How to Configure Offline Firewall Authentication

https://campus.barracuda.com/doc/48203093/

Offline firewall authentication works with all Barracuda NextGen Firewall F-Series services. The user is authenticated by the fwauth daemon. To implement offline firewall authentication, configure your firewall authentication settings and create an App Redirect firewall rule with the destination set to an internal firewall IP to let users access the fwauth service. The user can then use the Barracuda Authentication Client or the browser login. The fwauth service listens on 127.0.0.1. Depending on the type of authentication required, use the following ports:

- **TCP 80 –** Username/password authentication. (HTTP only) Use for external authentication servers (e.g., MSAD).
- **TCP 443 –** Username/password (HTTPS with automatic redirect to HTTPS for HTTP requests). Use for external authentication servers (e.g., MSAD).
- **TCP 448 –** Username/password (HTTP and HTTPS) with automatic redirection. Use for external authentication servers (e.g., MSAD).
- **TCP 444 –** X.509 certificate authentication. (HTTPS with automatic redirect to HTTPS for HTTP requests).
- **TCP 445 –** X.509 certificate plus username/password authentication. (HTTPS with automatic redirect to HTTPS for HTTP requests)

Step 1. Configure the Firewall authentication settings

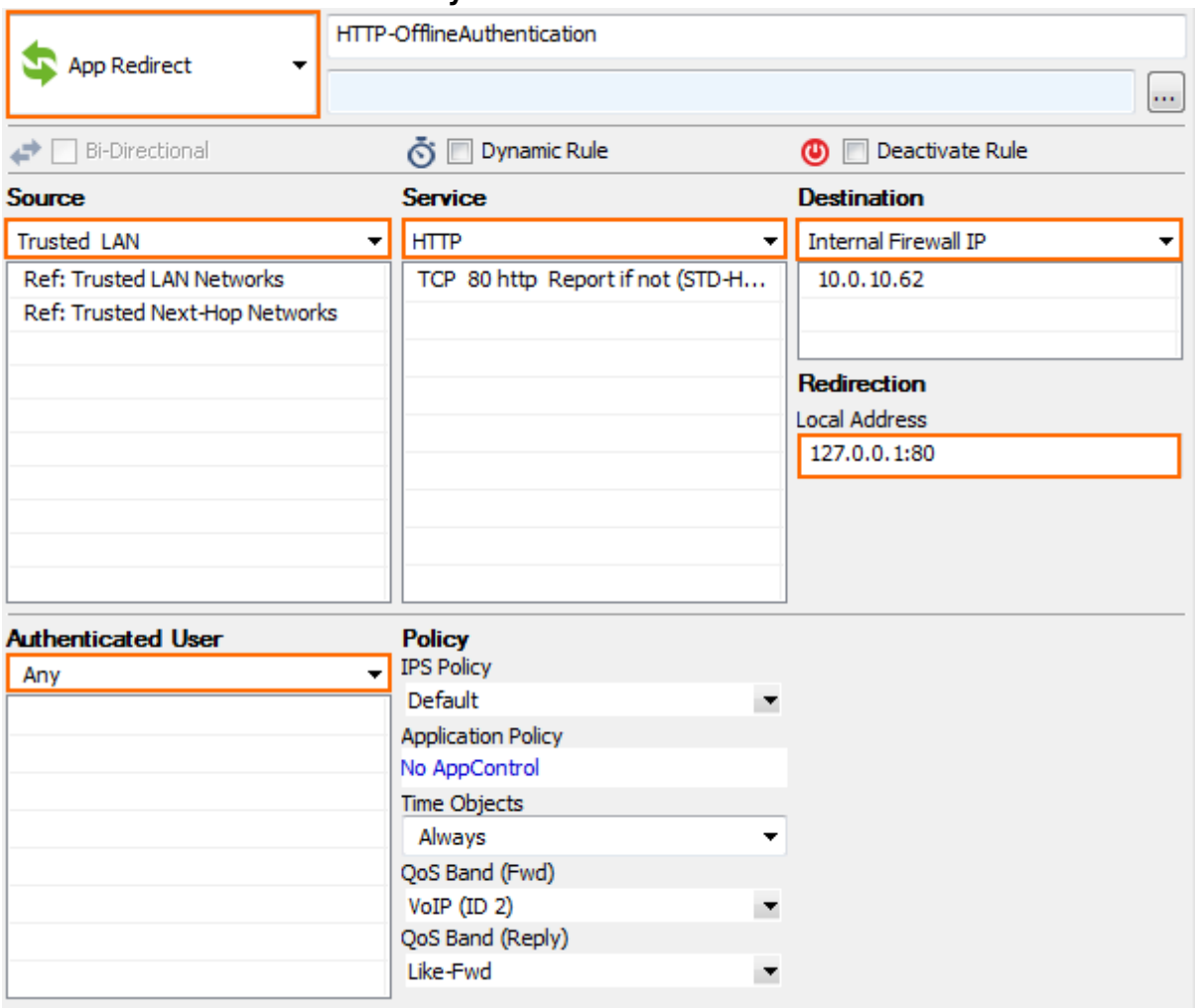
Set the HTTPS private key and certificate to activate firewall authentication.

