Configuración de VPN avanzada en el router VPN CVR100W

Objetivo

Una red privada virtual (VPN) se utiliza para conectar terminales en diferentes redes a través de una red pública, como Internet. Esta función permite a los usuarios remotos que se encuentran fuera de una red local conectarse de forma segura a la red a través de Internet.

En este artículo se explica cómo configurar VPN avanzada en el router VPN CVR100W. Para la configuración básica de VPN, refiérase al artículo *Basic VPN Setup on the CVR100W VPN Router*.

Dispositivos aplicables

Router VPN · CVR100W

Versión del software

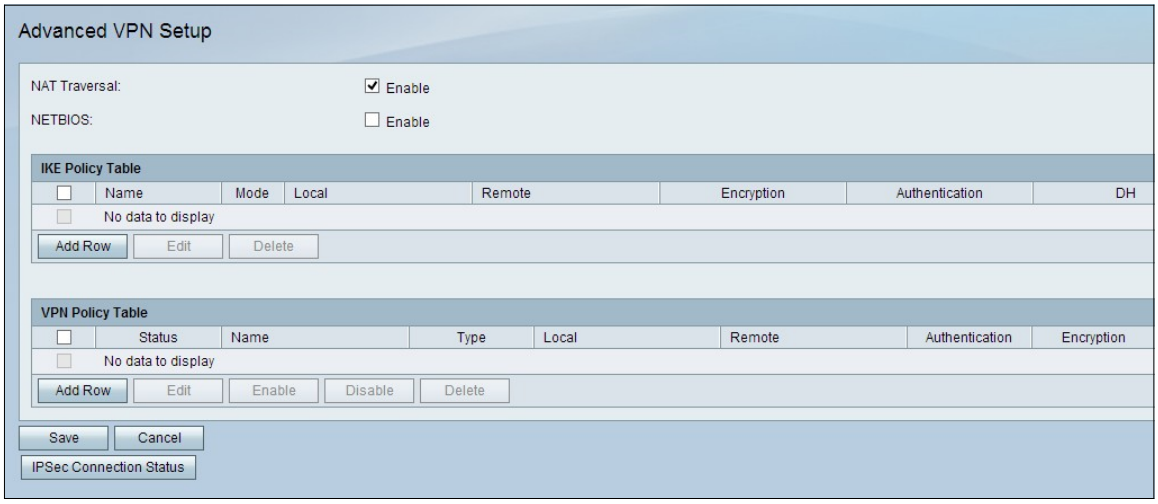
•1.0.1.19

Configuración avanzada de VPN

Parámetros iniciales

Este procedimiento explica cómo configurar los parámetros iniciales de Advanced VPN Setup.

Paso 1. Inicie sesión en la utilidad de configuración web y elija **VPN > Advanced VPN Setup** . Se abre la página *Advanced VPN Setup*:



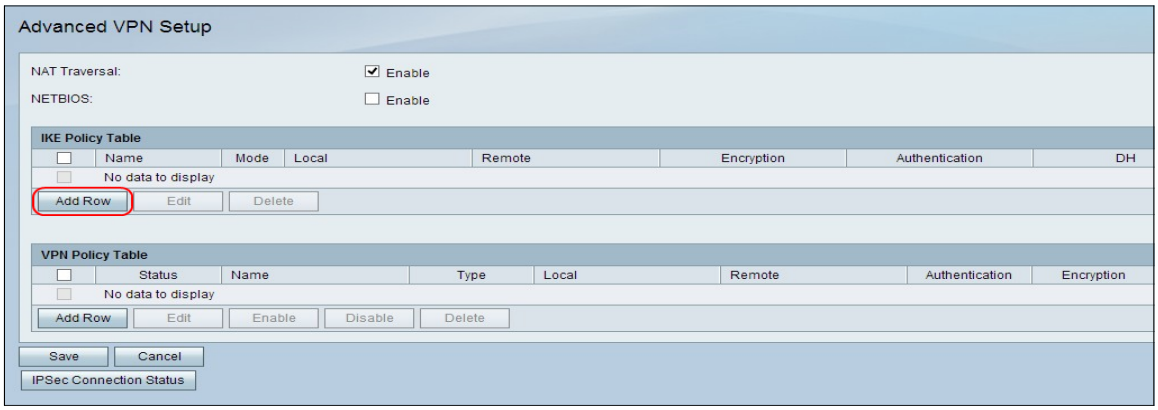
Paso 2. (Opcional) Para habilitar la traducción de direcciones de red (NAT) transversal para la conexión VPN, marque la casilla de verificación **Enable** en el campo NAT Traversal. NAT Traversal permite que se realice una conexión VPN entre gateways que utilizan NAT. Elija

esta opción si la conexión VPN pasa a través de una gateway habilitada para NAT.

