# Configuración de la conexión de red privada virtual (VPN) cliente a sitio en el router serie RV34x

## Objetivo

En una conexión de red privada virtual (VPN) cliente a sitio, los clientes de Internet pueden conectarse al servidor para acceder a la red corporativa o a la red de área local (LAN) detrás del servidor, pero aún así mantienen la seguridad de la red y sus recursos. Esta función es muy útil, ya que crea un nuevo túnel VPN que permitiría a los teletrabajadores y a los viajeros de negocios acceder a su red mediante el uso de un software cliente VPN sin poner en peligro la privacidad y la seguridad.

El objetivo de este documento es mostrarle cómo configurar la conexión VPN de cliente a sitio en el RV34x Series Router.

## Dispositivos aplicables

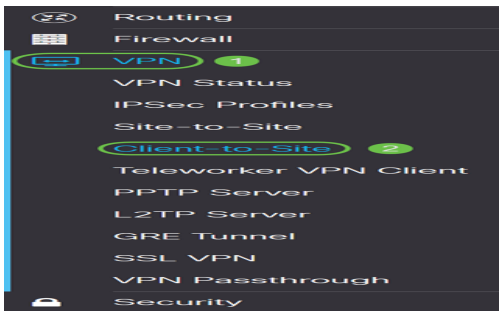
- Serie RV34x

## Versión del software

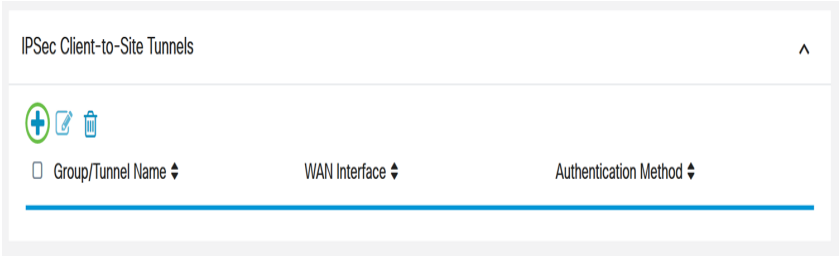
- 1.0.01.16

## Configuración de VPN de cliente a sitio

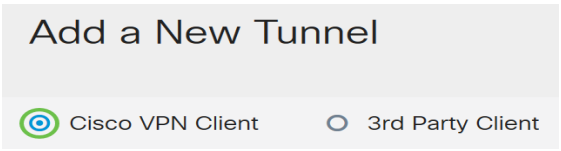
Paso 1. Inicie sesión en la utilidad basada en web del router y elija **VPN > Cliente a Sitio**.



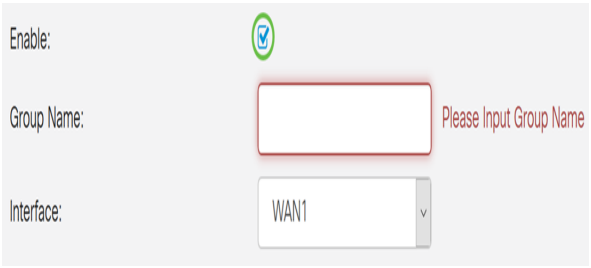

Paso 2. Haga clic en el botón **Add** en la sección IPSec Client-to-Site Tunnels.



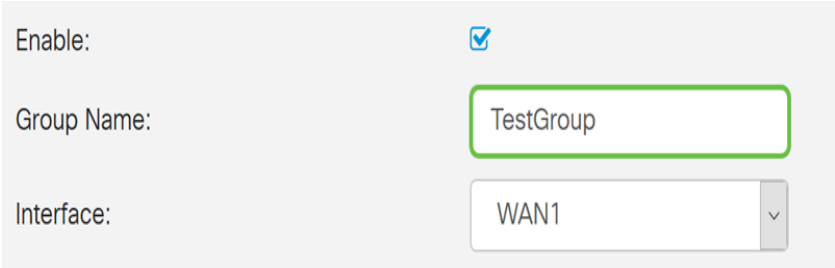

Paso 3. En el área *Add a New Tunnel* , haga clic en el botón de radio **Cisco VPN Client**.




