

Protezione da attacchi ARP su RV315W VPN Router

Obiettivo

Il protocollo ARP (Address Resolution Protocol) viene usato per tenere traccia di tutti i dispositivi collegati direttamente all'RV315W. La protezione ARP viene utilizzata per proteggere una rete dagli attacchi ARP. Quando un pacchetto arriva su un'interfaccia (porta/LAG) definita non attendibile, un attacco ARP confronta l'indirizzo IP e l'indirizzo MAC del pacchetto con gli indirizzi IP e gli indirizzi MAC definiti in precedenza nelle regole di controllo d'accesso ARP. Se gli indirizzi corrispondono, il pacchetto viene considerato valido e inoltrato, altrimenti viene scartato. Questo articolo spiega come configurare ARP Attack Protection su RV315W VPN Router.

Dispositivo applicabile

RV315W

Versione del software

•1.01.03

ARP Attack Protection

Passaggio 1. Accedere all'utility di configurazione Web e scegliere **Sicurezza > Protezione da attacchi ARP**. Viene visualizzata la pagina *ARP Attack Protection*:

ARP Attack Protection

ARP Attack Protection: Enable Disable

Enable Auto Learning: Enable Disable

ARP Flooding Threshold: 50 (30-1000)

ARP Broadcast Interval: 15 (0-65535, 0 means disabled)

Save 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="checkbox"/>

Add Delete

Passaggio 2. Nel campo Protezione da attacchi, fare clic sul pulsante di opzione **Enable** (Abilita) per abilitare la protezione da attacchi ARP sull'RV315W.

Passaggio 3. (Facoltativo) Per abilitare RV315W per l'apprendimento automatico, fare clic su **Abilita** nel campo Abilita apprendimento automatico. Questa funzione consente all'RV315W di riconoscere gli indirizzi IP e MAC validi sulla rete.

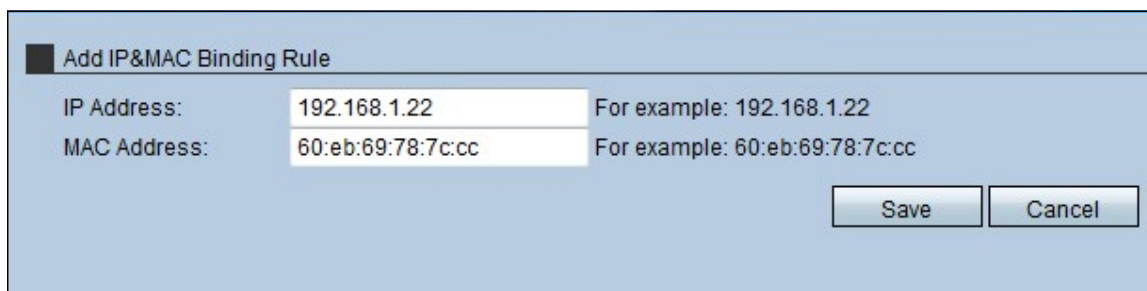
Passaggio 4. Immettere la quantità massima di pacchetti ARP che può essere ricevuta da RV315W al secondo. Se il dispositivo riceve un valore superiore a quello impostato, la protezione ARP viene applicata all'RV315W.

Passaggio 5. Inserire l'intervallo per la trasmissione ARP nel campo Intervallo trasmissione ARP. Questo intervallo determina la quantità di trasmissione ARP inviata.

Binding IP&MAC

Questa area consente all'amministratore di mappare un indirizzo IP e un indirizzo MAC per migliorare la sicurezza. Un host può accedere alla rete solo se l'indirizzo IP e l'indirizzo MAC dell'host corrispondono a quanto configurato nell'area dei binding IP e MAC.

Aggiungi binding IP&MAC



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

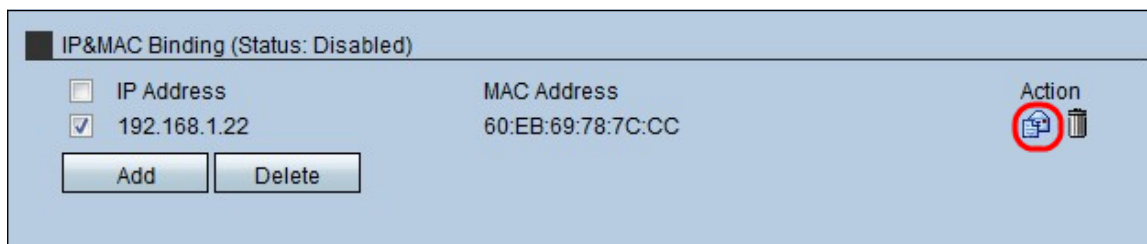
Passaggio 1. Fare clic su **Add** per aggiungere una nuova regola di binding IP&MAC. Viene visualizzata la pagina *Aggiungi regola di binding IP&MAC*:

Passaggio 2. Immettere l'indirizzo IP mappato con l'indirizzo MAC nel campo Indirizzo IP.

Passaggio 3. Immettere l'indirizzo MAC mappato con l'indirizzo IP nel campo Indirizzo MAC.

Passaggio 4. Fare clic su **Salva**. Questa regola viene visualizzata nell'elenco dei binding IP e MAC.

Modifica regola di binding IP&MAC



IP&MAC Binding (Status: Disabled)		
<input type="checkbox"/> IP Address	MAC Address	Action
<input checked="" type="checkbox"/> 192.168.1.22	60:EB:69:78:7C:CC	



Add Delete

Passaggio 1. Selezionare la casella di controllo della regola di binding IP&MAC da modificare.

Passaggio 2. Fare clic sull'icona **Inserisci** per modificare la regola di binding IP&MAC.

Elimina regola di binding IP&MAC

IP&MAC Binding (Status: Disabled)

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

Passaggio 1. Selezionare la casella di controllo della regola di binding IP&MAC da eliminare.

Passaggio 2. Fare clic sull'icona **Trashcan** per eliminare la regola di binding IP&MAC.