Configuración de VPN avanzada en RV215W

Objetivo

Una red privada virtual (VPN) es una conexión segura establecida dentro de una red o entre redes. Las VPN sirven para aislar el tráfico entre hosts y redes especificados del tráfico de redes y hosts no autorizados. En este artículo se explica cómo configurar Advanced VPN Setup en el RV215W.

Dispositivos aplicables

·RV215W

Versión del software

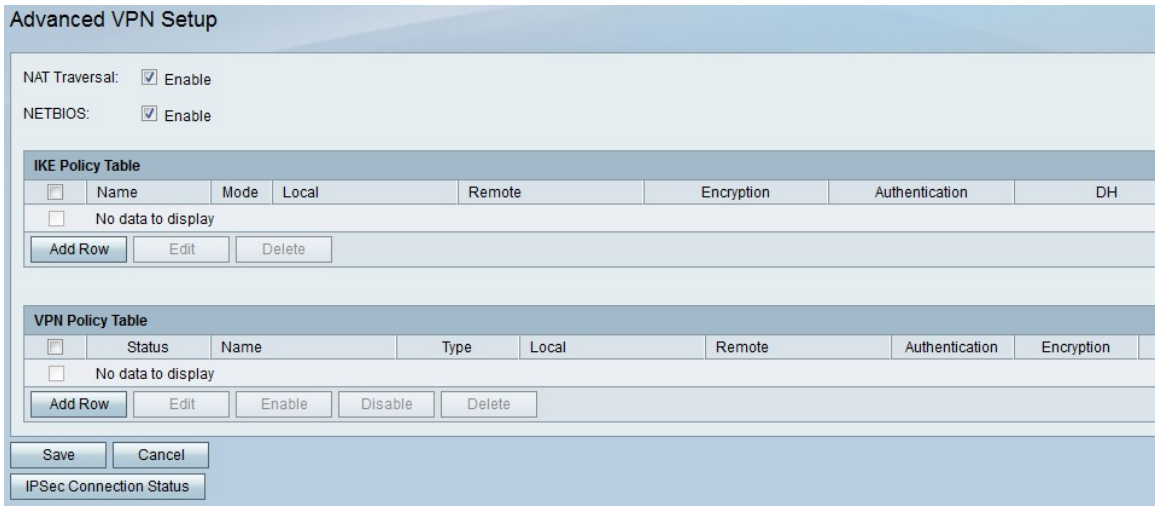
•1.1.0.5

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*:



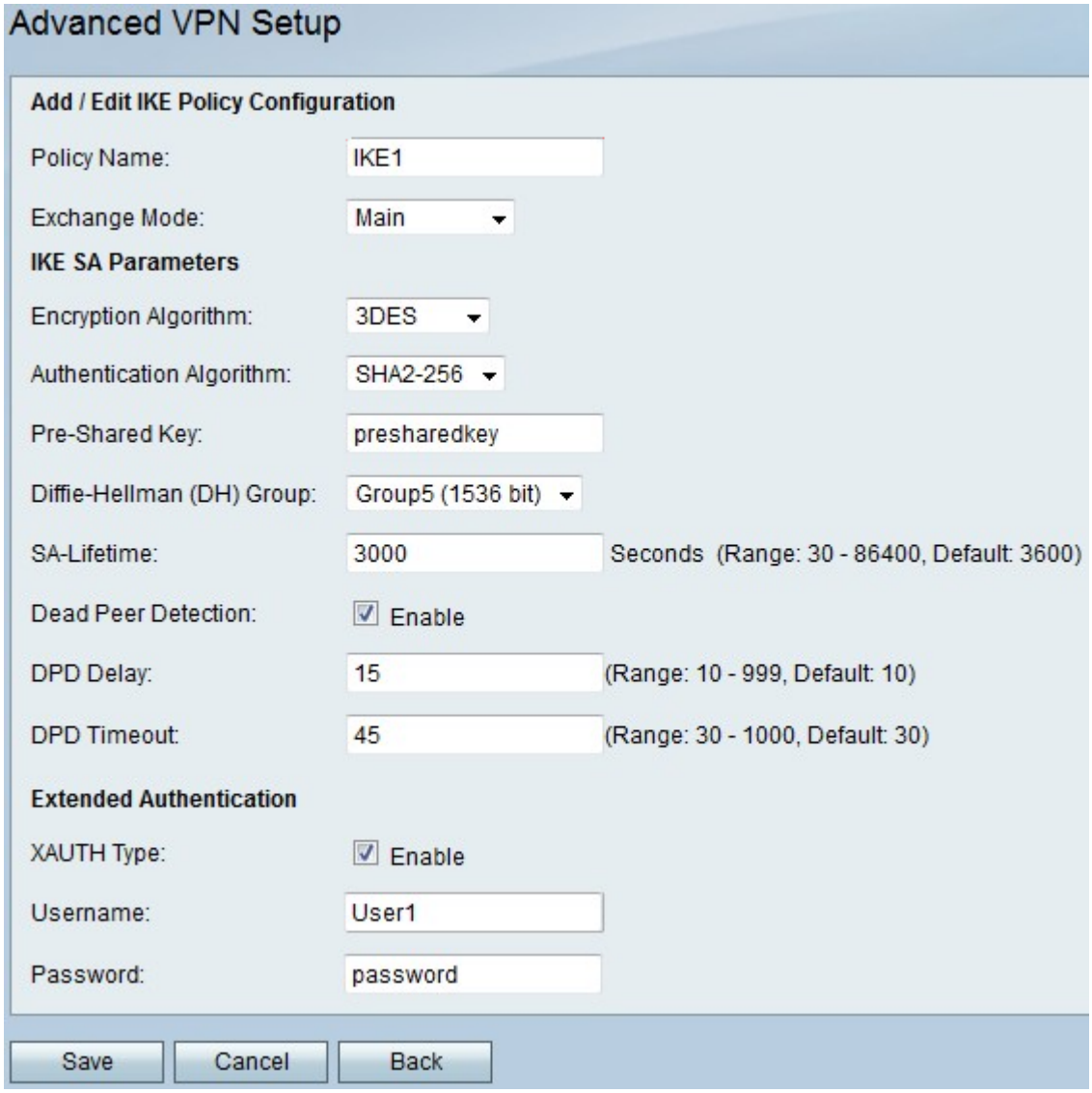
Paso 2. (Opcional) Marque la casilla de verificación **Enable** en el campo NAT Traversal si desea habilitar la traducción de direcciones de red (NAT) transversal para la conexión VPN. NAT Traversal permite que se realice una conexión VPN entre gateways que utilizan NAT. Elija esta opción si la conexión VPN pasa a través de una gateway habilitada para NAT.

Paso 3. (Opcional) Marque la casilla de verificación **Enable** en el campo NETBIOS si desea habilitar las transmisiones de Network Basic Input/Output System (NetBIOS) para que se envíen a través de la conexión VPN. 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. Para editar una política IKE, active la casilla de verificación de la política y haga clic en **Editar**. La página *Advanced VPN Setup* cambia:

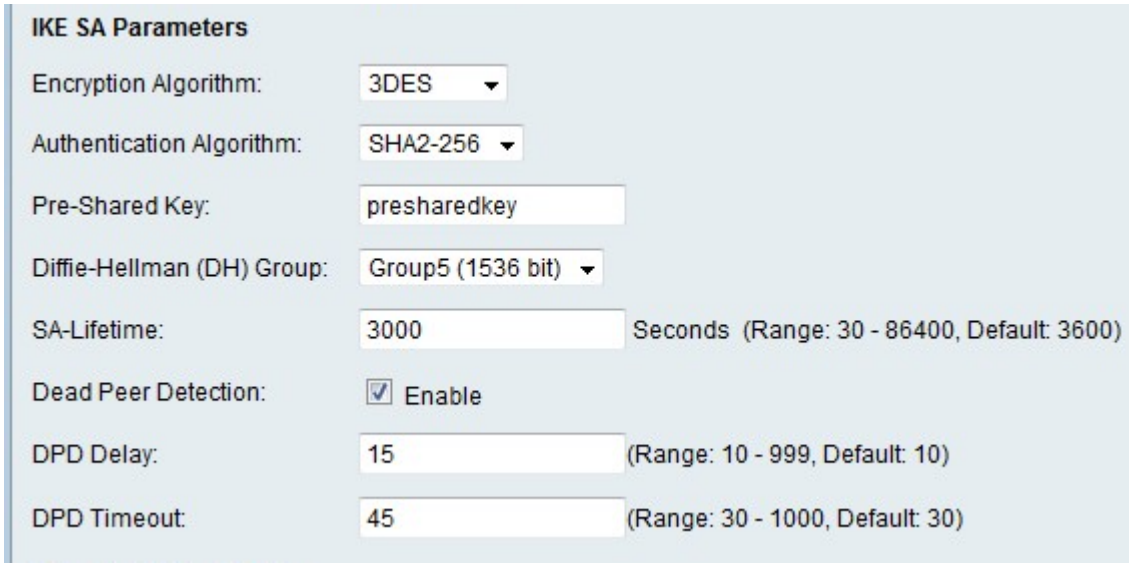


Paso 2. En el campo Policy Name (Nombre de política), introduzca un nombre para la política IKE.

Paso 3. En la lista desplegable Modo de intercambio, elija una opción.

·principal: esta opción permite que la política IKE funcione de forma más segura pero más lenta 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 con menos seguridad que el modo principal. Elija esta opción si se necesita una conexión VPN más rápida.



Paso 4. En la lista desplegable Algoritmo de cifrado, elija una opción.

·DES: el estándar de cifrado de datos (DES) es un método de encriptación antiguo de 56 bits que no es un método de encriptación muy seguro, pero que puede ser necesario para la compatibilidad con versiones anteriores.

·3DES: el triple estándar de cifrado de datos (3DES) es un método de encriptación sencillo de 168 bits que se utiliza para aumentar el tamaño de la clave porque cifra los datos tres veces. Esto proporciona más seguridad que DES, pero menos seguridad que 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. En general, AES también es más rápido y seguro que 3DES. 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 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 5. En la lista desplegable Authentication Algorithm (Algoritmo de autenticación), elija una opción.

·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: Secure Hash Function 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 con un valor hash de 256 bits (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 6. En el campo Pre-Shared Key (Clave precompartida), introduzca una clave precompartida que utilice la política IKE.

Paso 7. En la lista desplegable Grupo Diffie-Hellman (DH), seleccione el grupo DH que utiliza IKE. Los hosts de un grupo DH pueden intercambiar claves sin tener conocimiento

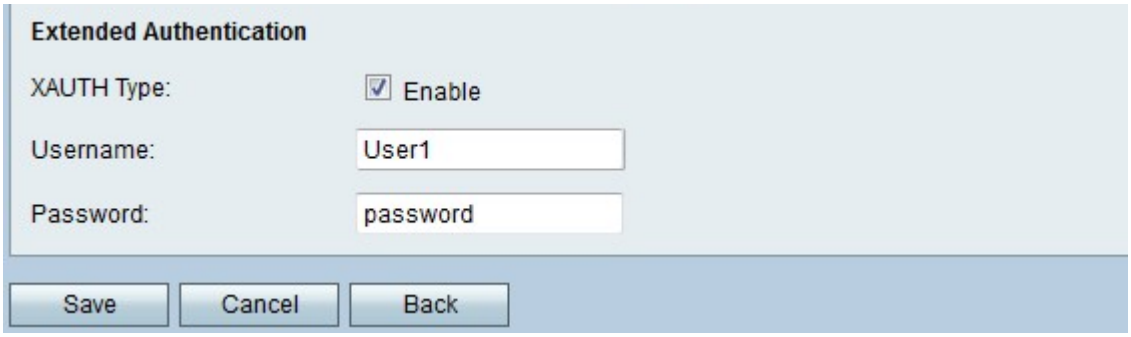
mutuo. Cuanto más alto sea el número de bit del grupo, más seguro será el grupo.