Paso 4. Marque la casilla de verificación **Enable** para habilitar la configuración.



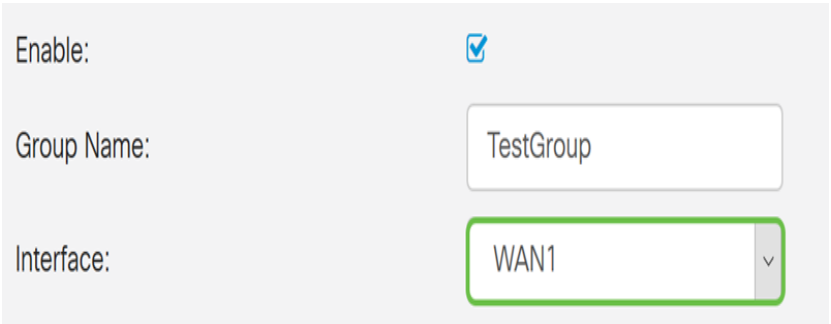

Paso 5. Introduzca un nombre de grupo en el campo proporcionado. Esto servirá como identificador para todos los miembros de este grupo durante las negociaciones de Intercambio de claves de Internet (IKE).




**Nota:** Introduzca caracteres entre A y Z o entre 0 y 9. No se permiten espacios ni caracteres especiales para el nombre del grupo. En este ejemplo, se utiliza TestGroup.

Paso 6. Haga clic en la lista desplegable para elegir la interfaz. Las opciones son:

- WAN1
- WAN2
- USB1
- USB2

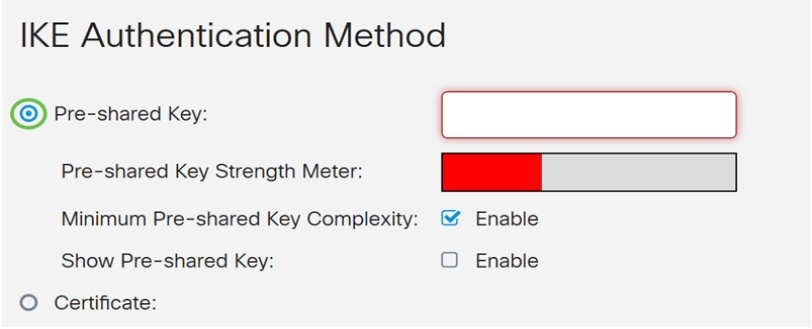



**Nota:** En este ejemplo, se elige WAN1. Esta es la configuración predeterminada.

Paso 7. En el área Método de autenticación IKE, elija un método de autenticación que se utilizará en las negociaciones IKE en el túnel basado en IKE. Las opciones son:

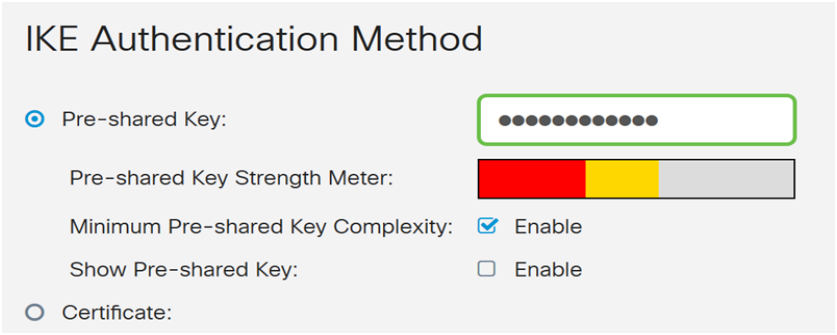
- Clave precompartida: los pares IKE se autentican mutuamente mediante la informática y el envío de un hash de datos con clave que incluye la clave precompartida. Si el par receptor puede crear el mismo hash independientemente usando su clave previamente

compartida, sabe que ambos pares deben compartir el mismo secreto, autenticando así al otro par. Las claves previamente compartidas no se amplían bien porque cada par IPSec se debe configurar con la clave previamente compartida de cada otro par con el que establece una sesión.
- Certificado — El certificado digital es un paquete que contiene información como una identidad de certificado del portador: nombre o dirección IP, la fecha de vencimiento del número de serie del certificado y una copia de la clave pública del portador del certificado. El formato de certificado digital estándar se define en la especificación X.509. X.509 versión 3 define la estructura de datos para los certificados.



