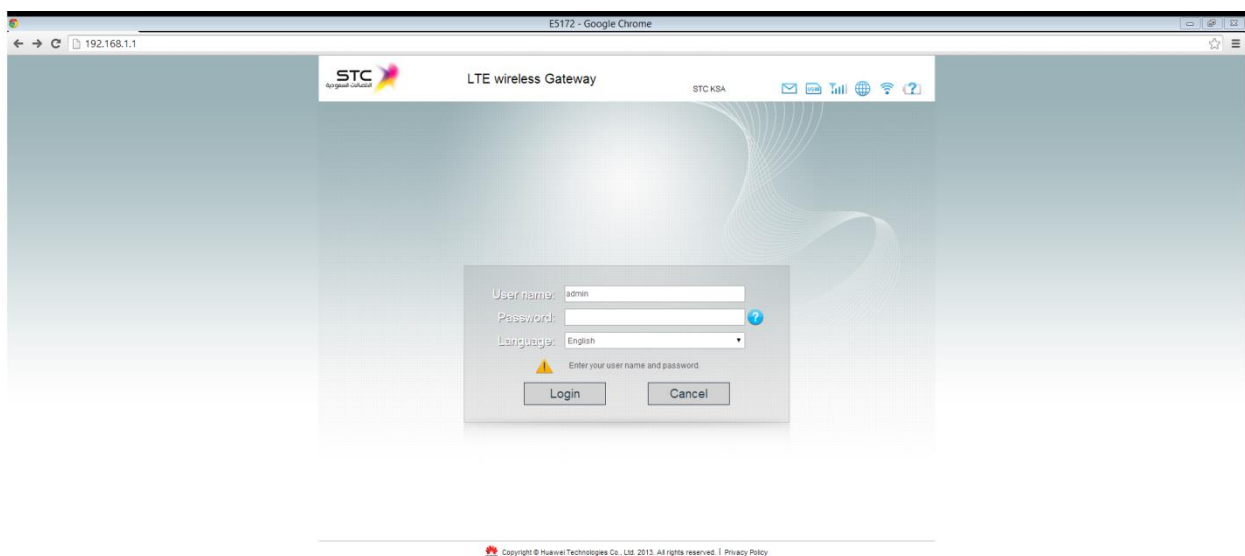


## Port Forwarding – STC Router

- 1) Port Forwarding Guide for STC Router
  - a) Open a web browser like Internet Explorer, Google Chrome or Firefox. Enter the internal IP address of your router in the address bar of your browser. For STC Routers, in general, it is http://192.168.1.1
  - b) User name: admin and Password: admin. Press Enter Key (Login).



2) Pops up below window

The screenshot shows the 'LTE wireless Gateway' status page. The left sidebar contains navigation links: Overview, Product Information, Quick Setup, and Update. The main content area is titled 'Overview' and includes the following sections:

- Internet Status:** USIM card status: USIM card normal; Network mode: 4G TDD; IPv4 status: Connected; IP address: 100.84.234.25; IPv4 DNS: 84.235.6.55, 84.235.57.230.
- Internet Usage:** Total traffic: 3.19 MB. Includes a 'Clear' button and a 'More >>>' link.
- Wi-Fi Status:** A table showing SSID, M/VC of stc, and IP Address for three different SSIDs.
- LAN Usage:** A table showing traffic statistics for ports.

Ports	Received				Sent			
	Total	Packets	Errors	Dropped	Total	Packets	Errors	Dropped
Wi-Fi	1.24 MB	6,850	0	0	6.47 MB	11,358	0	0

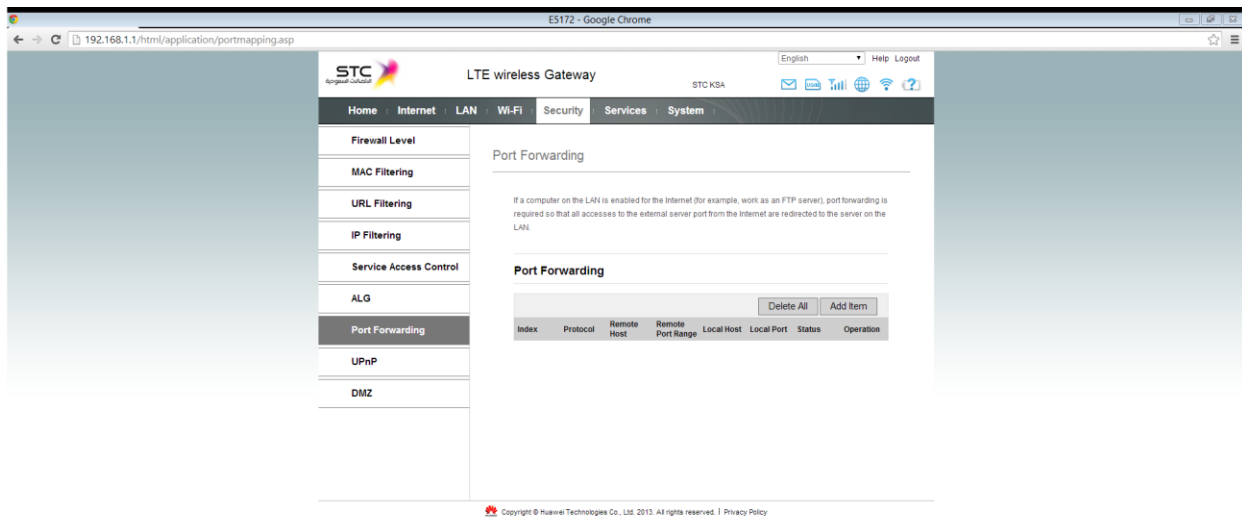
3) Click on Security and Pops up next window.

