# How to Configure Guest Access with a Confirmation Page

https://campus.barracuda.com/doc/79463021/

The guest access confirmation page allows you to control access to the Internet or other networks by only allowing authenticated users. Unauthenticated users are redirected to a customizable confirmation form on the Barracuda CloudGen Firewall. After clicking **Proceed** a user in the form LP-<IP Address> is created. Users who have already been authenticated or have been identified by the Barracuda DC Agent are not prompted to log in. The authentication expires after 20 minutes.

## Step 1. Enable Automatic Authentication Redirection

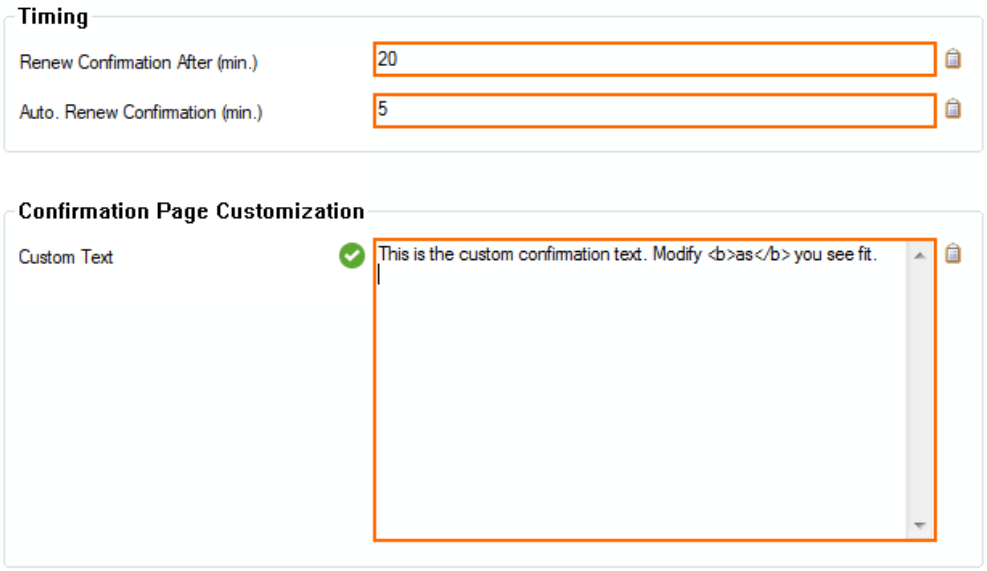
Enable automatic redirection for the clients that should be redirected to the confirmation page.

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Settings**.
2. Click **Lock**.
3. In the left menu, click **Authentication**.
4. Click **Edit** next to **Operational Settings**.
5. In the **Automatic Authentication Redirection** section, click **+** next to the **Affected networks** and add the source networks for the clients that should be redirected to the authentication page.
6. Click **OK**.
7. Click **Send Changes** and **Activate**.

## Step 2. Enter the Guest Access Confirmation Text

You can customize the text the user has to acknowledge.

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Settings** .
2. Click **Lock**.
3. In the left menu, click **Guest Access**.
4. (optional) Modify the **Renew Confirmation After (min.)** entry to configure a longer or shorter authentication expiration time.
5. (optional) Modify the **Auto Renew Confirmation (min.)** entry. During this time span (in minutes) the user is automatically logged in again without having to re-authenticate.
6. Enter a **Custom Text**. You can use HTML tags.

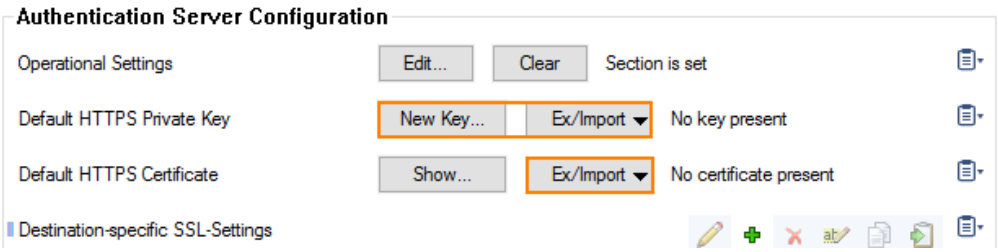



7. Click **Send Changes** and **Activate**.

## Step 3. Create Certificate for Authentification

For authentication, a private key and an HTTP certificate has to created.

1. Go to **CONFIGURATION > Configuration Tr ee > Box > Assigned Services > Firewall > Forwarding Settings.**
2. In the left menu, select **Authentication**.
3. If you want to create a new private HTTPS key, click **New Key...**
    1. The Key Length windows is displayed.
    2. Modify the key length or just click **OK** to accept.
4. (alternatively) If you want to import a private HTTPS key, click Ex/Import for **Default HTTPS Private Key**.
    1. **Import from Clipboard** – Select this list entry if you you have previously copied a key to the clipboard.
    2. Import from File – Select this entry if you want to import a key from a file.
5. For creating a new certificate, click **Ex/Import** for **Default HTTPS Certificate**.
    1. From the list, choose **Edit...** to fill out the form for the certificate and finally click **OK**.
    2. (alternatively) From the the list, choose **Import** to import information from different sources.



