

# Configurar un túnel de acceso remoto (de Cliente a Gateway) para los Clientes VPN en los routers VPN RV016, RV042, RV042G y RV082

## Objetivo

En este artículo, se explica cómo configurar el túnel de Red privada virtual (VPN) de acceso remoto del cliente al gateway en los routers VPN RV016, RV042, RV042G y RV082 con la ayuda de un software de cliente VPN externo como The Green Bow o VPN Tracker.

## Introducción

Una VPN es una red privada que se utiliza para conectar virtualmente dispositivos del usuario remoto a través de la red pública para proporcionar seguridad. VPN de túnel de acceso remoto es el proceso que se utiliza para configurar una VPN entre una computadora del cliente y una red. El cliente se configura en el escritorio o en la computadora portátil de los usuarios a través del software de cliente VPN. Permite a los usuarios conectarse de manera segura a la red en forma remota. La conexión VPN del cliente a la gateway es útil para que los empleados remotos se conecten a la red de la oficina de manera remota y segura.

## Dispositivos aplicables

- RV016
- RV042
- RV042G
- RV082

## Versión del software

- v4.2.2.08

## Configurar un túnel VPN

Paso 1. Inicie sesión en la utilidad de configuración web y elija **VPN > Client to Gateway**. Se abre la página *De Cliente a Gateway*:

### Client To Gateway

**Add a New Tunnel**

Tunnel     Group VPN

Tunnel No.                    1

Tunnel Name :               

Interface :                     ▼

Enable :                       

---

**Local Group Setup**

Local Security Gateway Type :     ▼

IP Address :                    0.0.0.0

Local Security Group Type :     ▼

IP Address :                   

Subnet Mask :                

---

**Remote Client Setup**

Remote Security Gateway Type :     ▼

▼ :               

---

**IPSec Setup**

## Agregar un nuevo túnel

Paso 1. Haga clic en el botón de opción correspondiente según el tipo de túnel que desee agregar.

- Túnel: representa un túnel para un solo usuario remoto.
- Grupo VPN: representa un túnel para un grupo de usuarios remoto.

### Client To Gateway

**Add a New Tunnel**

Tunnel     Group VPN

Tunnel No. : 1

Tunnel Name :

Interface :

Enable :

---

**Local Group Setup**

Local Security Gateway Type :

IP Address : 0.0.0.0

Local Security Group Type :

IP Address :

Subnet Mask :

---

**Remote Client Setup**

Remote Security Gateway Type :

:

---

**IPSec Setup**

El Número de túnel es un campo generado automáticamente que muestra el número del túnel.

**Client To Gateway**

Add a New Tunnel

Tunnel  Group VPN

Tunnel No. 1

Tunnel Name : tunnel\_1

Interface : WAN1

Enable :

---

**Local Group Setup**

Local Security Gateway Type : IP Only

IP Address : 0.0.0.0

Local Security Group Type : Subnet

IP Address : 192.168.1.0

Subnet Mask : 255.255.255.0

---

**Remote Client Setup**

Remote Security Gateway Type : IP Only

IP Address :

---

**IPSec Setup**

Paso 2. Introduzca un nombre para el túnel en el campo Tunnel Name (Nombre de túnel).

Paso 3. Elija la interfaz WAN adecuada que se utilizará para el túnel VPN en la lista desplegable Interfaz.

Paso 4. (Opcional) Para habilitar la VPN, marque la casilla de verificación en el campo Habilitar. Siempre está marcado de manera predeterminada.

## Configuración del grupo local

Paso 1. Elija el método de identificación del router adecuado para establecer un túnel VPN en la lista desplegable *Local Security Gateway*. Omita este paso si eligió VPN de grupo en el Paso 1 de la sección *Agregar un nuevo túnel*.

### Client To Gateway

**Add a New Tunnel**

Tunnel     Group VPN

Tunnel No. : 1

Tunnel Name : tunnel\_1

Interface : WAN1

Enable :

---

**Local Group Setup**

Local Security Gateway Type : IP Only

IP Address : [ ]

Local Security Group Type : [ ]

IP Address : [ ]

Subnet Mask : 255.255.255.0

---

**Remote Client Setup**

Remote Security Gateway Type : IP Only

IP Address : [ ]

---

**IPSec Setup**

Keying Mode : IKE with Preshared key

- Solo IP: es posible acceder al túnel a través de una dirección IP de WAN estática. Puede elegir esta opción solo si el router tiene una IP de WAN estática. La dirección IP de WAN estática aparece automáticamente.
- Autenticación de IP + Nombre de dominio (FQDN): es posible acceder al túnel a través de una dirección IP estática y un dominio registrado con Nombre de dominio totalmente calificado (FQDN). La dirección IP de WAN estática es un campo generado automáticamente.
- Autenticación de IP + Dirección de correo electrónico (FQDN DE USUARIO): es posible acceder al túnel a través de una dirección IP estática y una dirección de correo electrónico. La dirección IP de WAN estática es un campo generado automáticamente.
- Autenticación de IP dinámica + Nombre de dominio (FQDN): es posible acceder al túnel a través de una dirección IP dinámica y un dominio registrado.
- Autenticación de IP dinámica + Dirección de correo electrónico (FQDN DE USUARIO): es posible acceder al túnel a través de una dirección IP dinámica y una dirección de correo electrónico.

