

How to Configure Guest Access with a Confirmation Page

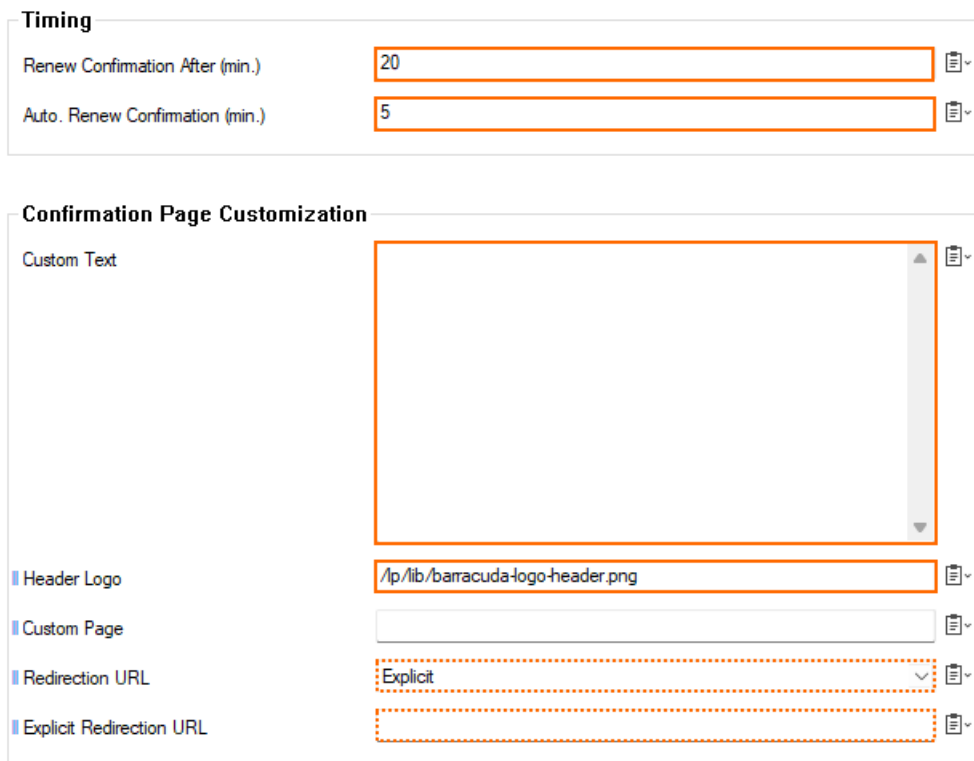
<https://campus.barracuda.com/doc/98210292/>

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. Enter the Guest Access Confirmation Text

Customize the confirmation message the users have to acknowledge when they get 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 **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. Navigate to the section **Confirmation Page Customization**.
7. Enter a **Custom Text**. You can use HTML tags.
8. (optional) If you want to redirect the guest to a custom webpage:
 1. In the left menu bar, click **Switch to Advanced**.
 2. From the list **Redirection URL**, select **Explicit**.
 3. Enter a valid URL into the edit field for **Explicit Redirection URL**.



The screenshot displays two configuration sections in the Barracuda CloudGen Firewall interface. The 'Timing' section contains two input fields: 'Renew Confirmation After (min.)' with the value '20' and 'Auto. Renew Confirmation (min.)' with the value '5'. The 'Confirmation Page Customization' section includes a large text area for 'Custom Text', a 'Header Logo' field with the path '/ip/lib/barracuda-logo-header.png', and three fields for redirection: 'Custom Page' (empty), 'Redirection URL' (set to 'Explicit'), and 'Explicit Redirection URL' (empty). Each field has a copy icon to its right.

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

Step 2. Create a Certificate for Authentication

For authentication, you must create a certificate and a private key.

