Configuración de la política de intercambio de claves de Internet (IKE) en los routers VPN RV130 y RV130W

Objetivo

Intercambio de claves de Internet (IKE) es un protocolo que establece una comunicación segura entre dos redes. Con IKE, los paquetes se cifran y bloquean y desbloquean con claves utilizadas por dos partes.

Debe crear una política de intercambio de claves de Internet antes de configurar una política VPN. Consulte *Configuración de la Política VPN en RV130 y RV130W* para obtener más información.

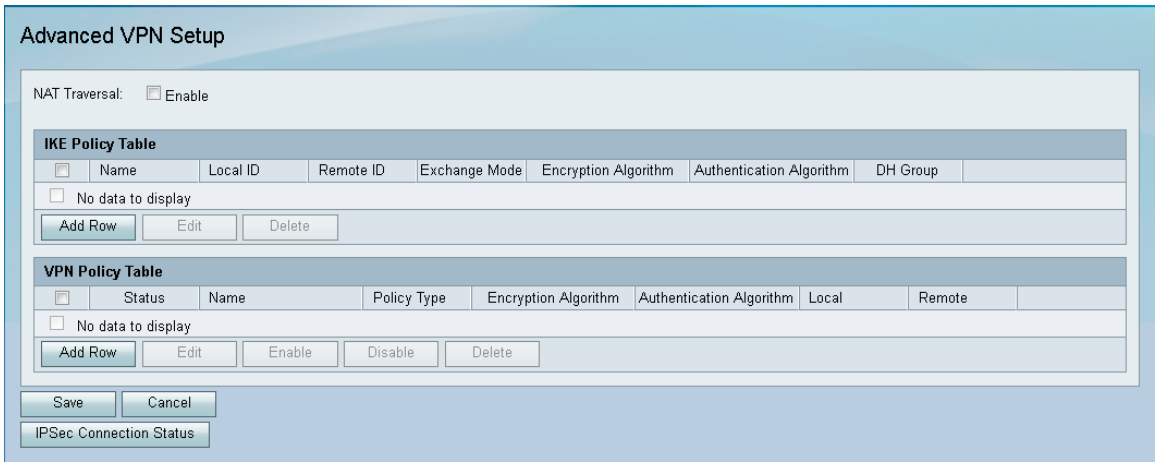
El objetivo de este documento es mostrarle cómo agregar un perfil IKE a los routers VPN RV130 y RV130W.

Dispositivos aplicables

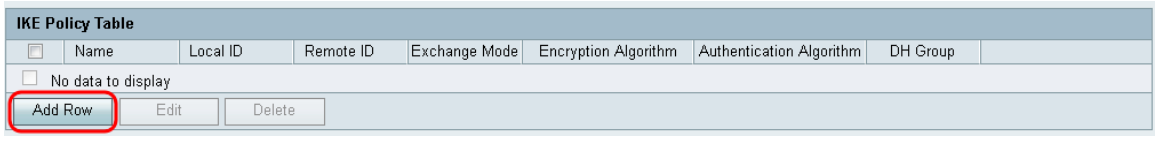
·RV130
· RV130W

Pasos del procedimiento

Paso 1. Utilice la utilidad de configuración del router para seleccionar **VPN > VPN IPSec de sitio a sitio > Configuración VPN avanzada** en el menú de la izquierda. Aparecerá la página *Advanced VPN Setup*:

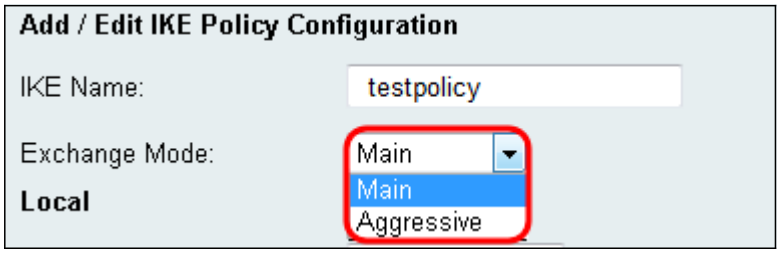


Paso 2. En la Tabla de Políticas IKE, haga clic en **Agregar Fila**. Aparecerá una nueva ventana:



Paso 3. Introduzca un nombre para la política IKE en el campo *Nombre IKE*.

