Configure la conectividad de la red privada virtual (VPN) AnyConnect en el router de la serie RV34x

Objetivo

El objetivo de este documento es mostrarle cómo configurar la conectividad de VPN de AnyConnect en el router de la serie RV34x.

Ventajas del uso de AnyConnect Secure Mobility Client:

1. Conectividad segura y persistente
2. Seguridad persistente y aplicación de políticas
3. Se puede implementar desde el dispositivo de seguridad adaptable (ASA) o desde los sistemas de implementación de software empresarial
4. Personalizable y traducible
5. Fácilmente configurado
6. Admite seguridad de protocolo de Internet (IPSec) y capa de sockets seguros (SSL)
7. Admite el protocolo Intercambio de claves de Internet versión 2.0 (IKEv2.0)

Introducción

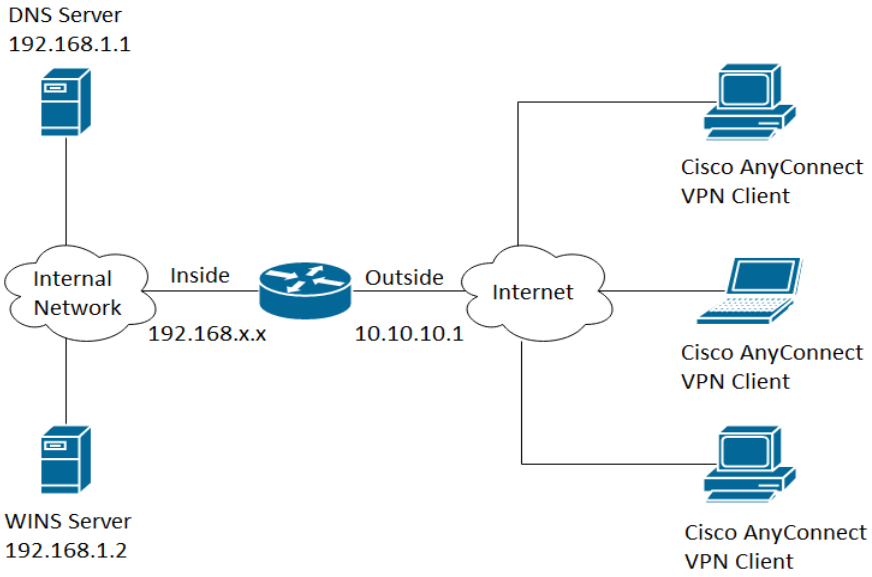
Una conexión de red privada virtual (VPN) permite a los usuarios acceder, enviar y recibir datos desde y hacia una red privada a través de una red pública o compartida como Internet, pero sigue garantizando conexiones seguras a una infraestructura de red subyacente para proteger la red privada y sus recursos.

Un cliente VPN es un software que se instala y ejecuta en un equipo que desea conectarse a la red remota. Este software cliente debe configurarse con la misma configuración que la del servidor VPN, como la dirección IP y la información de autenticación. Esta información de autenticación incluye el nombre de usuario y la clave previamente compartida que se utilizarán para cifrar los datos. Según la ubicación física de las redes que se van a conectar, un cliente VPN también puede ser un dispositivo de hardware. Esto suele suceder si la conexión VPN se utiliza para conectar dos redes que se encuentran en ubicaciones independientes.

Cisco AnyConnect Secure Mobility Client es una aplicación de software para conectarse a una VPN que funciona en varios sistemas operativos y configuraciones de hardware. Esta aplicación de software hace posible que los recursos remotos de otra red sean accesibles como si el usuario estuviera conectado directamente a su red, pero de una manera segura. Cisco AnyConnect Secure Mobility Client proporciona una nueva e innovadora forma de proteger a los usuarios móviles en plataformas informáticas o de teléfonos inteligentes, lo que proporciona una experiencia más fluida y siempre protegida para los usuarios finales y una aplicación de políticas completa para los administradores de TI.

En el router RV34x, a partir de la versión de firmware 1.0.3.15 y en el futuro, no es necesaria la licencia de AnyConnect. Sólo se cobrará por las licencias de cliente.

Para obtener información adicional sobre las licencias de AnyConnect en los routers de la serie RV340, consulte el artículo Licencias de AnyConnect para routers de la serie RV340.