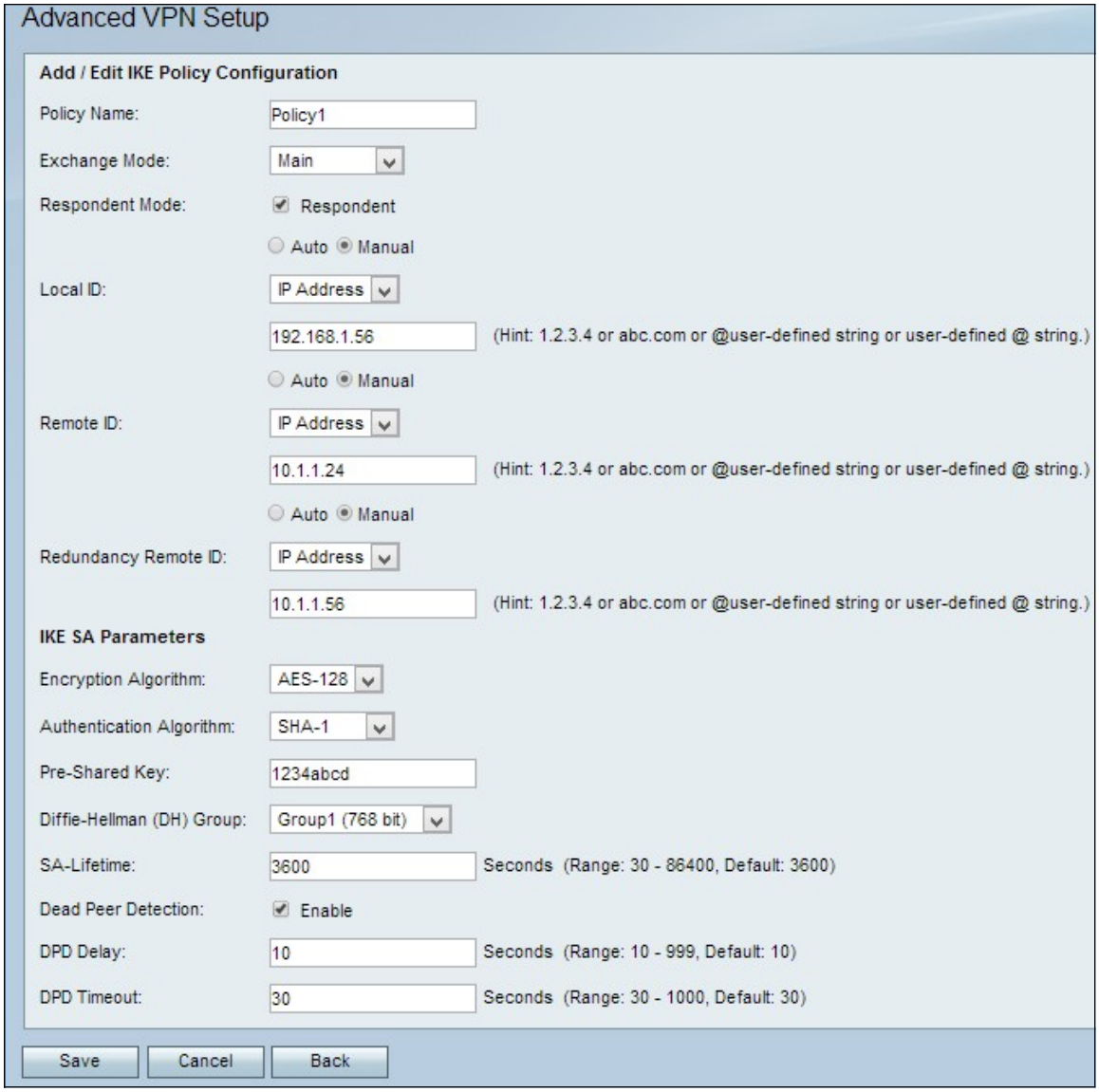
Paso 3. (Opcional) Para habilitar el envío de broadcasts de Network Basic Input/Output System (NetBIOS) a través de la conexión VPN, marque la casilla de verificación **Enable** en el campo NETBIOS. NetBIOS permite a los hosts comunicarse entre sí dentro de una LAN.

Configuración de política IKE

Internet Key Exchange (IKE) es un protocolo utilizado para establecer una conexión segura para la comunicación en una VPN. Esta conexión segura establecida se denomina Asociación de seguridad (SA). Este procedimiento explica cómo configurar una política IKE para la conexión VPN que se utilizará para la seguridad. Para que una VPN funcione correctamente, las políticas IKE para ambos puntos finales deben ser idénticas.



Paso 1. En la tabla de políticas IKE, haga clic en **Agregar fila** para crear una nueva política IKE. La página *Advanced VPN Setup* cambia:



Paso 2. En el campo Policy Name (Nombre de política), introduzca un nombre para la política IKE.

Paso 3. En la lista desplegable Modo de intercambio, elija una opción para identificar cómo funciona la política IKE.

·principal: esta opción permite que la política IKE funcione con mayor seguridad. Es más lento que el modo agresivo. Elija esta opción si se necesita una conexión VPN más segura.

·agresiva: esta opción permite que la política IKE funcione más rápido pero es menos segura que el modo principal. Elija esta opción si se necesita una conexión VPN más rápida.

Paso 4. (Opcional) Para activar el modo de encuestado, marque la casilla de verificación **Responsable**. Si el modo de respuesta está activado, el router VPN CVR100W sólo puede recibir la solicitud VPN del terminal VPN remoto.

Paso 5. En el campo ID local, haga clic en el botón de opción deseado para identificar cómo especificar el ID local.

·Automático: esta opción asigna automáticamente la ID local.

·Manual: esta opción se utiliza para asignar manualmente la ID local.

Paso 6. (Opcional) En la lista desplegable ID local, elija el método de identificación deseado para la red local.

Dirección IP ·: esta opción identifica la red local por una dirección IP pública.

·FQDN: esta opción utiliza un nombre de dominio completo (FQDN) para identificar la red local.

Paso 7. (Opcional) En el campo ID local, introduzca la dirección IP o el nombre de dominio. La entrada depende de la opción elegida en el paso 6.

Paso 8. En el campo Remote ID (ID remota), haga clic en el botón de opción deseado para identificar cómo especificar el ID remoto.

·Automático: esta opción asigna automáticamente la ID remota.