Paso 4. En el menú desplegable *Exchange Mode*, elija el modo en el que se utiliza un intercambio de claves para establecer una comunicación segura.

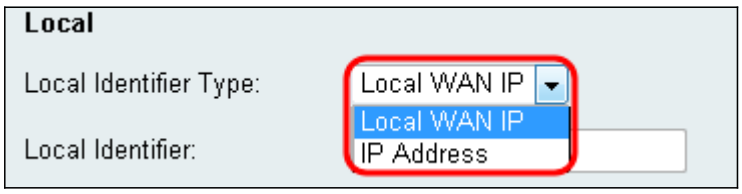


Las opciones disponibles se definen de la siguiente manera:

·Principal: protege la identidad de los compañeros para aumentar la seguridad.

·Agresivo: sin protección de la identidad del mismo nivel, pero proporciona una conexión más rápida.

Paso 5. En el menú desplegable *Tipo de Identificador Local*, seleccione el tipo de identidad que tiene el perfil.

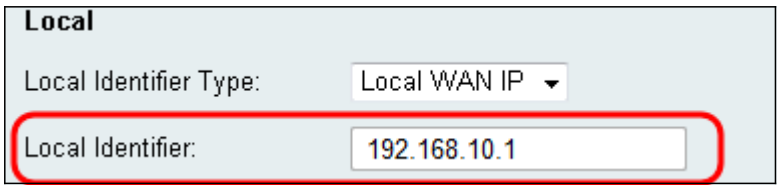


Las opciones disponibles se definen de la siguiente manera:

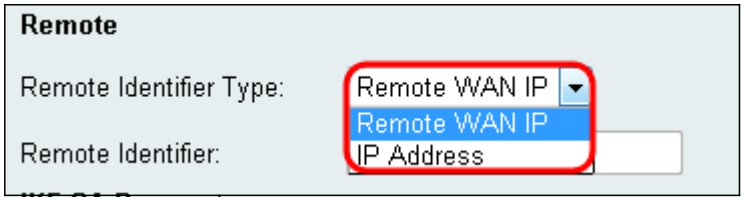
·IP de WAN local (Internet): se conecta a través de Internet.

·Dirección IP: cadena única de números separados por puntos que identifica cada máquina que utiliza el protocolo de Internet para comunicarse a través de una red.

Paso 6. (Opcional) Si selecciona **IP Address** en la lista desplegable del paso 5, introduzca la dirección IP local en el campo *Local Identifier*.



Paso 7. En el menú desplegable *Remote Identifier Type*, elija el tipo de identidad que tiene el perfil.

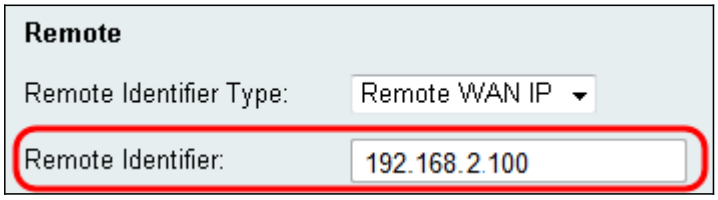


Las opciones disponibles se definen de la siguiente manera:

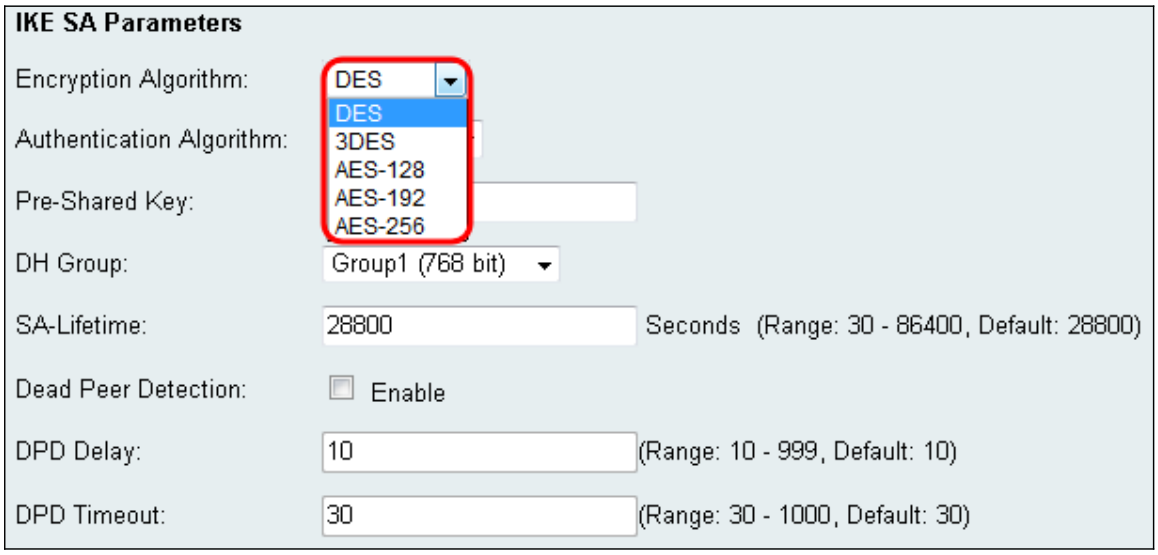
·IP de WAN local (Internet): se conecta a través de Internet.

·Dirección IP: cadena única de números separados por puntos que identifica cada máquina que utiliza el protocolo de Internet para comunicarse a través de una red.

Paso 8. (Opcional) Si selecciona **IP Address** en la lista desplegable del paso 7, introduzca la dirección IP remota en el campo *Remote Identifier*.



Paso 9. En el menú desplegable *Algoritmo de cifrado*, seleccione un algoritmo para cifrar las comunicaciones. **AES-128** se elige de forma predeterminada.



Las opciones disponibles se muestran de la siguiente manera, desde la menor hasta la mayor seguridad:

•DES: Data Encryption Standard.

·3DES: triple estándar de cifrado de datos.

·AES-128: el estándar de encriptación avanzado utiliza una clave de 128 bits.

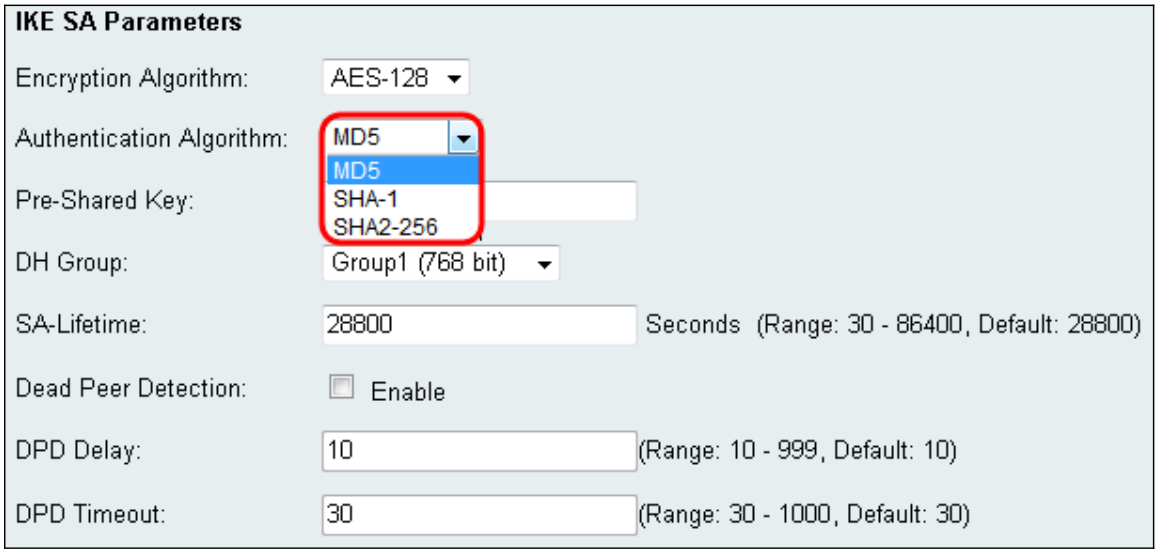
·AES-192: el estándar de encriptación avanzado utiliza una clave de 192 bits.