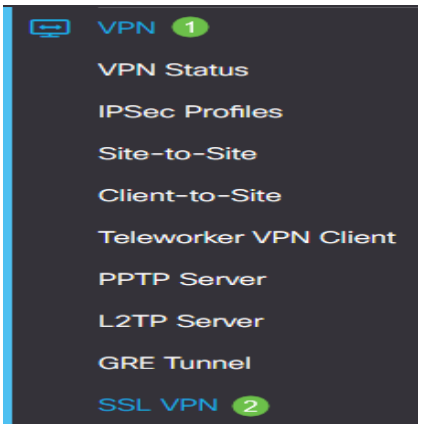
Dispositivos aplicables | Versión de firmware

- Cisco AnyConnect Secure Mobility Client | 4.4 (Descargar la última versión)
- Serie RV34x | 1.0.03.15 (Descargar la última versión)

Configuración de la conectividad VPN AnyConnect en el RV34x

Configuración de SSL VPN en el RV34x

Paso 1. Acceda a la utilidad basada en Web del router y seleccione **VPN > SSL VPN**.



Paso 2. Haga clic en el botón de opción **On** para habilitar el servidor Cisco SSL VPN.

Configuración de gateway obligatoria

Los siguientes parámetros de configuración son obligatorios:

Paso 3. Seleccione la interfaz de la puerta de enlace en la lista desplegable. Este será el puerto que se utilizará para pasar el tráfico a través de los túneles VPN SSL. Las opciones son:

- WAN1
- WAN2
- USB1
- USB2

Nota: En este ejemplo, se elige WAN1.

Paso 4. Introduzca el número de puerto que se utiliza para el gateway SSL VPN en el campo *Gateway Port* que va del 1 al 65535.

Nota: En este ejemplo, 8443 se utiliza como número de puerto.

Paso 5. Elija el archivo de certificado en la lista desplegable. Este certificado autentica a los usuarios que intentan acceder al recurso de red a través de los túneles VPN SSL. La lista desplegable contiene un certificado predeterminado y los certificados que se importan.

Nota: En este ejemplo, se elige Por defecto.

Paso 6. Ingrese la dirección IP del pool de direcciones del cliente en el campo *Pool de Direcciones del Cliente*. Este conjunto será el intervalo de direcciones IP que se asignarán a los clientes VPN remotos.

Nota: Asegúrese de que el intervalo de direcciones IP no se superpone con ninguna de las direcciones IP de la red local.

Nota: En este ejemplo, se utiliza 192.168.0.0.

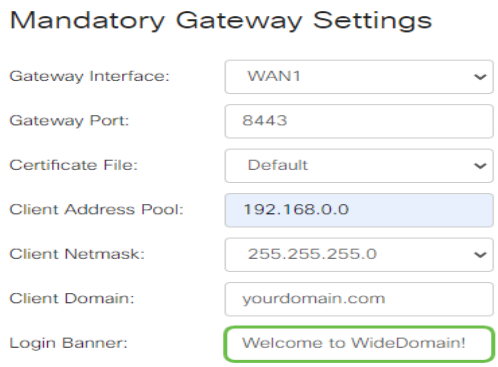
Paso 7. Elija la máscara de red de cliente en la lista desplegable.

Nota: En este ejemplo, se elige 255.255.255.128.

Paso 8. Ingrese el nombre de dominio del cliente en el campo *Dominio del Cliente*. Este será el nombre de dominio que debe enviarse a los clientes SSL VPN.

Nota: En este ejemplo, WideDomain.com se utiliza como nombre de dominio del cliente.

Paso 9. Introduzca el texto que aparecerá como banner de inicio de sesión en el campo *Login Banner*. Este será el banner que se mostrará cada vez que un cliente inicie sesión.

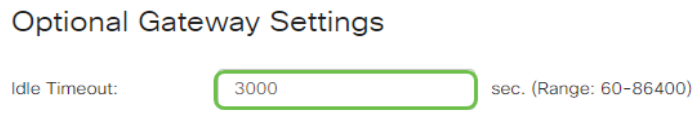


Nota: En este ejemplo, Welcome to Widedomain! (Bienvenido a Widedomain!) se utiliza como banner de inicio de sesión.

Configuración de gateway opcional

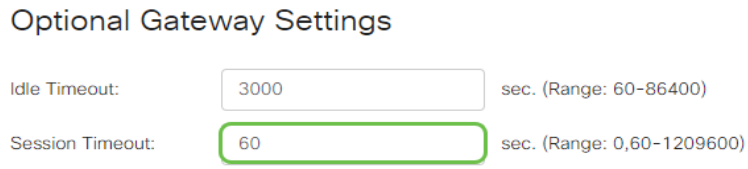
Los siguientes parámetros de configuración son opcionales:

Paso 1. Introduzca un valor en segundos para el tiempo de espera de inactividad comprendido entre 60 y 86400. Este será el tiempo que la sesión VPN SSL puede permanecer inactiva.



