Protección del ataque ARP en el VPN Router RV315W

Objetivo

El ARP (protocolo Protocolo de resolución de la dirección (ARP)) se utiliza para no perder de vista todos los dispositivos que estén conectados directamente con el RV315W. La protección ARP se utiliza para proteger una red contra los ataques ARP. Cuando un paquete llega en una interfaz (port/LAG) que se defina como untrusted, el ataque de la protección ARP compara el IP Address y el MAC address del paquete con los IP Addresses y los direccionamientos MAC definidos previamente en las reglas del control de acceso ARP. Si los direccionamientos hacen juego, se desecha el paquete se considera válido y se remite de otra manera el paquete. Este artículo explica cómo configurar la protección del ataque ARP en el VPN Router RV315W.

Dispositivo aplicable

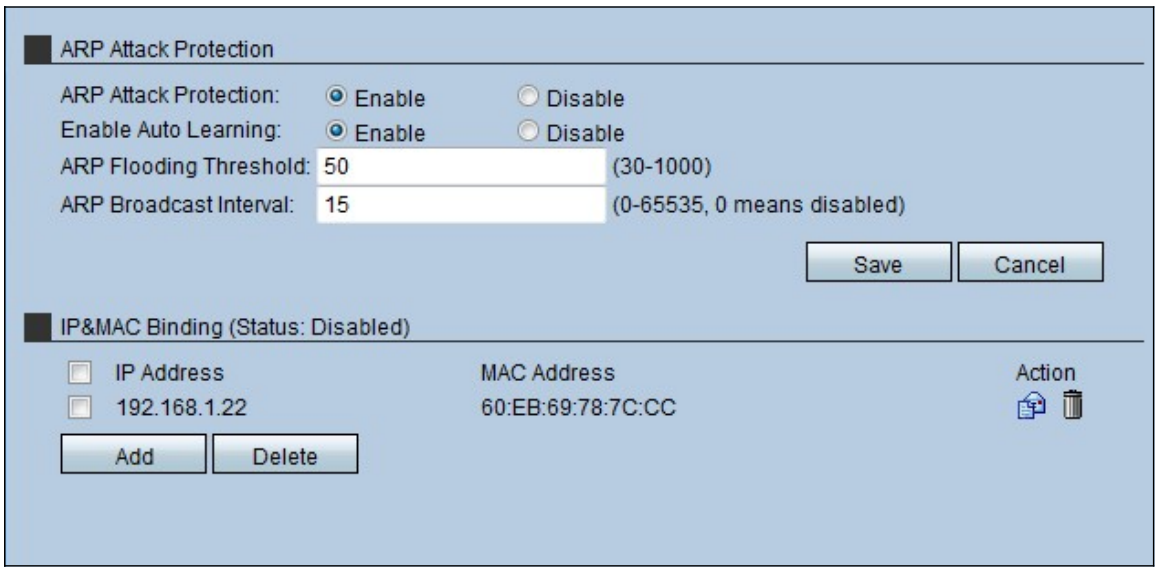
• RV315W

Versión del software

• 1.01.03

Protección del ataque ARP

Paso 1. Inicie sesión a la utilidad de configuración de la red y elija la **protección de la Seguridad > del ataque ARP**. La página de la *protección del ataque ARP* se abre:



Paso 2. En el campo de la protección del ataque, haga clic el botón de radio del **permiso** para habilitar la protección del ataque ARP en el RV315W.

El paso 3. (opcional) para habilitar el RV315W al auto aprende, hace clic el **permiso** en el campo de aprendizaje auto del permiso. Esta característica permite que el RV315W

reconozca qué IP Addresses y direcciones MAC son válidas en la red.