Manual de ·: esta opción se utiliza para asignar manualmente la ID remota

Paso 9. (Opcional) En la lista desplegable ID remoto, elija el método de identificación deseado para la red remota.

Dirección IP ·: esta opción identifica la red remota mediante una dirección IP pública.

·FQDN: esta opción utiliza un nombre de dominio completo (FQDN) para identificar la red remota.

Paso 10. (Opcional) En el campo Remote ID (ID remoto), introduzca la dirección IP o el nombre de dominio. La entrada depende de la opción elegida en el paso 9.

Paso 11. En el campo Redundancy Remote ID (ID remoto de redundancia), haga clic en el botón de opción deseado para identificar cómo especificar el ID remoto de redundancia. El ID remoto de redundancia es un ID remoto alternativo utilizado para configurar el túnel VPN en el gateway remoto.

·Automático: esta opción asigna automáticamente la ID remota de redundancia.

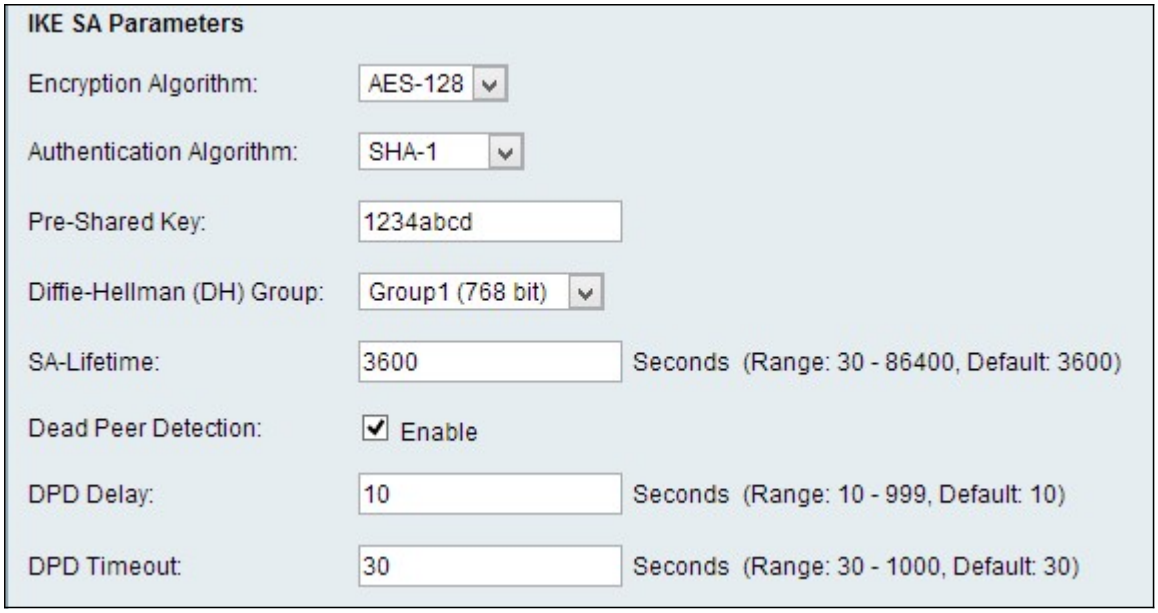
·Manual: esta opción se utiliza para asignar manualmente la ID remota de redundancia.

Paso 12. (Opcional) En la lista desplegable ID remoto de redundancia, elija el método de identificación deseado para la red de redundancia.

·dirección IP: esta opción identifica la red remota de redundancia por una dirección IP pública.

·FQDN: esta opción utiliza un nombre de dominio completo (FQDN) para identificar la red remota de redundancia.

Paso 13. (Opcional) En el campo Redundancy Remote ID (Identificador remoto de redundancia), introduzca la dirección IP o el nombre de dominio. La entrada depende de la opción elegida en el paso 12.



Paso 14. En la lista desplegable Algoritmo de cifrado, elija una opción para negociar la Asociación de seguridad (SA).

·DES: el estándar de cifrado de datos (DES) utiliza un tamaño de clave de 56 bits para el cifrado de datos. DES está obsoleto y debe utilizarse si un terminal sólo admite DES.

·3DES: estándar de cifrado de datos triple (3DES) realiza DES tres veces, pero varía el tamaño de la clave de 168 bits a 112 bits y de 112 bits a 56 bits según la ronda de DES realizada. 3DES es más seguro que DES y AES.

·AES-128: el estándar de cifrado avanzado con clave de 128 bits (AES-128) utiliza una clave de 128 bits para el cifrado AES. AES es más rápido y seguro que DES. Algunos tipos de hardware permiten que 3DES sea más rápido. AES-128 es más rápido pero menos seguro que AES-192 y AES-256.

·AES-192: AES-192 utiliza una clave de 192 bits para el cifrado AES. AES-192 es más lento pero más seguro que AES-128 y AES-192 es más rápido pero menos seguro que AES-256.

·AES-256: AES-256 utiliza una clave de 256 bits para el cifrado AES. AES-256 es más lento pero más seguro que AES-128 y AES-192.

Paso 15. En la lista desplegable Authentication Algorithm (Algoritmo de autenticación), elija una opción para autenticar el encabezado VPN.

·MD5: el algoritmo Message-Digest 5 (MD5) utiliza un valor hash de 128 bits para la autenticación. MD5 es menos seguro pero es más rápido que SHA-1 y SHA2-256.

·SHA-1: el algoritmo hash seguro 1 (SHA-1) utiliza un valor hash de 160 bits para la autenticación. SHA-1 es más lento pero más seguro que MD5 y SHA-1 es más rápido pero menos seguro que SHA2-256.