Nota: En este ejemplo, se utiliza 3000.

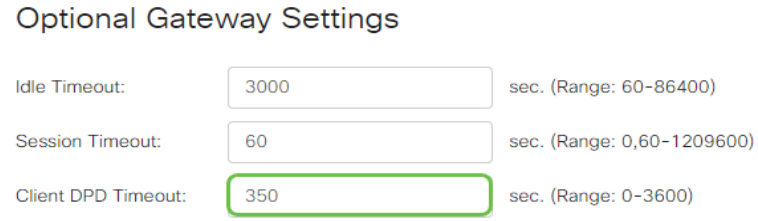
Paso 2. Introduzca un valor en segundos en el campo *Tiempo de espera de sesión*. Este es el tiempo que tarda la sesión de Protocolo de control de transmisión (TCP) o Protocolo de datagramas de usuario (UDP) en agotarse después del tiempo de inactividad especificado. El intervalo es de 60 a 1209600.



Nota: En este ejemplo, se utiliza 60.

Paso 3. Introduzca un valor en segundos en el campo *ClientDPD Timeout* que va de 0 a 3600. Este valor especifica el envío periódico de mensajes HELLO/ACK para comprobar el estado del túnel VPN.

Nota: esta función debe estar activada en ambos extremos del túnel VPN.

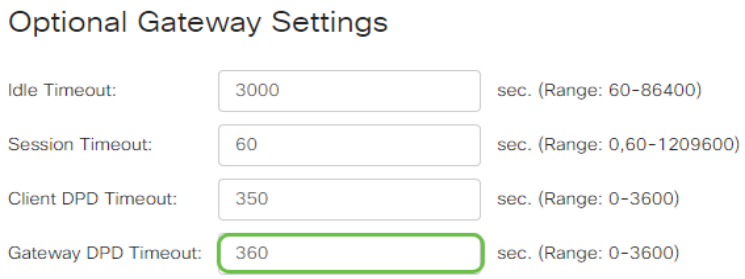


Nota: En este ejemplo, se utiliza 350.

Paso 4. Introduzca un valor en segundos en el campo *GatewayDPD Timeout* que va de 0 a 3600.

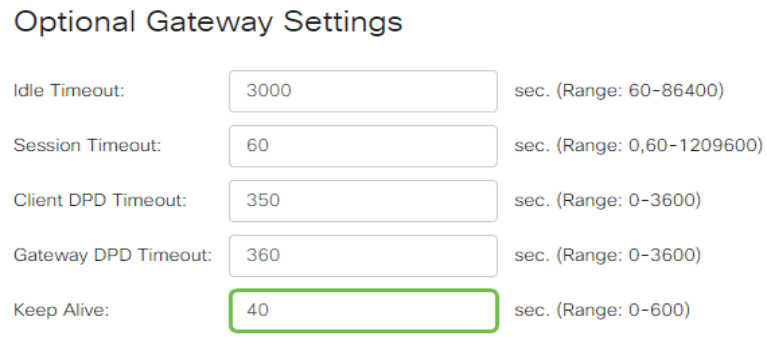
Este valor especifica el envío periódico de mensajes HELLO/ACK para comprobar el estado del túnel VPN.

Nota: esta función debe estar activada en ambos extremos del túnel VPN.



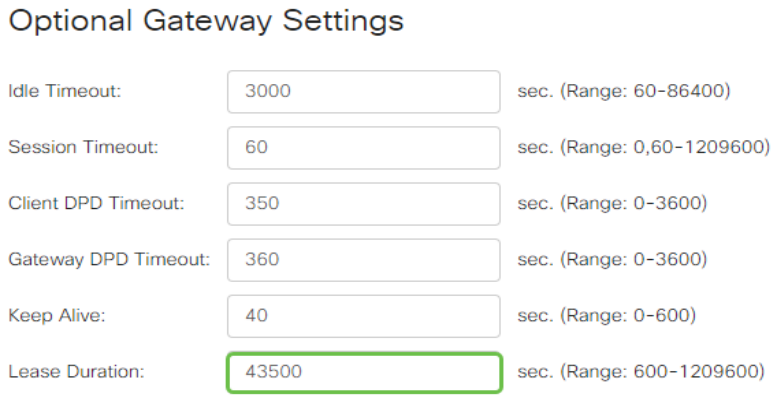
Nota: En este ejemplo, se utiliza 360.

Paso 5. Introduzca un valor en segundos en el campo *Keep Alive* que oscila entre 0 y 600. Esta función garantiza que el router esté siempre conectado a Internet. Si se interrumpe, intentará restablecer la conexión VPN.



