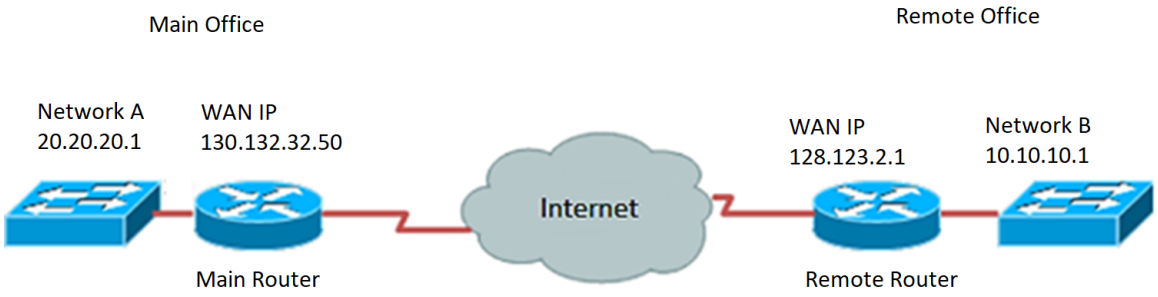
Configuración de la conexión de red privada virtual (VPN) mediante el asistente de configuración del router serie RV34x

Objetivo

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 garantiza la seguridad de las conexiones a una infraestructura de red subyacente para proteger la red privada y sus recursos.

Un túnel VPN establece una red privada que puede enviar datos de forma segura mediante cifrado y autenticación. Las oficinas corporativas utilizan principalmente la conexión VPN, ya que es útil y necesario permitir que sus empleados tengan acceso a su red privada aunque se encuentren fuera de la oficina.

La VPN permite que un host remoto actúe como si se encontrara en la misma red local. El router admite 50 túneles. El asistente de configuración de VPN permite configurar una conexión segura para el túnel IPSec de sitio a sitio. Esta función simplifica la configuración y evita la configuración compleja y los parámetros opcionales. De esta manera, cualquiera puede configurar el túnel IPSec de manera rápida y eficiente.



Ventajas del uso de una conexión VPN:

1. El uso de una conexión VPN ayuda a proteger los datos y recursos de la red confidenciales.
2. Proporciona comodidad y accesibilidad a los trabajadores remotos o a los empleados corporativos, ya que podrán acceder fácilmente a la oficina principal sin tener que estar físicamente presentes y, sin embargo, mantener la seguridad de la red privada y sus recursos.
3. La comunicación mediante una conexión VPN proporciona un mayor nivel de seguridad en comparación con otros métodos de comunicación remota. El nivel avanzado de tecnología actual lo hace posible, por lo que protege la red privada del acceso no autorizado.
4. Las ubicaciones geográficas reales de los usuarios están protegidas y no están expuestas a redes públicas o compartidas como Internet.
5. Agregar nuevos usuarios o grupos de usuarios a la red es fácil, ya que las VPN son muy ajustables. Es posible hacer que la red crezca sin la necesidad de componentes

nuevos adicionales o configuraciones complicadas.

Riesgos del uso de la conexión VPN:

1. Riesgo de seguridad debido a una configuración incorrecta. Dado que el diseño y la implementación de una VPN pueden ser complicados, es necesario confiar la tarea de configurar la conexión a un profesional con gran conocimiento y experiencia para asegurarse de que la seguridad de la red privada no se vea comprometida.
2. Confiabilidad. Puesto que una conexión VPN requiere conexión a Internet, es importante elegir un proveedor que esté probado y probado para proporcionar un excelente servicio de Internet y garantizar un tiempo de inactividad mínimo o nulo.
3. Escalabilidad. Si se trata de una situación en la que hay necesidad de agregar nueva infraestructura o establecer nuevas configuraciones, es posible que surjan problemas técnicos debido a la incompatibilidad, especialmente si se trata de productos o proveedores diferentes a los que ya está utilizando.
4. Problemas de seguridad para dispositivos móviles. A veces, cuando se utilizan dispositivos móviles al iniciar la conexión VPN, pueden surgir problemas de seguridad, especialmente cuando se utiliza la conexión inalámbrica. Algunos proveedores no verificados se presentan como "proveedores de VPN libres" e incluso pueden instalar malware en su equipo. Debido a esto, es posible añadir más medidas de seguridad para evitar estos problemas cuando se utilizan dispositivos móviles.
5. Velocidades de conexión lentas. Si utiliza un cliente VPN que proporciona un servicio VPN gratuito, es posible que la velocidad de conexión se ralentice, ya que estos proveedores no dan prioridad a las velocidades de conexión.

El objetivo de este documento es mostrarle cómo configurar la conexión VPN en el router de la serie RV34x mediante el asistente de configuración.