·SHA2-256: Secure Hash Algorithm 2 (SHA2-256) utiliza un valor hash de 256 bits para la autenticación. SHA2-256 es más lento pero seguro que MD5 y SHA-1.

Paso 16. En el campo Pre-Shared Key (Clave precompartida), introduzca una clave precompartida que utilice la política IKE.

Paso 17. En la lista desplegable Grupo Diffie-Hellman (DH), elija el grupo DH que IKE utiliza. Los hosts de un grupo DH pueden intercambiar claves sin tener conocimiento mutuo. Cuanto mayor sea el número de bits del grupo, mayor será la seguridad del grupo.

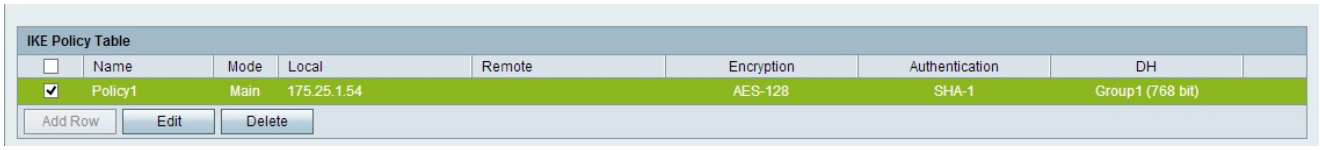
Paso 18. En el campo SA-Lifetime, introduzca cuánto tiempo (en segundos) dura la asociación de seguridad (SA) para la VPN antes de que se renueve la SA.

Paso 19. (Opcional) Para habilitar la detección de pares muertos (DPD), marque la casilla de verificación **Enable** en el campo Dead Peer Detection. DPD se utiliza para monitorear peers IKE para verificar si un peer ha dejado de funcionar. DPD evita el desperdicio de recursos de red en peers inactivos.

Paso 20. (Opcional) Para indicar la frecuencia con la que se comprueba la actividad del par, introduzca el intervalo de tiempo (en segundos) en el campo DPD Delay (Retraso de DPD). Esta opción está disponible si DPD está habilitado en el paso 19.

Paso 21. (Opcional) Para indicar cuánto tiempo debe esperar antes de que se descarte un par inactivo, introduzca cuánto tiempo (en segundos) en el campo DPD Timeout (Tiempo de espera de DPD). Esta opción está disponible si DPD está habilitado en el paso 19.

Paso 22. Click **Save**. La página *Advanced VPN Setup* original vuelve a aparecer.

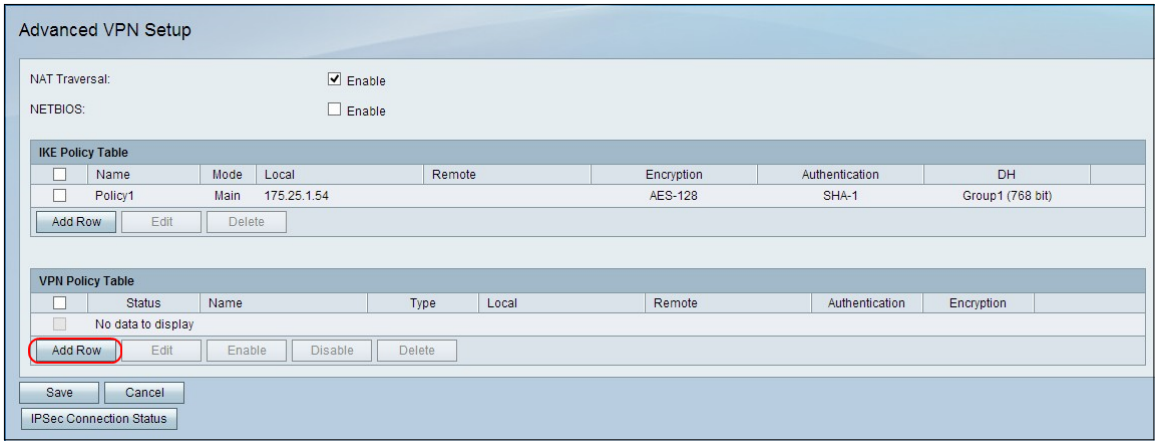


Paso 23. (Opcional) Para editar una política IKE en la tabla de políticas IKE, active la casilla de verificación de la política. A continuación, haga clic en **Editar**, edite los campos requeridos y haga clic en **Guardar**.

Paso 24. (Opcional) Para eliminar una política IKE en la tabla de políticas IKE, active la casilla de verificación de la política y haga clic en **Eliminar.** A continuación, haga clic en **Guardar**.

