

Configuración de políticas de grupo en el router serie RV34x

Objetivo

Una política de grupo es un conjunto de atributos orientados al usuario o pares de valores para las conexiones de seguridad de protocolo de Internet (IPSec) que se almacenan internamente (localmente) en el dispositivo o externamente en un servidor de servicio de usuario de acceso telefónico de autenticación remota (RADIUS) o protocolo ligero de acceso a directorios (LDAP). Un grupo de túnel utiliza una política de grupo que establece términos para las conexiones de usuario de la red privada virtual (VPN) después de establecer el túnel.

Las políticas de grupo permiten aplicar conjuntos completos de atributos a un usuario o a un grupo de usuarios, en lugar de tener que especificar cada atributo individualmente para cada usuario. También puede modificar los atributos de política de grupo para un usuario específico.

El objetivo de este documento es mostrarle cómo configurar las Políticas de Grupo en la Serie RV34x de Router VPN.

Dispositivos aplicables

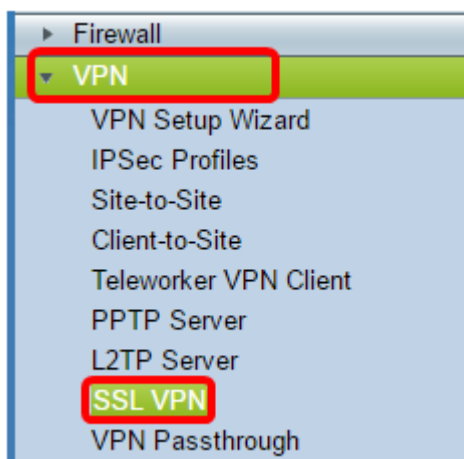
- Serie RV34x

Versión del software

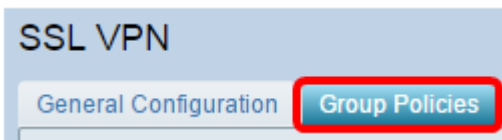
- 1.0.01.16

Configurar políticas de grupo

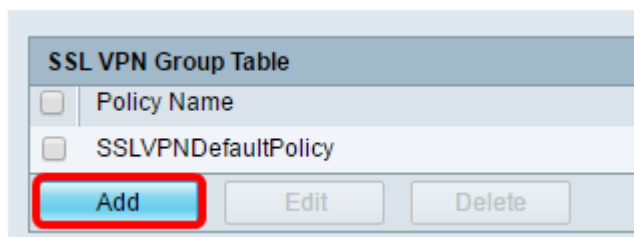
Paso 1. Inicie sesión en la utilidad basada en web del router y elija **VPN > SSL VPN**.



Paso 2. En el área SSL VPN, haga clic en la pestaña **Group Policies**.



Paso 3. Haga clic en el botón **Add** bajo la Tabla de Grupos de SSL VPN 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 política de grupo de la lista, que se denomina SSLVPNDefaultPolicy. Ésta es la política predeterminada proporcionada por el dispositivo.

Paso 4. Introduzca el nombre de política preferido en el campo *Policy Name*.

The image shows a form titled 'SSLVPN Group Policy - Add/Edit'. Under the heading 'Basic Settings', there are five input fields. The first field is labeled 'Policy Name:' and contains the text 'Group 1 Policy'. This field is highlighted with a red rectangular border. The other fields are 'Primary DNS:' (containing '192.168.1.1'), 'Secondary DNS:', 'Primary WINS:', and 'Secondary WINS:'.

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

Paso 5. Introduzca la dirección IP del DNS principal en el campo proporcionado. De forma predeterminada, esta dirección IP ya se ha suministrado.

The image shows the same form as in the previous step, titled 'SSLVPN Group Policy - Add/Edit'. Under the heading 'Basic Settings', the 'Primary DNS:' field now contains the IP address '192.168.1.1' and is highlighted with a red rectangular border. The other fields remain the same as in the previous step.

Nota: En este ejemplo, se utiliza 192.168.1.1.

Paso 6. (Opcional) Introduzca la dirección IP del DNS secundario en el campo proporcionado. Esto servirá como copia de seguridad en caso de que el DNS primario falle.

SSLVPN Group Policy - Add/Edit

Basic Settings

Policy Name:

Primary DNS:

Secondary DNS:

Primary WINS:

Secondary WINS:

Nota: En este ejemplo, se utiliza 192.168.1.2.

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

SSLVPN Group Policy - Add/Edit

Basic Settings

Policy Name:

Primary DNS:

Secondary DNS:

Primary WINS:

Secondary WINS:

Nota: En este ejemplo, se utiliza 192.168.1.1.

Paso 8. (Opcional) Introduzca la dirección IP del WINS secundario en el campo proporcionado.

SSLVPN Group Policy - Add/Edit

Basic Settings

Policy Name:

Primary DNS:

Secondary DNS:

Primary WINS:

Secondary WINS:

Nota: En este ejemplo, se utiliza 192.168.1.2.

Paso 9. (Opcional) Introduzca una descripción de la política en el campo *Descripción*.