The screenshot shows the 'Security' page for the LTE wireless Gateway. The left sidebar contains navigation links: Firewall Level, MAC Filtering, URL Filtering, IP Filtering, Service Access Control, ALG, Port Forwarding, UPnP, and DMZ. The main content area is titled 'Firewall Level' and includes the following configuration options:

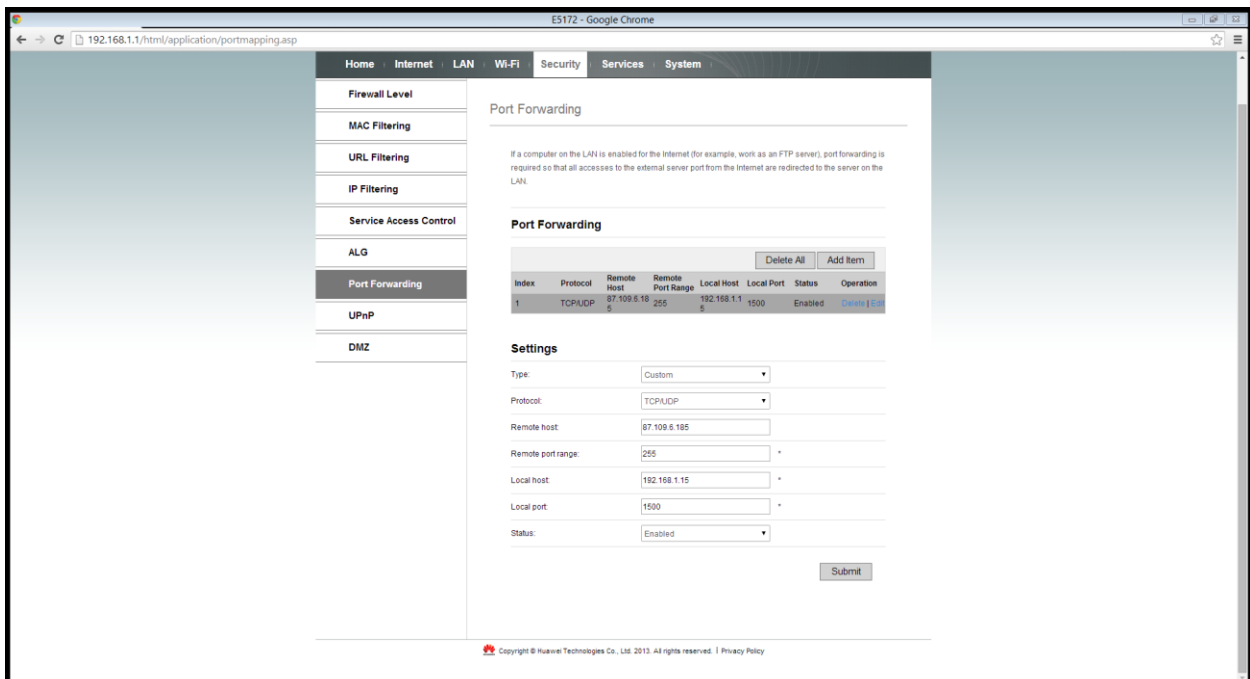
- Current firewall level:** Low (filtering disabled)
- Firewall level:** Low (filtering disabled)
- Stateful Packet Inspection (SPI) is enabled:** Inbound (from Internet to LAN) policy: Dropped; Remote authorized access will override the inbound policy; Outbound (from LAN to Internet) policy: Accepted.
- Filtering strategy:** Disabled
- MAC filtering:** Disabled
- IP filtering:** Disabled
- URL filtering:** Disabled
- DoS attack:**  Enable
- Block Denial of Service (DoS) attacks from the LAN and Internet, such as SYN floods and ping floods:**  Enable

Buttons for 'Submit' and 'Cancel' are located at the bottom right of the configuration area.

4. On the left side Click on Port forwarding and pops up below window:



5-Click on Add Item, and will pop up the below window:



In Setting: The Window needs to be filled as following:

- a- Type: Customer
- b- Protocol: TCP/UDP
- c- Remote Host: 192.168.1.15 (This is the IP address of this IP Camera, any IP Camera dos have different IP address)
- d- Remote Port Range 250 ( could be different)
- e- Local Host:87.109.6.185 (You can find it by typing: Whatismyipaddress in any browser)
- f- Local port : 150 (Your http port (typically 80) and can be changed)
- g- Status: Enabled
- h- Finally Click on Summit

6) The final Window looks like this:

