

# Configuración de la red privada virtual (VPN) avanzada en el firewall RV110W

## Objetivo

La red privada virtual (VPN) utiliza la red pública o Internet para establecer una red privada con el fin de comunicarse de forma segura. Un intercambio de claves de Internet (IKE) es un protocolo que establece una comunicación segura entre dos redes. Se utiliza para intercambiar una clave antes del flujo de tráfico, lo que garantiza la autenticidad de ambos extremos del túnel VPN.

Ambos extremos de la VPN deben seguir la misma política de VPN para comunicarse entre sí con éxito.

El objetivo de este documento es explicar cómo agregar un perfil IKE y configurar la política VPN en el RV110W Wireless Router.

## Dispositivos aplicables

·RV110W

## Versión del software

•1.2.0.9

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

IKE Policy Table							
<input type="checkbox"/>	Name	Mode	Local	Remote	Encryption	Authentication	DH
<input type="checkbox"/>	No data to display						
<input type="button" value="Add Row"/>	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>					

VPN Policy Table							
<input type="checkbox"/>	Status	Name	Type	Local	Remote	Authentication	Encryption
<input type="checkbox"/>	No data to display						
<input type="button" value="Add Row"/>	<input type="button" value="Edit"/>	<input type="button" value="Enable"/>	<input type="button" value="Disable"/>	<input type="button" value="Delete"/>			

**Advanced VPN Setup**

IKE Policy Table				
<input type="checkbox"/>	Name	Mode	Local	Remote
No data to display				
<input type="button" value="Add Row"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>				

VPN Policy Table				
<input type="checkbox"/>	Status	Name	Type	Local
No data to display				
<input type="button" value="Add Row"/> <input type="button" value="Edit"/> <input type="button" value="Enable"/> <input type="button" value="Disable"/> <input type="button" value="Delete"/>				

Paso 2. Haga clic en **Agregar fila** para crear una nueva política IKE. Se abre la página *Advanced VPN Setup*:

**Advanced VPN Setup**

**Add / Edit IKE Policy Configuration**

Policy Name:

Exchange Mode:  ▼

**IKE SA Parameters**

Encryption Algorithm:  ▼

Authentication Algorithm:  ▼

Pre-Shared Key:

Diffie-Hellman (DH) Group:  ▼

SA-Lifetime:  Seconds (Range: 30 - 86400, Default: 3600)

Dead Peer Detection:  Enable

DPD Delay:  (Range: 10 - 999, Default: 10)

DPD Timeout:  (Range: 30 - 1000, Default: 30)

Paso 3. En el campo *Policy Name*, ingrese un nombre para la política IKE para identificarlo fácilmente.

### Advanced VPN Setup

**Add / Edit IKE Policy Configuration**

Policy Name:

Exchange Mode: Main  
Main  
Aggressive

**IKE SA Parameters**

Encryption Algorithm:

Authentication Algorithm:

Pre-Shared Key:

Diffie-Hellman (DH) Group:

SA-Lifetime:  Seconds (Range: 30 - 86400, Default: 3600)

Dead Peer Detection:  Enable

DPD Delay:  (Range: 10 - 999, Default: 10)

DPD Timeout:  (Range: 30 - 1000, Default: 30)

Paso 4. Elija una opción de la lista desplegable *Modo Exchange*:

·principal: 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: 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.

### Advanced VPN Setup

**Add / Edit IKE Policy Configuration**

Policy Name:

Exchange Mode:

**IKE SA Parameters**

Encryption Algorithm: 

- DES
- 3DES
- AES-128
- AES-192
- AES-256

Authentication Algorithm:

Pre-Shared Key:

Diffie-Hellman (DH) Group:

SA-Lifetime:  Seconds (Range: 30 - 86400, Default: 3600)

Dead Peer Detection:  Enable

DPD Delay:  (Range: 10 - 999, Default: 10)

DPD Timeout:  (Range: 30 - 1000, Default: 30)

Paso 5. Elija un algoritmo de la lista desplegable *Algoritmo de cifrado*:

·DES: el estándar de cifrado de datos (DES) utiliza un tamaño de clave de 56 bits para el cifrado de datos. DES está desactualizado y se debe utilizar únicamente si un solo terminal 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. En general, AES también es más rápido pero menos seguro que 3DES, pero 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.