Dispositivos aplicables

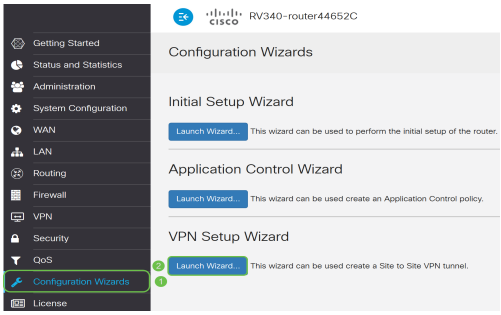
- Serie RV34x

Versión del software

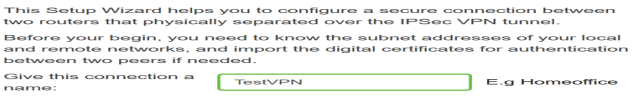
- 1.0.01.16

Configuración de la conexión VPN mediante el asistente de configuración

Paso 1. Inicie sesión en la utilidad basada en Web del router y elija **Asistente para configuración**. A continuación, haga clic en **Iniciar el asistente** en la sección *Asistente de configuración de VPN*.



Paso 2. En el campo proporcionado, introduzca un nombre para identificar esta conexión.



Nota: En este ejemplo, se utiliza TestVPN.

Paso 3. En el área Interface (Interfaz), haga clic en el menú desplegable y elija la interfaz que desea activar esta conexión. Las opciones son:

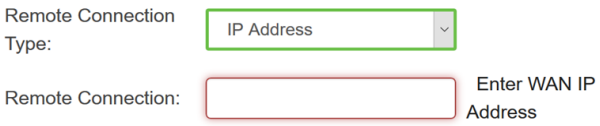
- WAN1
- WAN2
- USB1
- USB2

Nota: En este ejemplo, se utiliza WAN1.

Paso 4. Haga clic en Next (Siguiente).

Paso 5. Elija el tipo de conexión remota haciendo clic en la flecha desplegable. Las opciones son:

- Dirección IP: elija esta opción si desea utilizar la dirección IP del router remoto en el otro extremo del túnel VPN.
- FQDN: (Nombre de dominio completamente calificado) Elija esta opción si desea utilizar el nombre de dominio del router remoto en el otro extremo del túnel VPN.



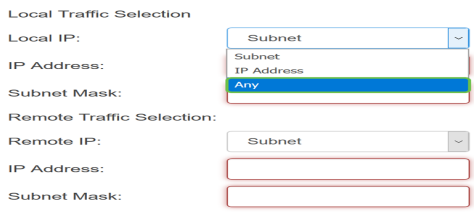
Nota: En este ejemplo, se elige la dirección IP.

Paso 6. Introduzca la dirección IP de WAN de la conexión remota en el campo proporcionado y, a continuación, haga clic en **Siguiente**.

Nota: En este ejemplo, se utiliza 128.123.2.1.

Paso 7. En el área Selección de tráfico local, haga clic en la lista desplegable para elegir la IP local. Las opciones son:

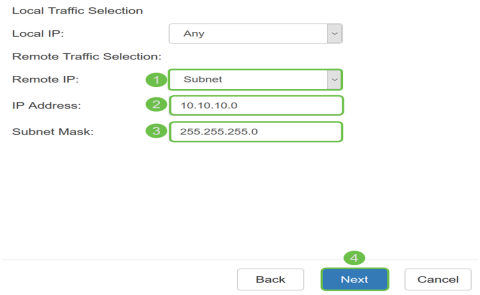
- Subred: elija esta opción si desea introducir la dirección IP y la máscara de subred de la red local.
- Dirección IP: seleccione esta opción si desea introducir sólo la dirección IP de la red local.
- Any — Elija esto si desea cualquiera de los dos.



Nota: En este ejemplo, se elige Any (Cualquiera).

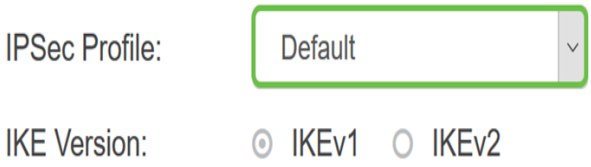
Paso 8. En el área Selección de tráfico remoto, haga clic en la flecha desplegable para elegir la IP remota. Ingrese la dirección IP remota y la máscara de subred en el campo proporcionado y luego haga clic en **Siguiente**. Las opciones son:

- Subred: seleccione esta opción si desea introducir la dirección IP y la máscara de subred de la red remota.
- Dirección IP: seleccione esta opción si desea introducir sólo la dirección IP de la red remota.



Nota: En este ejemplo, se elige Subred. Se ingresó 10.10.10.0 como dirección IP y 255.255.255.0 como máscara de subred.

Paso 9. Haga clic en la flecha desplegable del área Perfil IPSec para elegir el perfil que desea utilizar.



Nota: En este ejemplo, se elige Default.