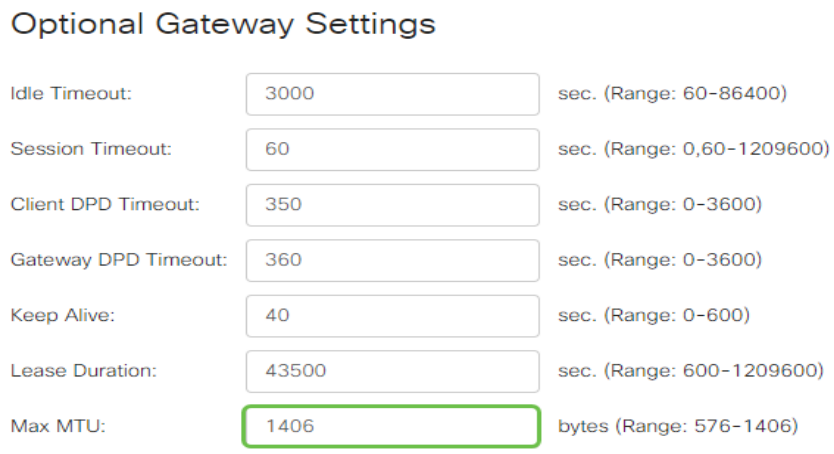
Nota: En este ejemplo, se utiliza 40.

Paso 6. Introduzca un valor en segundos para la duración del túnel que se va a conectar en el campo *Duración del arrendamiento*. El rango va de 600 a 1209600.



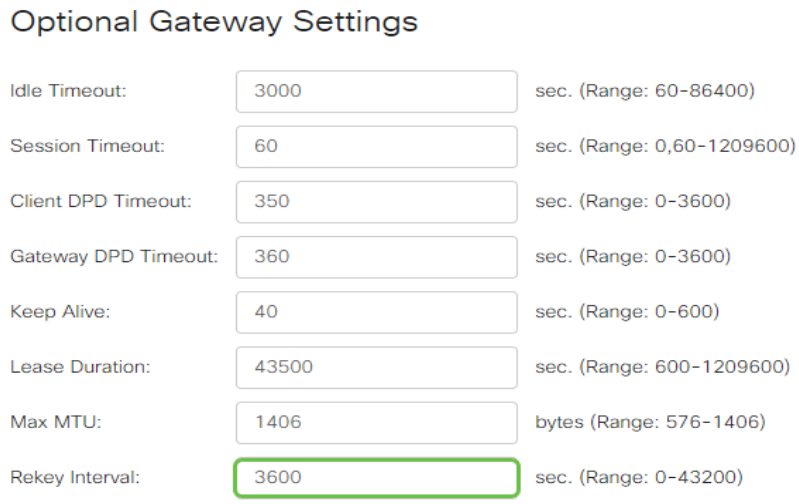
Nota: En este ejemplo, se utiliza 43500.

Paso 7. Introduzca el tamaño del paquete en bytes que se puede enviar a través de la red. El rango va de 576 a 1406.



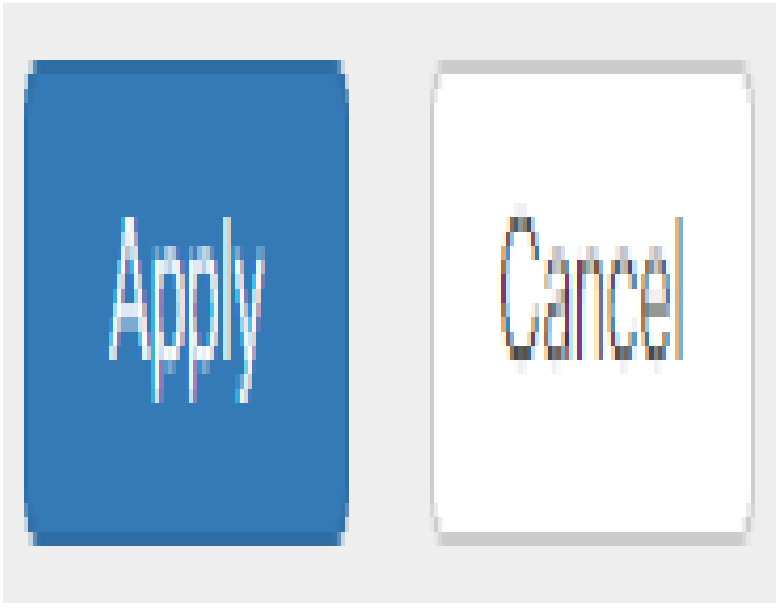
Nota: En este ejemplo, se utiliza 1406.

