Configuración de la red privada virtual (VPN) IPsec de sitio a sitio en un router RV132W o RV134W

Objetivo

Las redes privadas virtuales (VPN) de sitio a sitio se implementan en función de las políticas IPsec asignadas a las topologías VPN. Una política IPsec es un conjunto de parámetros que definen las características de la VPN de sitio a sitio, como los protocolos de seguridad y algoritmos que se utilizarán para proteger el tráfico en un túnel IPsec.

Los routers RV132W y RV134W admiten VPN IPsec de sitio a sitio para un único túnel VPN de gateway a gateway. Después de configurar los parámetros básicos de VPN, puede conectarse de forma segura a otro router habilitado para VPN. Por ejemplo, puede configurar el dispositivo en una sucursal para que se conecte a un router que conecte túneles VPN de sitio a sitio en el sitio corporativo, de modo que el sitio de la sucursal tenga acceso seguro a la red corporativa.

En este artículo se explica cómo configurar los parámetros básicos de VPN para una conexión IPsec de sitio a sitio en el router RV132W o RV134W.
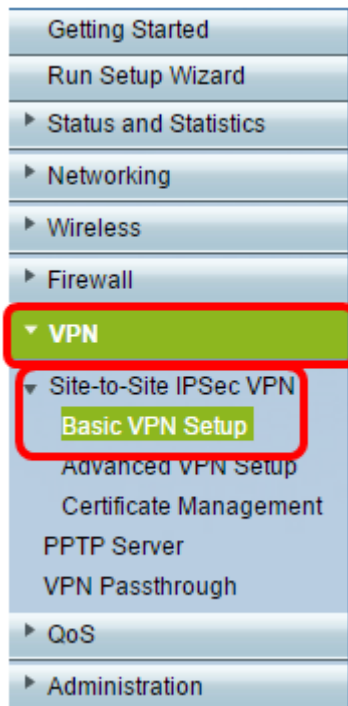
Dispositivos aplicables

- RV132W
- RV134W

Versión del software

- 1.0.0.17: RV132W
- 1.0.0.21 — RV134W

Configuración de VPN IPSec de sitio a sitio en un router

Paso 1. Inicie sesión en la utilidad basada en Web y elija **VPN > IPSec VPN de sitio a sitio > Configuración básica de VPN**.

Paso 2. En el campo *New Connection Name*, ingrese un nombre para el túnel VPN. El nombre sólo puede contener letras, números y guiones.

Nota: En este ejemplo, el nombre es Branch1.

Paso 3. En el campo *Pre-Shared Key*, ingrese la clave o contraseña previamente compartida, que se intercambiará entre los dos routers. La contraseña debe tener entre 8 y 49 caracteres.

Nota: En este ejemplo, la clave previamente compartida es Cisco1234$.

Paso 4. En la lista desplegable Protocol , elija el nombre del protocolo. Las opciones son:

- ESP: el protocolo Encapsulating Security Payload (ESP) proporciona autenticidad de origen, integridad y protección de confidencialidad de los paquetes.
- AH: el protocolo de encabezado de autenticación (AH) autentica el origen de los datagramas y garantiza la integridad de los datos.

Nota: En este ejemplo, se elige ESP.

Paso 5. Elija el punto final remoto en el menú desplegable. Las opciones son:

- Dirección IP: esta opción identificará el router al que se conectará el dispositivo con su dirección IP.
- FQDN: nombre de dominio completamente calificado (FQDN) identificará el router al que se conectará el dispositivo con su nombre de dominio.

