Configuración de la política del VPN en RV180 y RV180W

Objetivos

Este documento muestra el procedimiento para fijar las políticas del VPN en la Pequeña empresa RV180 de Cisco y el Firewall RV180W VPN.

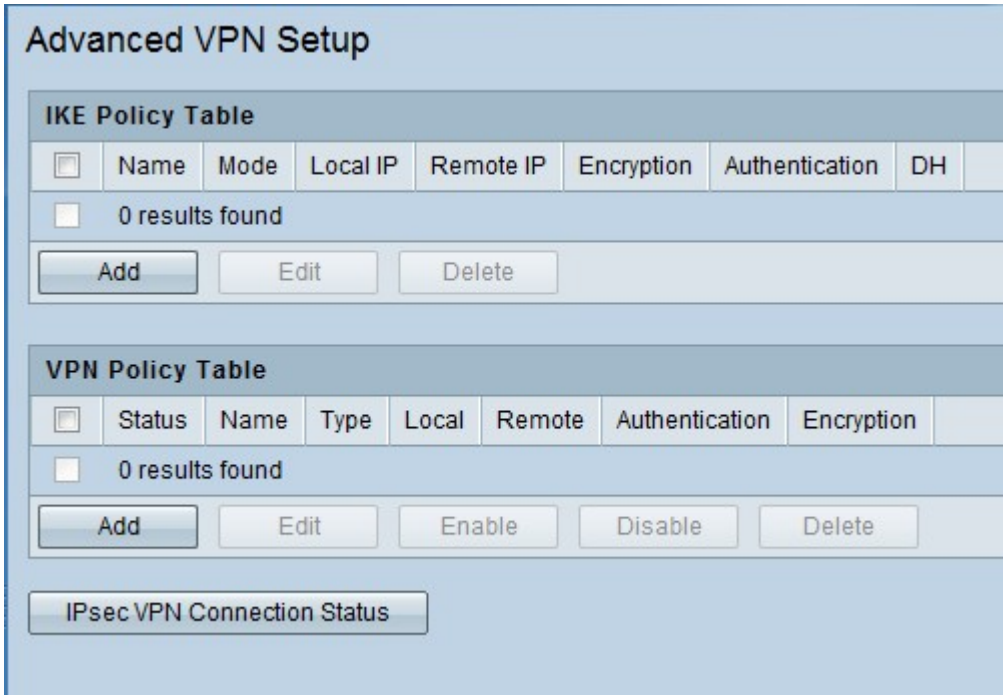
Las características de la política del VPN permiten que usted configure las configuraciones VPN para la directiva automática, directiva manual y el cifrado y los algoritmos de la integridad.

Dispositivos aplicables

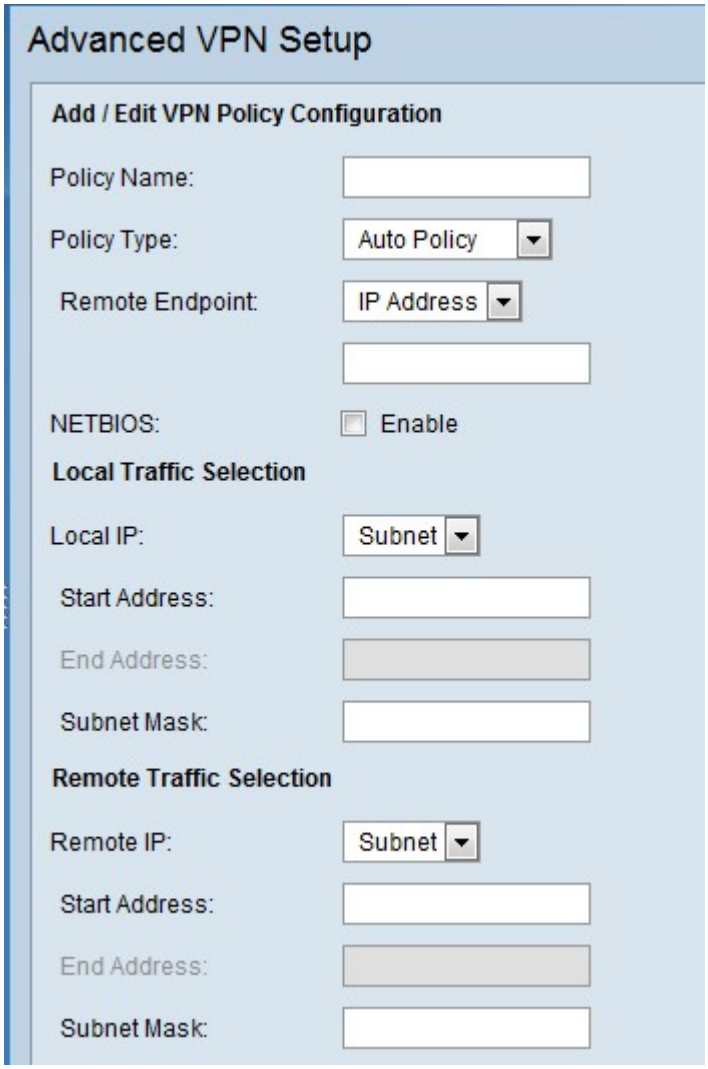
- RV180
- RV180W

Configuración de la política del VPN

Paso 1. Usando la utilidad de configuración, elija **VPN > IPSec > avanzó la configuración de VPN**. La página *avanzada de la configuración de VPN* se abre.