Paso 8. En el campo SA-Lifetime, introduzca cuánto tiempo en segundos dura una SA para la VPN antes de que se renueve la SA.

Paso 9. (Opcional) Active la casilla de verificación **Enable** en el campo Dead Peer Detection para habilitar Dead Peer Detection (DPD). DPD monitorea los pares IKE para ver si un par ha dejado de funcionar. DPD evita el desperdicio de recursos de red en peers inactivos.

Paso 10. (Opcional) Si ha activado DPD en el paso 9, introduzca la frecuencia (en segundos) con la que el par se comprueba si hay actividad en el campo DPD Delay (Retraso de DPD).

Paso 11. (Opcional) Si ha activado DPD en el paso 9, introduzca cuántos segundos esperar antes de que se descarte un par inactivo en el campo DPD Timeout (Tiempo de espera de DPD).



Paso 12. (Opcional) Marque la casilla de verificación **Enable** en el campo XAUTH Type para habilitar Extended Authentication (XAUTH). XAUTH permite que varios usuarios utilicen una única política VPN en lugar de una política VPN para cada usuario.

Paso 13. (Opcional) Si ha activado XAUTH en el paso 12, introduzca el nombre de usuario que se utilizará para la política en el campo Nombre de usuario.

Paso 14. (Opcional) Si ha activado XAUTH en el paso 12, introduzca la contraseña que desea utilizar para la política en el campo Password (Contraseña).

Paso 15. Click **Save**. La página *Advanced VPN Setup* original vuelve a aparecer.

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. Para editar una política VPN, active la casilla de verificación de la política y haga clic en **Editar**. La página *Advanced VPN Setup* cambia:

Advanced VPN Setup

Add / Edit VPN Policy Configuration

Policy Name: VPN1

Policy Type: Manual Policy

Remote Endpoint: IP Address

209.165.201.1 (Hint: 1.2.3.4 or abc.com)

Local Traffic Selection

Local IP: Subnet

IP Address: 192.168.1.0 (Hint: 1.2.3.4)

Subnet Mask: 255.255.255.0 (Hint: 255.255.255.0)

Remote Traffic Selection

Remote IP: Subnet

IP Address: 192.168.2.0 (Hint: 1.2.3.4)

Subnet Mask: 255.255.255.0 (Hint: 255.255.255.0)

Manual Policy Parameters

SPI-Incoming: 0xABCD

SPI-Outgoing: 0x1234

Encryption Algorithm: AES-256

Key-In: 123456789012345678!

Key-Out: 123456789012345678!

Integrity Algorithm: SHA2-256

Key-In: 123456789012345678!

Key-Out: 123456789012345678!

Auto Policy Parameters

SA-Lifetime: 20000 Seconds (Range: 30 - 86400, Default: 28800)

Encryption Algorithm: AES-256

Integrity Algorithm: SHA2-256

PFS Key Group: Enable

DH-Group 1(768 bit)

Select IKE Policy: IKE1

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.

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

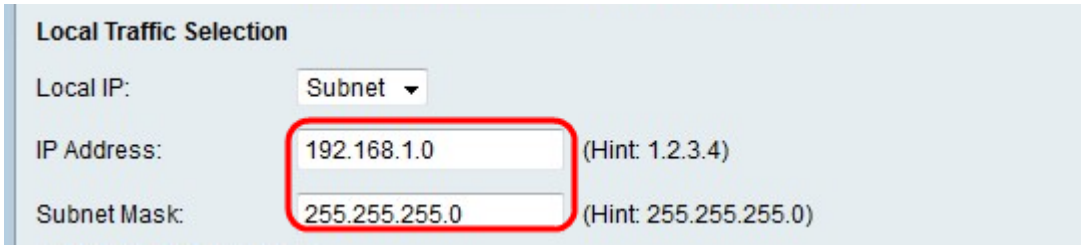
Política automática ·: esta opción utiliza una política IKE para la integridad de los datos y los intercambios de claves de cifrado.

