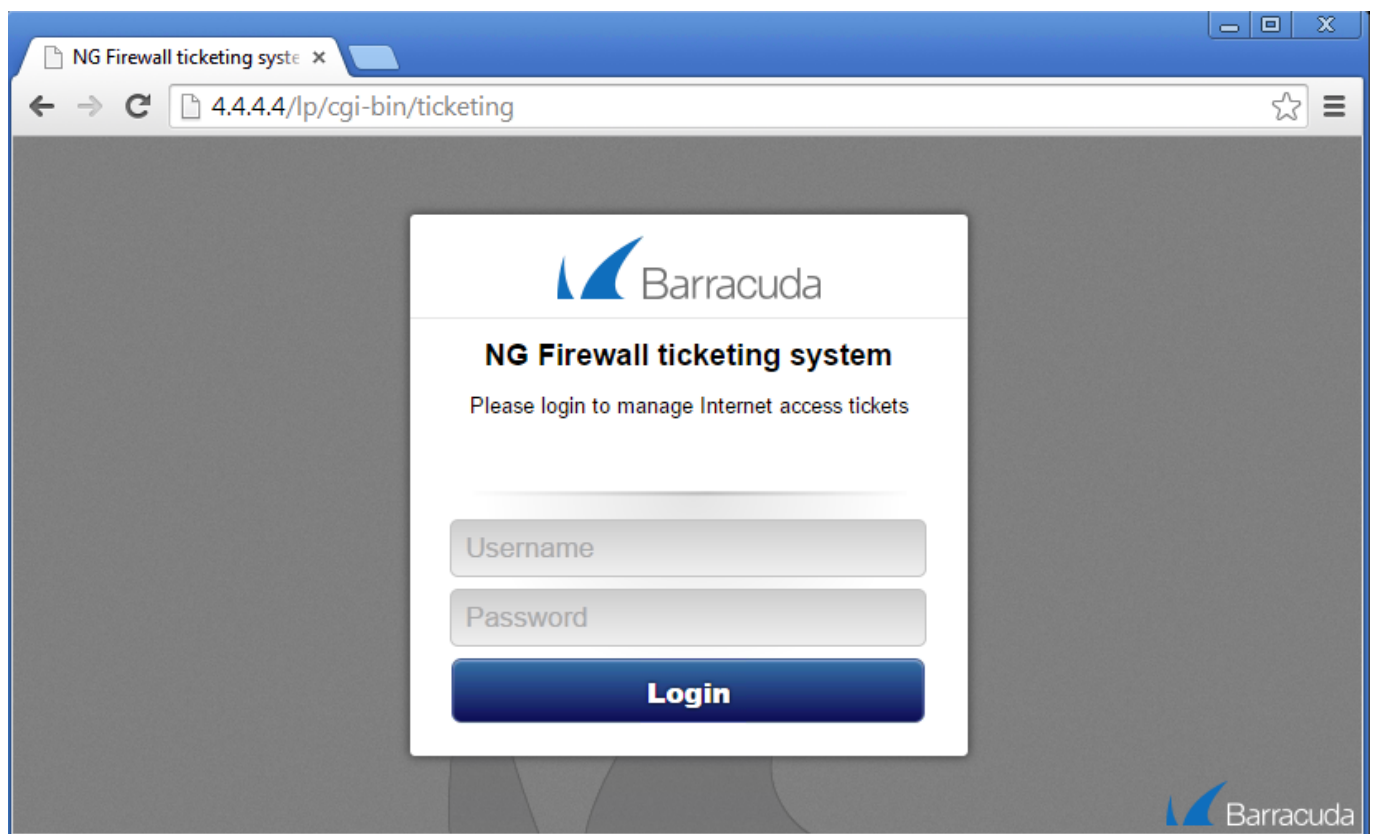


How to Configure Wi-Fi Guest Access

<https://campus.barracuda.com/doc/48203106/>

Wi-Fi guest access can be used only for Wi-Fi users. For a more generic guest access configuration (ticketing and confirmation page), see [Firewall Authentication and Guest Access](#).

You can configure a fully customizable web-based portal that displays a disclaimer and requests login credentials from users when they first try to access the Internet or special network segments. For example, you can configure a Guest Access page that looks similar to the following:



To administer tickets for the Guest Access, you can also enable a web-based backend user interface for creating, deleting, managing, or printing tickets.