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

Basic VPN Setup

About Basic VPN Setup

The basic VPN setup sets most parameters to defaults as proposed by the VPN Consortium (VPNC), and assumes a Pre-shared Key, which greatly simplifies setup. After creating the policies through the Basic VPN Setup, you can always update the parameters through the Policies menu

[View Default Settings]

Connection Name and Remote IP Type

New Connection Name:	Branch1
Pre-Shared Key:	Cisco1234$
Protocol:	ESP ▾

Endpoint Information

Remote Endpoint:	IP Address ▾	
	IP Address	
Remote WAN (Internet) IP Address:	FQDN	(Hint: 1.2.3.4 or abc.com)
Local WAN (Internet) IP Address:	192.168.100.121	

Secure Connection Remote Accessibility

Remote LAN (Local Network) IP Address:	10.10.100.162	(Hint: 1.2.3.4)
Remote LAN (Local Network) Subnet Mask:	255.0.0.0	(Hint: 255.255.255.0)
Local LAN (Local Network) IP Address:	192.168.100.128	(Hint: 1.2.3.4)
Local LAN (Local Network) Subnet Mask:	255.255.255.0	(Hint: 255.255.255.0)

[Save]   [Cancel]   [Back]

Paso 6. Introduzca la dirección IP (Internet) de WAN remota o FQDN en el campo *Remote WAN (Internet) IP Address (Dirección IP de WAN remota)*.

Nota: En este ejemplo, la dirección IP (Internet) de WAN remota es 10.11.12.13.

Paso 7. Verifique que la dirección IP de origen en el campo *Local WAN (Internet) IP Address (Dirección IP de WAN local)* sea correcta. Esto se genera automáticamente.

Nota: En este ejemplo, la dirección IP (Internet) de WAN local es 192.168.100.121.

Basic VPN Setup

About Basic VPN Setup

The basic VPN setup sets most parameters to defaults as proposed by the VPN Consortium (VPNC), and assumes a Pre-shared Key, which greatly simplifies setup. After creating the policies through the Basic VPN Setup, you can always update the parameters through the Policies menu

View Default Settings

Connection Name and Remote IP Type

New Connection Name:	Branch1
Pre-Shared Key:	Cisco1234$
Protocol:	ESP ▼

Endpoint Information

Remote Endpoint:	IP Address ▼	
Remote WAN (Internet) IP Address:	10.11.12.13	(Hint: 1.2.3.4 or abc.com)
Local WAN (Internet) IP Address:	192.168.100.121	

Secure Connection Remote Accessibility

Remote LAN (Local Network) IP Address:	10.10.100.162	(Hint: 1.2.3.4)
Remote LAN (Local Network) Subnet Mask:	255.0.0.0	(Hint: 255.255.255.0)
Local LAN (Local Network) IP Address:	192.168.100.128	(Hint: 1.2.3.4)
Local LAN (Local Network) Subnet Mask:	255.255.255.0	(Hint: 255.255.255.0)

Save   Cancel   Back

Paso 8. Introduzca la dirección IP de la red privada (LAN) del terminal remoto en el campo *Remote LAN (Local Network) IP Address*. Esta es la dirección IP de la red interna en el sitio remoto.

Nota: En este ejemplo, la dirección IP de LAN remota (red local) es 10.10.100.162.

Basic VPN Setup

About Basic VPN Setup

The basic VPN setup sets most parameters to defaults as proposed by the VPN Consortium (VPNC),
and assumes a Pre-shared Key, which greatly simplifies setup. After creating the policies through the Basic VPN Setup,
you can always update the parameters through the Policies menu

View Default Settings

Connection Name and Remote IP Type

New Connection Name:	Branch1
Pre-Shared Key:	Cisco1234$
Protocol:	ESP ▼

Endpoint Information

Remote Endpoint:	IP Address ▼	
Remote WAN (Internet) IP Address:	10.11.12.13	(Hint: 1.2.3.4 or abc.com)
Local WAN (Internet) IP Address:	192.168.100.121	

Secure Connection Remote Accessibility

Remote LAN (Local Network) IP Address:	10.10.100.162	(Hint: 1.2.3.4)
Remote LAN (Local Network) Subnet Mask:	255.0.0.0	(Hint: 255.255.255.0)
Local LAN (Local Network) IP Address:	192.168.100.128	(Hint: 1.2.3.4)
Local LAN (Local Network) Subnet Mask:	255.255.255.0	(Hint: 255.255.255.0)

Save   Cancel   Back

Paso 9. Verifique la máscara de subred de la red privada (LAN) del extremo remoto en el campo *Máscara de subred LAN remota (Internet).* Esto se genera automáticamente.

