How to Configure Wi-Fi

https://campus.barracuda.com/doc/8650770/

Barracuda NextGen Firewall X101 and X201 are equipped with a Wi-Fi network module supporting IEEE 802.11 b/g/n with a maximum transmission rate of 54 Mbps and 108 Mbps in SuperG mode for compatible client devices. Using WPA and WPA2 with a RADIUS authentication server, you can encrypt wireless networks. The Barracuda NextGen Firewall X-Series can serve up to three independent Wi-Fi networks with different SSIDs. You can configure each Wi-Fi network with a landing page serving either a confirmation message or a ticketing system for guest network access.

Step 1. Configure the Wi-Fi interface

To configure basic network settings for the Wi-Fi module:

1. Go to the **NETWORK > IP Configuration** page.
2. In the **Static Interface Configuration** section, edit one of the available Wi-Fi interfaces (ath0, ath2, ath3) if you want to change the IP address configuration.
3. Click **Save**.

Step 2. Configure the Wi-Fi settings

When the static Wi-Fi network interface is available, Wi-Fi can be activated. The SSID, wireless security, and authentication can also be adjusted.

1. Go to the **NETWORK > IP Configuration** page.
2. In the **Wi-Fi Link Configuration** section, select the **Activate Wi-Fi** check box to enable Wi-Fi.
3. From the **Location** list, select the country that your firewall is located in.
4. Click **Save Changes**.

Configure radio settings

To configure the radio channel and transmission rate:

1. Click **Configure Radio** and edit the radio settings.
   - For more transmission power and a bigger range of radio reception, select a higher **mW** value from the **Power** list.
   - For higher data throughput, select a higher **Mbps** value from the **Bitrate** list.
   - To bond two channels for a transmission rate of up to 108 Mbps, set **SuperG** to **Yes**. When you enable this setting, verify that all clients connecting to this access point support SuperG mode.

2. Click **Save Changes**.
3. At the top of the page, click the warning message to execute the new network configuration.
4. Log into the firewall again.

Configure a Wi-Fi access point

To edit a Wi-Fi access point:

1. Click **Edit** for the access point you want to enable (Wi-Fi, Wi-Fi2, Wi-Fi3).
2. In the **SSID** field, enter the Service Set IDentifier (SSID). This name is displayed to Wi-Fi clients that search for available Wi-Fi signals.
3. From the **Security Level** list, select one of the following options:
   - **High** – WPA2 (Recommended).
   - **Medium** – WPA.
   - **None** – No encryption.
4. From the **Authentication** list, select one of the following options:
   - **WPA-PSK** – Use this option when key management should be done locally on the firewall. Then define a preshared key.
   - **WPA-RADIUS/EAP** – Use this option when key management is done by a RADIUS server. Then enter the RADIUS server information into the **RADIUS Configuration** section.
5. To forward clients to a landing page that displays a **Confirmation Message** or serves a **Ticketing** system, enable the feature. To give clients direct access to the Wi-Fi network, select **None**.
6. Click **Save**.

Step 3. Enable the DHCP server

To assign IP addresses to clients that are connected to the Wi-Fi network, enable the DHCP server of the firewall.

1. Go to the **NETWORK > DHCP Server** page. Clients with an active lease are listed in the **Active Leases** section.
2. In the **DHCP Server** section, set **Enable DHCP Server** to **Yes**.
3. If you change the network configuration of the default Wi-Fi and Wi-Fi2 interfaces, modify the available subnets or create a new one.
4. Click **Save Changes**.

Step 4. Configure the access rule for Wi-Fi

There is a predefined access rule named WIFI-2-INTERNET that only applies to the first Wi-Fi network (ath0). To allow other networks, you can either edit a copy of the rule for the other networks or edit

the rule directly to include all subnets.

1. Go to the **FIREWALL > Firewall Rules** page.
2. To edit a copy of the WIFI-2-INTERNET rule:
    1. Copy the WIFI-2-INTERNET rule. The rule copy is created at the bottom of the rule set.
    2. Edit the WIFI-2-INTERNET-COPY rule.
    3. Click the **Advanced** tab and change **Interface Group** to **Wi-Fi2** or **Wi-Fi3**.
3. To directly edit the the WIFI-2-INTERNET rule to include all subnets:
    1. Edit the WIFI-2-INTERNET rule.
    2. Click the **Advanced** tab and select **Matching** from the **Interface Group** list.
    3. Click the **General** tab and change **Source** to specify the Wi-Fi subnets.
4. At the top of the rule editor window, click **Save**.

Step 5. Verify the order of the access rules

Because rules are processed from top to bottom in the rule set, arrange your rules in the correct order. Also verify that your rules are placed above the BLOCKALL rule; otherwise, the rules are blocked.

After adjusting the order of rules in the rule set, click **Save Changes**.