Paso 4. En la lista desplegable Terminal remoto, elija una opción.

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. En la lista desplegable Local IP (IP local), elija una opción.

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

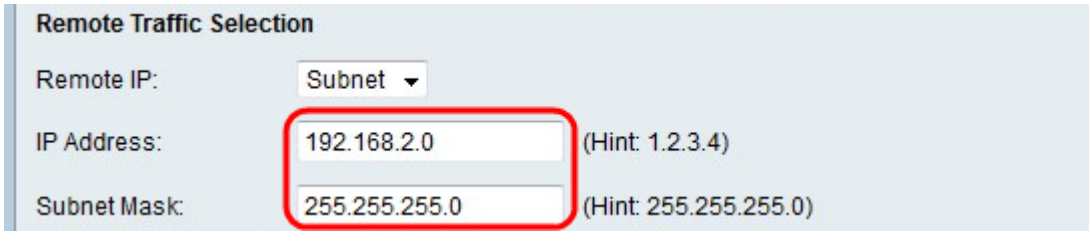
Paso 8. (Opcional) Si eligió Subred en el Paso 6, introduzca la máscara de subred para la subred local en el campo Subnet Mask (Máscara de subred).

Paso 9. En la lista desplegable IP remota, elija una opción.

·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

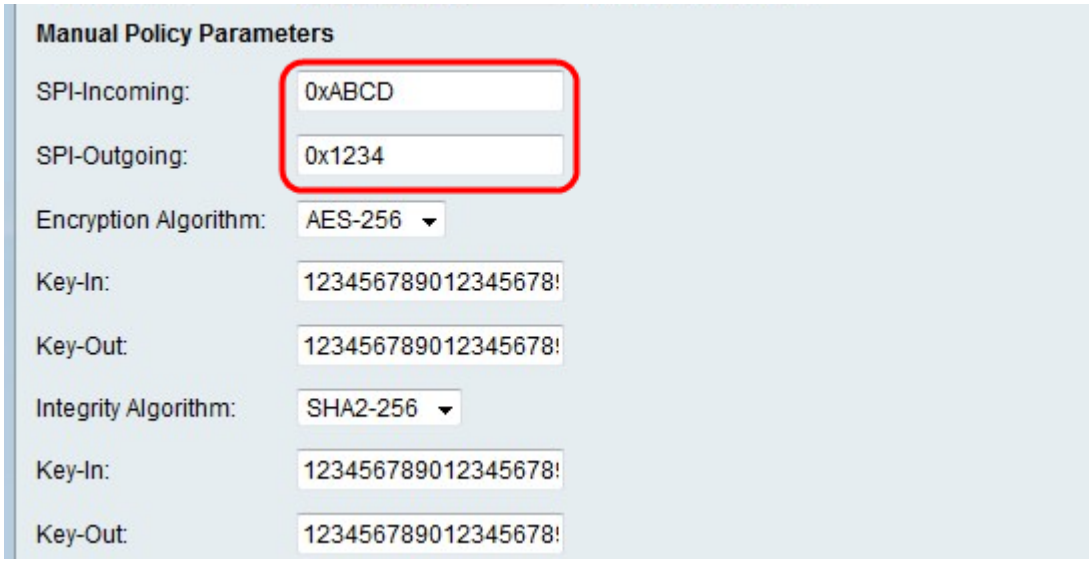
remota.



Paso 10. En el campo IP Address (Dirección IP), introduzca la dirección IP de host o subred de la subred o el host remotos.

Paso 11. (Opcional) Si eligió Subred en el Paso 9, introduzca la máscara de subred para la subred remota en el campo Subnet Mask (Máscara de subred).

Nota: Si selecciona Política Manual en el Paso 3, lleve a cabo los pasos 12 a 19; de lo contrario, omita el paso 20.



Paso 12. En el campo SPI-Incoming, introduzca una etiqueta de tres a ocho caracteres hexadecimales para el índice de parámetros de seguridad (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.