Step 1. Enable Guest Access

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > Wi-Fi > Wi-Fi AP Configuration**.
2. Click **Lock**.
3. From the **Guest Access** list, select either **Confirmation** or **Ticketing**. If you want to disable

the Guest Access, select **None**.

- Click **Send Changes** and **Activate**.

Step 2. Configure Guest Access

- Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > Firewall > Forwarding Settings**.
- In the left menu, select **Guest Access**.
- Click **Lock**.
- You can specify the following settings for the Guest Access:

Section	Setting	Description
Timing	Renew Confirmation After (min.)	The time period after which users must re-enter their login credentials. When deleting ticketing users, the user can still access the guest network for the duration of this value. To force a user to be blocked immediately, you must delete the ticketing or confirmation user in FIREWALL > Users and terminate all existing firewall sessions in FIREWALL > Live for that user.
	Auto. Renew Confirmation	Confirmation is automatically renewed within this time period, after the last confirmation has timed out. The user does not need to re-enter login credentials.
Customization (Confirmation)	Custom Text	Custom text that is displayed on the confirmation window. If left blank, the default Barracuda Networks disclaimer is displayed.
	Header Logo	(Only visible in advanced view) The customizable header image for confirmation Guest Access. In order for the web server to access the header logo for Guest Access, the image file must be stored in the directory <code>/lp/lib</code> . Therefore, it is necessary to enter the full path, which consists of the path and the fully qualified file name that also includes the file type. For example: <code>/lp/lib/myCustomLogoHeader.png</code> Add the fully qualified path, including the file name with the file name extension as the reference for the header logo. For example: <code>/lp/lib/myCustomLogoHeader.png</code> The maximum size for the image is 250 x 60 pixels.
	Custom Page	(Only visible in advanced view) A custom <code>index.html</code> file for the Guest Access. See the description below this table to learn how to configure the custom HTML code. Before specifying an <code>index.html</code> page in this field, you must upload it. From the Configuration menu in the left navigation pane, click Authentication Messages . Add the file to the Custom HTML Files table.

Customization (Ticketing)	Custom Text	Custom text that is displayed on the confirmation window. If left blank, the default Barracuda Networks disclaimer is displayed.
	Header Logo	(Only visible in advanced view) The customizable header image for ticketing Guest Access. From the Configuration menu in the left navigation pane, click Authentication Messages . Add the picture to the Custom HTML Files table within the LP sub-directory.
	Custom Page	(Only visible in advanced view) A custom <i>index.html</i> file for the Guest Access. See the description below this table to learn how to configure the custom HTML code. Before specifying an <i>index.html</i> page in this field, you must upload it. From the Configuration menu in the left navigation pane, click Authentication Messages . Add the file to the Custom HTML Files table.
Ticketing Administration User	Username	The username for the administrator of the ticketing list backend page.
	Password	The password for the administrator of the ticketing list backend page.
Additional Guest Access Networks	Network	Defines additional network segments (except the Wi-Fi network where Guest Access is served to clients). You can select a network object or manually enter a network segment.
	Type	The type of Guest Access for the additional network segments. You can select Confirmation or Ticketing .

The customizable *index.html* page mentioned above is also the HTML template for the **Next Token**, **New Pin**, **Accept New Pin**, and **One-time Password Authentication** pages. You can use special tags in HTML comments within the *index.html* to enter content to be displayed only on the respective pages. The following tags are available:

- Next token: %%NEXTTOKENMSG-BEGIN%% %%NEXTTOKENMSG-END%%
- New pin: %%NEWPIN-BEGIN%% %%NEWPIN-END%%
- Accept new server-generated PIN: %%ACCEPTNEWPIN-BEGIN%% %%ACCEPTNEWPIN-END%%
- One-time password authentication: %%OTP-BEGIN%% %%OTP-END%%

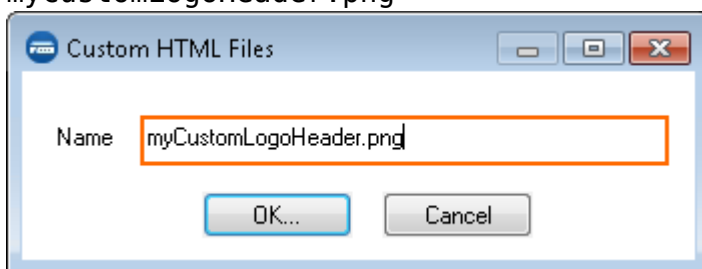
Start your conditional HTML code block with a comment tag (`<!--`) directly followed by the respective special opening tag, and end it with a closing comment tag (`-->`) directly preceded by the respective special ending tag.