·AES-256: Estándar de encriptación avanzado que utiliza una clave de 256 bits.

Nota: AES es el método estándar de encriptación en DES y 3DES para obtener un mayor rendimiento y seguridad. Al ampliar la clave AES, se aumentará la seguridad con una

disminución del rendimiento. Se recomienda AES-128 ya que proporciona el mejor compromiso entre velocidad y seguridad.

Paso 10. En el menú desplegable *Authentication Algorithm*, seleccione un algoritmo para autenticar las comunicaciones. **SHA-1** se elige de forma predeterminada.



Las opciones disponibles se definen de la siguiente manera:

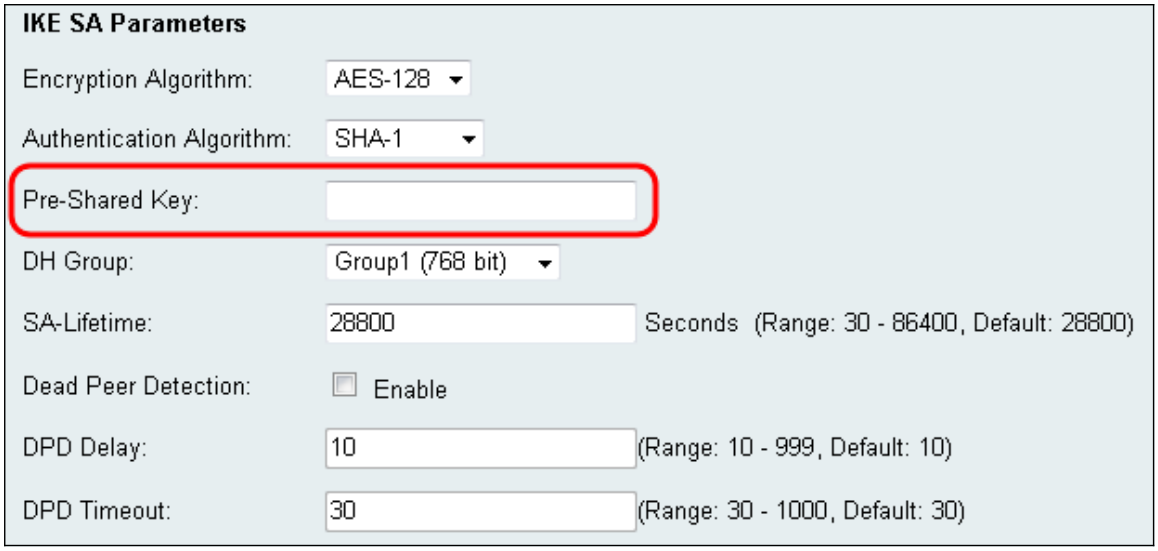
·MD5: el algoritmo de resumen del mensaje tiene un valor de hash de 128 bits.

·SHA-1: el algoritmo hash seguro tiene un valor de hash de 160 bits.