Paso 2. En la sección de la tabla de la política del VPN, haga click en Add



Paso 3. Ingrese un nombre único es el campo de nombre de la directiva para que la directiva sea fijada.

Paso 4. Elija el tipo apropiado de la directiva de la lista desplegable del **tipo de la directiva**.

- Directiva auto — Los parámetros se podían fijar automáticamente. En este caso además de las directivas se requiere que el protocolo IKE (intercambio de claves de Internet) negocia entre los dos puntos finales de VPN.

- Directiva manual — En este caso todas las configuraciones que incluyen las configuraciones para las claves para el VPN hacen un túnel se entran manualmente para cada punto final.

Paso 5. Elija el tipo de identificador IP que identificaría el gateway en el punto final remoto de la lista desplegable del **punto final remoto**.

- Dirección IP — Dirección IP del gateway en el punto final remoto.
- FQDN (Nombre de dominio totalmente calificado (FQDN)) — Inserte el Nombre de dominio totalmente calificado (FQDN) del gateway en el punto final del remore.

Paso 6. Para permitir a los broadcastes de NetBIOS para viajar a través del VPN haga un túnel, marque el checkbox del **permiso**.

La selección y el telecontrol del tráfico local trafican la selección

Paso 1. Para ambas áreas configure las configuraciones siguientes:

- Local/IP remoto — Elija el tipo de identificador que usted quiere proporcionar para el punto extremo:
  - Cualquier - que éste especifique el tráfico es de punto extremo dado (local o remoto). Ambos no pueden ser elegidos.
  - El solo - esto limita la directiva a un host. Inserte la dirección IP del host que será parte del VPN en el campo de la dirección IP del comienzo.
  - El - del rango esto permite que los ordenadores dentro del rango de dirección IP especificada conecten con el VPN. Inserte la dirección IP del comienzo y la dirección IP del extremo en los campos adecuados.
  - El - de la subred esto permite que los ordenadores dentro de un alcance del IP Address conecten con el VPN. Inserte la dirección IP del comienzo y la dirección IP del extremo en los campos adecuados. También inserte a la máscara de subred de la red en el campo de la máscara de subred.

DNS dividido

El DNS dividido permite que el RV120W adquiera el DNS del punto extremo remoto sin pasar a través de Internet.

Paso 1. Para habilitar el DNS dividido marque la casilla de verificación del **permiso**.

Paso 2. En el Domain Name Server 1 campo, inserta una dirección IP del Domain Name Server. Esta dirección IP sería utilizada para resolver solamente el dominio insertado en el Domain Name 1 campo.

Paso 3. En el campo del Domain Name Server 2, inserte una dirección IP del Domain Name Server. Esta dirección IP sería utilizada para resolver solamente el dominio insertado en el campo del Domain Name 2.

Parámetros manuales de la directiva

Paso 1. Inserte el valor hexadecimal entre 3 y 8 en los campos SPI-entrantes y SPI-salientes.

Paso 2. Elija los algoritmos de encripción apropiados de la lista desplegable del **algoritmo de encripción**.

Paso 3. Inserte el valor hexadecimal entre 3 y 8 en los campos SPI-entrantes y SPI-salientes.

Paso 4. Inserte la clave de encripción de la política de entrada en Clave-en el campo.

Paso 5. Inserte la clave de encripción de la política de salida en el campo de la clave-Hacia fuera.

Paso 6. Elija el algoritmo apropiado de la integridad de la lista desplegable del **algoritmo de la integridad**. Este algoritmo verificará la integridad de los datos.

Paso 7. Inserte la clave de la integridad de la política de entrada en Clave-en el campo.

Paso 8. Inserte la clave de la integridad de la política de salida en el campo de la clave-Hacia fuera.

Parámetros autos de la directiva

Paso 1. En el campo del curso de la vida SA ingrese la duración de la asociación de seguridad. Elija la unidad apropiada para el campo del curso de la vida SA en la lista desplegable.

- Segundos — El valor predeterminado es 3600 segundos. El valor mínimo es 300 segundos.
- Kilobytes — Después del valor especificado de los kilobytes en este campo se renegocia el SA. El valor mínimo es 1920000 KB.

Paso 2. Elija los algoritmos de encripción apropiados de la lista desplegable del **algoritmo de encripción**.

Paso 3. Elija el algoritmo apropiado de la integridad de la lista desplegable del **algoritmo de la integridad**. Este algoritmo verificará la integridad de los datos.

Paso 4. Para permitir a la perfecta reserva hacia adelante para mejorar la Seguridad, marque el checkbox del **permiso**. Elija el apropiado intercambio de claves Diffie-Hellman del **campo del grupo de la clave PFS.** lista desplegable.

Paso 5. Elija la política IKE apropiada de la lista desplegable **selecta de la política IKE**.