Template:Networking rutos configuration example guest wifi

☐

Contents

Introduction

Most of us are aware, that network security is extremely important. If your WiFi network is not properly secured, it makes you and all of your home or office resources vulnerable to a variety of security threats. To stay ahead of the curve, many companies and home users have guest WiFi. Unlike your regular WiFi network that you or your company members use, the guest WiFi network restricts what your guests can do in your network. It gives visitors access to the Internet connection, but nothing else making you or your company a lot more secure. This chapter is a guide on configuring a guest WiFi.

Configuring router (RUTX)

Before you start configuring the router **turn on "Advanced WebUI" mode**. You can do that by clicking the "Basic" button under "Mode", which is located at the top-right corner of the WebUI.

New WiFi AP

Login to the router's WebUI, navigate to the **Network → Wireless** page. Click **Add**. You can use either, 2.4GHz or 5GHz WiFi. Then you will be forwarded to the configuration window.
1.
2.
3.
4.

On **General Setup** tab do the following:
1. **Enable** instance.
2. Select mode **Access Point**.
3. Enter a custom **ESSID**.
4. Expand the drop-down menu **Network**.
5. Uncheck the **lan** interface.
6. Create a new interface, enter a custom name **Guest**.

Switch to **Wireless Security** tab and do the following:
1. Select **Encryption** type.
2. Select **Cipher** type.
3. Enter **Key**.
4. **Save&Apply** changes.

Wait for configuration to apply. Two Wireless Access
Points should be enabled
1.
2.
3.
4.

New LAN interface

Now go to **Network → Interfaces** and press **Edit** next to
your newly created LAN interface:
1.

In the **General setup** section, do the following:
1. Select **Protocol** - Static. Confirm by clicking "SWITCH
PROTOCOL".
2. Enter a **IPv4 address**.
3. Enter a **IPv4 netmask**.
4. Enable **DHCP server**.
5. Press **Save&Apply**.

Firewall rules

Navigate to **Network → Firewall → General Settings**.
There create a new **Zone** rule by pressing **Add** button.
Then you will be forwarded to the configuration window.
1.

In the **ZONE** page, do the following:
1. Enter a custom **Name**.
2. Add new created "*Guest*" LAN to **Covered networks**.
3. Select WAN interfaces for **Allow forward to
destination zones**.
4. Select WAN interfaces for **Allow forward from
destination zones**.
5. **Save&Apply** changes.
6.

In order to disable WebUI or SSH access to RUTX from
Guest's WiFi network navigate to the **Network →
Firewall → Traffic Rules** page and do the following:
1. Enter a custom **Name**.
2. Select "*guest_zone*" for **Source zone**.
3. Select "*lan*" for **Destination zone**.
4. Click the **Add** button. Then you will be forwarded to
the configuration window.

Do the following in the **TRAFFIC RULES** page:
1. **Enable** instance.
2. Change the **Destination zone** to "*Device (input)*".
3. Enter the **Destination port** to reject. By default ports 22, 80, 443 are used to access the web user interface and SSH.
4. Change the **Action** to "*Reject*".
5. **Save&Apply** changes.
6.

Results

If you've followed all the steps presented above, your configuration should be finished. If you are near a RUT, that is, in a wireless zone, turn on WiFi on your device and view the available networks. You should see the available SSID - "RUTX_WiFi_2G" and "Guest_WiFi". Select one of them and enter the appropriate WiFi password.

Wireless users connected to SSID: "**RUTX_WIFI**", will be assign to "LAN", and will get IP from main pool **192.168.1.0/24**.

LAN users are able to access any data from pool 192.168.1.0/24. For example they can access Web UI.
1.
2.
3.
4.

Wireless users connected to SSID: "**GUEST'S_WIFI**", will be assign to LAN "Guest", and will get IP from new pool **10.10.10.0/24**.
1.
2.
3.

Guest hosts are unable to access any data from pool 192.168.1.0/24. And access to RUTX Web UI or SSH is restricted.
1.
2.
3.