### Advanced VPN Setup

**Add / Edit IKE Policy Configuration**

Policy Name:

Exchange Mode:

**IKE SA Parameters**

Encryption Algorithm:

Authentication Algorithm:

Pre-Shared Key:

Diffie-Hellman (DH) Group:

SA-Lifetime:  Seconds (Range: 30 - 86400, Default: 3600)

Dead Peer Detection:  Enable

DPD Delay:  (Range: 10 - 999, Default: 10)

DPD Timeout:  (Range: 30 - 1000, Default: 30)

Paso 6. Elija la autenticación deseada en la lista desplegable *Algoritmo de autenticación*:

·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.

### Advanced VPN Setup

**Add / Edit IKE Policy Configuration**

Policy Name:

Exchange Mode:

**IKE SA Parameters**

Encryption Algorithm:

Authentication Algorithm:

**Pre-Shared Key:**

Diffie-Hellman (DH) Group:

SA-Lifetime:  Seconds (Range: 30 - 86400, Default: 3600)

Dead Peer Detection:  Enable

DPD Delay:  (Range: 10 - 999, Default: 10)

DPD Timeout:  (Range: 30 - 1000, Default: 30)

Paso 7. En el campo *Pre-Shared Key*, ingrese una clave previamente compartida que utilice la política IKE.

### Advanced VPN Setup

**Add / Edit IKE Policy Configuration**

Policy Name:

Exchange Mode:

**IKE SA Parameters**

Encryption Algorithm:

Authentication Algorithm:

Pre-Shared Key:

Diffie-Hellman (DH) Group:

SA-Lifetime:  Seconds (Range: 30 - 86400, Default: 3600)

Dead Peer Detection:  Enable

DPD Delay:  (Range: 10 - 999, Default: 10)

DPD Timeout:  (Range: 30 - 1000, Default: 30)

Paso 8. En la lista desplegable *Diffie-Hellman (DH) Group*, elija 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.

- Grupo 1 - 768 bits: la clave de seguridad más baja y el grupo de autenticación más inseguro. Pero requiere menos tiempo para calcular las claves IKE. Se prefiere esta opción si la velocidad de la red es baja.
- Grupo 2 - 1024 bits: la clave de mayor resistencia y el grupo de autenticación más seguro. Pero necesita un tiempo para calcular las claves IKE.
- Grupo 5 - 1536 bits: representa la clave de máxima seguridad y el grupo de autenticación más seguro. Necesita más tiempo para calcular las claves IKE. Se prefiere si la velocidad de la red es alta.

**Advanced VPN Setup**

Add / Edit IKE Policy Configuration

Policy Name:

Exchange Mode:

**IKE SA Parameters**

Encryption Algorithm:

Authentication Algorithm:

Pre-Shared Key:

Diffie-Hellman (DH) Group:

SA-Lifetime:  Seconds (Range: 30 - 86400, Default: 3600)

Dead Peer Detection:  Enable

DPD Delay:  (Range: 10 - 999, Default: 10)

DPD Timeout:  (Range: 30 - 1000, Default: 30)

Paso 9. Introduzca cuánto tiempo (en segundos) dura una SA para la VPN antes de que se renueve la SA en el campo *SA-Lifetime*.

Paso 10. (Opcional) Marque la casilla de verificación **Enable** en el campo *Dead Peer Detection* para habilitar Dead Peer Detection. Deed Peer Detection monitorea los pares IKE para ver si un par ha dejado de funcionar. La Detección de Peer Muerto evita el desperdicio de recursos de red en peers inactivos.

Paso 11. (Opcional) Si ha activado Deed Peer Detection en el Paso 9, introduzca la frecuencia (en segundos) con la que el par se comprueba si hay actividad en el campo *Deed Peer Delay*.

Paso 12. (Opcional) Si ha activado Deed Peer Detection en el Paso 9, introduzca cuántos segundos esperar antes de que se descarte un par inactivo en el campo Deed Peer Detection Timeout (Tiempo de espera de detección de puntos inactivos).

Paso 13. Haga clic en **Guardar** para aplicar todos los parámetros.

## Configuración de Política VPN

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

Advanced VPN Setup

<input type="checkbox"/>	Name	Mode	Local	Remote	Encryption	Authentication	DH
<input type="checkbox"/>	No data to display						
Add Row Edit Delete							

<input type="checkbox"/>	Status	Name	Type	Local	Remote	Authentication	Encryption
<input type="checkbox"/>	No data to display						
Add Row Edit Enable Disable Delete							

Save Cancel

IPSec Connection Status

Advanced VPN Setup

 Configuration settings have been saved successfully

<input type="checkbox"/>	Name	Mode	Local	Remote
<input type="checkbox"/>	policy1	Aggressive		
Add Row Edit Delete				

<input type="checkbox"/>	Status	Name	Type	Local
<input type="checkbox"/>	No data to display			
Add Row Edit Enable Disable Delete				

Save Cancel

IPSec Connection Status

Paso 2. Haga clic en **Agregar** fila desde la *Tabla de Políticas de VPN*. Aparece la ventana *Advanced VPN Policy Setup*:

Advanced VPN Setup

**Add / Edit VPN Policy Configuration**

Policy Name:

Policy Type:  ▼

Remote Endpoint:  ▼

(Hint: 1.2.3.4 or abc.com)

**Local Traffic Selection**

Local IP:  ▼

IP Address:  (Hint: 1.2.3.4)

Subnet Mask:  (Hint: 255.255.255.0)

**Remote Traffic Selection**

## Agregar/Editar configuración de política VPN



Advanced VPN Setup

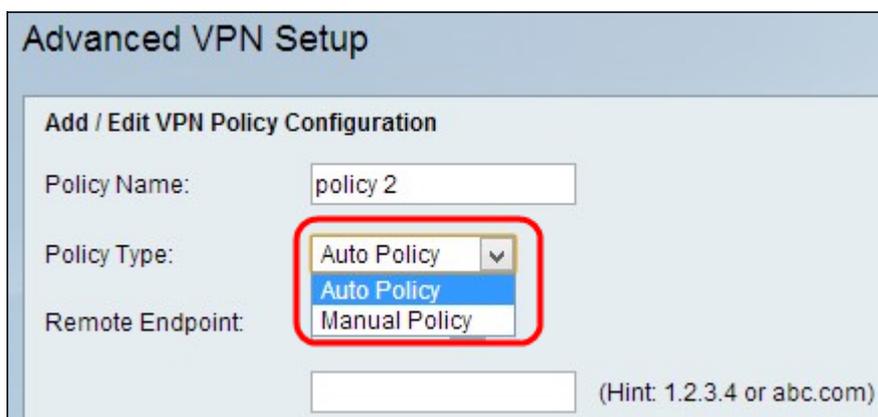
Add / Edit VPN Policy Configuration

Policy Name:

Policy Type:

Remote Endpoint:  (Hint: 1.2.3.4 or abc.com)

Paso 1. Introduzca un nombre único para la política en el campo *Policy Name* para identificarlo fácilmente.



Advanced VPN Setup

Add / Edit VPN Policy Configuration

Policy Name:

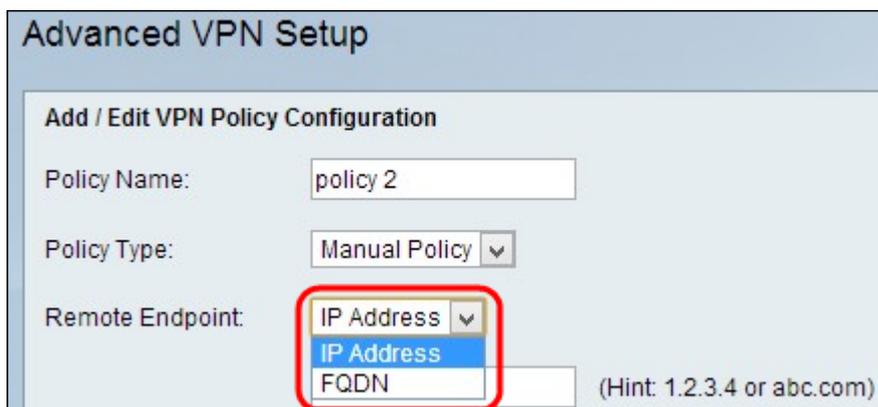
Policy Type:

Remote Endpoint:  (Hint: 1.2.3.4 or abc.com)

Paso 2. Elija el tipo de directiva adecuado en la lista desplegable *Tipo de directiva*.

Política automática :: los parámetros se pueden establecer automáticamente. En este caso, además de las políticas, se requiere que el protocolo IKE (Intercambio de claves de Internet) negocie entre los dos terminales VPN.

Política manual :: en este caso, todas las configuraciones que incluyen las claves para el túnel VPN, se introducen manualmente para cada terminal.



Advanced VPN Setup

Add / Edit VPN Policy Configuration

Policy Name:

Policy Type:

Remote Endpoint:  (Hint: 1.2.3.4 or abc.com)

Paso 3. Elija el tipo de identificador IP que identifica el gateway en el extremo remoto de la lista desplegable *Remote Endpoint*.

Dirección IP :: dirección IP del gateway en el extremo remoto. Si elige esta opción, introduzca la dirección IP en el campo correspondiente.

·FQDN (nombre de dominio completamente calificado): introduzca el nombre de dominio

completamente calificado del gateway en el extremo remoto. Si elige esta opción, introduzca el nombre de dominio completo en el campo proporcionado.

## Selección de tráfico local



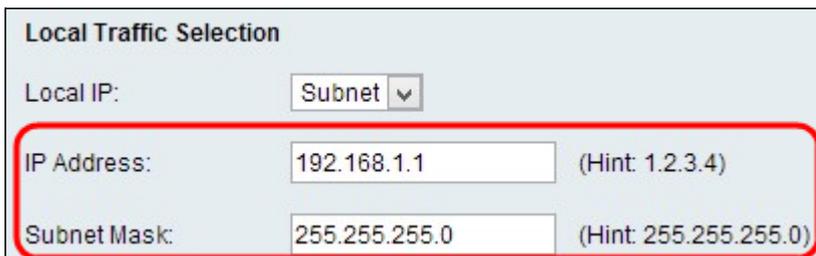
The screenshot shows the 'Local Traffic Selection' form. The 'Local IP:' dropdown menu is open, showing 'Single' (selected) and 'Subnet' options. The 'IP Address:' and 'Subnet Mask:' fields are empty. A red box highlights the dropdown menu.

Paso 1. Elija el tipo de identificador que desea proporcionar para el punto final en la lista desplegable *IP local*.



The screenshot shows the 'Local Traffic Selection' form with 'Single' selected in the 'Local IP:' dropdown. The 'IP Address:' field contains '192.168.1.1' and is highlighted with a red box. The 'Subnet Mask:' field is empty.

·Single: esto limita la política a un host. Si elige esta opción, ingrese la dirección IP en el campo *IP address* .



The screenshot shows the 'Local Traffic Selection' form with 'Subnet' selected in the 'Local IP:' dropdown. The 'IP Address:' field contains '192.168.1.1' and the 'Subnet Mask:' field contains '255.255.255.0'. Both fields are highlighted with a red box.

·Subred: es una máscara que define los límites de una IP. Esto sólo permite que los hosts de la subred especificada se conecten a la VPN. Para conectarse a VPN, un ordenador se selecciona mediante una operación AND lógica. Se selecciona un equipo si la IP se encuentra dentro del mismo rango requerido. Si elige esta opción, introduzca la dirección IP y la subred en los campos Dirección IP y Subred.

## Selección de tráfico remoto



The screenshot shows the 'Remote Traffic Selection' form. The 'Remote IP:' dropdown menu is open, showing 'Single' (selected) and 'Subnet' options. The 'IP Address:' and 'Subnet Mask:' fields are empty. A red box highlights the dropdown menu.

Paso 1. Elija el tipo de identificador que desea proporcionar para el punto final en la lista desplegable *IP local*:

**Remote Traffic Selection**

Remote IP:  ▼

IP Address:  (Hint: 1.2.3.4)

Subnet Mask:  (Hint: 255.255.255.0)

·Single: esto limita la política a un host. Si elige esta opción, ingrese la dirección IP en el campo *IP address*.

**Remote Traffic Selection**

Remote IP:  ▼

IP Address:  (Hint: 1.2.3.4)

Subnet Mask:  (Hint: 255.255.255.0)

·Subred: es una máscara que define los límites de una IP. Esto sólo permite que los hosts de la subred especificada se conecten a la VPN. Para conectarse a VPN, un ordenador se selecciona mediante una operación AND lógica. Se selecciona un equipo si la IP se encuentra dentro del mismo rango requerido. Si elige esta opción, introduzca la dirección IP y la subred en los campos Dirección IP y Subred.

## Parámetros de política manual

Para configurar los parámetros de política manuales, elija **Manual Policy** de la *lista desplegable Tipo de política* en el Paso 2 de la sección *Agregar/Editar configuración de política de VPN*.

**Manual Policy Parameters**

SPI-Incoming:

SPI-Outgoing:

Encryption Algorithm:  ▼

Key-In:

Key-Out:

Integrity Algorithm:  ▼

Key-In:

Key-Out:

Paso 1. Introduzca un valor hexadecimal entre 3 y 8 en el campo *SPI-Incoming*. La inspección exhaustiva de paquetes (SPI) es una tecnología denominada Inspección profunda de paquetes. SPI implementa una serie de funciones de seguridad que ayudan a mantener la seguridad de la red del equipo. El valor SPI-Incoming se corresponde con el SPI-Outgoing del dispositivo anterior. Cualquier valor es aceptable, siempre y cuando el extremo VPN remoto tenga el mismo valor en su campo *SPI-Saliente*.

Paso 2. Introduzca un valor hexadecimal entre 3 y 8 en el campo *SPI-Saliente*.

**Manual Policy Parameters**

SPI-Incoming:

SPI-Outgoing:

Encryption Algorithm: 

- AES-128
- 3DES
- DES
- AES-128
- AES-192
- AES-256

Key-In:

Key-Out:

Integrity Algorithm:

Key-In:

Key-Out:

Paso 3. Elija el algoritmo de cifrado adecuado en la lista desplegable Algoritmo de cifrado.

·DES: el estándar de cifrado de datos (DES) utiliza un tamaño de clave de 56 bits para el cifrado de datos. DES está desactualizado y se debe utilizar únicamente si un solo terminal 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. En general, AES también es más rápido pero menos seguro que 3DES, pero 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.

**Manual Policy Parameters**

SPI-Incoming:

SPI-Outgoing:

Encryption Algorithm:

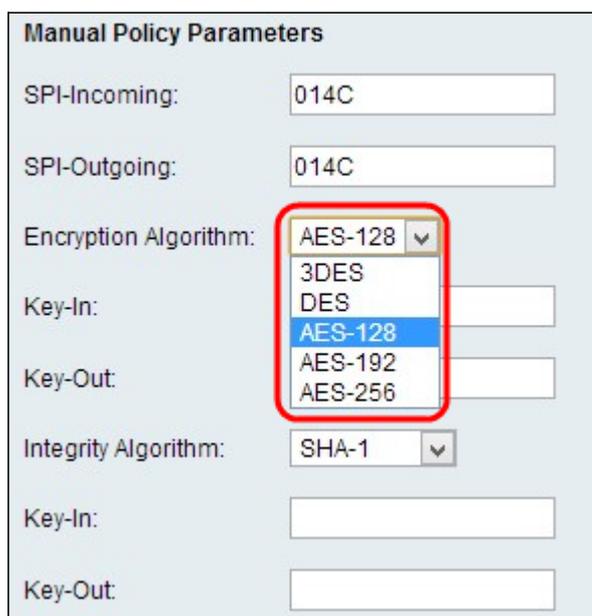
Integrity Algorithm:

Key-In:

Key-Out:

Paso 4. Introduzca la clave de cifrado de la política entrante en el campo *Key-In*. La longitud de la clave depende del algoritmo elegido en el Paso 3.