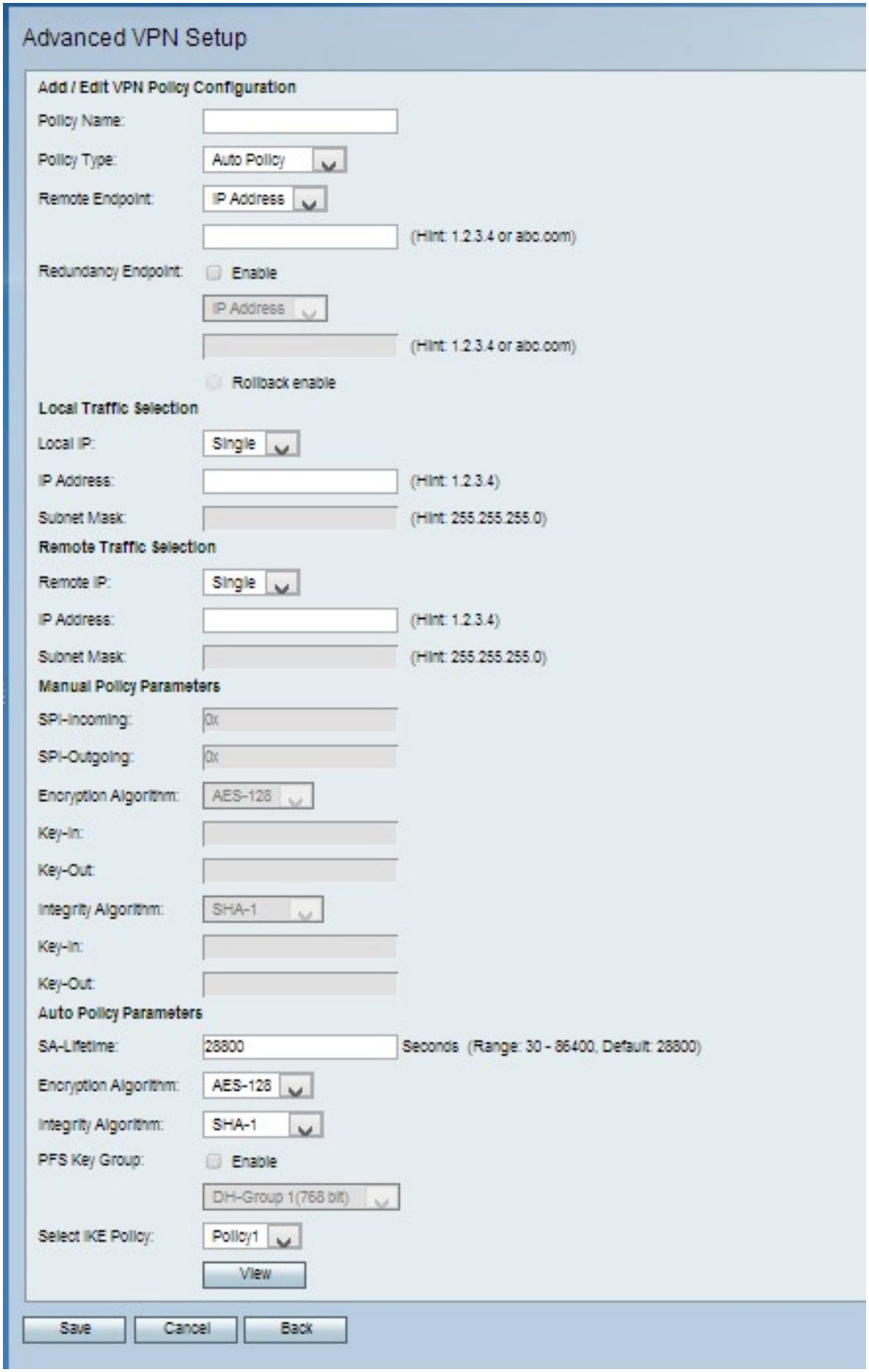
Configuración de política VPN

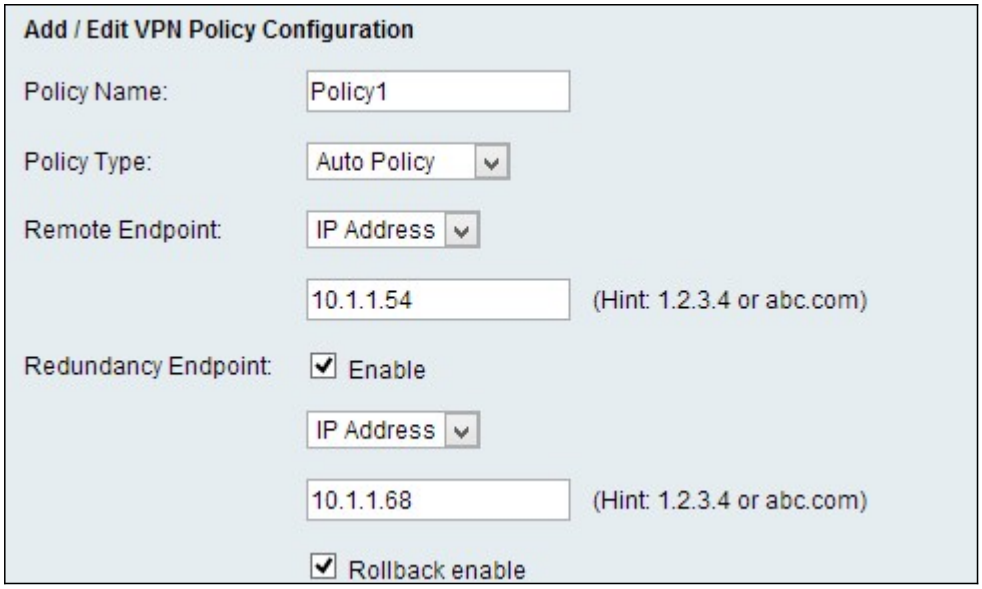
Este procedimiento explica cómo configurar una política VPN para la conexión VPN que se va a utilizar. Para que una VPN funcione correctamente, las políticas de VPN para ambos puntos finales deben ser idénticas.



Paso 1. En la Tabla de Políticas de VPN, haga clic en **Agregar Fila** para crear una nueva

política de VPN. La página *Advanced VPN Setup* cambia:





Paso 2. En el campo Policy Name (Nombre de política), introduzca un nombre para la política VPN.

Paso 3. En la lista desplegable Tipo de directiva, elija una opción para identificar cómo se generan los parámetros del túnel VPN.

Política manual ·: esta opción permite configurar las claves para el cifrado e integridad de los datos.

