How to Configure Guest Access with the Ticketing System

https://campus.barracuda.com/doc/42044438/

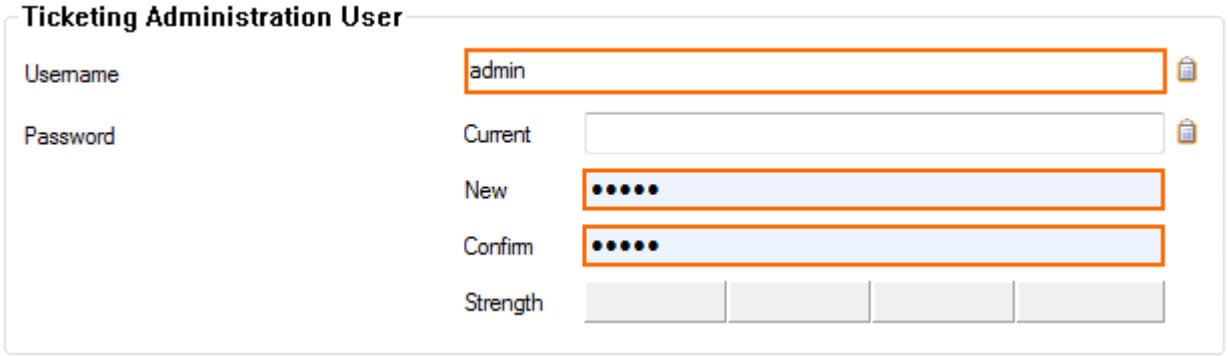
Set up a login or ticketing system to temporarily grant access to guest users. Ticketing admins assign guest tickets to the users. The user credentials on these tickets are then used by the guest users when prompted to authenticate. Tickets expire after a set period of time chosen by the ticket administrator.

In this article:

Step 1. Create the SSL Certificate and Ticket Admin User

Create or upload an SSL certificate for the ticketing interface and create the ticketing admin user.

1. Go to the **Forwarding Settings** page (**Config** > **Box** > **Virtual Servers** > ***your virtual server*** > **Assigned Services** > **Firewall**).
2. In the left menu, select **Authentication**.
3. Click **Lock**.
4. Import or create the **Default HTTPS Private Key** and **Default HTTPS Certificate**.
   This SSL certificate is also used by inline and offline firewall authentication. If inline authentication is used the **Name** of the certificate must be the IP address or a FQDN resolving to the IP address of the Barracuda NG Firewall. This value is used to redirect the client to the authentication daemon.
5. In the left menu, click on **Guest Access**.
6. (optional) Enter a custom **Confirmation text** for the ticketing interface.
7. In the **Ticketing Administration User** section, enter **Username** and **Password** for the ticketing admin. You can only create one ticket admin.