The following code block writes the token ID into a hidden form field and is therefore always required. Copy and paste it into your HTML page.


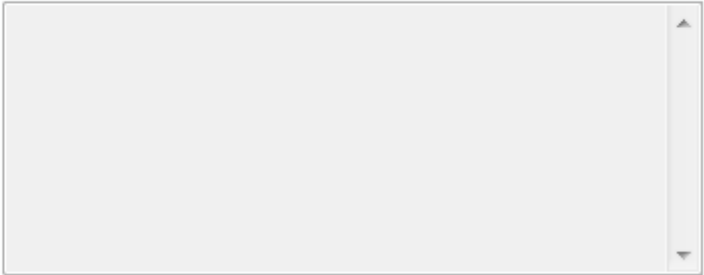


(optional) Step 3. Upload Custom Header Logo for Guest Access

In case you want to display custom header logos for Guest Access, you must upload the image file. Note that in order for the web server to access the file, it is necessary to set the path to `/lp/lib`.

1. In the left menu, click **Authentication Messages**
2. Click **+** to add a custom image header file.
3. In the window, enter the full file name including the file extension, i.e., `myCustomLogoHeader.png`



4. From **Type**, select **Binary**.
5. Enter `/lp/lib` for the **Path**.
6. Click **Ex/Import** to select the source where to upload the header logo image from.