Paso 2. Introduzca el nombre del dominio completamente calificado registrado en el campo Nombre de dominio si selecciona *Autenticación de IP + Nombre de dominio (FQDN)* o *Autenticación de IP + Nombre de dominio (FQDN)* en el paso 1.

Paso 3. Introduzca la dirección de correo electrónico en el campo Dirección de correo electrónico si selecciona *Autenticación IP + Dirección de correo electrónico (FQDN de USUARIO)* o *Autenticación IP dinámica + Dirección de correo electrónico (FQDN de USUARIO)* en el paso 1.

Paso 4. Elija el usuario o grupo de usuarios de LAN local adecuado que pueden acceder al túnel VPN en la lista desplegable *Grupo de seguridad local*. El valor predeterminado es Subred.

- IP: sólo un dispositivo LAN específico puede acceder al túnel. Si elige esta opción, introduzca la dirección IP del dispositivo LAN en el campo Dirección IP. La IP predeterminada es 192.168.1.0.
- Subred: todos los dispositivos LAN en una subred específica pueden acceder al túnel. Si elige esta opción, introduzca la dirección IP y la máscara de subred de los dispositivos LAN en los campos Dirección IP y Máscara de subred respectivamente. La máscara predeterminada es 255.255.255.0.
- Rango de IP: un rango de dispositivos LAN puede acceder al túnel. Si elige esta opción, ingrese la dirección IP inicial y final en los campos IP inicial e IP final respectivamente. El rango predeterminado es de 192.168.1.0 a 192.168.1.254.

### Client To Gateway

**Add a New Tunnel**

Tunnel       Group VPN

Tunnel No. : 1

Tunnel Name :

Interface :  ▼

Enable :

---

**Local Group Setup**

Local Security Gateway Type :  ▼

IP Address : 0.0.0.0

Local Security Group Type : 

▼
 

- IP
- Subnet
- IP Range

IP Address :

Subnet Mask :

---

**Remote Client Setup**

Remote Security Gateway Type :  ▼

▼ :

---

**IPSec Setup**

Keying Mode :  ▼

Paso 5. Haga clic en **Guardar para guardar la configuración.**

## Configuración de cliente remoto

Paso 1. Si elige Túnel, elija el método de identificación de cliente adecuado para establecer un túnel VPN de la lista desplegable *Tipo de gateway de seguridad remoto*. El valor predeterminado es IP únicamente. Omita este paso si se eligió VPN de grupo en el Paso 1 de la sección *Agregar un nuevo túnel*.

### Client To Gateway

**Add a New Tunnel**

Tunnel     Group VPN

Tunnel No. : 1

Tunnel Name :

Interface :

Enable :

---

**Local Group Setup**

Local Security Gateway Type :

IP Address :

Local Security Group Type :

IP Address :

Subnet Mask :

---

**Remote Client Setup**

Remote Security Gateway Type :

IP Address :

---

**IPSec Setup**

Keying Mode :

- **IP únicamente:** es posible acceder al túnel a través de la dirección IP de WAN estática del cliente únicamente. Debe conocer la IP de WAN estática del cliente para utilizar esta opción.
- **Autenticación de IP + Nombre de dominio (FQDN):** es posible acceder al túnel a través de una dirección IP estática del cliente y un dominio registrado.
- **Autenticación de IP + Dirección de correo electrónico (FQDN DE USUARIO):** es posible acceder al túnel a través de una dirección IP estática del cliente y una dirección de correo electrónico.
- **Autenticación de IP dinámica + Nombre de dominio (FQDN):** es posible acceder al túnel a través de una dirección IP dinámica del cliente y un dominio registrado.
- **Autenticación de IP dinámica + Dirección de correo electrónico (FQDN DE USUARIO):** es posible acceder al túnel a través de una dirección IP dinámica del cliente y una dirección de correo electrónico.

Paso 2. Introduzca la dirección IP del cliente remoto en el campo *IP Address* si ha seleccionado *IP Only* (*Sólo IP*), *IP + Domain Name (FQDN)* o *IP + E-mail Address (FQDN de usuario)* Authentication en el paso 1.

Paso 3. Elija la opción adecuada de la lista desplegable para introducir la dirección IP si la conoce o resuelva la dirección IP del servidor DNS si selecciona *Sólo IP* o *Autenticación de nombre de dominio (FQDN)* e *IP + Dirección de correo electrónico (FQDN de USUARIO)* en el paso 1.

- **Dirección IP:** representa la dirección IP estática del cliente remoto. Escriba la dirección IP estática en el campo.
- **IP mediante resolución de DNS:** representa el nombre de dominio de la dirección IP que recupera la dirección IP automáticamente a través del servidor DNS local si no conoce la dirección IP estática del

cliente remoto. Ingrese el nombre de dominio de la dirección IP en el campo.

Paso 4. Ingrese el nombre de dominio de la dirección IP en el campo Nombre de dominio si elige *Autenticación IP + Nombre de dominio (FQDN)* o *Autenticación IP dinámica + Nombre de dominio (FQDN)* en el Paso 1.

Paso 5. Introduzca la dirección de correo electrónico en el campo Dirección de correo electrónico si selecciona *Autenticación IP + Dirección de correo electrónico (FQDN de USUARIO)* o *Autenticación IP dinámica + Dirección de correo electrónico (FQDN de USUARIO)* en el paso 1.