Política automática ·: esta opción utiliza una política IKE para la integridad de los datos y los intercambios de claves de cifrado.

Paso 4. En la lista desplegable Terminal remoto, elija una opción para especificar cómo asignar manualmente el ID remoto.

Dirección IP ·: esta opción identifica la red remota mediante una dirección IP pública.

·FQDN: esta opción utiliza un nombre de dominio completo (FQDN) para identificar la red remota.

Paso 5. En el campo text-entry bajo la lista desplegable Remote Endpoint, introduzca la dirección IP pública o el nombre de dominio de la dirección remota.

Paso 6. (Opcional) Para habilitar la redundancia, marque la casilla de verificación **Enable** en el campo Redundancy Endpoint. La opción de punto final de redundancia permite que el router VPN CVR100W se conecte a un punto final VPN de reserva cuando falle la conexión VPN principal.

Paso 7. (Opcional) Para asignar manualmente la ID de redundancia, elija una opción de la lista desplegable Punto final de redundancia.

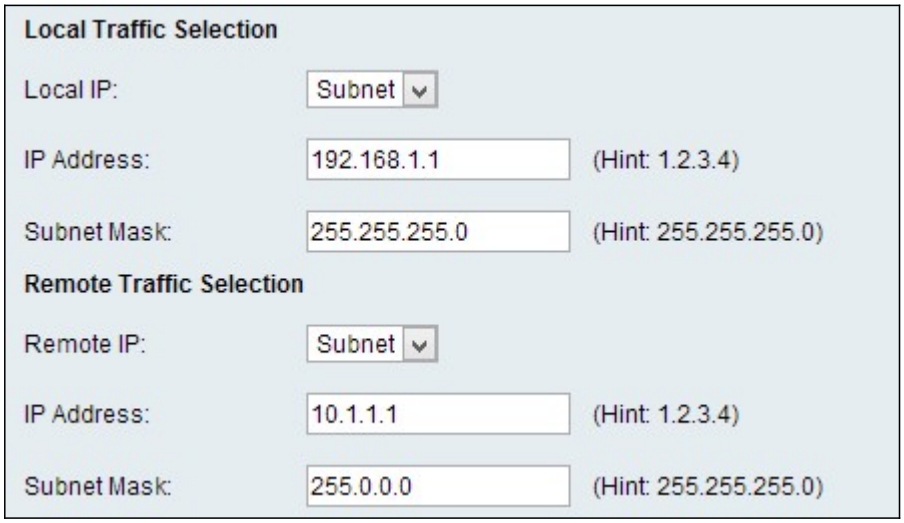
·dirección IP: esta opción identifica la red remota de redundancia por una dirección IP pública.

·FQDN: esta opción utiliza un nombre de dominio completo (FQDN) para identificar la red remota de redundancia.

Paso 8. (Opcional) Para introducir la dirección de redundancia, en el campo de entrada de texto debajo de la lista desplegable Punto final de redundancia, introduzca la dirección IP

pública o el nombre de dominio.

Paso 9. (Opcional) Para activar la reversión, marque la casilla de verificación **Rollback enable**. Esta opción habilita el switching automático de la conexión VPN de respaldo a la conexión VPN primaria cuando la conexión VPN primaria se ha recuperado de una falla.



Paso 10. En la lista desplegable IP local, elija una opción para identificar qué hosts se ven afectados por la política.

·Single: esta opción utiliza un único host como punto de conexión VPN local.

·Subred: esta opción utiliza una subred de la red local como punto de conexión VPN local.

Paso 11. En el campo IP Address (Dirección IP), introduzca la dirección IP de host o subred de la subred o el host local.

Paso 12. (Opcional) Si se elige la opción Subred en el Paso 10, introduzca la máscara de subred para la subred local en el campo Subnet Mask (Máscara de subred).

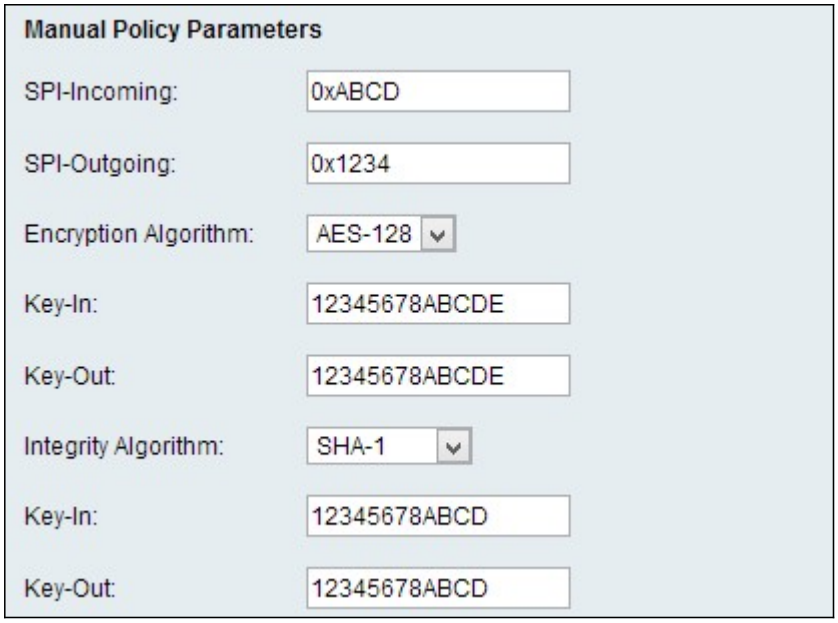
Paso 13. En la lista desplegable IP remota, elija una opción para identificar qué hosts se ven afectados por la política.

·Single: esta opción utiliza un único host como punto de conexión VPN remota.