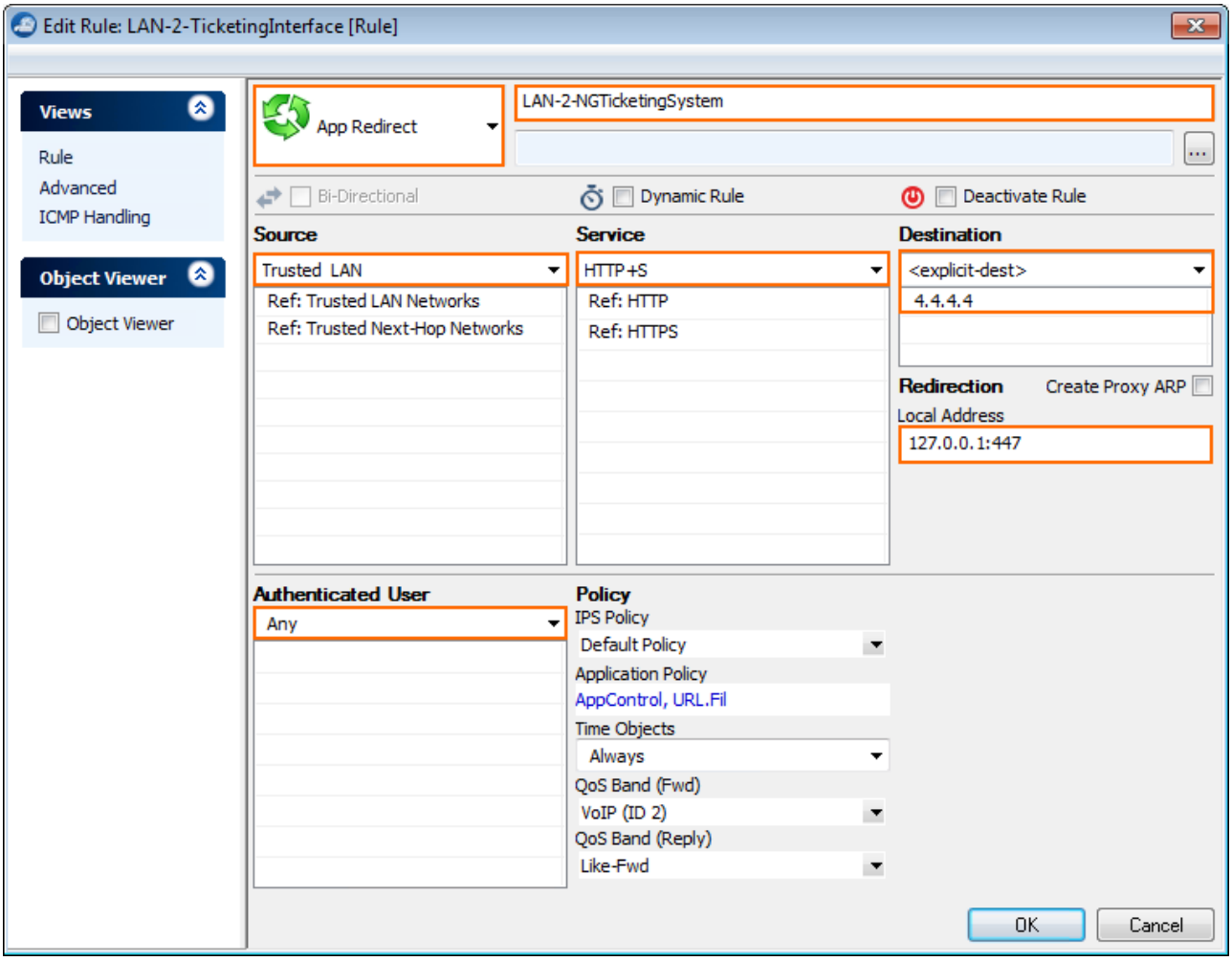


8. Click **Send Changes** and **Activate**.

Step 2. Create an Access Rule to access the NG Firewall Admin Ticketing Interface

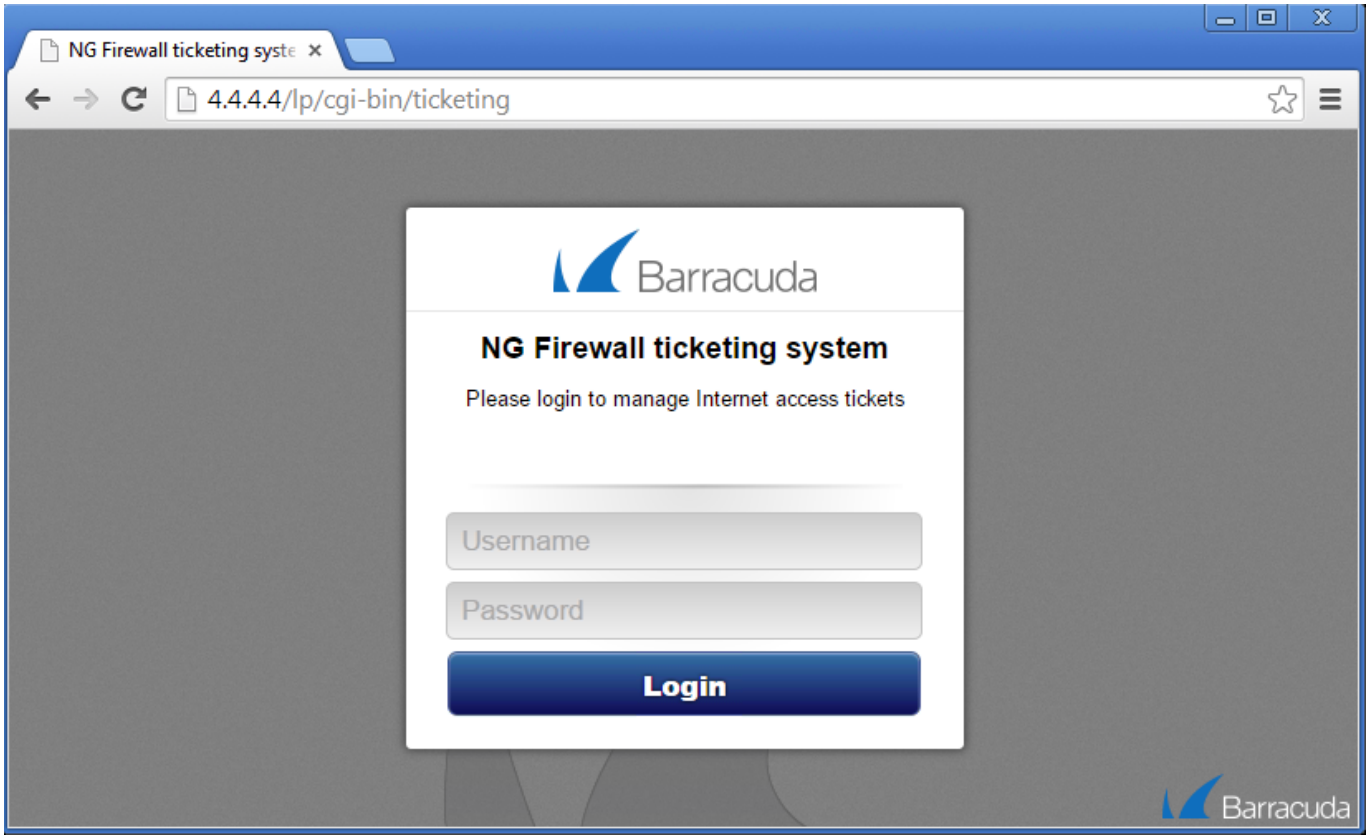
Create an app redirect access rule to access the NG Firewall ticketing system. This interface is used to create tickets for guest users.