Paso 8. Introduzca el tiempo del intervalo de retransmisión en el campo *Rekey Interval*. La función Rekey permite que las claves SSL se renegocien después de que se haya establecido la sesión. El intervalo es de 0 a 43200.



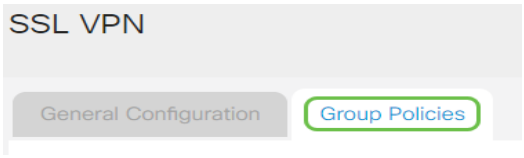
Nota: En este ejemplo, se utiliza 3600.

Paso 9. Haga clic en Apply (Aplicar).

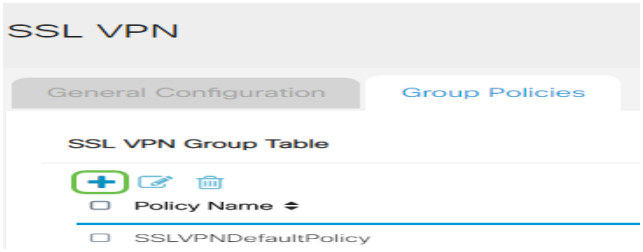


Configurar directivas de grupo

Paso 1. Haga clic en la ficha **Directivas de grupo**.



Paso 2. Haga clic en el botón **Add** debajo de la SSL VPN Group Table para agregar una política de grupo.

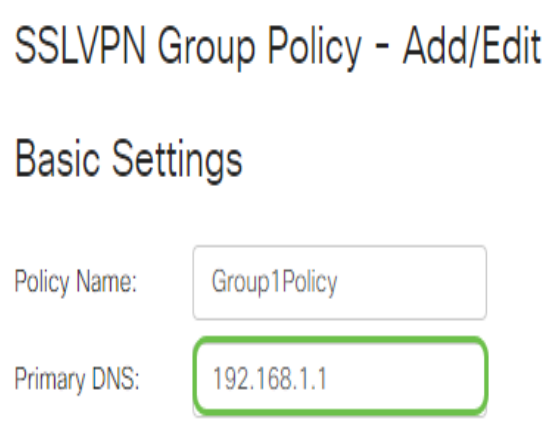


Nota: La tabla SSL VPN Group mostrará la lista de políticas de grupo en el dispositivo. También puede editar la primera directiva de grupo de la lista, que se denomina SSLVPNDefaultPolicy. Esta es la política predeterminada proporcionada por el dispositivo.

Paso 3. Introduzca el nombre de la política que prefiera en el campo *Nombre de Política*.

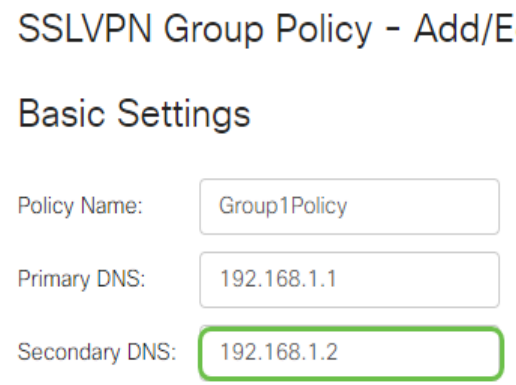
Nota: En este ejemplo, se utiliza la Directiva de grupo 1.

Paso 4. Introduzca la dirección IP del DNS principal en el campo proporcionado. De forma predeterminada, esta dirección IP ya se proporciona.



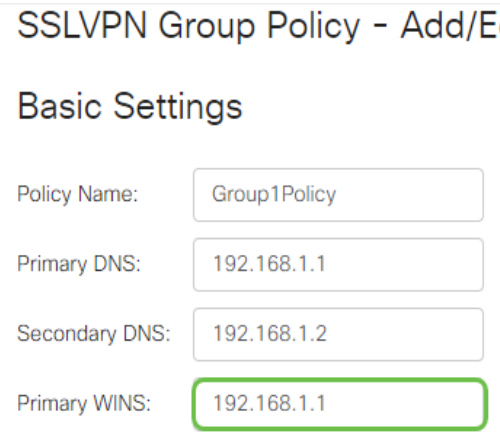
Nota: En este ejemplo, se utiliza 192.168.1.1.

Paso 5. (Opcional) Introduzca la dirección IP del DNS secundario en el campo proporcionado. Esto servirá como respaldo en caso de que el DNS primario falle.