Nota: En este ejemplo, la máscara de subred LAN remota (red local) es 255.0.0.0.

Basic VPN Setup

About Basic VPN Setup

The basic VPN setup sets most parameters to defaults as proposed by the VPN Consortium (VPNC), and assumes a Pre-shared Key, which greatly simplifies setup. After creating the policies through the Basic VPN Setup, you can always update the parameters through the Policies menu

View Default Settings

Connection Name and Remote IP Type

New Connection Name: Branch1

Pre-Shared Key: Cisco1234$

Protocol: ESP ▼

Endpoint Information

Remote Endpoint: IP Address ▼

Remote WAN (Internet) IP Address: 10.11.12.13   (Hint: 1.2.3.4 or abc.com)

Local WAN (Internet) IP Address: 192.168.100.121

Secure Connection Remote Accessibility

Remote LAN (Local Network) IP Address: 10.10.100.162   (Hint: 1.2.3.4)

Remote LAN (Local Network) Subnet Mask: 255.0.0.0   (Hint: 255.255.255.0)

Local LAN (Local Network) IP Address: 192.168.100.128   (Hint: 1.2.3.4)

Local LAN (Local Network) Subnet Mask: 255.255.255.0   (Hint: 255.255.255.0)

Save   Cancel   Back

Paso 10. Introduzca la dirección IP de la red privada (LAN) de la red local en el campo *Local LAN (Local Network) IP Address*. Esta es la dirección IP de la red interna en el dispositivo.

Nota: En este ejemplo, la dirección IP LAN local (red local) es 192.168.100.128.

Basic VPN Setup

About Basic VPN Setup

The basic VPN setup sets most parameters to defaults as proposed by the VPN Consortium (VPNC), and assumes a Pre-shared Key, which greatly simplifies setup. After creating the policies through the Basic VPN Setup, you can always update the parameters through the Policies menu

[View Default Settings]

Connection Name and Remote IP Type

New Connection Name: Branch1

Pre-Shared Key: Cisco1234$

Protocol: ESP ▾

Endpoint Information

Remote Endpoint: IP Address ▾

Remote WAN (Internet) IP Address: 10.11.12.13   (Hint: 1.2.3.4 or abc.com)

Local WAN (Internet) IP Address: 192.168.100.121

Secure Connection Remote Accessibility

Remote LAN (Local Network) IP Address: 10.10.100.162   (Hint: 1.2.3.4)

Remote LAN (Local Network) Subnet Mask: 255.0.0.0   (Hint: 255.255.255.0)

Local LAN (Local Network) IP Address: 192.168.100.128   Hint: 1.2.3.4)

Local LAN (Local Network) Subnet Mask: 255.255.255.0   (Hint: 255.255.255.0)

[Save]   [Cancel]   [Back]

Paso 11. Verifique la máscara de subred de la red privada (LAN) del extremo local en el campo *Local LAN (Local Network) Subnet Mask*. Esto se genera automáticamente.

Nota: En este ejemplo, la máscara de subred LAN local (red local) es 255.255.255.0.

Nota: Las direcciones IP de WAN remota y LAN remota no pueden estar en la misma subred. Por ejemplo, una dirección IP LAN remota de 192.168.1.100 y una dirección IP LAN local de 192.168.1.115 causan un conflicto cuando el tráfico se rutea a través de la VPN. El tercer octeto debe ser diferente para que las direcciones IP estén en subredes diferentes. Por ejemplo, es aceptable una dirección IP LAN remota de 192.168.1.199 y una dirección IP LAN local de 192.168.2.100.

Paso 12. Click **Save**.

Ahora debería haber configurado correctamente la VPN IPsec de sitio a sitio en el router RV132W o RV134W.