How to Configure the Captive Portal

https://campus.barracuda.com/doc/11142125/

The captive portal intercepts unauthorized users HTTP or HTTPS connections and redirects them to a login page. After successful authentication the user is forwarded to the original destination. This type of authentication is used to allow HTTP/HTTPS access to authenticated users. Access rules using inline authentication do not block non HTTP or HTTPS traffic even from unauthorized users. To avoid browser certificate errors, use a signed SSL certificate or install the root certificate of the self-signed certificate on all client computers using Inline Authentication.

Before you begin:

- Verify that the confirmation message and ticketing features are disabled. Go to the **NETWORK**> **IP Configuration** page and edit the relevant Wi-Fi interface to specify that there is no Landing Page.
- Before configuring the captive portal for use with Wi-Fi, see How to Configure Wi-Fi to verify that you have correctly configured Wi-Fi. Also ensure that users are connected to the Wi-Fi network of the Barracuda NextGen X-Series Firewall.

Configure the Captive Portal

1. Go to the **FIREWALL > Captive Portal** page.
2. In the **Basic Configuration** section, enable the captive portal, specify the networks from which unauthenticated users are redirected to the captive portal, select the method of authenticating users, and edit the user access policies.
3. If you are using local authentication, go to the **USERS > Local Authentication** page to create your list of allowed users and groups.
4. On the **FIREWALL > Firewall Rules** page, set up a firewall rule (plus one for Wi-Fi, if applicable) to allow traffic for authenticated users. For example, you can create a firewall rule with the following settings to allow successfully authenticated users from a Wi-Fi network at 192.168.201.0/24 to access the Internet. When using the default firewall rules of an X-Series Firewall, no additional rule is necessary because the LAN-2-Internet rule allows Internet access from the trusted LAN.
   - **General** tab
     - **Action**: **Allow**
     - **Connection**: **Dynamic SNAT**
     - **Service**: **HTTP+S**
     - **Source**: `192.168.201.0/24`
     - **Destination**: **Internet** (Network Object)
   - **Users/Time** tab
     - Add **All Authenticated Users**.

5. Add a BLOCK access rule to block unauthenticated users with a source IP address in the captive portal network. Place this rule below your custom rule or below the **LAN-2-Internet** rule.
   - **General** tab
     - **Action**: **Block**
     - **Service**: **Any**
     - **Source**: `192.168.201.0/24`
     - **Destination**: **Any** (Network Object)
   - **Users/Time** tab
     - **Authenticated Users** must be empty.

Barracuda Networks recommends that you select **Unclassified** for the **Classification** of the network interface that serves the captive portal.

SSL Certificate and Encryption Settings

To avoid browser warnings caused by using a self-signed certificate, you can upload a signed certificate or your own trusted server certificate to the Barracuda NextGen Firewall Certificate Manager.

1. Go to **ADVANCED > Certificate Manger** page.
2. Upload or create an SSL certificate for the captive portal. For more information, see How to Use and Manage Certificates with the Certificate Manager.

   The **Common Name** of the certificate must contain an IP address or hostname resolving to the IP address the captive portal is listening on.
3. Go to the **FIREWALL > Captive Portal** page.
4. In the **HTTPS Configuration** section, select the **Encryption**:
   - **TLS Strong Encryption**– (Recommended) TLS with strong ciphers. Currently the following cipher string is used for strong encryption: HIGH:!aECDH:!ADH:!3DES:!MD5:!DSS:!RC4:!EXP:!eNULL:!NULL:!aNULL.
   - **TLS/SSLv3** – TLS and SSLv3 with no restriction on which ciphers can be used.
   - **TLS/SSLv3/SSLv2** – TLS, SSLv3, and SSLv2 with no restriction on which ciphers can be used.
   - **TLS All Ciphers** – TLS with no restriction on which ciphers can be used.
5. Select the SSL certificate you created or uploaded to the **Certificate Manager** from the **Singed Certificate** list.
6. Click **Save**:

Monitoring and Managing Authentication Users

On the **BASIC > User Activity** page, you can view currently authenticated users. You can also disconnect specific users.