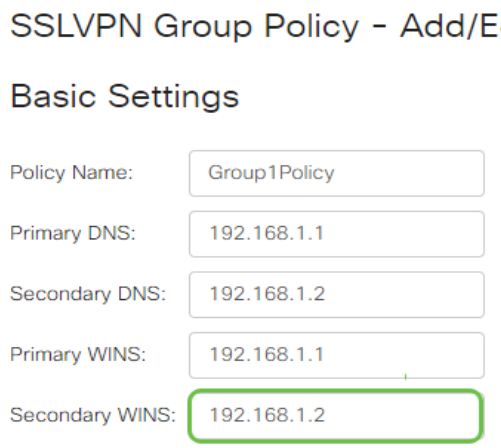
Nota: En este ejemplo, se utiliza 192.168.1.2.

Paso 6. (Opcional) Introduzca la dirección IP del WINS principal en el campo proporcionado.



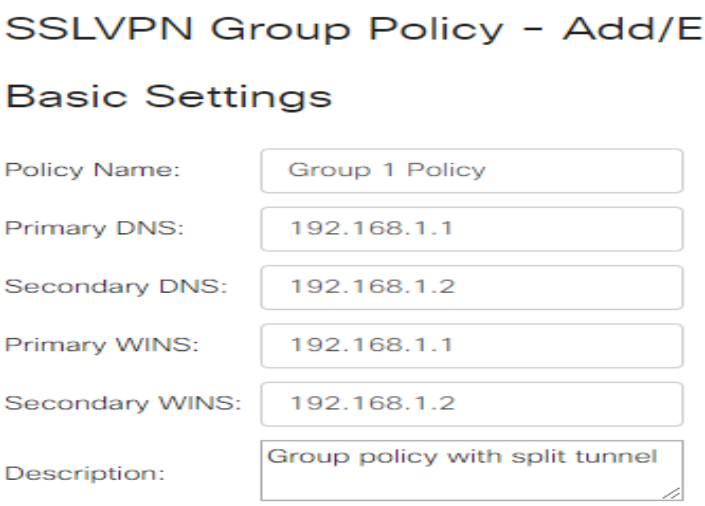
Nota: En este ejemplo, se utiliza 192.168.1.1.

Paso 7. (Opcional) Introduzca la dirección IP del WINS secundario en el campo proporcionado.



Nota: En este ejemplo, se utiliza 192.168.1.2.

Paso 8. (Opcional) Introduzca una descripción de la política en el campo *Descripción*.



Nota: En este ejemplo, se utiliza la política de grupo con túnel dividido.

Paso 9. (Opcional) Haga clic en un botón de opción para elegir la directiva de proxy de Internet Explorer (MSIE) para habilitar la configuración de proxy de Microsoft Internet Explorer (MSIE) para establecer el túnel VPN. Las opciones son:

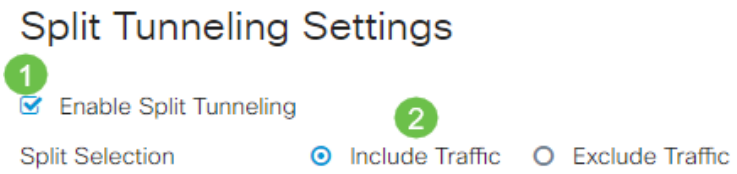
- None (Ninguno): permite al explorador no utilizar ninguna configuración de proxy.
- Automático: permite al explorador detectar automáticamente los parámetros de proxy.
- Bypass-local: permite al explorador omitir los parámetros de proxy configurados en el usuario remoto.
- Deshabilitado: deshabilita la configuración de proxy de MSIE.

Nota: En este ejemplo, se elige Disabled (Desactivado). Éste es el parámetro predeterminado.

Paso 10. (Opcional) En el área Configuración de tunelización dividida, marque la casilla de verificación **Habilitar tunelización dividida** para permitir que el tráfico con destino a Internet se envíe directamente a Internet sin cifrar. La tunelización completa envía todo el tráfico al dispositivo final, donde se enruta a los recursos de destino, eliminando la red corporativa de la

ruta para el acceso web.

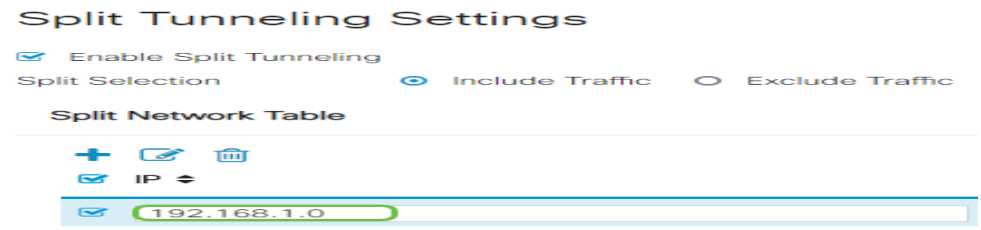
Paso 11. (Opcional) Haga clic en un botón de opción para elegir si desea incluir o excluir el tráfico al aplicar la tunelización dividida.