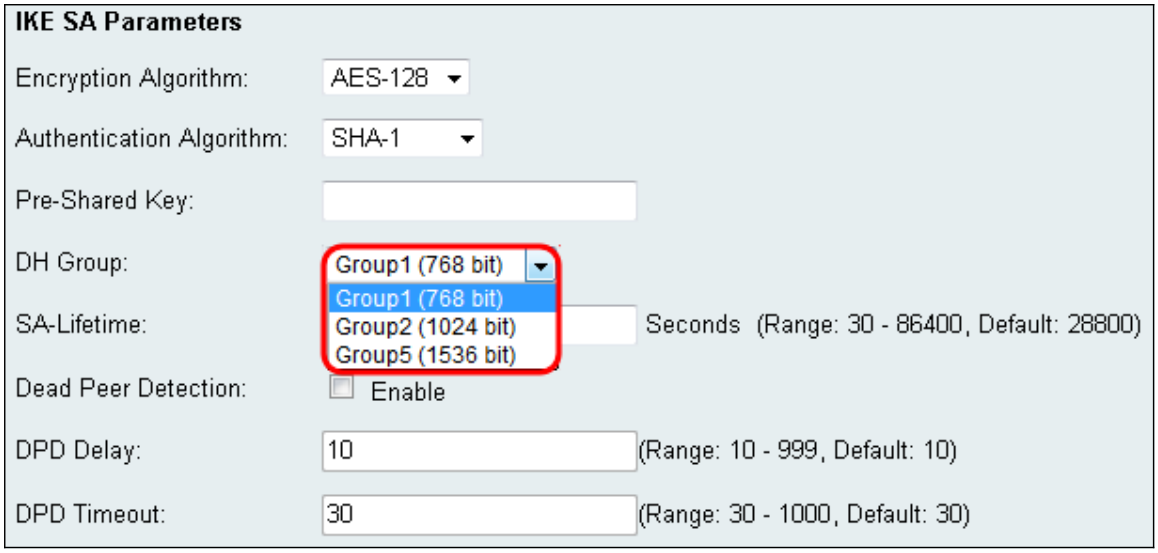
·SHA2-256: algoritmo hash seguro con un valor de hash de 256 bits.

Nota: MD5 y SHA son funciones de hash criptográficas. Toman un fragmento de datos, lo compactan y crean una salida hexadecimal única que normalmente no es reproducible. MD5 básicamente no proporciona seguridad contra colisiones de hashing y solo se debe utilizar en entornos de pequeñas empresas en los que no se necesita resistencia a colisiones. SHA1 es una mejor opción que el MD5 porque ofrece mejor seguridad a velocidades insignificantemente más lentas. Para obtener los mejores resultados, SHA2-256 no tiene ataques conocidos de relevancia práctica y ofrecerá la mejor seguridad. Como se ha mencionado anteriormente, una mayor seguridad implica velocidades más lentas.

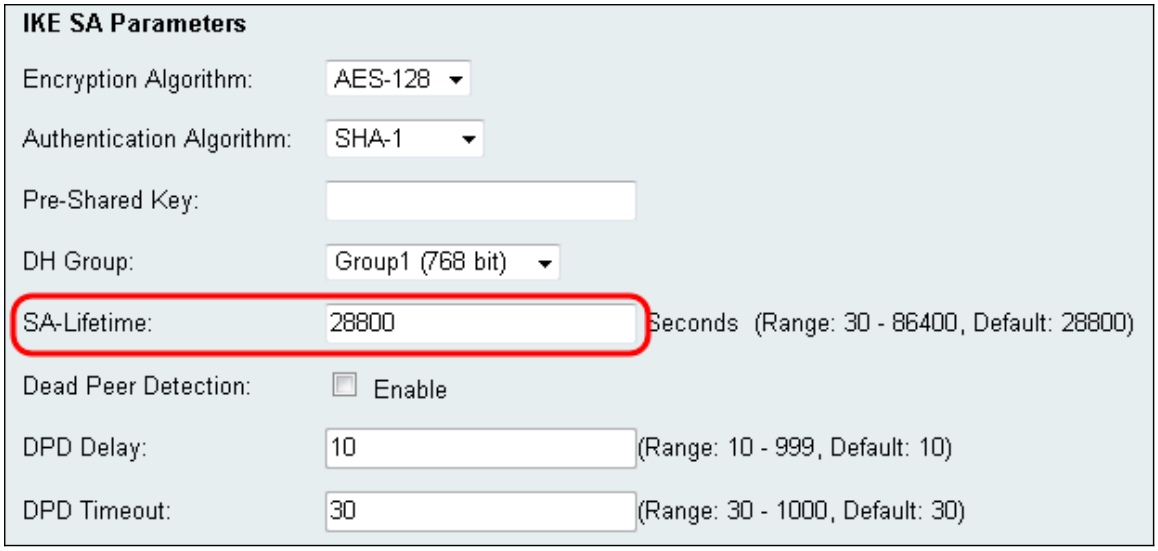
Paso 11. En el campo *Pre-Shared Key*, ingrese una contraseña que tenga entre 8 y 49 caracteres de longitud.