Paso 6. Si elige grupo, elija el tipo de cliente remoto adecuado en la lista desplegable *Cliente remoto*. Omita este paso si se eligió VPN de túnel en el Paso 1 de la sección *Agregar un nuevo túnel*.

- Nombre de dominio (FQDN): es posible acceder al túnel a través de un dominio registrado. Si elige esta opción, introduzca el nombre del dominio registrado en el campo Nombre de dominio.
- Dirección de correo electrónico (FQDN de USUARIO): Se puede acceder al túnel mediante una dirección de correo electrónico del cliente. Si elige esta opción, ingrese la Dirección de correo electrónico en el campo Dirección de correo electrónico.
- Cliente VPN de Microsoft XP/2000: es posible acceder al túnel a través del software de Windows Microsoft XP o Microsoft 2000. Los usuarios remotos con software de cliente VPN de Microsoft pueden acceder al túnel a través del software.

**Client To Gateway**

**Add a New Group VPN**

Tunnel  Group VPN

Group No. 1

Tunnel Name : Tunnel\_2

Interface : WAN2

Enable :

---

**Local Group Setup**

Local Security Group Type : Subnet

IP Address : 192.168.1.0

Subnet Mask : 255.255.255.0

---

**Remote Client Setup**

Remote Client : Microsoft XP/2000 VPN Client

Domain Name(FQDN)

Email Address(USER FQDN)

Microsoft XP/2000 VPN Client

---

**IPSec Setup**

Keying Mode : IKE with Preshared key

Phase 1 DH Group : Group 1 - 768 bit

Paso 7. Haga clic en **Guardar para guardar la configuración.**

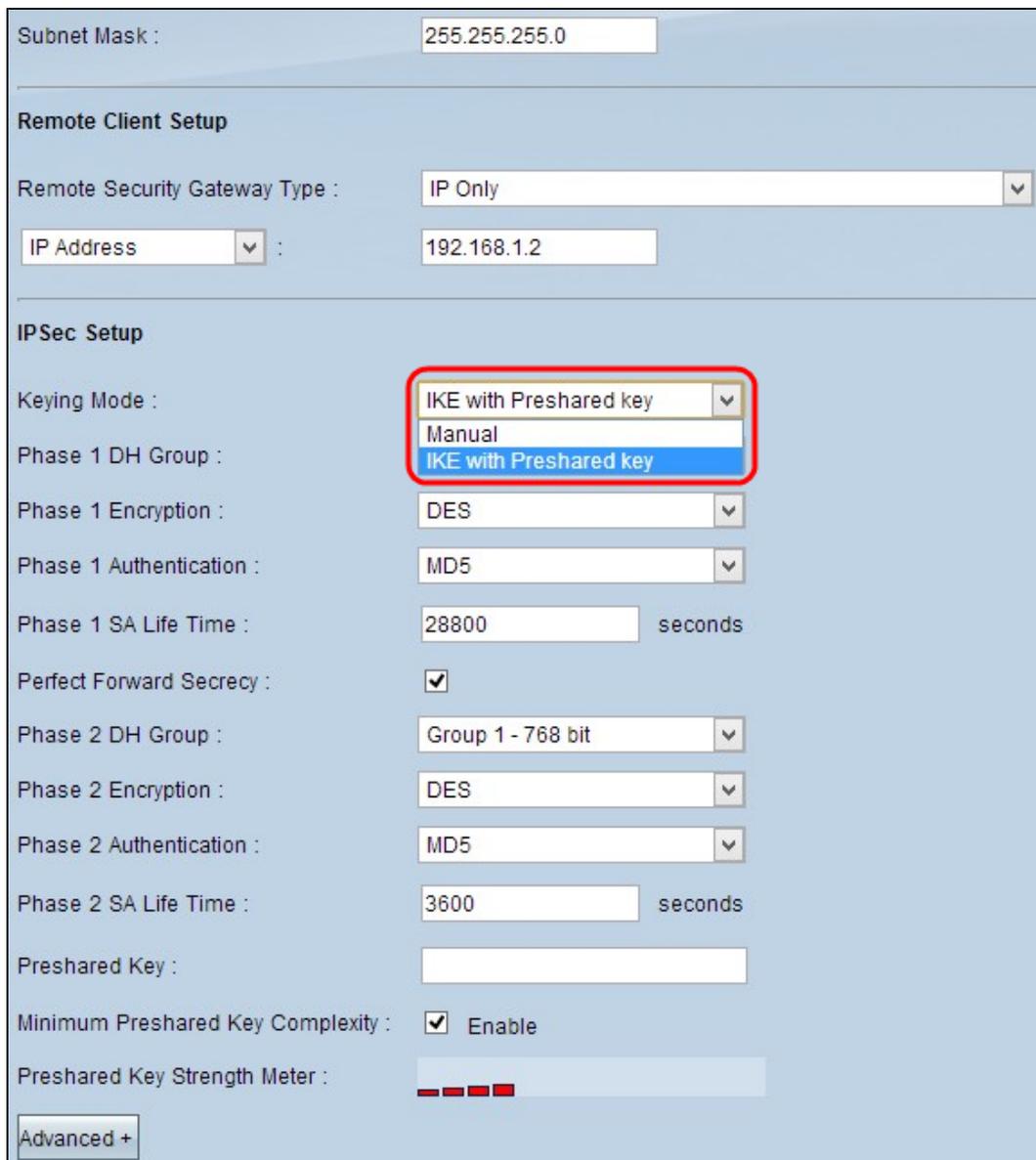
## Configuración de IPsec

El protocolo de seguridad de Internet (IPsec) es un protocolo de seguridad de capa de Internet que proporciona seguridad integral mediante la autenticación y el cifrado durante cualquier sesión de comunicación.