SSLVPN Group Policy - Add/Edit

Basic Settings

Policy Name:

Primary DNS:

Secondary DNS:

Primary WINS:

Secondary WINS:

Description:

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

Paso 10. (Opcional) Haga clic en un botón de opción para elegir la política de proxy de IE para habilitar los parámetros de proxy de Microsoft Internet Explorer (MSIE) para establecer el túnel VPN. Las opciones son:

- Ninguno: permite que el explorador no utilice ninguna configuración de proxy.
- Automático: permite que el explorador detecte automáticamente la configuración del proxy.
- Bypass-local: permite al explorador omitir los parámetros de proxy configurados en el usuario remoto.
- Desactivado: desactiva la configuración del proxy MSIE.

IE Proxy Settings

IE Proxy Policy None Auto Bypass-local Disabled

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

Paso 11. (Opcional) En el área Configuración de Tunelización Dividida, marque la casilla de verificación **Habilitar Tunelización Dividida** para permitir que el tráfico destinado a Internet se envíe sin cifrar directamente a Internet. La tunelización completa envía todo el tráfico al dispositivo final donde luego se enruta a los recursos de destino, eliminando la red corporativa de la ruta para el acceso web.

IE Proxy Settings

IE Proxy Policy None Auto Bypass-local Disabled

Split Tunneling Settings

Enable Split Tunneling

Paso 12. (Opcional) Haga clic en un botón de opción para elegir si incluir o excluir el tráfico al aplicar la tunelización dividida.

Split Tunneling Settings

Enable Split Tunneling

Split Selection

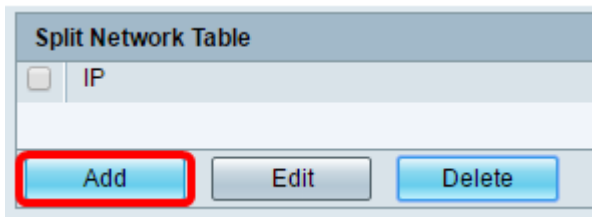


Include Traffic

Exclude Traffic

Nota: En este ejemplo, se elige Incluir tráfico.

Paso 13. En Split Network Table (Tabla de red dividida), haga clic en el botón **Add** para agregar la excepción split Network (Red dividida).

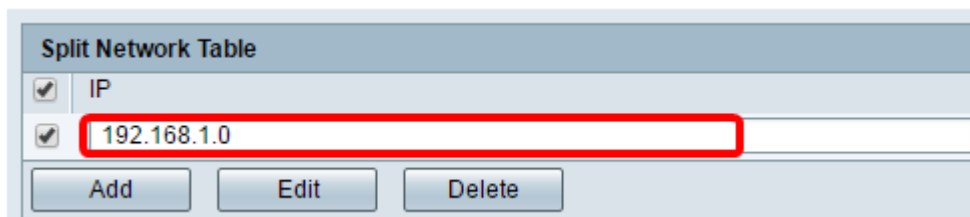


Split Network Table

<input type="checkbox"/>	IP
--------------------------	----

Add Edit Delete

Paso 14. Introduzca la dirección IP de la red en el campo proporcionado.



Split Network Table

<input checked="" type="checkbox"/>	IP
<input checked="" type="checkbox"/>	192.168.1.0

Add Edit Delete

Nota: En este ejemplo, se utiliza 192.168.1.0.

Paso 15. En Split DNS Table (Dividir tabla DNS), haga clic en el botón **Add** para agregar la excepción de DNS dividido.

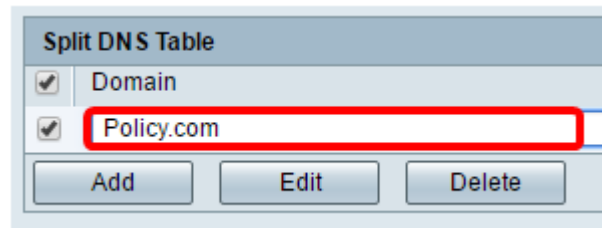


Split DNS Table

<input type="checkbox"/>	Domain
--------------------------	--------

Add Edit Delete

Paso 16. Introduzca el nombre de dominio en el campo proporcionado.



Split DNS Table

<input checked="" type="checkbox"/>	Domain
<input checked="" type="checkbox"/>	Policy.com

Add Edit Delete

Nota: En este ejemplo, se utiliza Policy.com.

Paso 17. Haga clic en Apply (Aplicar).

Split DNS Table	
<input checked="" type="checkbox"/>	Domain
<input checked="" type="checkbox"/>	Policy.com

Add Edit Delete

Apply Cancel

Una vez guardados correctamente los parámetros, se le redirigirá a la Tabla de Grupos de VPN SSL que muestra la política de grupo recién agregada.

General Configuration Group Policies

SSL VPN Group Table	
Policy Name	Description
<input type="checkbox"/> Group 1 Policy	Group Policy with Split Tunneling
<input type="checkbox"/> SSLVPNDefaultPolicy	

Add Edit Delete

Apply Cancel

Ahora debería haber configurado correctamente las políticas de grupo en el router serie RV34x.

Si desea ver la guía de configuración sencilla del RV340. haga clic [aquí](#).

Si desea ver la guía de administración del RV340. haga clic [aquí](#). La información de políticas de grupo se encuentra en la página 93.