

HOW CAN I CONFIGURE C54BRS4A FIREWALL?



To configure C54BRS4A firewall you need access to configuration menu. Start your web browser (like: Internet Explorer, FireFox or Safari).

Enter IP address of the device in address bar from your web browser, by default: <http://192.168.0.1>

Go to **Advanced -> Firewall**

Firewall Rules: Set Enabled to activate firewall

Name: Write a rule name

Action: Select if you want to create a deny rule or Allow rule.

Source:

Interface: You can select ANY (for any WAN or LAN connection), WAN (wireless connection), LAN (wired connection)

IP range Start: Write network IP address or IP start range that you want deny or allow.

IP range End: Write network IP address or IP end range that you want deny or allow. If you want apply the rule for only one computer write again same IP address than IP range Start.

Destination:

Interface: You can select ANY (for any WAN or LAN connection), WAN (wireless connection), LAN (wired connection)

IP range Start: Write network IP address or IP start range that you want deny or allow.

IP range End: Write network IP address or IP end range that you want deny or allow. If you want apply the rule for only one computer write again same IP address than IP range Start.

Protocol: Select if you want deny or allow TCP, UDP protocol or both.

Port range: Write the ports that you want deny or allow to external IP address.

Schedule: Select when you want to apply this rule, select **ALWAYS** if you want this rule active forever.
 In this example we have created a rule named “Prueba” and we have blocked IP range from 192.168.0.100 to 192.168.1.120 to don’t have access from 80.32.107.2 to 80.32.107.254 IP range.

The screenshot shows the 'Set Firewall Rule' configuration page. The 'Firewall Rules' section is active. Below it, the 'Firewall Rules List' shows a table with one row of 'N/A' values. The 'Set Firewall Rule' form contains the following fields:

- Firewall Rules: Enabled Disabled
- Name:
- Action: Allow Deny

	Interface	IP Range Start	IP Range End	Protocol	Port Range
Source:	ANY	192.168.0.100	192.168.1.120		
Destination:	ANY	80.32.107.2	80.32.107.254	ALL	* - *
Schedule:	Always				

Buttons:

Click on **Apply**.

The screenshot shows the 'Firewall Rules List' table after the rule has been applied. The table contains one rule:

	Action	Name	Protocol	Source	Destination	Schedule	
1. <input checked="" type="checkbox"/>	Deny	Prueba	ALL	ANY 192.168.0.100 192.168.1.120	ANY 80.32.107.2 80.32.107.254	* - *	Always <input type="button" value="↑"/> <input type="button" value="↓"/> <input type="button" value="✎"/> <input type="button" value="✖"/>