Type	Binary	
Path	/lp/lib/	
HTML		
Binary	Ex/Import 	No data set 

7. Click **OK**.
8. Click **Send Changes**.
9. Click **Activate**.

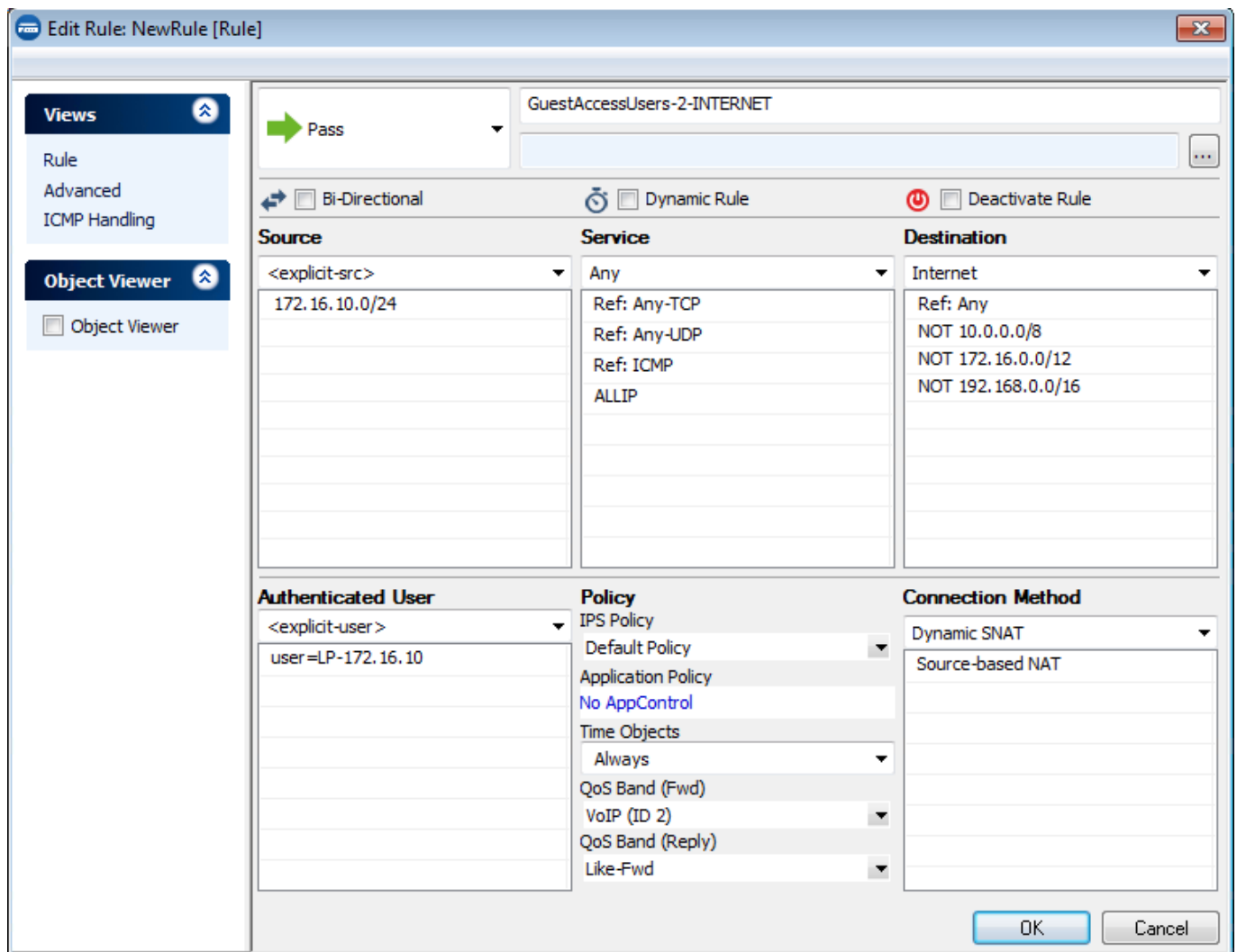
View Authenticated Users

To see a list of authenticated users, go to the **FIREWALL > Users** page. On this page, successfully authenticated users are listed with either the LP- or TKT- prefix, followed by the IP address of the client.

Authenticated Users in Access Rules

Using the IP addresses on the **FIREWALL > Users** page, you can create access rules to regulate network access for authenticated users. In the rule editor window, specify the authenticated users in the **Authenticated User** field.

For example, a user is successfully authenticated from the Guest Access on a client with the IP address of 172.16.10.100. On the **FIREWALL > Users** page, the authenticated user is displayed with the following identity: LP-172.16.10.100. In the following access rule example, this identity string is used to allow Internet access for users that are authenticated on the Guest Access in the 172.16.10.0/24 network:



Edit Rule: NewRule [Rule]

Views: Rule, Advanced, ICMP Handling

Object Viewer: Object Viewer

Rule Name: GuestAccessUsers-2-INTERNET

Action: Pass

Bi-Directional: ☐ Dynamic Rule: ☐ Deactivate Rule: ☐

Source	Service	Destination
<explicit-src> 172.16.10.0/24	Any Ref: Any-TCP Ref: Any-UDP Ref: ICMP ALLIP	Internet Ref: Any NOT 10.0.0.0/8 NOT 172.16.0.0/12 NOT 192.168.0.0/16

Authenticated User	Policy	Connection Method
<explicit-user> user=LP-172.16.10	IPS Policy Default Policy Application Policy No AppControl Time Objects Always QoS Band (Fwd) VoIP (ID 2) QoS Band (Reply) Like-Fwd	Dynamic SNAT Source-based NAT