Paso 12. En el menú desplegable *Grupo DH*, elija un grupo DH. El número de bits indica el nivel de seguridad. Ambos extremos de la conexión deben estar en el mismo grupo.

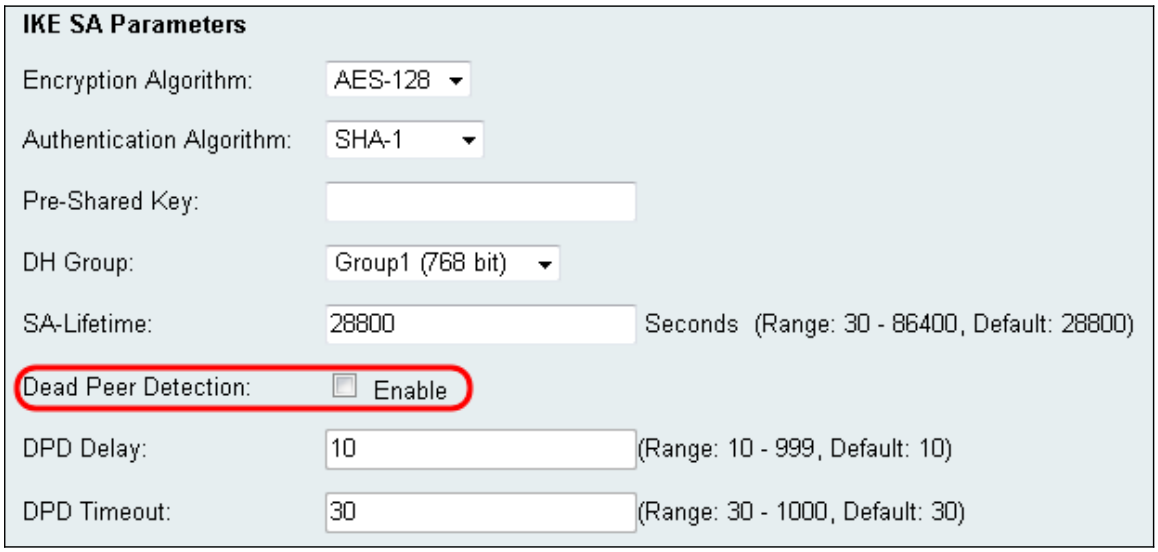


Paso 13. En el campo *SA-Lifetime*, ingrese cuánto tiempo será válida la asociación de seguridad en segundos. El valor predeterminado es 28800 segundos.

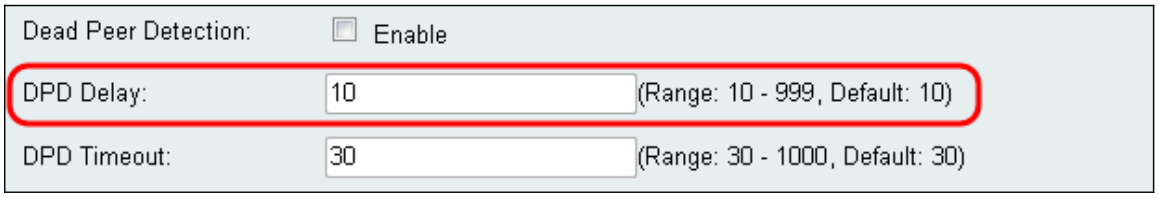


Paso 14. (Opcional) Marque la casilla de verificación **Enable** en el campo *Dead Peer Detection* si desea inhabilitar una conexión con peer inactivo. Vaya al paso 17 si no ha