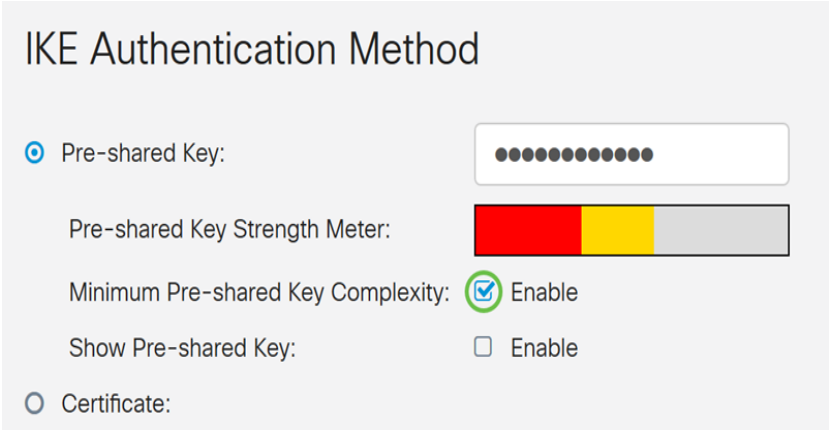

**Nota:** En este ejemplo, se elige la clave precompartida. Esta es la configuración predeterminada.

Paso 8. Introduzca una clave previamente compartida en el campo proporcionado. Esta será la clave de autenticación entre su grupo de peers IKE.

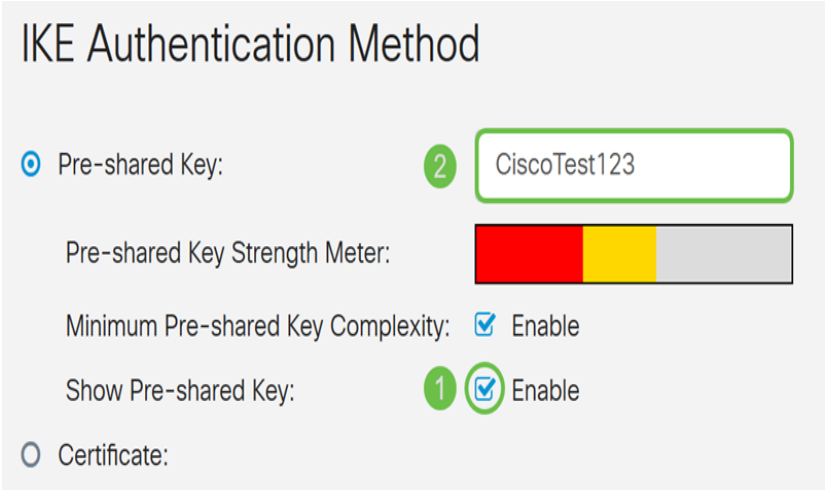



Paso 9. (Opcional) Marque la casilla de verificación **Enable** para la Complejidad de Clave Previamente Compartida Mínima para ver el Medidor de Potencia de Clave Previamente Compartida y determinar la fuerza de su clave. La solidez de la clave se define de la siguiente manera:

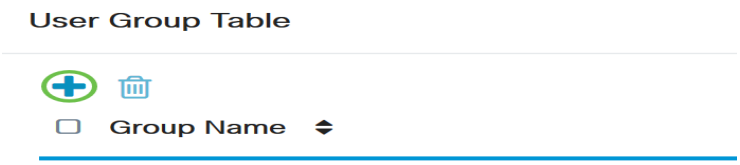
- Rojo: la contraseña es débil.
- Naranja: la contraseña es bastante fuerte.
- Verde: la contraseña es fuerte.