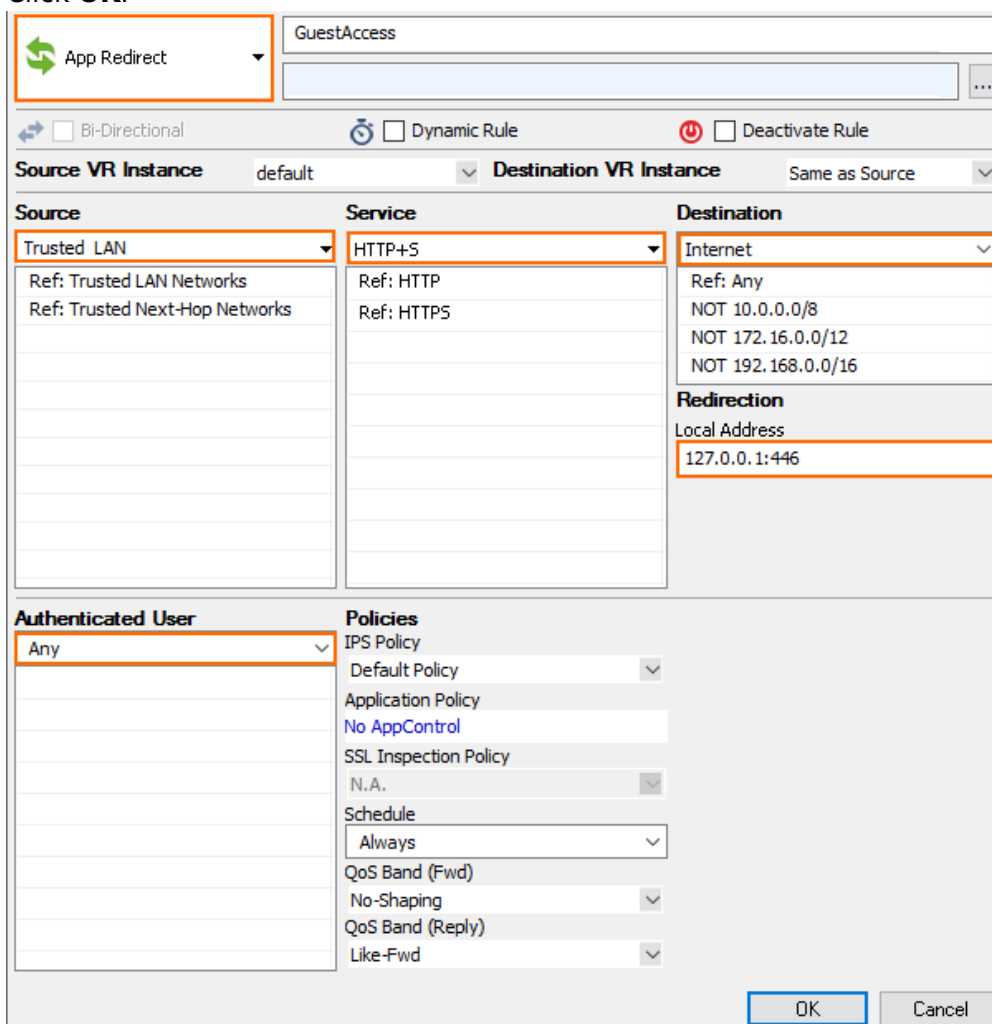
1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Settings**.
2. In the left menu, select **Authentication**.
3. Click **Lock**.
4. Import or create the **Default HTTPS Certificate** and **Default HTTPS Private Key**.
The **Name** of the certificate must be the IP address or a FQDN resolving to the IP address of the Barracuda CloudGen Firewall. This value is used to redirect the client to the authentication daemon.
5. Click **Send Changes** and **Activate**.

Step 3 Create an App Redirect Access Rule and Pass Access Rule

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. Additionally, 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 Tree > 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**.



The screenshot shows the configuration window for an 'App Redirect' rule. The rule name is 'GuestAccess'. The action is 'App Redirect'. The source is 'Trusted LAN', the service is 'HTTP+S', and the destination is 'Internet'. The redirection local address is '127.0.0.1:446'. The authenticated user is 'Any'. The policies are set to: IPS Policy (Default Policy), Application Policy (No AppControl), SSL Inspection Policy (N.A.), Schedule (Always), QoS Band (Fwd) (No-Shaping), and QoS Band (Reply) (Like-Fwd). The 'OK' button is highlighted.