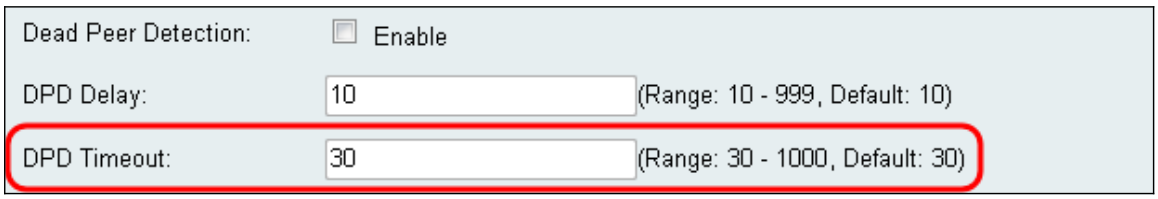
activado la detección de puntos inactivos.



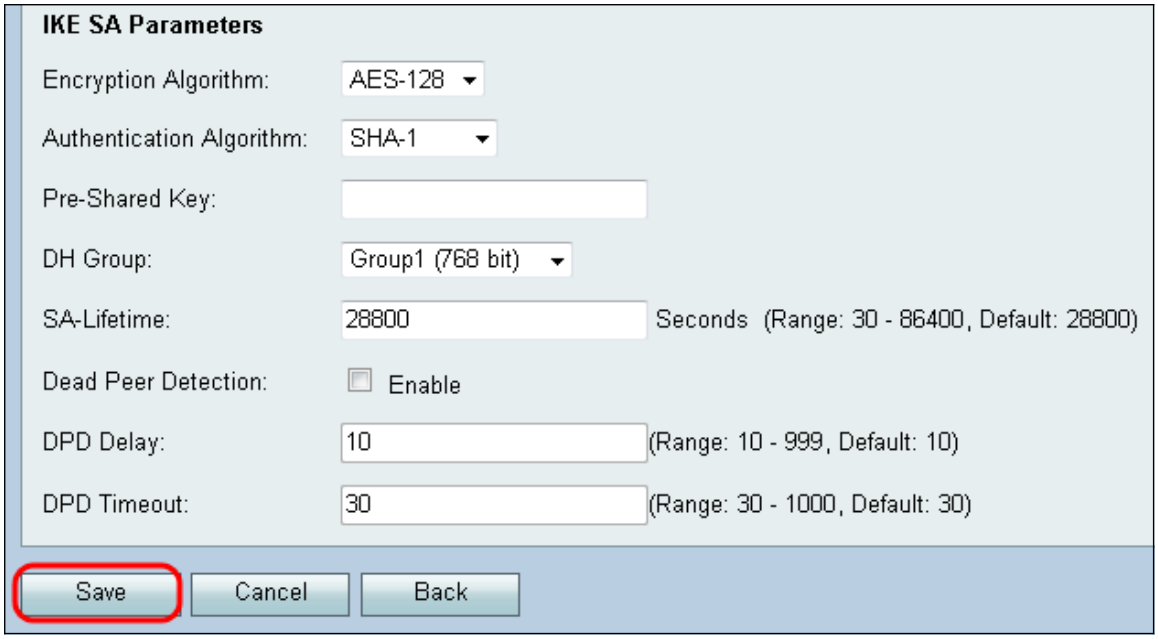
Paso 15. (Opcional) Si ha activado la detección de puntos inactivos, introduzca un valor en el campo *Retraso DPD*. Este valor especificará cuánto tiempo esperará el router para verificar la conectividad del cliente.



Paso 16. (Opcional) Si ha activado la detección de puntos inactivos, introduzca un valor en el campo *Tiempo de espera DPD*. Este valor especificará cuánto tiempo permanecerá conectado el cliente hasta que se agote el tiempo de espera.



Paso 17. Haga clic en **Guardar** para guardar los cambios.


IKE SA Parameters
Encryption Algorithm:
AES-128
Authentication Algorithm:
SHA-1
Pre-Shared Key:
DH Group:
Group1 (768 bit)
SA-Lifetime:
28800
Seconds (Range: 30 - 86400, Default: 28800)
Dead Peer Detection:
Enable
DPD Delay:
10
(Range: 10 - 999, Default: 10)
DPD Timeout:
30
(Range: 30 - 1000, Default: 30)
Save
Cancel
Back

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).