·Subred: esta opción utiliza una subred de la red remota como punto de conexión VPN remota.

Paso 14. En el campo IP Address (Dirección IP), introduzca la dirección IP de host o subred de la subred o el host remotos.

Paso 15. (Opcional) Si se elige la opción Subred en el Paso 13, introduzca la máscara de subred para la subred remota en el campo Subnet Mask (Máscara de subred).



Nota: Si se elige la opción Política manual en el paso 3, realice los pasos 16 a 23; Caso contrario, siga con el paso 24.

Paso 16. En el campo SPI-Incoming, introduzca de tres a ocho caracteres hexadecimales para la etiqueta Security Parameter Index (SPI) para el tráfico entrante en la conexión VPN. La etiqueta SPI se utiliza para distinguir el tráfico de una sesión del tráfico de otras sesiones. El SPI entrante en un lado del túnel debe ser el SPI saliente del otro lado del túnel.

Paso 17. En el campo SPI-Saliente, introduzca de tres a ocho caracteres hexadecimales para la etiqueta SPI para el tráfico saliente en la conexión VPN. La etiqueta SPI se utiliza para distinguir el tráfico de una sesión del tráfico de otras sesiones. El SPI saliente en un lado del túnel debe ser el SPI entrante del otro lado del túnel.

Paso 18. En la lista desplegable Algoritmo de cifrado, elija una opción para negociar la Asociación de seguridad (SA).

·DES: el estándar de cifrado de datos (DES) utiliza un tamaño de clave de 56 bits para el cifrado de datos. DES está obsoleto y debe utilizarse si un terminal sólo admite DES.

·3DES: estándar de cifrado de datos triple (3DES) realiza DES tres veces, pero varía el tamaño de la clave de 168 bits a 112 bits y de 112 bits a 56 bits según la ronda de DES realizada. 3DES es más seguro que DES y AES.

·AES-128: el estándar de cifrado avanzado con clave de 128 bits (AES-128) utiliza una clave de 128 bits para el cifrado AES. AES es más rápido y seguro que DES. Algunos tipos de hardware permiten que 3DES sea más rápido. AES-128 es más rápido pero menos seguro que AES-192 y AES-256.

·AES-192: AES-192 utiliza una clave de 192 bits para el cifrado AES. AES-192 es más lento pero más seguro que AES-128 y AES-192 es más rápido pero menos seguro que AES-256.

·AES-256: AES-256 utiliza una clave de 256 bits para el cifrado AES. AES-256 es más lento pero más seguro que AES-128 y AES-192.

Paso 19. En el campo Key-In (Clave de entrada), introduzca una clave para la política entrante. La longitud de la clave depende del algoritmo elegido en el Paso 18.

·DES utiliza una clave de 8 caracteres.

·3DES utiliza una clave de 24 caracteres.

·AES-128 utiliza una clave de 12 caracteres.

·AES-192 utiliza una clave de 24 caracteres.

·AES-256 utiliza una clave de 32 caracteres.

Paso 20. En el campo Key-Out (Clave de salida), introduzca una clave para la directiva saliente. La longitud de la clave depende del algoritmo elegido en el Paso 18. La longitud de la clave depende del algoritmo elegido en el Paso 18.

·DES utiliza una clave de 8 caracteres.

·3DES utiliza una clave de 24 caracteres.

·AES-128 utiliza una clave de 12 caracteres.

·AES-192 utiliza una clave de 24 caracteres.

·AES-256 utiliza una clave de 32 caracteres.

Paso 21. En la lista desplegable Algoritmo de integridad, elija una opción para autenticar el encabezado VPN.

·MD5: el algoritmo Message-Digest 5 (MD5) utiliza un valor hash de 128 bits para la autenticación. MD5 es menos seguro pero más rápido que SHA-1 y SHA2-256.

·SHA-1: el algoritmo hash seguro 1 (SHA-1) utiliza un valor hash de 160 bits para la autenticación. SHA-1 es más lento pero más seguro que MD5 y SHA-1 es más rápido pero menos seguro que SHA2-256.

·SHA2-256: Secure Hash Algorithm 2 (SHA2-256) utiliza un valor hash de 256 bits para la autenticación. SHA2-256 es más lento pero más seguro que MD5 y SHA-1.

Paso 22. En el campo Key-In (Clave de entrada), introduzca una clave para la política entrante. La longitud de la clave depende del algoritmo elegido en el Paso 21.

·MD5 utiliza una clave de 16 caracteres.

·SHA-1 utiliza una clave de 20 caracteres.

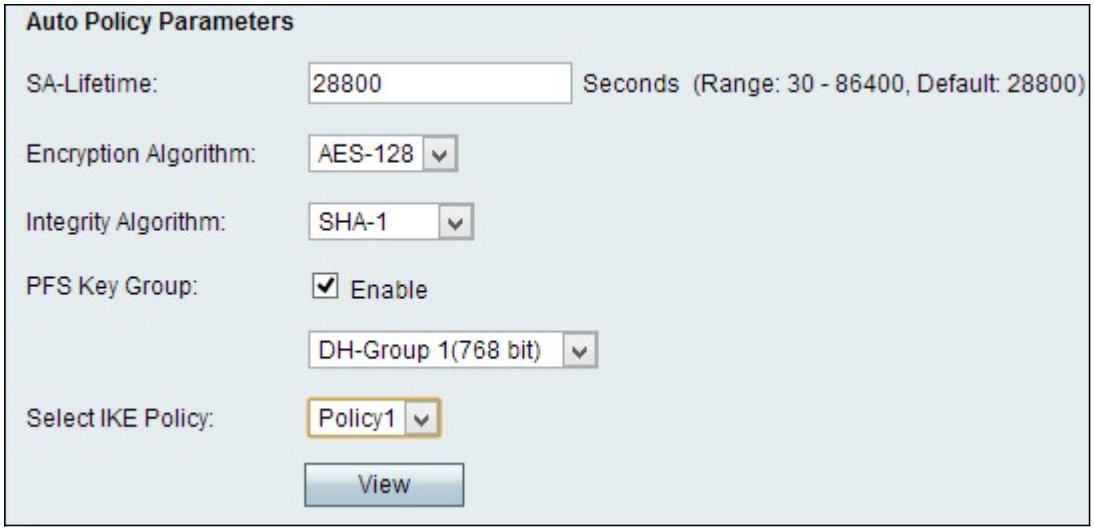
·SHA2-256 utiliza una clave de 32 caracteres.

