



**How To Guide:**  
*Configuration for ARP Spoofing Attack Prevention*

## *Introduction*

With ***IP-MAC Binding***, we can protect business network from ARP spoofing attacks. It works based on the correct IP-MAC Binding entries. The IP-MAC entries is manually entered or imported to the appliance. When receiving an ARP packet, the appliance checks whether it matches any of the IP-MAC Binding entries. If not, the appliance will ignore the ARP packets. In this way, the appliance blocks the possibly spoofed ARP packets.

To configure the IP-MAC Binding on the Q-Balancer appliance, navigate to the **Firewall > IP-MAC Binding** on the UI and follow the steps below to complete the setting:

> Click on **Add**

IP-MAC Binding

Drop packet if not on the list

Overview

ADD DELETE IMPORT CSV

<input type="checkbox"/>	Edit	Enabled	DHCP	↑↓
<input type="checkbox"/>		<input checked="" type="checkbox"/>	-	
<input type="checkbox"/>		<input checked="" type="checkbox"/>	-	

> Type in the ARP entries and enable **DHCP** individually if necessary

	Enabled	DHCP <input type="checkbox"/>	IP	MAC
	<input checked="" type="checkbox"/>	<input type="checkbox"/>	100.100.1.2	00-60-e0-6a-2b-9f
	<input checked="" type="checkbox"/>	<input type="checkbox"/>	100.100.1.5	00-00-00-08-cd-02

> Click on **OK** when it is done.

> If necessary, enable *Drop Packet if not on the list*

IP-MAC Binding

Drop packet if not on the list

Overview

Privileges

ADD

DELETE

IMPORT CSV



Edit

Enabled

DHCP ↑↓

IP



MAC



-

100.100.1.2

00-60-e0-6a-2b-9f



-

100.100.1.5

00-00-00-08-cd-02