**Nota:** Puede marcar la casilla de verificación **Enable** en el campo *Show Pre-shared Key* para verificar su contraseña en texto sin formato.

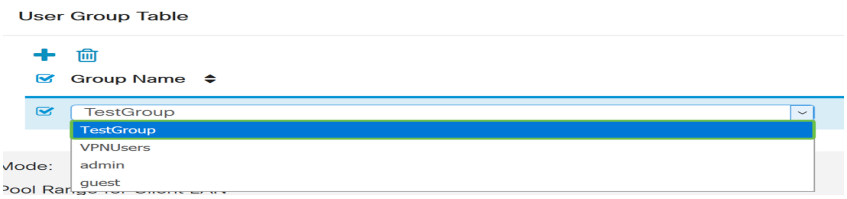



Paso 10. (Opcional) Haga clic en el icono **más** de la tabla Grupo de usuarios para agregar un grupo.




Paso 11. (Opcional) Elija de la lista desplegable si el grupo de usuarios es para admin o para invitados. Si ha creado su propio grupo de usuarios con cuentas de usuario, puede seleccionarlo. En este ejemplo, seleccionaremos TestGroup.

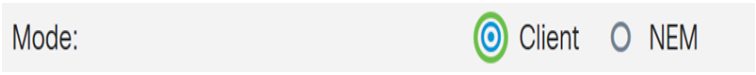
**Nota:** TestGroup es un grupo de usuarios que hemos creado en **Configuración del sistema > Grupos de usuarios**.




**Nota:** En este ejemplo, se elige TestGroup. También puede activar la casilla junto al grupo de usuarios y, a continuación, hacer clic en el botón **Eliminar** si desea eliminar un grupo de usuarios.

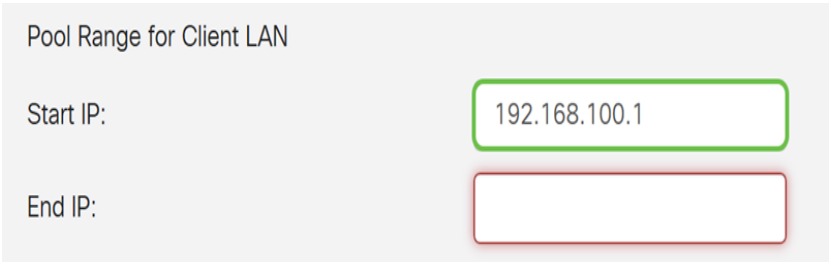
Paso 12. Haga clic en un botón de opción para elegir un modo. Las opciones son:

- Cliente: esta opción permite al cliente solicitar una dirección IP y el servidor suministra las direcciones IP del rango de direcciones configurado.
- Network Extension Mode (NEM): esta opción permite a los clientes proponer su subred para la que se deben aplicar servicios VPN en el tráfico entre la LAN detrás del servidor y la subred propuesta por el cliente.



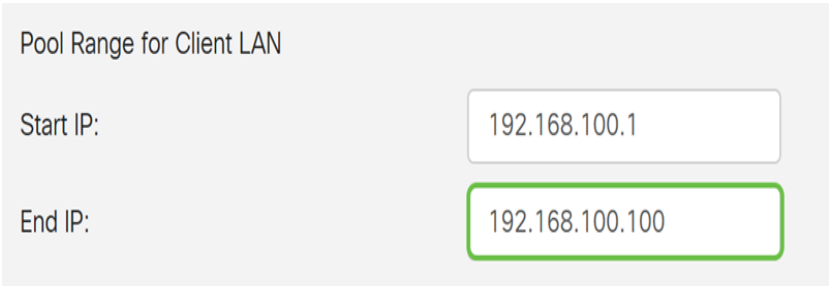

**Nota:** En este ejemplo, se elige Cliente.

Paso 13. Ingrese la dirección IP inicial en el campo *Start IP*. Esta será la primera dirección IP del conjunto que se puede asignar a un cliente.