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > Firewall > Forwarding Settings**.
2. In the left menu, click on **Authentication**.
3. Click **Lock**.
4. (optional) **Edit** the **Operational Settings**.
5. Upload or create the **HTTPS Private Key** and **Certificate.**
6. Select the **Authentication Scheme** from the list. E.g., **MS Active Directory**. For more information, see Authentication.
7. Click **Send Changes** and **Activate**.

Step 2. Create access rules for offline authentication

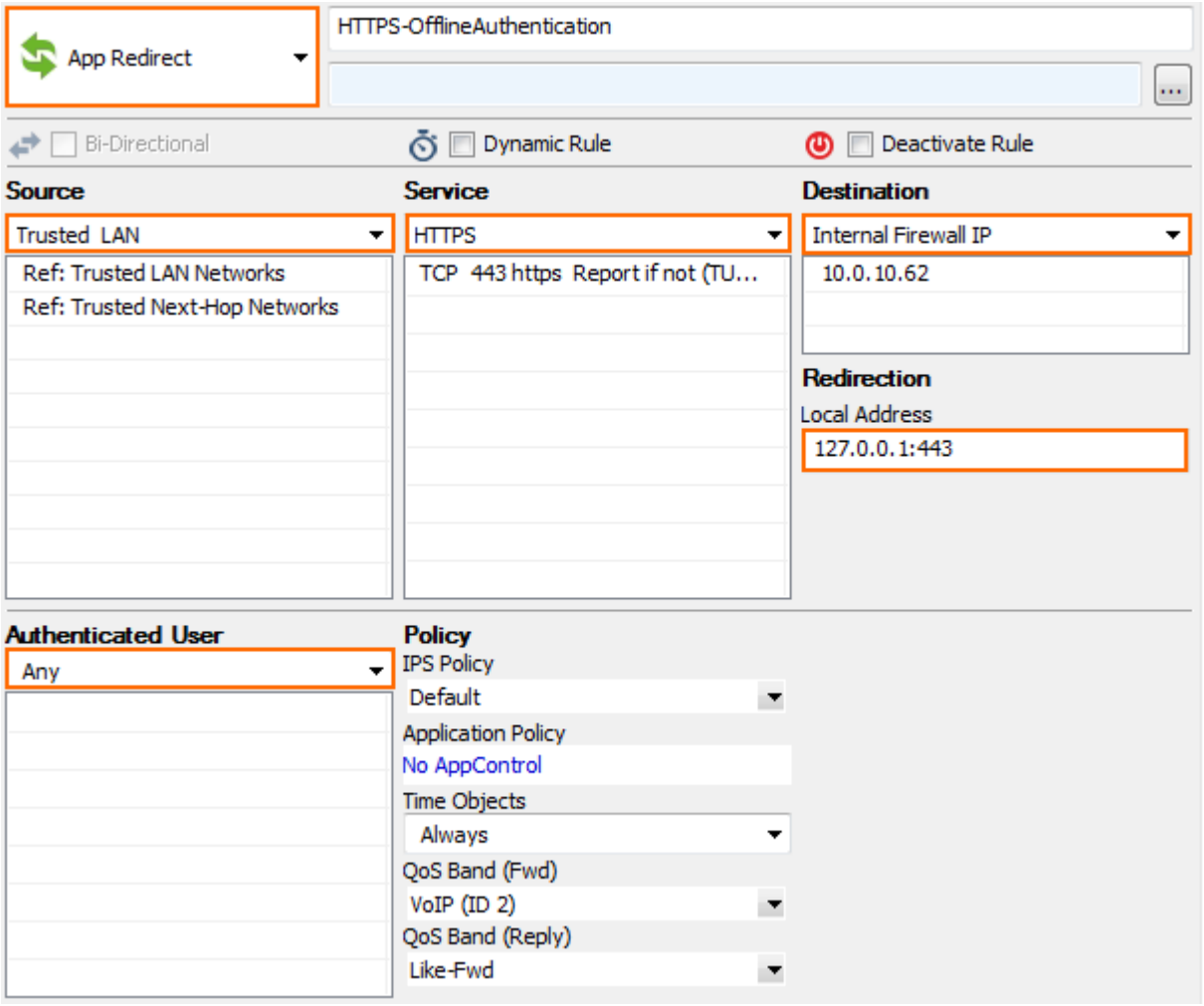
To let users go directly to the firewall login page, to log out or log in, set the **Destination IP** to an internal firewall IP (not the management IP).

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > Firewall > Forwarding Rules**.
2. Click **Lock**.
3. Create an **App Redirect** firewall for HTTP traffic:
   - **Source** – Select **Trusted Networks**, or enter the internal network for the clients who need to authenticate.
   - **Service** – Select **HTTP**.
   - **Destination** – Enter an internal IP used by the firewall service. Do not use the management IP.
   - **Redirection** – Enter `127.0.0.1:`. Enter the port of the authentication method supporting HTTP: 80, 444,445,448 - see list on the top of the page.
   - **Authenticated User** – Select **Any**.



4. (optional) Create an **App Redirect** firewall rule for HTTPS traffic:
   - **Source** – Select **Trusted Networks**, or enter the internal network for the clients who need to authenticate.
   - **Service** – Select **HTTPS**.
   - **Destination** – Enter an internal IP used by the firewall service. Do not use the management IP.
   - **Redirection** – Enter `127.0.0.1:`. Enter the port of the authentication method supporting HTTP: 443, 444, 445, 448 - see list on the top of the page.

- **Authenticated User** – Select **Any**.

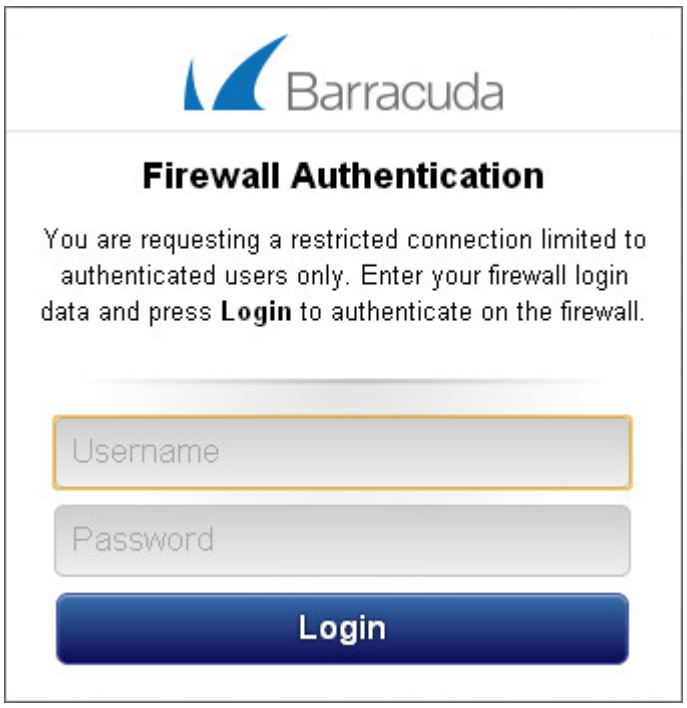


5. Move the redirect rules above the **INTERNET-2-LAN** rule.
6. Click **Send Changes** and **Activate**.

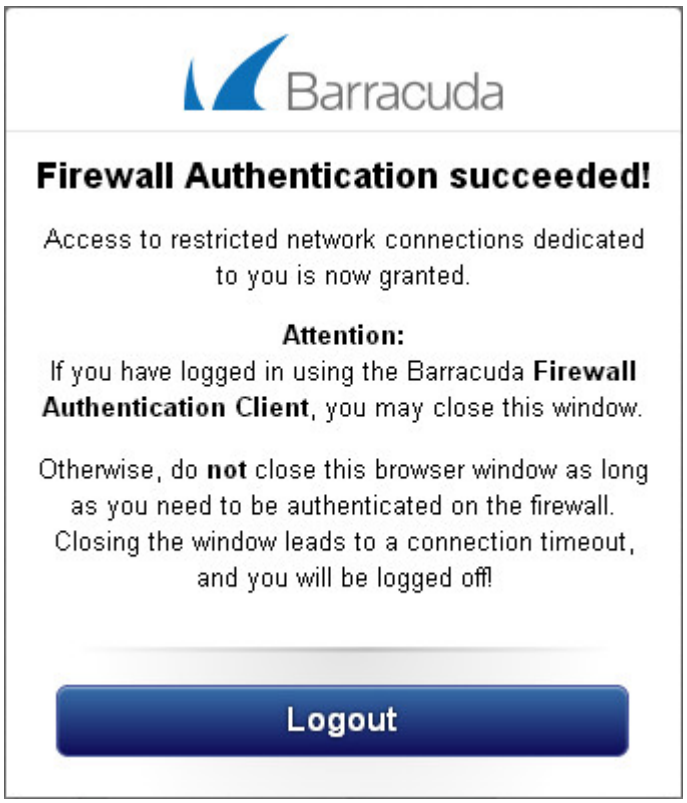
Step 3. Authenticate to the Barracuda NextGen Firewall F-Series

After implementing offline authentication, you can use it to log into the Barracuda NextGen Firewall F-Series.

1. Go to **http://**
2. On the login screen, enter your user credentials.



After you are successfully authenticated, you receive the following message:



Keep the authentication page open for as long as you need to be connected to the Barracuda NextGen Firewall F-Series. If you close the browser, you are automatically logged out after five minutes. This limitation does not apply if you are using the Authentication Client to log in.

Figures

1. FWAuth_OFF01.png
2. FWAuth_OFF02.png
3. auth_login.png
4. auth_login_success.png