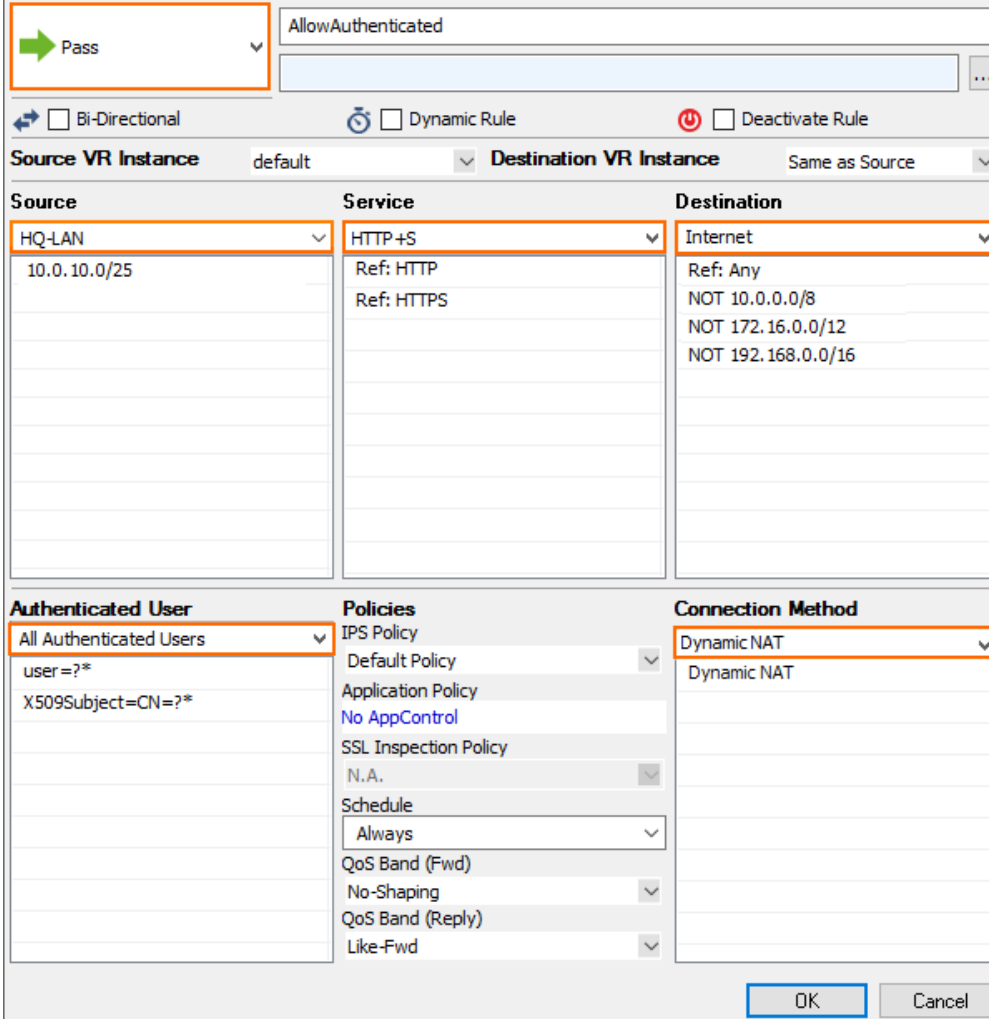
Source	Service	Destination
Trusted LAN	HTTP+S	Internet

Authenticated User	Policies
Any	IPS Policy: Default Policy
	Application Policy: No AppControl
	SSL Inspection Policy: N.A.
	Schedule: Always
	QoS Band (Fwd): No-Shaping
	QoS Band (Reply): Like-Fwd

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**.



Pass

AllowAuthenticated

☐ Bi-Directional ☐ Dynamic Rule ☐ Deactivate Rule

Source VR Instance: default Destination VR Instance: Same as Source



Source	Service	Destination
HQ-LAN 10.0.10.0/25	HTTP+S Ref: HTTP Ref: HTTPS	Internet Ref: Any NOT 10.0.0.0/8 NOT 172.16.0.0/12 NOT 192.168.0.0/16

Authenticated User	Policies	Connection Method
All Authenticated Users user=?* X509Subject=CN=?*	IPS Policy Default Policy Application Policy No AppControl SSL Inspection Policy N.A. Schedule Always QoS Band (Fwd) No-Shaping QoS Band (Reply) Like-Fwd	Dynamic NAT Dynamic NAT

OK Cancel

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.

Guest Access (2)							
Pass	AllowAuthenticated		HTTP+S	Trusted LAN	All Authenticated Users	Internet	Always
Dynamic SNAT			TCP 443, TCP 80		X509Subject=CN=?*, user=?*	0.0.0.0/0, NOT 10.0.0.0/8, ...	
App Redirect	GuestAccess		HTTP+S	Trusted LAN	Any	Internet	Always
127.0.0.1:446			TCP 443, TCP 80			0.0.0.0/0, NOT 10.0.0.0/8, ...	

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_confirm_with_optional_redirect_01.png
2. CP_confirm02.png
3. CP_Auth_Users.png
4. CP_Rule_Order.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.