Paso 13. En el campo SPI-Saliente, introduzca entre tres y ocho caracteres hexadecimales para la etiqueta SPI para el tráfico saliente en la conexión VPN.

Paso 14. En la lista desplegable Algoritmo de cifrado, elija una opción.

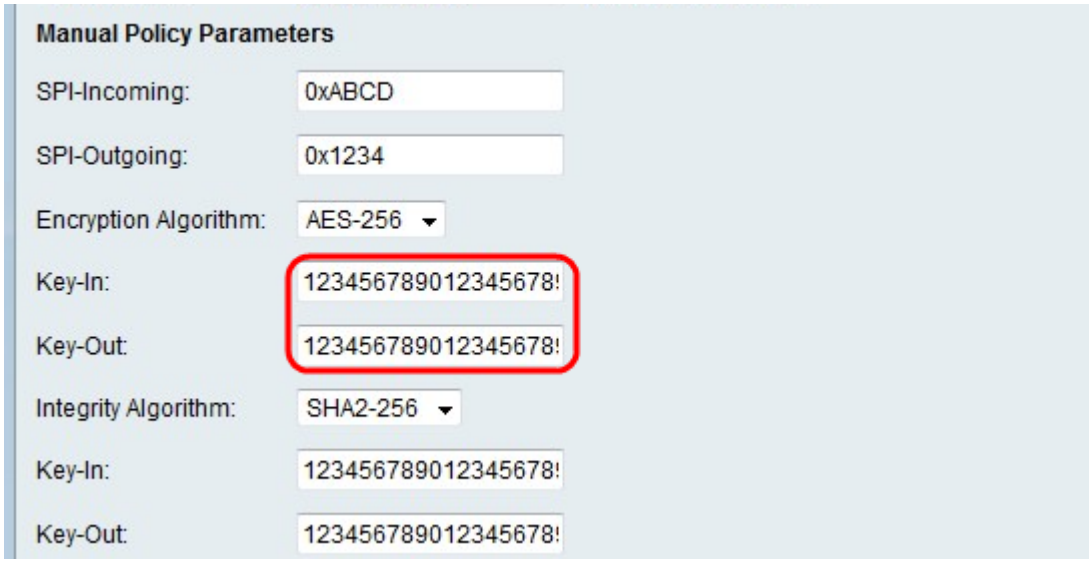
·DES: el estándar de cifrado de datos (DES) es un método de encriptación antiguo de 56 bits que no es un método de encriptación muy seguro, pero que puede ser necesario para la compatibilidad con versiones anteriores.

·3DES: el triple estándar de cifrado de datos (3DES) es un método de encriptación sencillo de 168 bits que se utiliza para aumentar el tamaño de la clave porque cifra los datos tres veces. Esto proporciona más seguridad que DES, pero menos seguridad que 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. En general, AES también es más rápido y seguro que 3DES. 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 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 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 14.

·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.

