Configure the Barracuda Web Application Firewall from the Web Interface

https://campus.barracuda.com/doc/4259884/

After specifying the IP address of the Barracuda Web Application Firewall and opening the necessary ports on your corporate firewall, configure the Barracuda Web Application Firewall from the web administration interface. This interface is accessed from a web browser on any machine that can communicate with the appliance, so it must be on the same network, or have routing set up accordingly.

Secure Access

To ensure the highest security, use HTTPS to configure your Barracuda Web Application Firewall web interface. In addition, Barracuda Networks recommends requiring HTTPS to connect to the Barracuda Web Application Firewall. To configure this setting, go to the **ADVANCED > Secure Administration** page in the Barracuda Web Application Firewall web interface.

To configure the Barracuda Web Application Firewall:

1. From a web browser, for HTTP access, enter the IP address of the Barracuda Web Application Firewall followed by port 8000. For example: **http://192.168.200.200:8000**.
   For HTTPS access, enter: **https://192.168.200.200**
2. To log into the administration interface, enter username: **admin** and password: **admin**.
3. Select **BASIC > IP Configuration**, and perform the following steps:
    1. Enter the following information in the LAN IP Address Configuration section:
        1. **IP Address** – The address that connects the Barracuda Web Application Firewall to the Real Server network. *If **Client Impersonation** is set to **Yes** on the **BASIC > Services** page, then an additional IP address should be configured on the LAN subnet of the Barracuda Web Application Firewall and this should be the default gateway configured on the back-end real servers.*
        2. **Subnet Mask** – The subnet mask tied to the LAN.
    2. Enter the IP address of your primary and secondary DNS servers (if these have not yet been set up).
    3. Enter the default hostname and default domain name of the Barracuda Web Application Firewall.
4. Click **Save**.
5. Select **BASIC > Administration**, and do the following steps:
    1. Assign a new administration password to the Barracuda Web Application Firewall (optional but highly recommended).
    2. Make sure the local time zone is set correctly. Time on the Barracuda Web Application

Firewall is automatically updated via NTP (Network Time Protocol). It requires that port 123 is opened for outbound UDP (User Datagram Protocol) traffic on your firewall (if the Barracuda Web Application Firewall is located behind one). It is important to set the time zone correctly because it is used to coordinate traffic distribution and timestamps appear in all logs and reports.

3. If desired, change the port number used to access the Barracuda Web Application Firewall administration interface. The default port is 8000.
4. Enter a web administration session expiration length (in minutes), after which an administrator will be required to log back in.
5. (*Optional*) Specify your local SMTP server. Enter the email address for your Administrator where the system should send threat email alerts and notifications.
6. Click **Save**.