1. Open the **Forwarding Rules** page (**Config > Full Config > Virtual Servers > *your virtual server* > Assigned Services > Firewall**).
2. Click **Lock**.
3. Create an **App Redirect** access rule:
   - **Action** – Select **App Redirect**.
   - **Source** – Select the source network(s) the ticketing system is access from.
   - **Service** – Select **HTTP+S**.
   - **Destination** – Enter the IP address for the admin ticketing interface. You can use any free IP address or an IP address on the Barracuda NG Firewall which does not have a listener on port 80 and 443.
   - **Redirection** – Enter `127.0.0.1:447`
   - **Authenticated User** – Select **Any** or a user object containing the users allowed to create guest tickets.
4. Click **OK**.



5. Place the access rule so that it is the first rule to match for HTTP+S traffic to the chosen NG ticketing system IP address.
6. Click **Send Changes** and **Activate**.

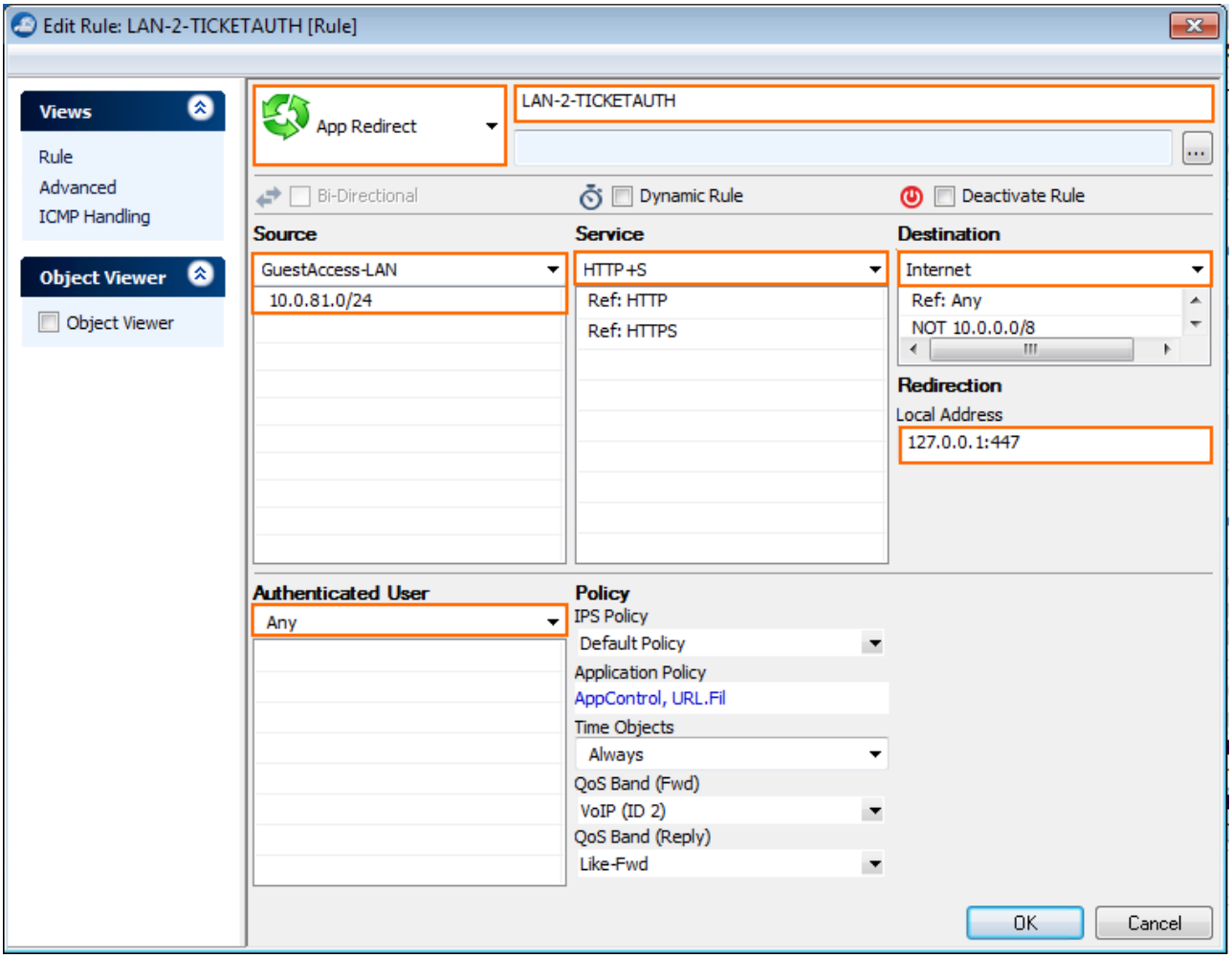
The admin ticketing interface is now reachable via `https://4.4.4.4/lp/cgi-bin/ticketing`. (If you used 4.4.4.4 as the destination IP address in the access rule.)