Paso 23. En el campo Key-Out (Clave de salida), introduzca una clave para la directiva saliente. La longitud de la clave depende del algoritmo elegido en el Paso 21. La longitud de la clave depende del algoritmo elegido en el Paso 21.

·MD5 utiliza una clave de 16 caracteres.

·SHA-1 utiliza una clave de 20 caracteres.

·SHA2-256 utiliza una clave de 32 caracteres.



Nota: Si selecciona Política automática en el paso 3, realice los pasos 24 a 29; Caso contrario, siga con el paso 31.

Paso 24. En el campo SA-Lifetime, introduzca cuánto tiempo dura la SA en segundos antes de la renovación.

Paso 25. En la lista desplegable Algoritmo de cifrado, elija una opción para negociar la Asociación de seguridad (SA).

·DES: el estándar de cifrado de datos (DES) utiliza un tamaño de clave de 56 bits para el cifrado de datos. DES está obsoleto y debe utilizarse si un terminal sólo admite DES.

·3DES: estándar de cifrado de datos triple (3DES) realiza DES tres veces, pero varía el tamaño de la clave de 168 bits a 112 bits y de 112 bits a 56 bits según la ronda de DES realizada. 3DES es más seguro que DES y AES.

·AES-128: el estándar de cifrado avanzado con clave de 128 bits (AES-128) utiliza una clave de 128 bits para el cifrado AES. AES es más rápido y seguro que DES. Algunos tipos de hardware permiten que 3DES sea más rápido. AES-128 es más rápido pero menos seguro que AES-192 y AES-256.

·AES-192: AES-192 utiliza una clave de 192 bits para el cifrado AES. AES-192 es más lento pero más seguro que AES-128 y AES-192 es más rápido pero menos seguro que AES-256.

·AES-256: AES-256 utiliza una clave de 256 bits para el cifrado AES. AES-256 es más lento pero más seguro que AES-128 y AES-192.

Paso 26. En la lista desplegable Algoritmo de integridad, elija una opción para autenticar el encabezado VPN.

·MD5: el algoritmo Message-Digest 5 (MD5) utiliza un valor hash de 128 bits para la autenticación. MD5 es menos seguro pero más rápido que SHA-1 y SHA2-256.

·SHA-1: el algoritmo hash seguro 1 (SHA-1) utiliza un valor hash de 160 bits para la autenticación. SHA-1 es más lento pero más seguro que MD5 y SHA-1 es más rápido pero menos seguro que SHA2-256.

·SHA2-256: Secure Hash Algorithm 2 (SHA2-256) utiliza un valor hash de 256 bits para la

autenticación. SHA2-256 es más lento pero seguro que MD5 y SHA-1.

Paso 27. Marque la casilla de verificación **Enable** en el campo PFS Key Group para habilitar Perfect Forward Secrecy (PFS). PFS aumenta la seguridad de VPN, pero reduce la velocidad de conexión.

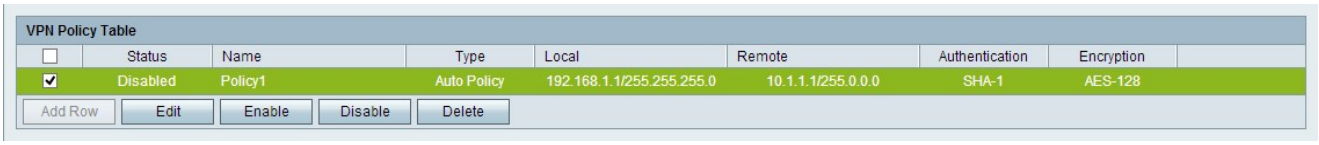
Paso 28. (Opcional) Si optó por activar PFS en el paso 27, elija un grupo Diffie-Hellman (DH) para unirse desde la lista desplegable, debajo del campo PFS Key Group (Grupo de claves PFS). Cuanto mayor sea el número de grupo, mayor será la seguridad del grupo.

Paso 29. En la lista desplegable Seleccionar política IKE, elija la política IKE que desea utilizar para la política VPN.

Paso 30. (Opcional) Si hace clic en **View**, se le dirige a la sección de configuración IKE de la página *Advanced VPN Setup*.

Paso 31. Click **Save**. La página *Advanced VPN Setup* original vuelve a aparecer.

Paso 32. Click **Save**.



Paso 33. (Opcional) Para editar una política VPN en la tabla de políticas VPN, marque la casilla de verificación de la política. A continuación, haga clic en **Editar**, edite los campos requeridos y haga clic en **Guardar**.

Paso 34. (Opcional) Para eliminar una política VPN en la Tabla de Políticas de VPN, active la casilla de verificación de la política, haga clic en **Eliminar** y, a continuación, haga clic en **Guardar**.