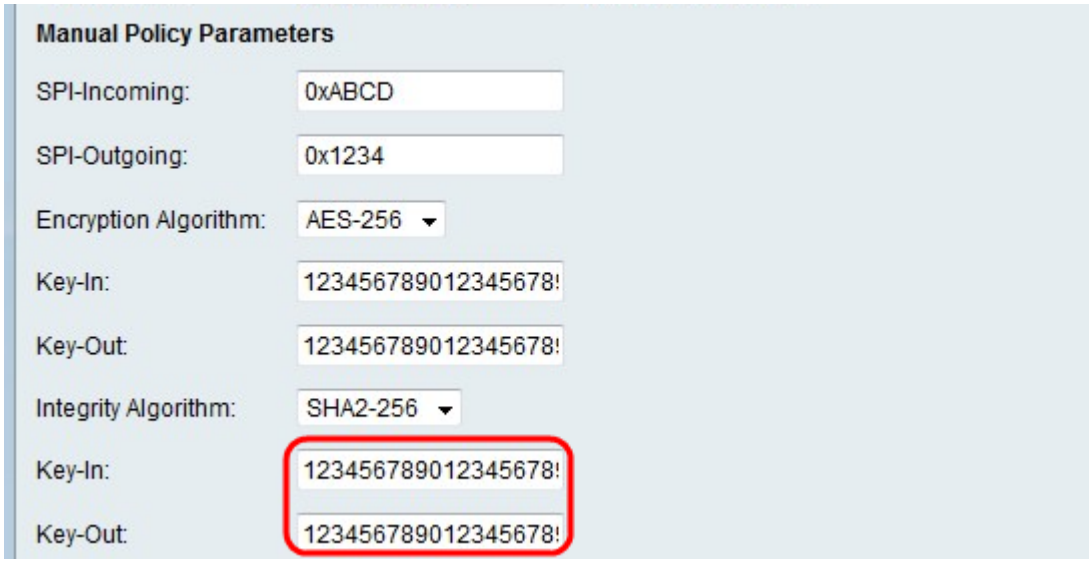
Paso 16. En el campo Key-Out (Clave de salida), introduzca una clave para la directiva saliente. La longitud de la clave depende del algoritmo elegido en el Paso 14. Las longitudes clave son las mismas que en el paso 15.

Paso 17. En la lista desplegable Algoritmo de integridad, elija una opción.

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

·SHA-1: Secure Hash Function 1 (SHA-1) utiliza un valor hash de 160 bits para la integridad de los datos. 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 con un valor hash de 256 bits (SHA2-256) utiliza un valor hash de 256 bits para la integridad de los datos. SHA2-256 es más lento pero seguro que MD5 y SHA-1.



Paso 18. 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 17.

·MD5 utiliza una clave de 16 caracteres.

·SHA-1 utiliza una clave de 20 caracteres.

·SHA2-256 utiliza una clave de 32 caracteres.

Paso 19. 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 17. Las longitudes clave son las mismas que en el paso 18.

Nota: Si selecciona Política automática en el paso 3, lleve a cabo los pasos 20 a 25; Caso contrario, siga con el paso 26.

Paso 20. En el campo SA-Lifetime, introduzca cuánto tiempo dura la SA en segundos antes de la renovación.

Paso 21. En la lista desplegable Algoritmo de cifrado, elija una opción.

·DES: el estándar de cifrado de datos (DES) es un método de encriptación antiguo de 56 bits que no es un método de encriptación muy seguro, pero que puede ser necesario para la compatibilidad con versiones anteriores.

·3DES: el triple estándar de cifrado de datos (3DES) es un método de encriptación sencillo

de 168 bits que se utiliza para aumentar el tamaño de la clave porque cifra los datos tres veces. Esto proporciona más seguridad que DES, pero menos seguridad que 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. En general, AES también es más rápido y seguro que 3DES. 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 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 22. En la lista desplegable Algoritmo de integridad, elija una opción.

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

·SHA-1: Secure Hash Function 1 (SHA-1) utiliza un valor hash de 160 bits para la integridad de los datos. 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 con un valor hash de 256 bits (SHA2-256) utiliza un valor hash de 256 bits para la integridad de los datos. SHA2-256 es más lento pero seguro que MD5 y SHA-1.

Paso 23. Marque la casilla de verificación **Enable** en PFS Key Group para habilitar Perfect Forward Secrecy (PFS). PFS aumenta la seguridad de VPN, pero reduce la velocidad de conexión.

Paso 24. (Opcional) Si optó por activar PFS en el Paso 23, elija un grupo Diffie-Hellman (DH) para unirse a la lista desplegable siguiente. Cuanto mayor sea el número de grupo, mayor será la seguridad del grupo.

Paso 25. En la lista desplegable Seleccionar política IKE, elija la política IKE que desea utilizar para la política VPN.

Nota: Si hace clic en **Ver**, se le dirige a la sección de configuración IKE de la página *Advanced VPN Setup*.

Paso 26. Click **Save**. La página *Advanced VPN Setup* original vuelve a aparecer.

Paso 27. Click **Save**.