Paso 5. Introduzca la clave de cifrado de la política saliente en el campo *Key-Out*.



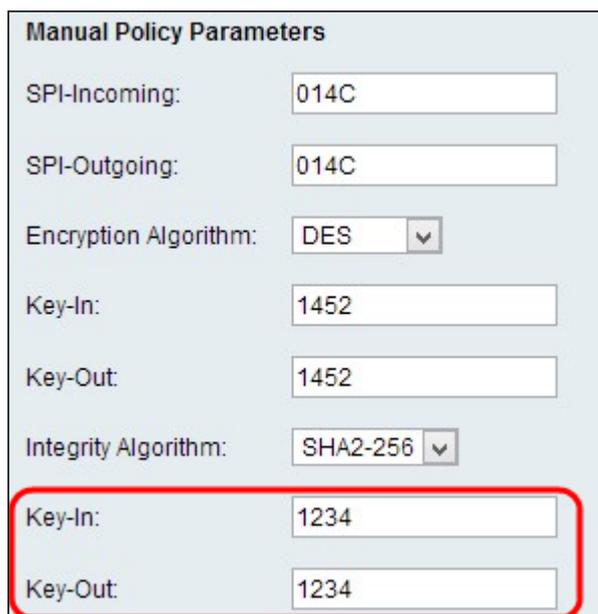
The screenshot shows the 'Manual Policy Parameters' form. The 'Encryption Algorithm' dropdown menu is open, showing options: AES-128 (selected), 3DES, DES, AES-128, AES-192, and AES-256. The 'Key-In' and 'Key-Out' fields are empty. The 'Integrity Algorithm' dropdown is set to SHA-1. The 'SPI-Incoming' and 'SPI-Outgoing' fields contain '014C'.

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

·MD5: este algoritmo especifica la longitud de la clave en 16 caracteres. Message-Digest Algorithm 5 (MD5) no es resistente a las colisiones y es adecuado para aplicaciones como certificados SSL o firmas digitales que se basan en esta propiedad. MD5 comprime cualquier flujo de bytes en un valor de 128 bits, pero SHA lo comprime en un valor de 160 bits. MD5 es ligeramente más barato de calcular, sin embargo MD5 es una versión más antigua del algoritmo hash y es vulnerable a los ataques de colisión.

·SHA1: Secure Hash Algorithm versión 1 (SHA1) es una función hash de 160 bits más segura que MD5, pero tarda más tiempo en calcularse.

·SHA2-256: este algoritmo especifica la longitud de la clave en 32 caracteres.



The screenshot shows the 'Manual Policy Parameters' form. The 'Encryption Algorithm' dropdown is set to DES. The 'Key-In' and 'Key-Out' fields contain '1452'. The 'Integrity Algorithm' dropdown is set to SHA2-256. The 'SPI-Incoming' and 'SPI-Outgoing' fields contain '014C'. The 'Key-In' and 'Key-Out' fields at the bottom are highlighted with a red box and contain '1234'.

Paso 7. Introduzca la clave de integridad (para ESP con modo de integridad) para la política entrante. La longitud de la clave depende del algoritmo elegido en el Paso 6.

Paso 8. Introduzca la clave de integridad de la política saliente en el campo Key-Out (Clave de salida). La conexión VPN se configura para el saliente al entrante, por lo tanto las claves salientes

de un extremo deben coincidir con las claves entrantes del otro extremo.

**Nota:** SPI-Incoming y Outgoing, Encryption Algorithm, Integrity Algorithm y Keys deben ser los mismos en el otro extremo del túnel VPN para una conexión correcta.

## Parámetros de política automática

Auto Policy Parameters

SA-Lifetime: 2800 Seconds (Range: 30 - 86400, Default: 28800)

Encryption Algorithm: AES-128

Integrity Algorithm: SHA-1

PFS Key Group:  Enable

DH-Group 1(768 bit)

Select IKE Policy: policy1

View

Paso 1. Introduzca la duración de la asociación de seguridad (SA) en segundos en el campo Tiempo de vida de SA. La vida útil de SA es cuando cualquier clave ha alcanzado su vida útil, cualquier SA asociada se renueva automáticamente.