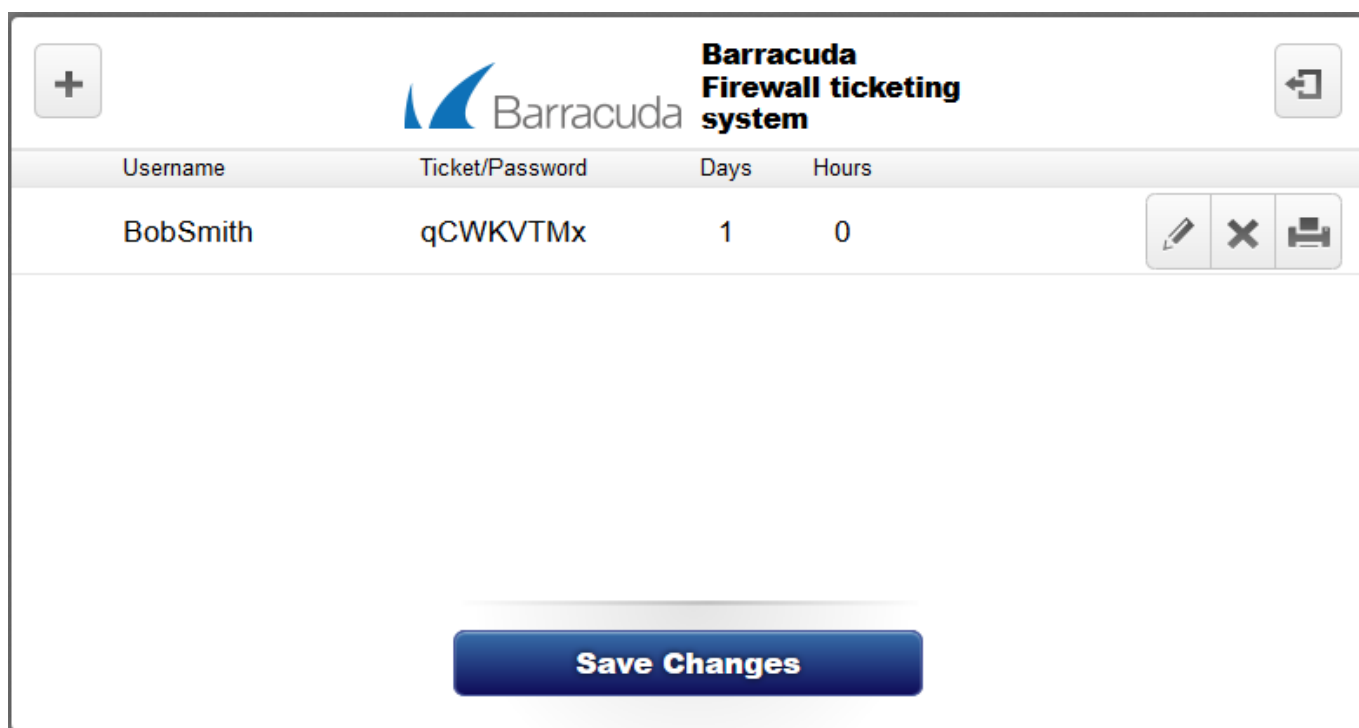
OK Cancel

The user=LP-172.16.10 string indicates that this access rule applies only to users who are residing in the 172.16.10.0/24 network and are currently authenticated through the Guest Access.

For more information on creating access rules, see [Access Rules](#).

Guest Access Ticketing System

To administer tickets for the Guest Access, the NextGen Firewall F-Series offers a web-based backend user interface for creating, deleting, managing, or printing tickets.