Nota: En este ejemplo, se elige Incluir tráfico.

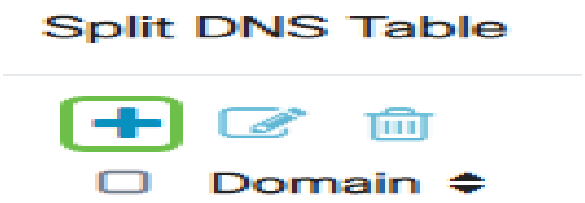
Paso 12. En la tabla de red dividida, haga clic en el botón **Add** para agregar la excepción de red dividida.

Paso 13. Introduzca la dirección IP de la red en el campo proporcionado.



Nota: En este ejemplo, se utiliza 192.168.1.0.

Paso 14. En la Tabla de DNS dividido, haga clic en el botón **Agregar** para agregar la excepción de DNS dividido.

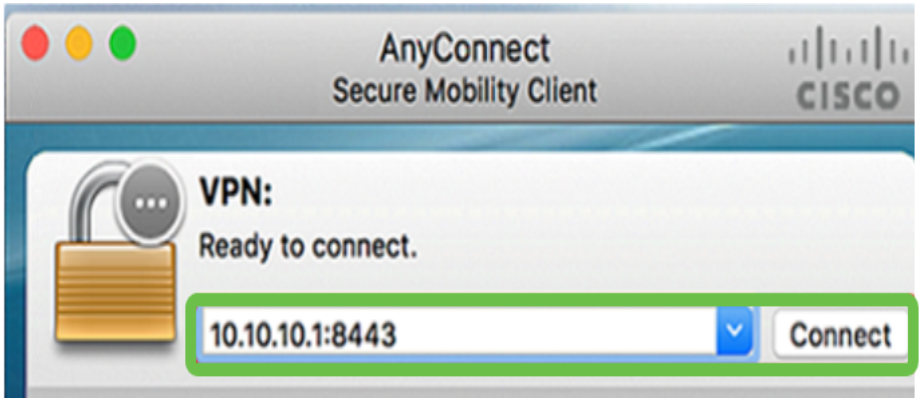


Paso 15. Introduzca el nombre de dominio en el campo proporcionado y, a continuación, haga clic en **Apply**.

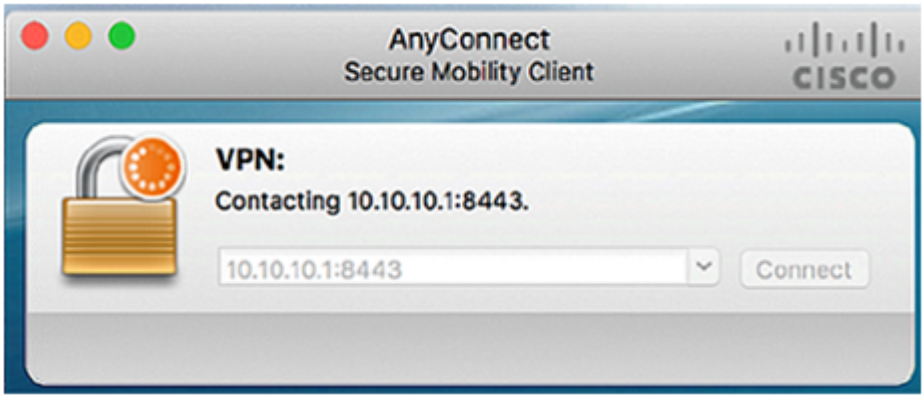
Verifique la conectividad VPN de AnyConnect

Paso 1. Haga clic en el icono **AnyConnect Secure Mobility Client**.

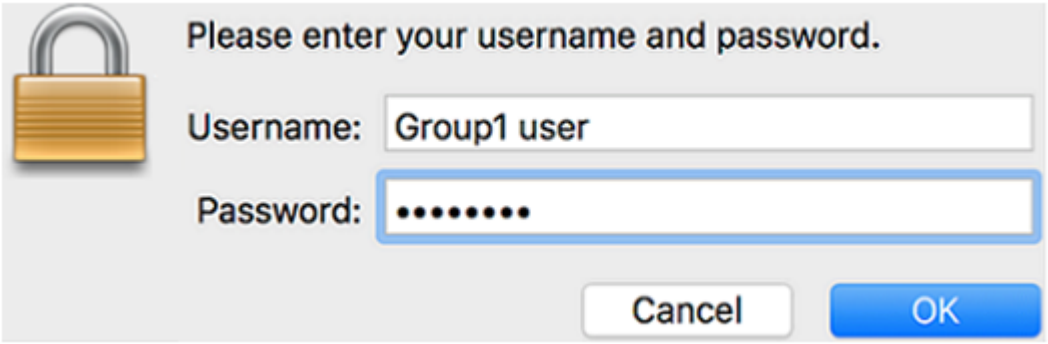
Paso 2. En la ventana AnyConnect Secure Mobility Client, introduzca la dirección IP y el número de puerto de la puerta de enlace separados por dos puntos (:) y, a continuación, haga clic en **Connect**.



