Configure the Barracuda Web Application Firewall from the Web Interface

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

After you specify the IP address of the Barracuda Web Application Firewall and open the necessary ports on your corporate firewall, configure the Barracuda Web Application Firewall from the web administration interface. You can access this interface from a web browser on any machine that communicates with the appliance. The machine must be on the same network or have routing set up accordingly.

Secure Access

Barracuda strongly recommends using HTTPS to configure and connect to the Barracuda Web Application Firewall to ensure the highest security. 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, enter the IP address of the Barracuda Web Application Firewall followed by port 8000 for HTTP access. For example, `http://192.168.200.200:8000` .
   For HTTPS access, use `https://192.168.200.200`.
2. To log into the administration interface, enter **admin** for the username. For the password:
   If your appliance serial number is higher than 1311431, then the default administrator password is the *numeric portion of the serial number*. If your serial number is 1311431 or lower, then the default administrator password is *admin*. For help finding the serial number of your appliance, see Serial Number for Hardware and Virtual Appliances.
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 connecting the Barracuda Web Application Firewall to the Real Server network. If **Client Impersonation** is set to **Yes** in the **BASIC > Services** page, then an additional IP address should be configured on the LAN subnet of the Barracuda Web Application Firewall. This IP address 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 perform the following steps:
   1. Assign a new administration password to the Barracuda Web Application Firewall

(Optional but strongly recommended).

2. Verify that the local time zone is correctly set. The time on the Barracuda Web Application Firewall is automatically updated via NTP (Network Time Protocol). NTP requires port 123 to be 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 the logs and reports.
3. Change the port number used to access the Barracuda Web Application Firewall administration interface. The default port is 8000. *(Optional)*
4. Enter a web administration session expiration length (in minutes), after which an administrator will be required to log back in.
5. Specify your local SMTP server, and enter an email address for your administrator where the system will send threat email alerts and notifications. *(Optional)*

6. Click **Save**.