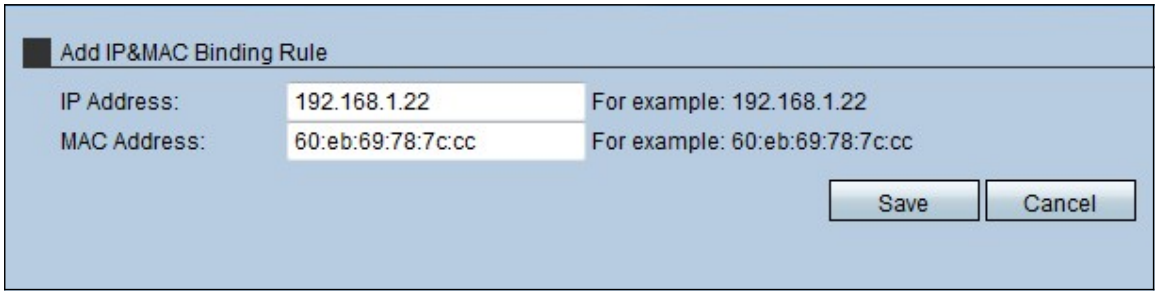
Paso 4. Ingrese la cantidad máxima de paquetes ARP que el RV315W pueda recibir por segundo. Si el dispositivo recibe más que el valor se fija que, la protección ARP se aplica al RV315W.

Paso 5. Ingrese el intervalo para el ARP transmitido en el campo del intervalo del broadcast ARP. Este intervalo determina la cantidad de broadcast ARP enviada.

Atascamiento IP&MAC

Esta área permite que el administrador asocie una dirección IP y una dirección MAC para aumentar la Seguridad. Un host puede acceder solamente la red si la dirección IP y la dirección MAC de la coincidencia del host qué se configura en el área obligatoria IP&MAC.

Agregue un atascamiento IP&MAC



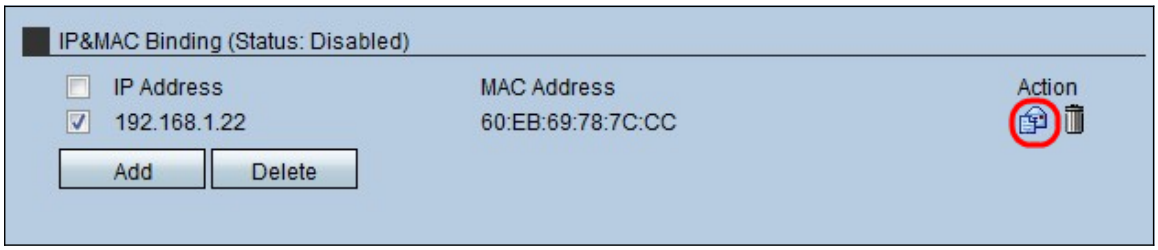
Paso 1. El tecleo **agrega** para agregar una nueva norma vinculante IP&MAC. Esto *agrega la página de la norma vinculante IP&MAC se abre:*

Paso 2. Ingrese el IP Address que se asocia con el MAC address en el campo del IP Address.

Paso 3. Ingrese el MAC address que se asocia con el IP Address en el campo del MAC address.

Paso 4. **Salvaguardia del** tecleo**.** Esta regla se visualiza en la lista obligatoria IP&MAC.

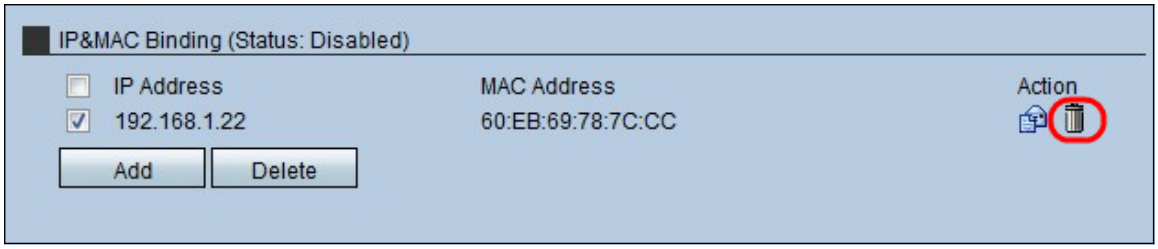
Edite una norma vinculante IP&MAC



Paso 1. Marque la casilla de verificación de la norma vinculante IP&MAC que debe ser editada.

Paso 2. Haga clic el icono de la **envoltura** para editar la norma vinculante IP&MAC.

Borre la norma vinculante IP&MAC



Paso 1. Marque la casilla de verificación de la norma vinculante IP&MAC que debe ser borrada.

Paso 2. Haga clic el icono de **Trashcan** para borrar la norma vinculante IP&MAC.