Auto Policy Parameters

SA-Lifetime: 2800 Seconds (Range: 30 - 86400, Default: 28800)

Encryption Algorithm: AES-128

Integrity Algorithm: SHA-1

PFS Key Group:  Enable

DH-Group 1(768 bit)

Select IKE Policy: policy1

View

Paso 2. Elija el algoritmo de cifrado adecuado en la lista desplegable Algoritmo de cifrado:

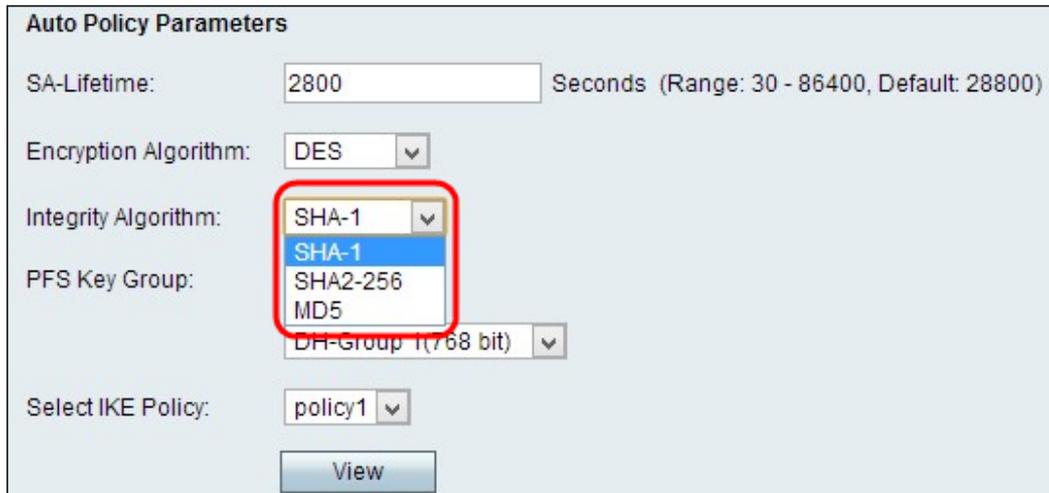
·DES: el estándar de cifrado de datos (DES) utiliza un tamaño de clave de 56 bits para el cifrado de datos. DES está desactualizado y se debe utilizar únicamente si un solo terminal admite DES.

·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. En general, AES también es más rápido pero menos seguro que 3DES, pero 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.



Auto Policy Parameters

SA-Lifetime: 2800 Seconds (Range: 30 - 86400, Default: 28800)

Encryption Algorithm: DES

Integrity Algorithm: SHA-1

PFS Key Group: SHA2-256

DH-Group 1(768 bit)