Nota: En este ejemplo, se utiliza 10.10.10.1:8443. El software mostrará ahora que está en contacto con la red remota.

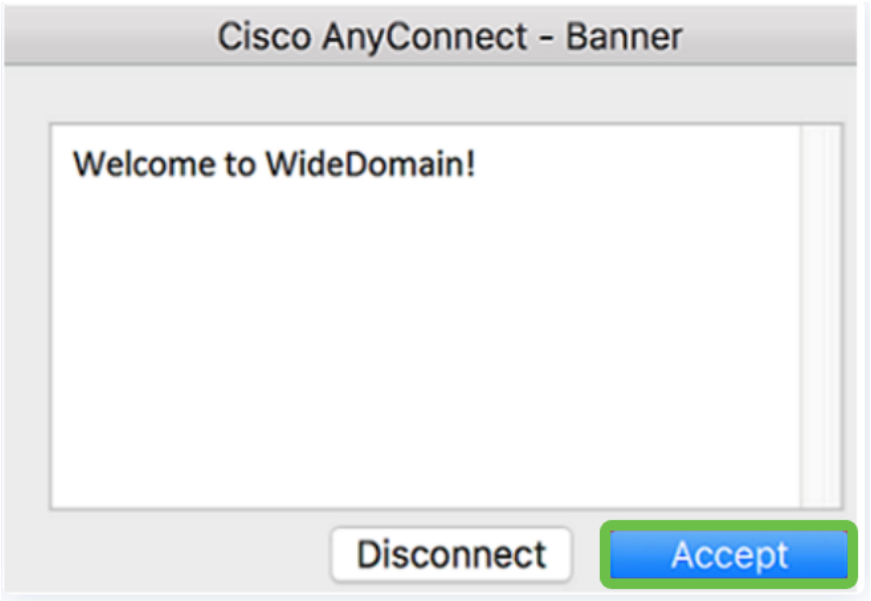


Paso 3. Introduzca el nombre de usuario y la contraseña del servidor en los campos correspondientes y, a continuación, haga clic en **Aceptar**.

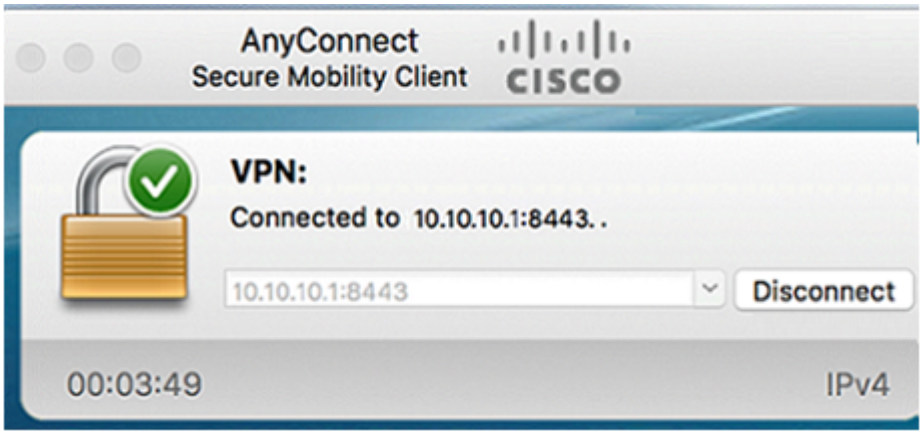


Nota: En este ejemplo, el usuario Group1 se utiliza como nombre de usuario.

Paso 4. Tan pronto como se establezca la conexión, aparecerá el banner de inicio de sesión. Haga clic en **Aceptar**.



La ventana de AnyConnect debe indicar la conexión VPN correcta a la red.



Paso 5. (Opcional) Para desconectarse de la red, haga clic en **Desconectar**.

Ahora debería haber configurado correctamente la conectividad VPN de AnyConnect mediante un router serie RV34x.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).