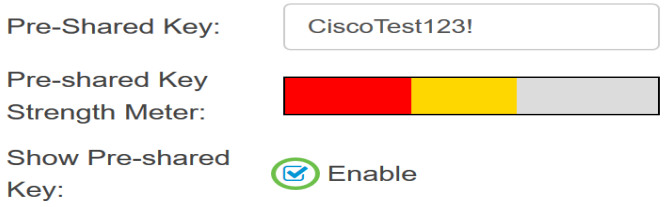
Paso 10. En el área Opciones de la fase 1, introduzca la clave previamente compartida para esta conexión en el campo proporcionado. Se trata de la clave previamente compartida que se utilizará para autenticar el par de intercambio remoto de claves de Internet (IKE). Ambos extremos del túnel VPN deben utilizar la misma clave previamente compartida. Se permite utilizar hasta 30 caracteres o valores hexadecimales para esta clave.

Nota: Se recomienda encarecidamente cambiar la clave previamente compartida con regularidad para mantener la seguridad de la conexión VPN.

Nota: El medidor de potencia de clave precompartida indica la fuerza de la clave que ha introducido en función de lo siguiente:

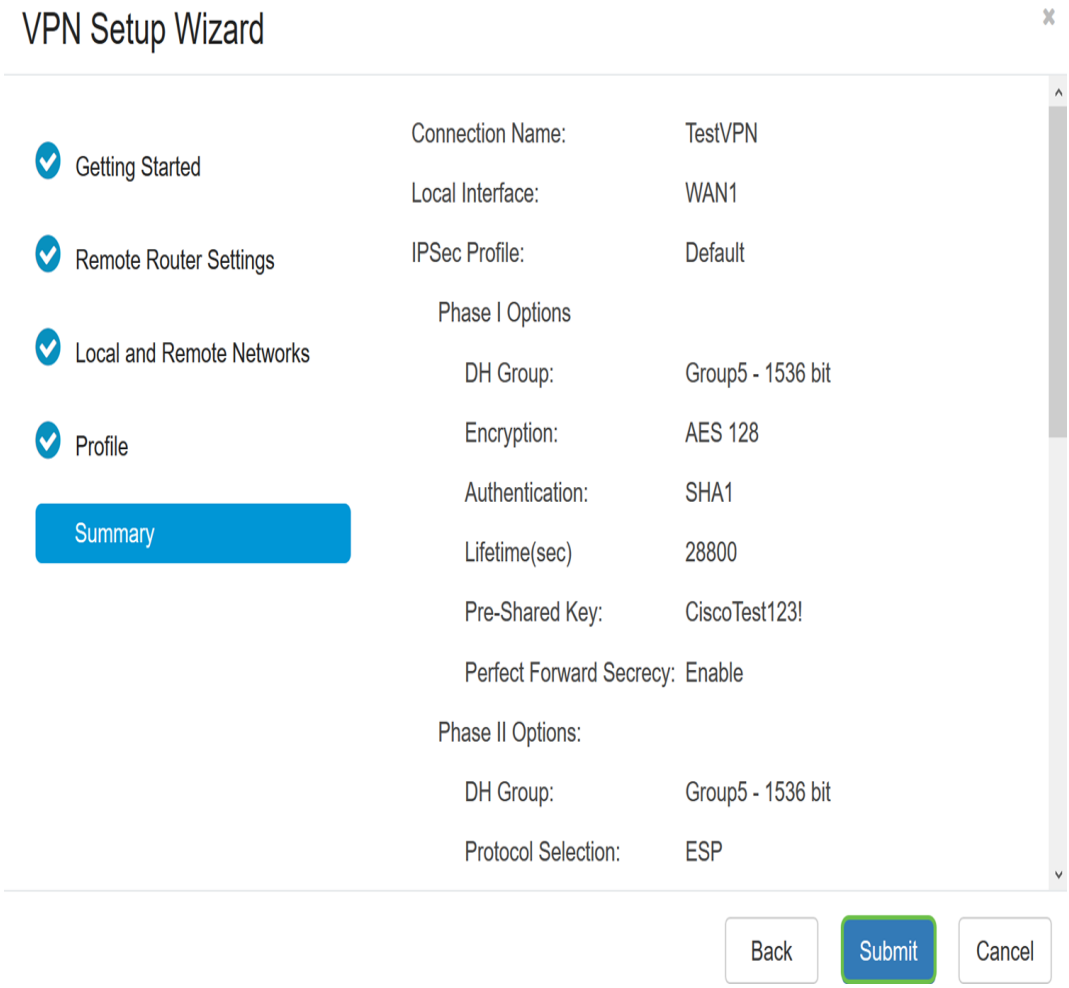
- Rojo: la contraseña es débil.
- Ámbar: la contraseña es bastante fuerte.
- Verde: la contraseña es fuerte.

Paso 11. (Opcional) También puede marcar la casilla de verificación **Enable** en Mostrar texto sin formato cuando lo edite para ver la contraseña en texto sin formato.



Paso 12. Haga clic en **Next**.  .

Paso 13. A continuación, la página mostrará todos los detalles de configuración de la conexión VPN. Haga clic en Submit (Enviar).



Ahora debería haber configurado correctamente la conexión VPN en el router de la serie RV34x mediante el asistente de configuración. Para conectar correctamente una VPN de sitio a sitio, deberá configurar el asistente de configuración en el router remoto.