Select IKE Policy: policy1

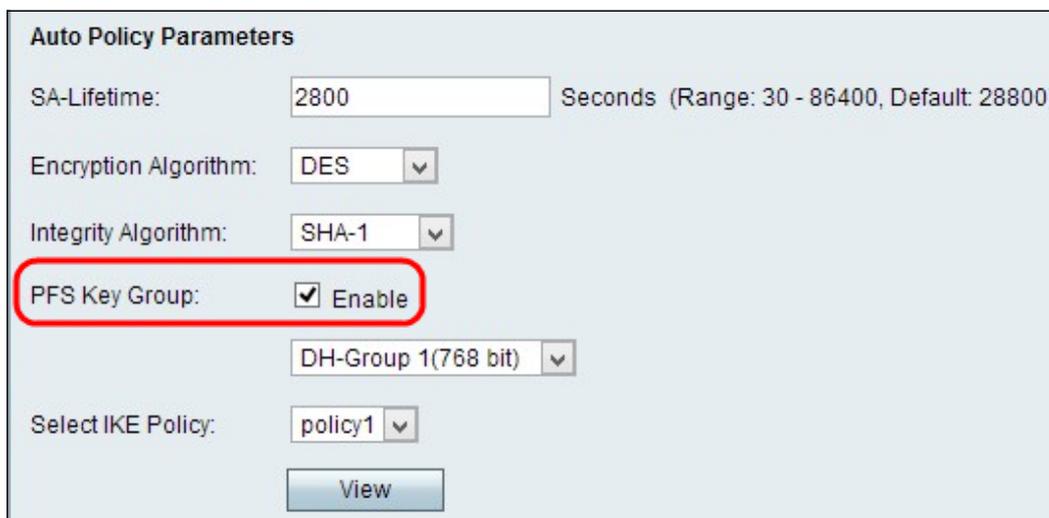
View

Paso 3. Elija el algoritmo de integridad adecuado de la lista desplegable Algoritmo de integridad. Este algoritmo verifica la integridad de los datos.

·MD5: este algoritmo especifica la longitud de la clave en 16 caracteres. Message-Digest Algorithm 5 (MD5) no es resistente a las colisiones y es adecuado para aplicaciones como certificados SSL o firmas digitales que se basan en esta propiedad. MD5 comprime cualquier flujo de bytes en un valor de 128 bits, pero SHA lo comprime en un valor de 160 bits. MD5 es ligeramente más barato de calcular, sin embargo MD5 es una versión más antigua del algoritmo hash y es vulnerable a los ataques de colisión.

·SHA1: Secure Hash Algorithm versión 1 (SHA1) es una función hash de 160 bits más segura que MD5, pero tarda más tiempo en calcularse.

·SHA2-256: este algoritmo especifica la longitud de la clave en 32 caracteres.



Auto Policy Parameters

SA-Lifetime: 2800 Seconds (Range: 30 - 86400, Default: 28800)

Encryption Algorithm: DES

Integrity Algorithm: SHA-1

PFS Key Group:  Enable

DH-Group 1(768 bit)

Select IKE Policy: policy1

View

Paso 4. (Opcional) Marque la casilla de verificación **Enable** en el campo *PFS Key Group* para habilitar Perfect Forward Secrecy, que es para mejorar la seguridad.

**Auto Policy Parameters**

SA-Lifetime: 2800 Seconds (Range: 30 - 86400, Default: 28800)

Encryption Algorithm: DES

Integrity Algorithm: SHA-1

PFS Key Group:  Enable

Select IKE Policy: **DH-Group 1(768 bit)**  
 DH-Group 2(1024 bit)  
 DH-Group 5(1536 bit)

View

Paso 5. Si ha activado **Enable** en el Paso 4, elija el intercambio de claves Diffie-Hellman apropiado en la lista desplegable del campo *Grupo de claves PFS*.

·Grupo 1 - 768 bits: representa la clave de seguridad más baja y el grupo de autenticación más inseguro. Pero necesita menos tiempo para calcular las claves IKE. Se prefiere si la velocidad de la red es baja.

·Grupo 2 - 1024 bits: representa una clave de mayor resistencia y un grupo de autenticación más seguro. Pero necesita un tiempo para calcular las claves IKE.

·Grupo 5 - 1536 bits: representa la clave de máxima seguridad y el grupo de autenticación más seguro. Necesita más tiempo para calcular las claves IKE. Se prefiere si la velocidad de la red es alta.

**Auto Policy Parameters**

SA-Lifetime: 2800 Seconds (Range: 30 - 86400, Default: 28800)

Encryption Algorithm: DES

Integrity Algorithm: SHA-1

PFS Key Group:  Enable

DH-Group 1(768 bit)

Select IKE Policy: **policy1**  
 policy1

view

Paso 6. Elija la política IKE adecuada en la lista desplegable *Seleccionar 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). Para que una VPN funcione correctamente, las políticas IKE para ambos puntos finales deben ser idénticas.

Paso 7. Haga clic en **Guardar** para aplicar todos los parámetros.

**Nota:** El tiempo de vida, el algoritmo de cifrado, el algoritmo de integridad, el grupo de claves PFS y la política IKE deben ser los mismos en el otro extremo del túnel VPN para una conexión correcta.

Si desea ver más artículos sobre el RV110W, haga clic [aquí](#).