

How to Configure NGF Local Authentication

<https://campus.barracuda.com/doc/41116188/>

Configure NGF local authentication to locally administer users and groups on the Barracuda NG Firewall. With NGF local authentication, you can refer to local users and groups when creating firewall rules, VPN tunnels, and services.

Configure NGF Local Authentication

1. Open the **Authentication Service** page (**Config > Full Config > Box > Infrastructure Services**).
2. In the left navigation pane, select **NGF Local Authentication**.
3. Click **Lock**.
4. Enable **NGF Local Scheme** as authentication scheme.
5. In the **Users** table, add an entry for each user that you are administering with the local authentication scheme. For each entry, you can configure the following settings:
 - **Username** – Authentication name of the user.
 - **Password** – Initial user password.
 - **Mail address** – Email address for the user.
6. If group information is queried from a different authentication scheme, select the scheme from the **User Info Helper Scheme** list. For example, select **LDAP** if group information must be queried from an LDAP directory.
7. Click **Send Changes** and **Activate**.

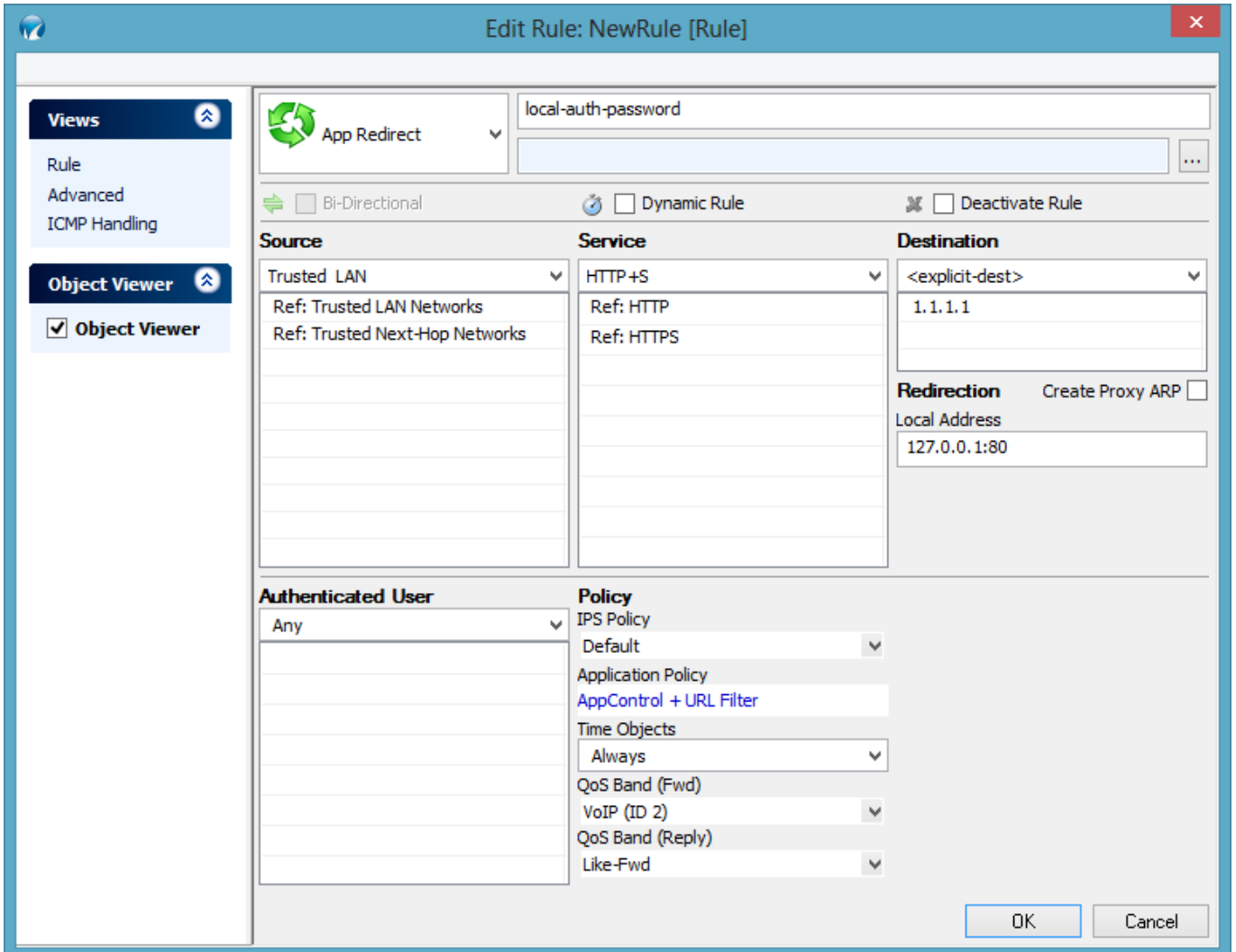
Changing User Passwords

When using NGF local authentication, you can also provide users the option of managing and changing their passwords. This is done by creating an access rule to redirect HTTP/S requests (port 80/443) to the local web server of the system.

Create an [App Redirect firewall rule](#) with the following settings:

- **Action** – App Redirect
- **Source** – Trusted LAN (LAN network users)
- **Service** – HTTP+S
- **Destination** – Choose a custom IP address to be entered by the user to access the web interface. For example: 1.1.1.1
- **Redirection** – IP address of the local web server, together with the HTTP/S port. For example: 127.0.0.1:80

The **Redirection** IP address must also be configured on the Barracuda NG Firewall.



The screenshot shows the 'Edit Rule: NewRule [Rule]' configuration window. The interface includes a sidebar with 'Views' (Rule, Advanced, ICMP Handling) and 'Object Viewer' (Object Viewer checked). The main configuration area is divided into several sections:

- App Redirect:** A dropdown menu set to 'App Redirect' with a text input field containing 'local-auth-password'.
- Options:** Checkboxes for 'Bi-Directional', 'Dynamic Rule', and 'Deactivate Rule'.
- Source:** A dropdown menu set to 'Trusted LAN' with references to 'Trusted LAN Networks' and 'Trusted Next-Hop Networks'.
- Service:** A dropdown menu set to 'HTTP+S' with references to 'HTTP' and 'HTTPS'.
- Destination:** A dropdown menu set to '<explicit-dest>' with a text input field containing '1.1.1.1'.
- Redirection:** A checkbox for 'Create Proxy ARP' and a text input field for 'Local Address' containing '127.0.0.1:80'.
- Authenticated User:** A dropdown menu set to 'Any'.
- Policy:** A dropdown menu set to 'IPS Policy' with sub-sections for 'Default', 'Application Policy' (set to 'AppControl + URL Filter'), 'Time Objects' (set to 'Always'), 'QoS Band (Fwd)', 'VoIP (ID 2)', 'QoS Band (Reply)', and 'Like-Fwd'.

Buttons for 'OK' and 'Cancel' are located at the bottom right of the window.

After you create and activate this firewall rule, users can enter `http://1.1.1.1/cgi-bin/ngflocalpasswd` into a web browser to change their password.

Figures

1. pg_rd_new.png

© Barracuda Networks Inc., 2019 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.