**Nota:** Para que IPsec funcione, dos extremos de la VPN deben tener los mismos métodos de cifrado, descifrado y autenticación. Además, la clave de Confidencialidad directa perfecta debe ser la misma en ambos lados del túnel.

Paso 1. Elija el modo adecuado de administración de claves para garantizar la seguridad en la lista desplegable *Modo de claves*. El modo predeterminado es *IKE con clave previamente compartida*.

- **Manual:** un modo de seguridad personalizado para generar una nueva clave de seguridad por sí mismo y sin negociación con la clave. Es el mejor para usar durante la solución de problemas y el entorno estático pequeño. Si elige VPN de grupo en el Paso 1 de la sección Agregar un nuevo túnel, esta opción está deshabilitada.
- **IKE con clave previamente compartida:** el protocolo de Intercambio de claves por Internet (IKE) se utiliza para generar e intercambiar automáticamente una clave previamente compartida para establecer la comunicación de autenticación para el túnel.



The screenshot displays the configuration interface for IPsec. At the top, the Subnet Mask is set to 255.255.255.0. Below this is the Remote Client Setup section, where the Remote Security Gateway Type is set to IP Only and the IP Address is 192.168.1.2. The main section is IPsec Setup, where the Keying Mode dropdown menu is highlighted with a red box. The dropdown menu shows three options: 'IKE with Preshared key' (selected), 'Manual', and 'IKE with Preshared key'. Other settings include Phase 1 Encryption (DES), Phase 1 Authentication (MD5), Phase 1 SA Life Time (28800 seconds), Perfect Forward Secrecy (checked), Phase 2 DH Group (Group 1 - 768 bit), Phase 2 Encryption (DES), Phase 2 Authentication (MD5), Phase 2 SA Life Time (3600 seconds), Preshared Key (empty field), Minimum Preshared Key Complexity (checked, Enable), and Preshared Key Strength Meter (a progress bar with four red segments). An 'Advanced +' button is located at the bottom left.

## Configuración del modo de clave manual

Paso 1. Introduzca el valor hexadecimal único para el Índice de parámetros de seguridad (SPI) entrante en el campo *SPI entrante*. SPI se transporta en el encabezado del Protocolo de carga útil de seguridad encapsulada (ESP), y juntos determinan la protección del paquete entrante. Puede ingresar de 100 a ffffffff. El SPI entrante del router local debe coincidir con el SPI saliente del router remoto.

Paso 2. Introduzca el valor hexadecimal único para el Índice de parámetros de seguridad (SPI) saliente en el campo *SPI saliente*. SPI se transporta en el encabezado del Protocolo de carga útil de seguridad encapsulada (ESP), y juntos determinan la protección del paquete saliente. Puede ingresar de 100 a ffffffff. El SPI saliente del router remoto debe coincidir con el SPI entrante del router local.

The image shows a configuration interface for a remote client setup. It is divided into two main sections: 'Remote Client Setup' and 'IPsec Setup'. In the 'Remote Client Setup' section, 'Remote Security Gateway Type' is set to 'IP Only' and 'IP Address' is '192.168.1.2'. The 'IPsec Setup' section has 'Keying Mode' set to 'Manual'. The 'Incoming SPI' field is highlighted with a red box and contains the value '100A'. The 'Outgoing SPI' field contains the value '1BCD'. Below these, 'Encryption' is set to 'DES' and 'Authentication' is set to 'MD5'. There are empty text input fields for 'Encryption Key' and 'Authentication Key'.

Paso 3. Elija el método de encriptación adecuado para los datos en la lista desplegable *Encryption*. El cifrado recomendado es *3DES*. El túnel VPN necesita utilizar el mismo método de cifrado para ambos extremos.

- DES: el estándar de cifrado de datos (DES) utiliza una clave de 56 bits para el cifrado de datos. DES está desactualizado y se debe utilizar únicamente si un solo terminal admite DES.
- 3DES: El triple estándar de cifrado de datos (3DES) es un método de cifrado simple de 168 bits. 3DES cifra los datos tres veces, lo que proporciona más seguridad y, luego, DES.

**IPSec Setup**

Keying Mode :

Incoming SPI :

Outgoing SPI :

Encryption :

Authentication :

Encryption Key :

Authentication Key :

Paso 4. Elija el método de autenticación adecuado para los datos de la lista desplegable *Authentication*. La autenticación recomendada es *SHA1*, ya que es más segura que *MD5*. El túnel VPN necesita utilizar el mismo método de autenticación para ambos extremos.

- MD5: el algoritmo de resumen de mensajes (MD5) representa una función de hash hexadecimal de 32 dígitos que proporciona protección a los datos frente a ataques malintencionados mediante el cálculo de la suma de comprobación.
- SHA1 - Secure Hash Algorithm versión 1 (SHA1) es una función de hash de 160 bits que es más segura que MD5, pero tarda más tiempo en calcularse.

**IPSec Setup**

Keying Mode :

Incoming SPI :

Outgoing SPI :

Encryption :

Authentication :

Encryption Key :

Authentication Key :

Paso 5. Introduzca la clave para cifrar y descifrar los datos en el campo *Encryption Key*. Si elige DES como método de cifrado en el Paso 3, ingrese un valor hexadecimal de 16 dígitos. Si elige 3DES como método de cifrado en el Paso 3, introduzca un valor hexadecimal de 40 dígitos.

Paso 6. Ingrese una clave previamente compartida para autenticar el tráfico en el campo *Authentication Key*. Si elige MD5 como método de cifrado en el Paso 4, introduzca un valor hexadecimal de 32 dígitos. Si elige SHA1 como método de cifrado en el Paso 4, introduzca un valor hexadecimal de 40 dígitos. El túnel VPN necesita utilizar la misma clave previamente compartida para ambos extremos.

**IPSec Setup**

Keying Mode :	Manual
Incoming SPI :	100A
Outgoing SPI :	1BCD
Encryption :	DES
Authentication :	MD5
Encryption Key :	ABC12675BC0ACD
Authentication Key :	AC67BCD00A12876CB

Paso 7. Haga clic en **Guardar para guardar la configuración.**

### **IKE con configuración del modo de clave previamente compartida**

Paso 1. Elija el grupo DH de fase 1 adecuado de la lista desplegable *Grupo DH de fase 1*. La Fase 1 se utiliza para establecer la Asociación de seguridad lógica (SA) simplex entre los dos extremos del túnel para admitir la comunicación segura de autenticación. Diffie-Hellman (DH) es un protocolo de intercambio de claves criptográficas que se utiliza para determinar la fuerza de la clave durante la Fase 1 y también comparte la clave secreta para autenticar la comunicación.

- Grupo 1: 768 bits: la clave de menor seguridad 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 seguridad y el grupo de autenticación más seguro. Pero necesita un tiempo para calcular las claves IKE.
- Grupo 1: 1536 bits: representa la clave de mayor 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.

**IPSec Setup**

Keying Mode : IKE with Preshared key

Phase 1 DH Group : Group 1 - 768 bit

Phase 1 Encryption : Group 1 - 768 bit

Phase 1 Authentication : MD5

Phase 1 SA Life Time : 28800 seconds

Perfect Forward Secrecy :

Phase 2 DH Group : Group 1 - 768 bit

Phase 2 Encryption : DES

Phase 2 Authentication : MD5

Phase 2 SA Life Time : 3600 seconds

Preshared Key :

Minimum Preshared Key Complexity :  Enable

Preshared Key Strength Meter :

Advanced +

Paso 2. Elija el cifrado de fase 1 adecuado para cifrar la clave en la lista desplegable *Cifrado de fase 1*. Se recomienda usar 3DES, ya que es el método de cifrado más seguro. El túnel VPN necesita utilizar el mismo método de cifrado para ambos extremos.

- DES: el estándar de cifrado de datos (DES) utiliza una clave de 56 bits para el cifrado de datos. DES está desactualizado y se debe utilizar únicamente si un solo terminal admite DES.
- 3DES: El triple estándar de cifrado de datos (3DES) es un método de cifrado simple de 168 bits. 3DES cifra los datos tres veces, lo que proporciona más seguridad y, luego, DES.
- AES-128 - Estándar de cifrado avanzado (AES) es un método de cifrado de 128 bits que transforma el texto sin formato en texto cifrado a través de 10 ciclos de repetición.
- AES-192 - Estándar de cifrado avanzado (AES) es un método de cifrado de 192 bits que transforma el texto sin formato en texto cifrado a través de 12 ciclos de repetición. AES-192 es más seguro que AES-128.
- AES-256 - Estándar de cifrado avanzado (AES) es un método de cifrado de 256 bits que transforma el texto sin formato en texto cifrado a través de 14 ciclos de repetición. AES-256 es el método de cifrado más seguro.

**IPSec Setup**

Keying Mode : IKE with Preshared key

Phase 1 DH Group : Group 1 - 768 bit

Phase 1 Encryption : DES

Phase 1 Authentication : DES

Phase 1 SA Life Time :

Perfect Forward Secrecy :

Phase 2 DH Group : Group 1 - 768 bit

Phase 2 Encryption : DES

Phase 2 Authentication : MD5

Phase 2 SA Life Time : 3600 seconds

Preshared Key :

Minimum Preshared Key Complexity :  Enable

Preshared Key Strength Meter :

Advanced +

Paso 3. Elija el método de autenticación de fase 1 adecuado de la lista desplegable *Autenticación de fase 1*. El túnel VPN necesita utilizar el mismo método de autenticación para ambos extremos.

- MD5: el algoritmo de resumen de mensajes (MD5) representa una función de hash hexadecimal de 32 dígitos que proporciona protección a los datos frente a ataques malintencionados mediante el cálculo de la suma de comprobación.
- SHA1 - Secure Hash Algorithm versión 1 (SHA1) es una función de hash de 160 bits que es más segura que MD5, pero tarda más tiempo en calcularse.

**IPSec Setup**

Keying Mode : IKE with Preshared key

Phase 1 DH Group : Group 1 - 768 bit

Phase 1 Encryption : DES

Phase 1 Authentication : MD5

Phase 1 SA Life Time : 3600 seconds

Perfect Forward Secrecy :

Phase 2 DH Group : Group 1 - 768 bit

Phase 2 Encryption : DES

Phase 2 Authentication : MD5

Phase 2 SA Life Time : 3600 seconds

Preshared Key :

Minimum Preshared Key Complexity :  Enable

Preshared Key Strength Meter :

Advanced +

Paso 4. Introduzca la cantidad de tiempo en segundos durante los cuales las claves de la fase 1 son válidas y el túnel VPN permanece activo en el campo *Phase 1 SA Life Time*.

Paso 5. Marque la casilla de verificación **Confidencialidad directa perfecta para proporcionar más protección a las claves**. Esta opción permite que el router genere una nueva clave si se ve comprometida alguna clave. Los datos cifrados solo se ponen en riesgo a través de la clave comprometida. Por lo tanto, proporciona una comunicación más segura y autenticada, ya que protege otras claves a pesar de que se vea comprometida una clave. Esta es una acción recomendada, ya que proporciona más seguridad.

**IPSec Setup**

Keying Mode :

Phase 1 DH Group :

Phase 1 Encryption :

Phase 1 Authentication :

Phase 1 SA Life Time :  seconds

Perfect Forward Secrecy :

Phase 2 DH Group :

Phase 2 Encryption :

Phase 2 Authentication :

Phase 2 SA Life Time :  seconds

Preshared Key :

Minimum Preshared Key Complexity :  Enable

Preshared Key Strength Meter : 

Paso 6. Elija el grupo DH de fase 2 adecuado de la lista desplegable *Grupo DH de fase 2*. La fase 2 utiliza la asociación de seguridad y se utiliza para determinar la seguridad del paquete de datos mientras los paquetes de datos pasan por los dos terminales.

- Grupo 1: 768 bits: representa la clave de menor seguridad 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 la clave de mayor seguridad y el grupo de autenticación más seguro. Pero necesita un tiempo para calcular las claves IKE.
- Grupo 1: 1536 bits: representa la clave de mayor 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.

**IPSec Setup**

Keying Mode : IKE with Preshared key

Phase 1 DH Group : Group 2 - 1024 bit

Phase 1 Encryption : DES

Phase 1 Authentication : SHA1

Phase 1 SA Life Time : 27600 seconds

Perfect Forward Secrecy :

Phase 2 DH Group : Group 1 - 768 bit

Phase 2 Encryption : MD5

Phase 2 Authentication : MD5

Phase 2 SA Life Time : 3600 seconds

Preshared Key :

Minimum Preshared Key Complexity :  Enable

Preshared Key Strength Meter :

Advanced +

Paso 7. Elija la encriptación de fase 2 adecuada para encriptar la clave de la lista desplegable *encriptación de fase 2*. Se recomienda usar AES-256, ya que es el método de cifrado más seguro. El túnel VPN necesita utilizar el mismo método de cifrado para ambos extremos.

- DES: el estándar de cifrado de datos (DES) utiliza una clave de 56 bits para el cifrado de datos. DES está desactualizado y se debe utilizar únicamente si un solo terminal admite DES.
- 3DES: El triple estándar de cifrado de datos (3DES) es un método de cifrado simple de 168 bits. 3DES cifra los datos tres veces, lo que proporciona más seguridad y, luego, DES.
- AES-128 - Estándar de cifrado avanzado (AES) es un método de cifrado de 128 bits que transforma el texto sin formato en texto cifrado a través de 10 ciclos de repetición.
- AES-192 - Estándar de cifrado avanzado (AES) es un método de cifrado de 192 bits que transforma el texto sin formato en texto cifrado a través de 12 ciclos de repetición. AES-192 es más seguro que AES-128.
- AES-256 - Estándar de cifrado avanzado (AES) es un método de cifrado de 256 bits que transforma el texto sin formato en texto cifrado a través de 14 ciclos de repetición. AES-256 es el método de cifrado más seguro.

**IPSec Setup**

Keying Mode : IKE with Preshared key

Phase 1 DH Group : Group 2 - 1024 bit

Phase 1 Encryption : DES

Phase 1 Authentication : SHA1

Phase 1 SA Life Time : 27600 seconds

Perfect Forward Secrecy :

Phase 2 DH Group : Group 1 - 768 bit

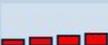
Phase 2 Encryption : DES

Phase 2 Authentication : **DES**

Phase 2 SA Life Time :

Preshared Key :

Minimum Preshared Key Complexity :  Enable

Preshared Key Strength Meter : 

Advanced +

Paso 8. Elija el método de autenticación apropiado de la lista desplegable *Phase 2 Authentication*. El túnel VPN necesita utilizar el mismo método de autenticación para ambos extremos.

- MD5: el algoritmo de resumen de mensajes (MD5) representa una función de hash hexadecimal de 32 dígitos que proporciona protección a los datos frente a ataques malintencionados mediante el cálculo de la suma de comprobación.
- SHA1 - Secure Hash Algorithm versión 1 (SHA1) es una función de hash de 160 bits que es más segura que MD5, pero tarda más tiempo en calcularse.
- Nulo: No se usa ningún método de autenticación.