Step 3. Create an Access Rule to redirect Users to the User Ticketing Login

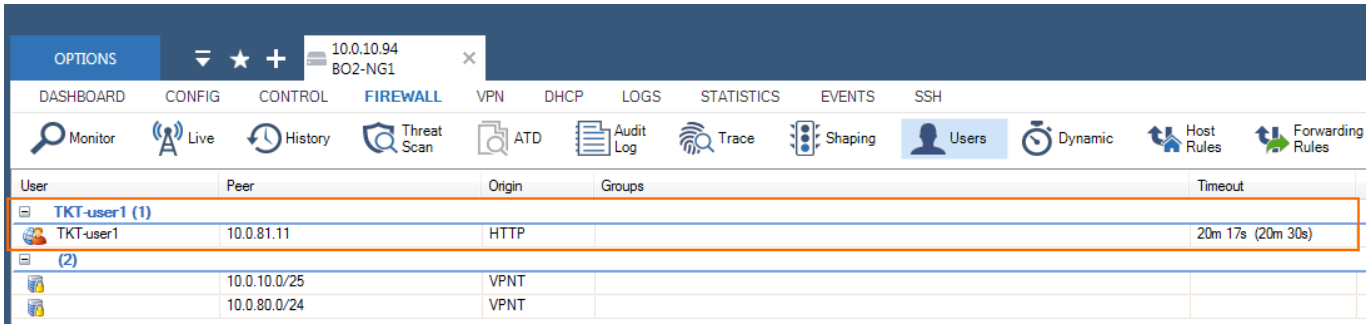
Create an app redirect access rule that redirects the user to the FWauth daemon on port TCP 447 on the Barracuda NG Firewall. FWauth on port 447 displays the ticketing login page and redirects the user to the original URL after successful authentication.

1. Open the **Forwarding Rules** page (**Config > Full Config > Virtual Servers > *your virtual server* > Assigned Services > Firewall**).
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 `127.0.0.1:447`
   - **Authenticated User** – Select **Any**.
4. Click **OK**.



5. Place the access rule so that it is the first rule to match for HTTP+S and unauthenticated users for the source network, but after the rule allowing unauthenticated DNS access if the DNS server is not in the local network.
6. Click **Send Changes** and **Activate**.

Unauthorized users accessing the Internet or restricted network resources from the source network are redirected to the user ticketing login page. After entering the ticketing user and password, they are automatically forwarded to the website they originally wanted to visit. A TKT- user is created and valid for 20 minutes until you need to reauthenticate. Open the **FIREWALL > Users** page to see the authenticated users.



Next Steps

For more information on how to create guest user tickets and use them to login, see How to Manage Guest Tickets - User's Guide.

Figures

1. GuestAccess03.png
2. GuestAccess02.png
3. GuestAccess01.png
4. GuestAccess04.png
5. GuestAccess05.png