

RV315W VPN路由器的ARP攻擊防護

目標

ARP (地址解析協定) 用於跟蹤直接連線到RV315W的所有裝置。ARP保護用於保護網路免受ARP攻擊。當資料包到達定義為不可信的介面 (埠/LAG) 時，ARP保護攻擊會將資料包的IP地址和MAC地址與先前在ARP訪問控制規則中定義的IP地址和MAC地址進行比較。如果地址匹配，則資料包將被視為有效並轉發，否則資料包將被丟棄。本文說明如何在RV315W VPN路由器上配置ARP攻擊保護。

適用的裝置

·RV315W

軟體版本

·1.01.03

ARP攻擊防護

步驟1.登入到Web配置實用程式，然後選擇**Security > ARP Attack Protection**。將打開**ARP攻擊保護**頁面：

ARP Attack Protection		
ARP Attack Protection:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Enable Auto Learning:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
ARP Flooding Threshold:	50 (30-1000)	
ARP Broadcast Interval:	15 (0-65535, 0 means disabled)	
<input type="button" value="Save"/> <input type="button" value="Cancel"/>		
IP&MAC Binding (Status: Disabled)		
IP Address	MAC Address	Action
<input type="checkbox"/> 192.168.1.22	60:EB:69:78:7C:CC	<input type="button" value="Add"/> <input type="button" value="Delete"/>

步驟2.在Attack Protection (攻擊保護) 欄位中，點選**Enable** 單選按鈕以在RV315W上啟用ARP攻擊保護。

步驟3. (可選) 要啟用RV315W自動學習，請在Enable Auto Learning欄位中按一下**Enable**。此功能允許RV315W識別網路中有效的IP地址和MAC地址。

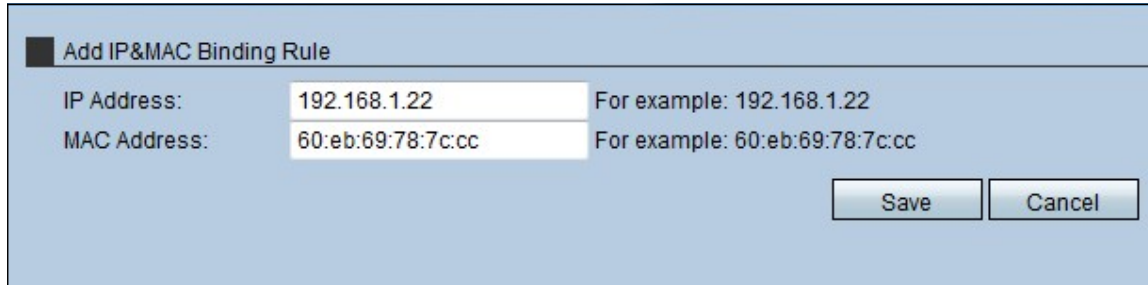
步驟4.輸入RV315W每秒可接收的最大ARP資料包數。如果裝置收到的值大於設定的值，則ARP保護將應用於RV315W。

步驟5.在ARP Broadcast Interval欄位中輸入ARP廣播的時間間隔。此間隔確定發出的ARP廣播量。

IP&MAC繫結

此區域允許管理員對映IP地址和MAC地址以增強安全性。僅當主機的IP地址和MAC地址與IP&MAC繫結區域中的配置匹配時，主機才能訪問網路。

新增IP&MAC繫結



Add IP&MAC Binding Rule

IP Address: 192.168.1.22 For example: 192.168.1.22

MAC Address: 60:eb:69:78:7c:cc For example: 60:eb:69:78:7c:cc

Save Cancel

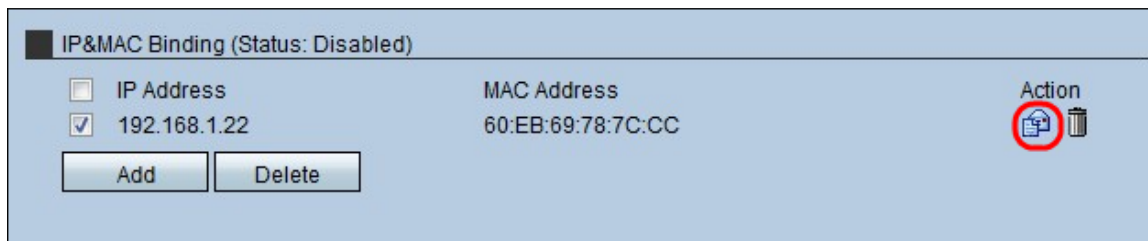
步驟1.按一下**Add**新增新的IP&MAC繫結規則。此時將開啟**新增IP&MAC繫結規則**頁：


步驟2.在「IP地址」欄位中輸入與MAC地址對映的IP地址。

步驟3.在「MAC地址」欄位中輸入與IP地址對映的MAC地址。

步驟4.按一下「**Save**」。此規則顯示在IP&MAC繫結清單中。

編輯IP&MAC繫結規則



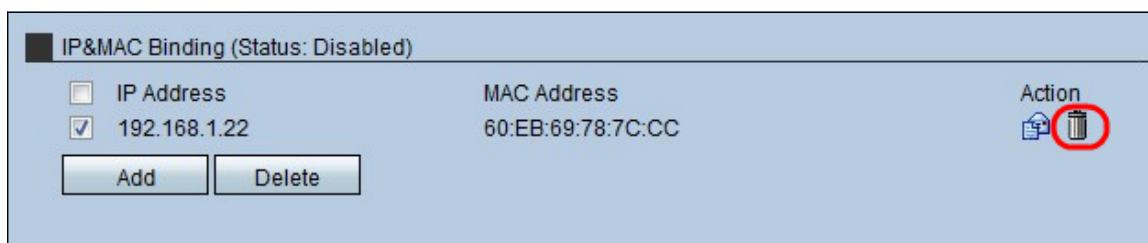
IP Address	MAC Address	Action
<input checked="" type="checkbox"/> 192.168.1.22	60:EB:69:78:7C:CC	 



Add Delete

步驟1.選中要編輯的IP&MAC繫結規則的覈取方塊。

步驟2.按一下**Envelop**圖示編輯IP&MAC繫結規則。

刪除IP&MAC繫結規則



IP Address	MAC Address	Action
<input checked="" type="checkbox"/> 192.168.1.22	60:EB:69:78:7C:CC	 

Add Delete

步驟1.選中要刪除的IP&MAC繫結規則的覈取方塊。

步驟2.按一下**Trashcan**圖示刪除IP&MAC繫結規則。