redundantes de Site-to-Site VPN para realizar la conmutación por error

Estos son algunos de los aprendizajes clave de esta lección de la unidad:

- AWS Site-to-Site VPN es una solución con alta disponibilidad que permite conectar de forma segura la red en las instalaciones o el sitio de su sucursal a la VPC.
- AWS Site-to-Site VPN admite el direccionamiento estático y dinámico.
- Puede establecer varias conexiones de VPN entre múltiples dispositivos de gateway de cliente y una única gateway privada virtual.

INICIO