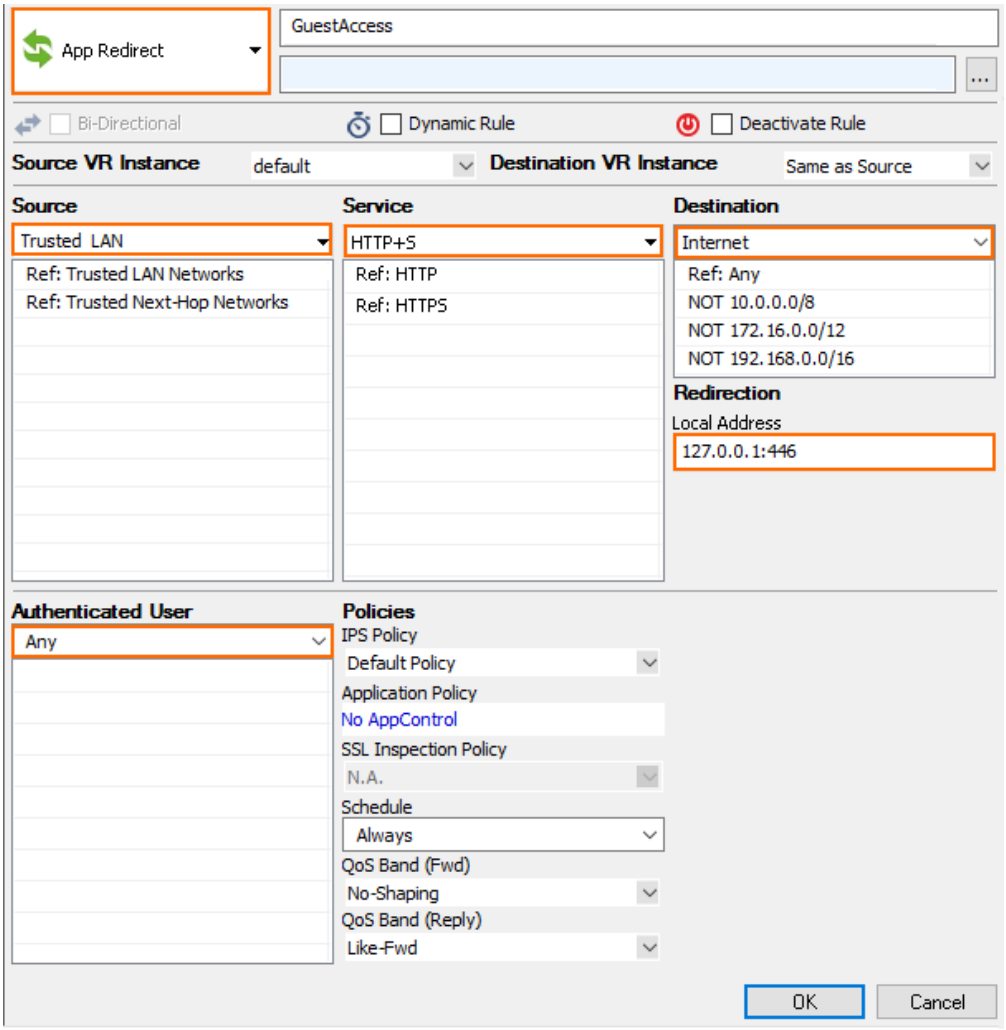

6. Click **Send Changes**.

7. Click **Activate**.

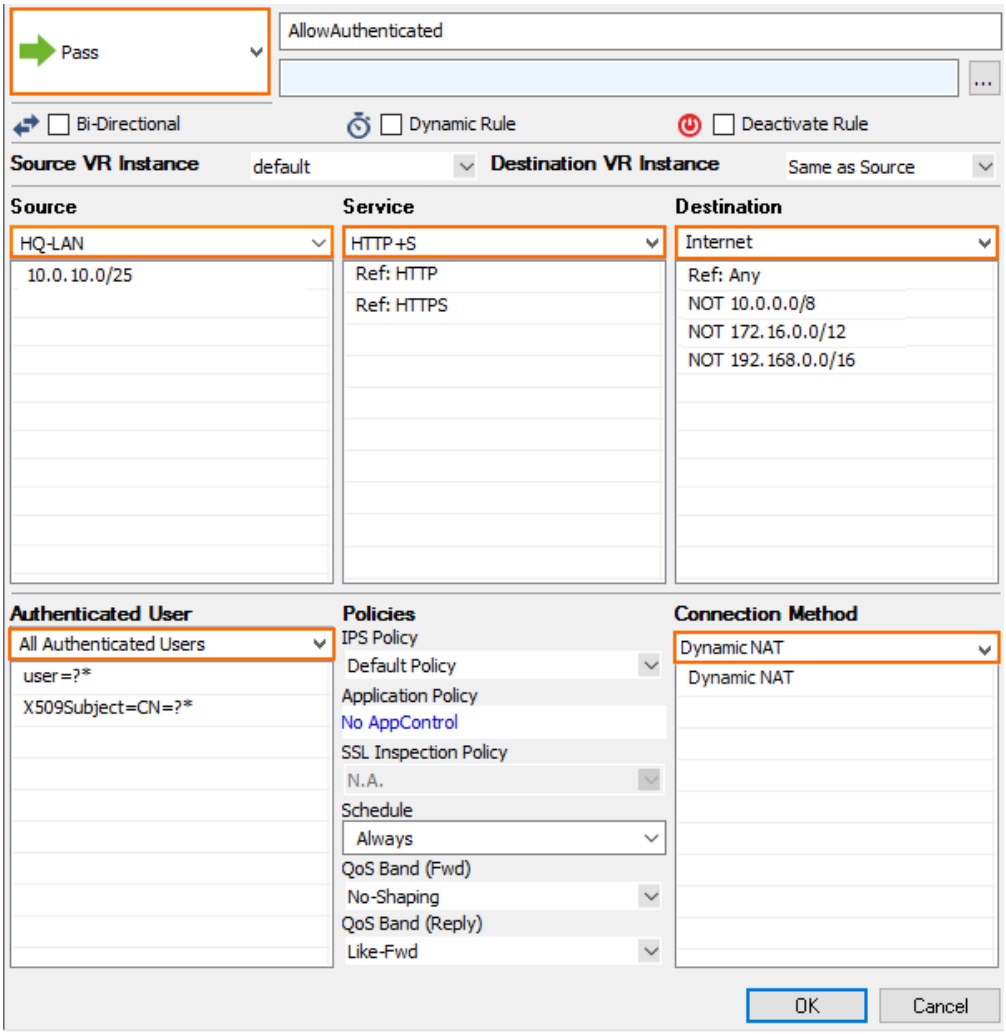
## Step 4. Create an App Redirect Access Rule and Pass Access Rule (Optional)

Create an app redirect access rule that redirects the user to the FWauth daemon on Port TCP 446 on the Barracuda CloudGen Firewall, which displays the confirmation page and redirects the user afterwards. Additonally, create a pass access rule that allows HTTP and HTTPS access for authenticated users only. If your access rule set already contains a pass rule that allows Internet access for HTTP/HTTPS traffic, make sure to modify it according to the settings below and place it above the app redirect access rule.

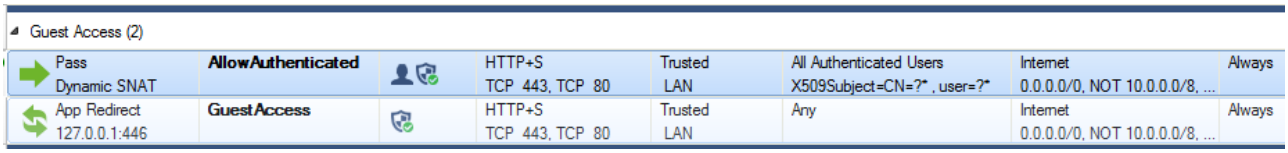
1. Go to **CONFIGURATION > Configuration Tr ee > Box > Assigned Services > Firewall > Forwarding Rules**.
2. Click **Lock**.
3. Create an **App Redirect** access rule:
   - **Action** – Select **App Redirect**.
   - **Source** – Select the source network(s).
   - **Service** – Select **HTTP+S**. Since the user has to use a browser to access the confirmation page, limit the service to HTTP and HTTPS.
   - **Destination** – Select the destination. E.g., **Internet**.
   - **Redirection** – Enter `127.0.0.1:446`
   - **Authenticated User** – Select **Any**.
4. Click **OK**.




5. Create an **Pass** access rule:
   - **Action** – Select **Pass**.
   - **Source** – Select the source network(s).
   - **Service** – Select **HTTP+S**.
   - **Destination** – Select the destination. E.g., **Internet**.
   - **Connection Method** – Select **Dynamic Source NAT**
   - **Authenticated User** – Select **All Authenticated Users**.
6. Click **OK** .




7. Place the access rule so that it is the first rule to match for HTTP+S and unauthenticated users, but after the rule allowing DNS access if the DNS server is not in the local network.
8. Verify the correct access rule order.




9. Click **Send Changes** and **Activate**.

## Log in Using the Guest Access Confirmation Page

1. Open the browser and enter an URL.
2. If you are unauthenticated, you are redirected to the confirmation page.
3. Click **Proceed**.
4. You are now redirected to the original URL.

## Figures

1. CP_confirm01.png
2. firewall_forwarding_settings_https_create_certificate.png
3. CP_confirm02.png
4. CP_Auth_Users.png
5. CP_Rule_Order.png