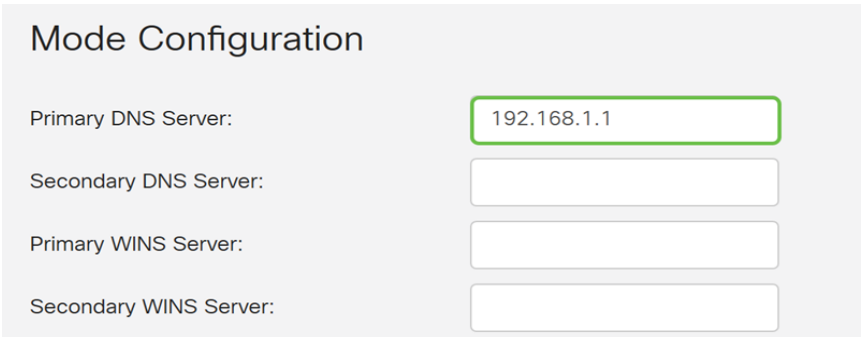

**Nota:** En este ejemplo, se utiliza 192.168.100.1.

Paso 14. Ingrese la dirección IP final en el campo *End IP*. Esta será la última dirección IP del conjunto que se puede asignar a un cliente.




**Nota:** En este ejemplo, se utiliza 192.168.100.100.

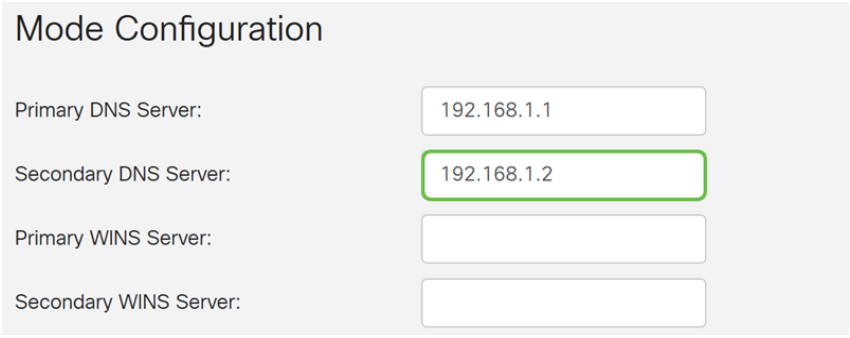
Paso 15. (Opcional) En el área *Mode Configuration*, ingrese la dirección IP del servidor DNS primario en el campo proporcionado.




**Nota:** En este ejemplo, se utiliza 192.168.1.1.

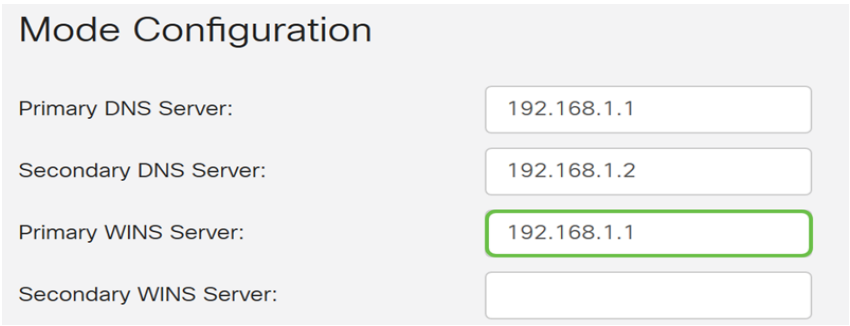
Paso 16. (Opcional) Introduzca la dirección IP del servidor DNS secundario en el campo

proporcionado.



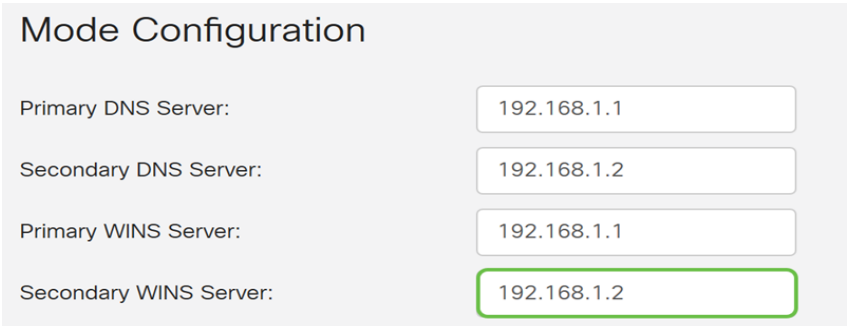

**Nota:** En este ejemplo, se utiliza 192.168.1.2.

Paso 17. (Opcional) Introduzca la dirección IP del servidor WINS principal en el campo proporcionado.




**Nota:** En este ejemplo, se utiliza 192.168.1.1.

Paso 18. (Opcional) Introduzca la dirección IP del servidor WINS secundario en el campo proporcionado.




**Nota:** En este ejemplo, se utiliza 192.168.1.2.

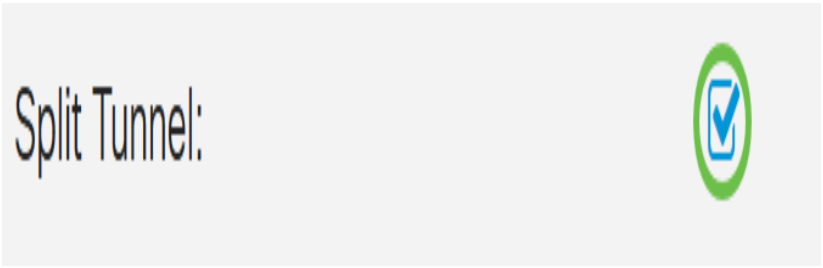
Paso 19. (Opcional) Introduzca el dominio predeterminado que se utilizará en la red remota en el campo proporcionado.

**Nota:** En este ejemplo, se utiliza sample.com.

Paso 20. (Opcional) En el campo *Backup Server 1*, ingrese la dirección IP o el nombre de dominio del servidor de respaldo. Aquí será donde el dispositivo puede iniciar la conexión VPN en caso de que falle el servidor VPN IPSec primario. Puede introducir hasta tres servidores de copia de seguridad en los campos proporcionados. El Servidor de respaldo 1 tiene la prioridad más alta entre los tres servidores y el Servidor de respaldo 3 tiene la menor prioridad.

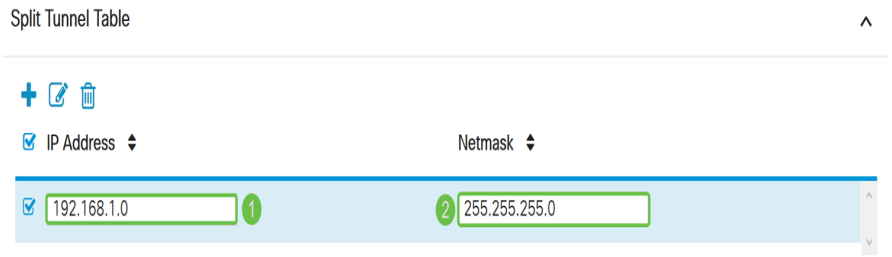

**Nota:** En este ejemplo, Example.com se utiliza para el Servidor de respaldo 1.

Paso 21. (Opcional) Marque la casilla de verificación **Dividir túnel** para habilitar el túnel dividido. La tunelización dividida le permite acceder a los recursos de una red privada e Internet al mismo tiempo.



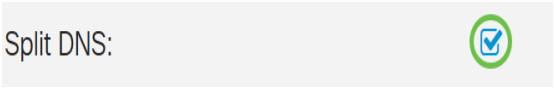

Paso 22. (Opcional) En la *Tabla de Túnel Dividido*, haga clic en el **icono más** para agregar una dirección IP para túnel dividido.