**IPSec Setup**

Keying Mode : IKE with Preshared key

Phase 1 DH Group : Group 2 - 1024 bit

Phase 1 Encryption : DES

Phase 1 Authentication : SHA1

Phase 1 SA Life Time : 27600 seconds

Perfect Forward Secrecy :

Phase 2 DH Group : Group 1 - 768 bit

Phase 2 Encryption : DES

Phase 2 Authentication : MD5

Phase 2 SA Life Time :

Preshared Key :

Minimum Preshared Key Complexity :  Enable

Preshared Key Strength Meter : 

Advanced +

Paso 9. Introduzca la cantidad de tiempo en segundos durante los cuales las claves de la fase 2 son válidas y el túnel VPN permanece activo en el campo *Phase 2 SA Life Time*.

Paso 10. Ingrese una clave previamente compartida entre los pares IKE para autenticar a los pares en el campo *Clave previamente compartida*. Se pueden utilizar hasta 30 hexadecimales y caracteres como clave previamente compartida. El túnel VPN necesita utilizar la misma clave previamente compartida para ambos extremos.

**Nota:** Se recomienda encarecidamente cambiar con frecuencia la clave previamente compartida entre los pares IKE para que la VPN permanezca protegida.

Paso 11. Marque la casilla de verificación **Complejidad mínima de claves previamente compartidas si desea habilitar el medidor de seguridad para la clave previamente compartida**. Se utiliza para determinar la seguridad de la clave previamente compartida a través de barras de color.

**Nota:** El *medidor de fuerza de clave previamente compartida* muestra la fuerza de la clave previamente compartida a través de barras de colores. El color rojo indica una seguridad débil, el amarillo indica una seguridad aceptable y el verde indica una seguridad sólida.

**IPSec Setup**

Keying Mode :

Phase 1 DH Group :

Phase 1 Encryption :

Phase 1 Authentication :

Phase 1 SA Life Time :  seconds

Perfect Forward Secrecy :

Phase 2 DH Group :

Phase 2 Encryption :

Phase 2 Authentication :

Phase 2 SA Life Time :  seconds

Preshared Key :

Minimum Preshared Key Complexity :  Enable

Preshared Key Strength Meter :

Paso 12. Haga clic en **Guardar para guardar la configuración.**

### **IKE avanzada con configuración del modo de clave previamente compartida**

Paso 1. Haga clic en **Advanced** para mostrar los parámetros avanzados de IKE con clave previamente compartida.

**Advanced**

Aggressive Mode

Compress (Support IP Payload Compression Protocol(IPComp))

Keep-Alive

AH Hash Algorithm

NetBIOS Broadcast

NAT Traversal

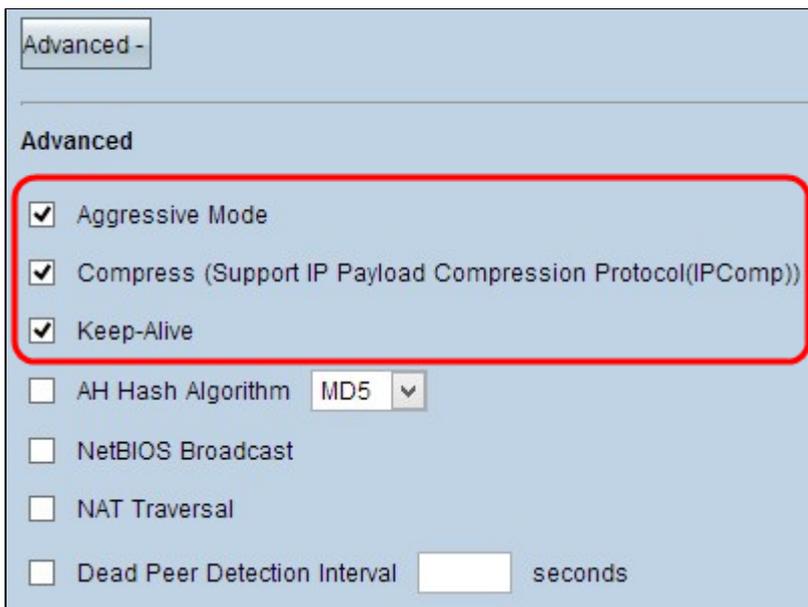
Dead Peer Detection Interval  seconds

Paso 2. Marque la casilla de verificación **Modo agresivo si la velocidad de la red es baja**. Esto intercambia los ID de los terminales del túnel en texto no cifrado durante la conexión de SA (Fase 1), lo que requiere menos tiempo para el intercambio pero es menos seguro.

**Nota:** El modo agresivo no está disponible para la conexión VPN de cliente de grupo a gateway.

Paso 3. Marque la casilla de verificación **Compress (Support IP Payload Compression Protocol (IPComp))** si desea comprimir el tamaño de los datagramas IP. IPComp es un protocolo de compresión IP que se utiliza para comprimir el tamaño del datagrama IP. La compresión IP es útil si la velocidad de la red es baja y el usuario desea transmitir rápidamente los datos sin pérdidas a través de la red lenta, pero no proporciona ninguna seguridad.

Paso 4. Marque la casilla de verificación **Señal de mantenimiento si desea que la conexión del túnel VPN permanezca siempre activa**. La señal de mantenimiento ayuda a restablecer las conexiones inmediatamente si alguna conexión se vuelve inactiva.