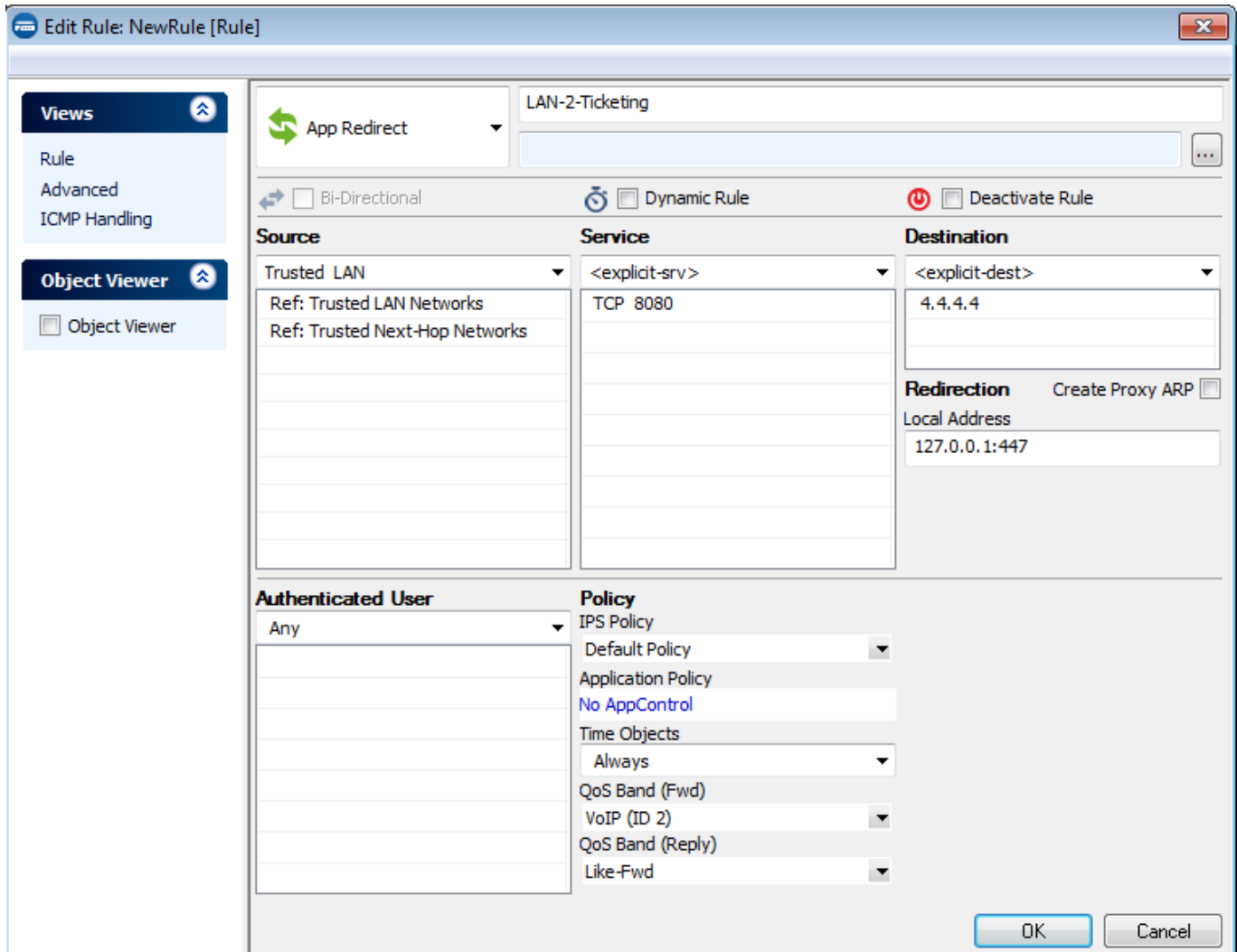
Username	Ticket/Password	Days	Hours
BobSmith	qCWKVTMx	1	0

Save Changes

Access to the Admin Ticket Interface

HTTP requests (port 80/443) that are addressed to the system that is running the Guest Access must be forwarded to the local web server of the system. Create an access rule that forwards these HTTP requests to the local web server.

It is recommended that you use TCP port 8080 (or similar). For more information, see [How to Create an App Redirect Access Rule](#).



Edit Rule: NewRule [Rule]

Views

- Rule
- Advanced
- ICMP Handling

Object Viewer

- Object Viewer

App Redirect **LAN-2-Ticketing**

☐ Bi-Directional ☐ Dynamic Rule ☐ Deactivate Rule

Source	Service	Destination
Trusted LAN	<explicit-srv>	<explicit-dest>
Ref: Trusted LAN Networks	TCP 8080	4.4.4.4
Ref: Trusted Next-Hop Networks		

Redirection ☐ Create Proxy ARP

Local Address
127.0.0.1:447

Authenticated User	Policy
Any	IPS Policy
	Default Policy
	Application Policy
	No AppControl
	Time Objects
	Always
	QoS Band (Fwd)
	VoIP (ID 2)
	QoS Band (Reply)
	Like-Fwd

OK **Cancel**

Ticketing Next Steps

After you create an access rule that grants access to the ticket system, you can connect to the ticketing interface from a web browser.

1. In a web browser, enter: `http:///lp/cgi-bin/ticketing`
2. On the ticketing system login page, enter the login credentials that you specified in the **Ticketing Administration User** section when configuring the Guest Access.

For more information, see [How to Manage Guest Tickets - User's Guide](#).

Figures

1. GuestAccess01.png
2. MyCustomLogoHeader.png
3. select_header_image_logo_for_upload.png
4. Wifi_GA_02.png
5. ticket_admin_3.PNG
6. Wifi_GA_01.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.