Paso 23. (Opcional) Introduzca la dirección IP y la máscara de red del túnel dividido en los campos proporcionados.

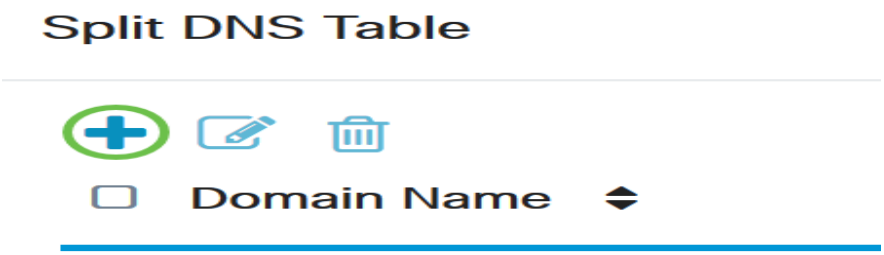



**Nota:** En este ejemplo, se utilizan 192.168.1.0 y 255.255.255.0. También puede marcar la casilla y hacer clic en los botones **Add**, **Edit** y **Delete** para agregar, editar o eliminar un túnel dividido, respectivamente.

Paso 24. (Opcional) Marque la casilla de verificación **Dividir DNS** para habilitar el DNS dividido. La división de DNS permite crear servidores DNS independientes para redes internas y externas a fin de mantener la seguridad y la privacidad de los recursos de red.



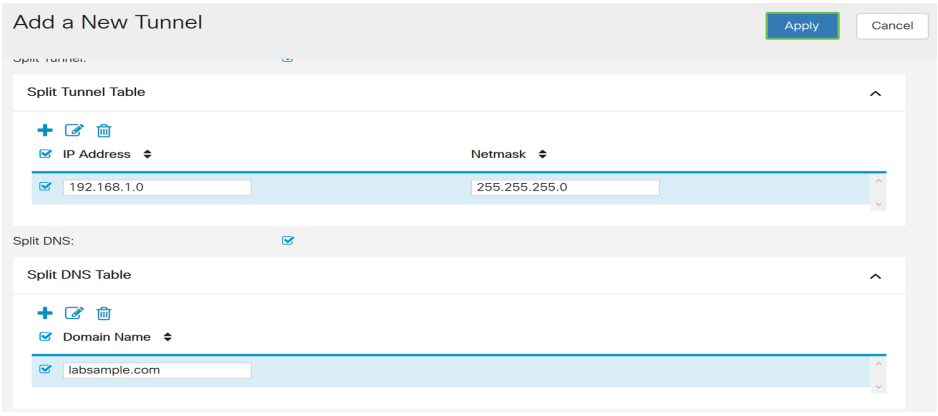

Paso 25. (Opcional) Haga clic en el icono **más** bajo la *Tabla DNS Dividida* para agregar un nombre de dominio para DNS dividido.




Paso 26. (Opcional) Introduzca el nombre de dominio del DNS dividido en el campo proporcionado.


**Nota:** En este ejemplo, se utiliza labsample.com. También puede marcar la casilla y hacer clic en los botones **Add**, **Edit** y **Delete** para agregar, editar o eliminar un DNS dividido, respectivamente.

Paso 27. Haga clic en Apply (Aplicar).




# Conclusión

Ahora debería haber configurado correctamente la conexión cliente a sitio en el router serie RV34x.

Haga clic en los siguientes artículos para obtener más información sobre los siguientes

temas:

- Configuración de un cliente VPN de teletrabajador en el router serie RV34x
- Utilice el cliente VPNGreenBow para conectarse con el router serie RV34x
- Cree una cuenta de usuario para VPN Client Setup en el router RV34x
- Creación de un grupo de usuarios para la configuración de VPN en el router RV34x

## Ver un vídeo relacionado con este artículo...

Haga clic aquí para ver otras charlas técnicas de Cisco