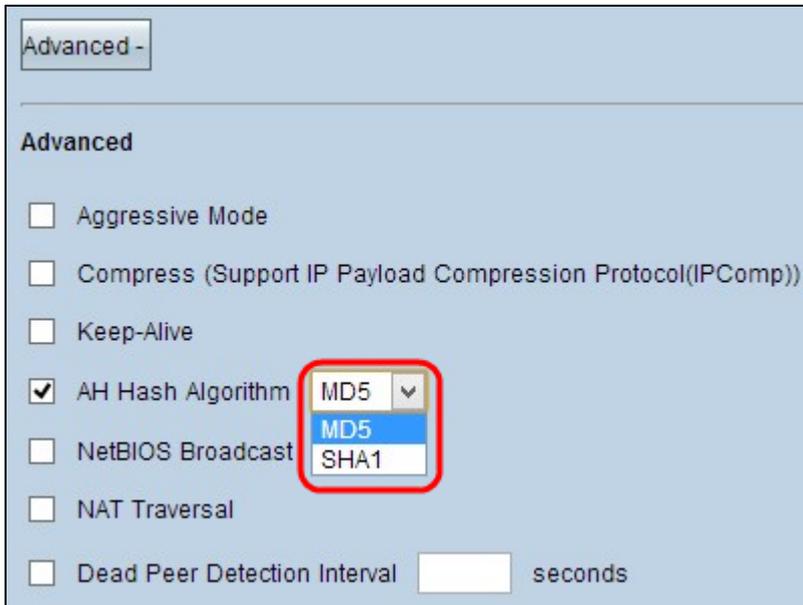
Advanced -

Advanced

- Aggressive Mode
- Compress (Support IP Payload Compression Protocol(IPComp))
- Keep-Alive
- AH Hash Algorithm MD5
- NetBIOS Broadcast
- NAT Traversal
- Dead Peer Detection Interval seconds

Paso 5. Marque la casilla de verificación **Algoritmo de hash AH si desea habilitar el Encabezado de autenticación (AH)**. AH proporciona autenticación a los datos de origen, integridad de los datos mediante checksum y protección al encabezado de IP. El túnel debe tener el mismo algoritmo para ambos lados.

- MD5: el algoritmo de resumen de mensajes (MD5) representa una función de hash hexadecimal de 128 dígitos que proporciona protección a los datos frente a ataques malintencionados mediante el cálculo de la suma de comprobación.
- SHA1 - Secure Hash Algorithm versión 1 (SHA1) es una función de hash de 160 bits que es más segura que MD5, pero tarda más tiempo en calcularse.

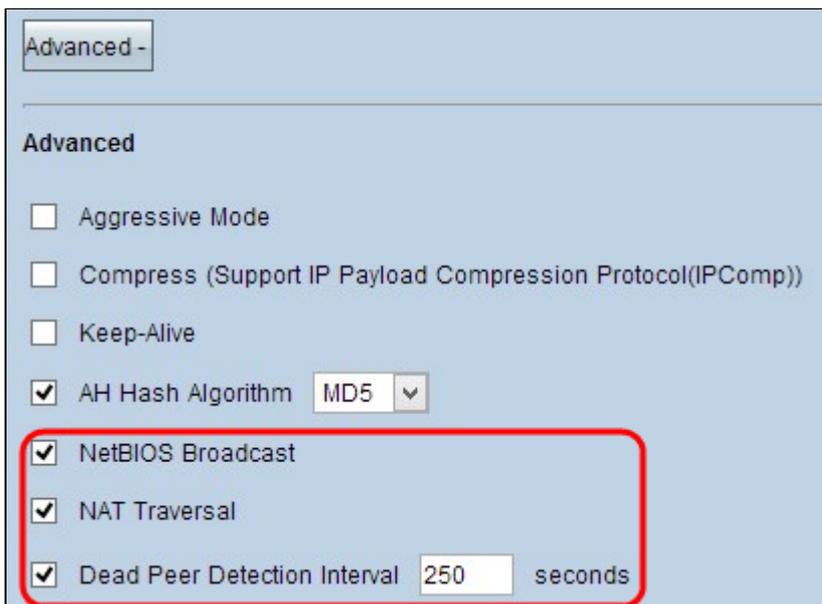


Paso 6. Verifique la **Difusión de NetBIOS** si desea permitir el tráfico que no se puede enrutar a través del túnel VPN. Los valores predeterminados no están marcados. NetBIOS se utiliza para detectar recursos de red, como impresoras, computadoras, etc. en la red a través de algunas aplicaciones de software y funciones de Windows, como el Entorno de red.

Paso 7. Marque la casilla de verificación **NAT Traversal** si desea acceder a Internet desde su LAN privada a través de una dirección IP pública. Si el router VPN está detrás de una gateway NAT, marque esta casilla de verificación para habilitar NAT Traversal. Ambos extremos del túnel deben tener la misma configuración.

Paso 8. Verifique el **Intervalo de detección de pares inactivos** para verificar la actividad del túnel VPN mediante saludo o ACK de manera periódica. Si marca esta casilla de verificación, ingrese la duración o el intervalo deseado de los mensajes de saludo.

**Nota:** Puede configurar el intervalo de detección de puntos inactivos sólo para una conexión VPN de cliente a gateway individual, no para una conexión VPN de cliente a gateway de grupo.



Paso 9. Haga clic en **Guardar** para guardar la configuración.

Ahora ha aprendido cómo configurar el túnel VPN de acceso remoto del cliente al gateway en los routers VPN RV016, RV042, RV042G y RV082.

## 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).