

## 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

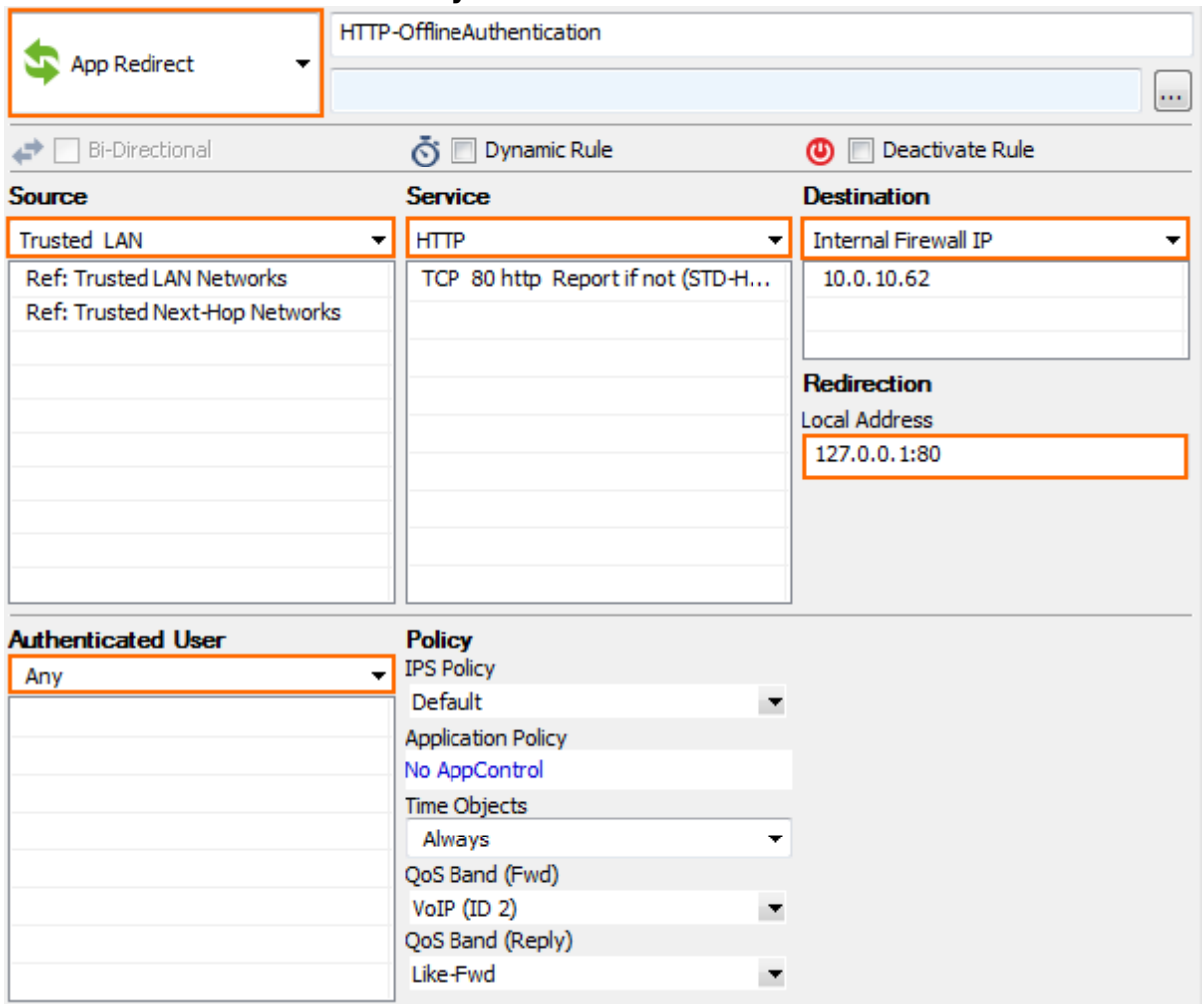
Set the HTTPS private key and certificate to activate firewall authentication.

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:
  - o **Source** - Select **Trusted Networks**, or enter the internal network for the clients who need to authenticate.
  - o **Service** - Select **HTTP**.
  - o **Destination** - Enter an internal IP used by the firewall service. Do not use the management IP.
  - o **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.
  - o **Authenticated User** - Select **Any**.

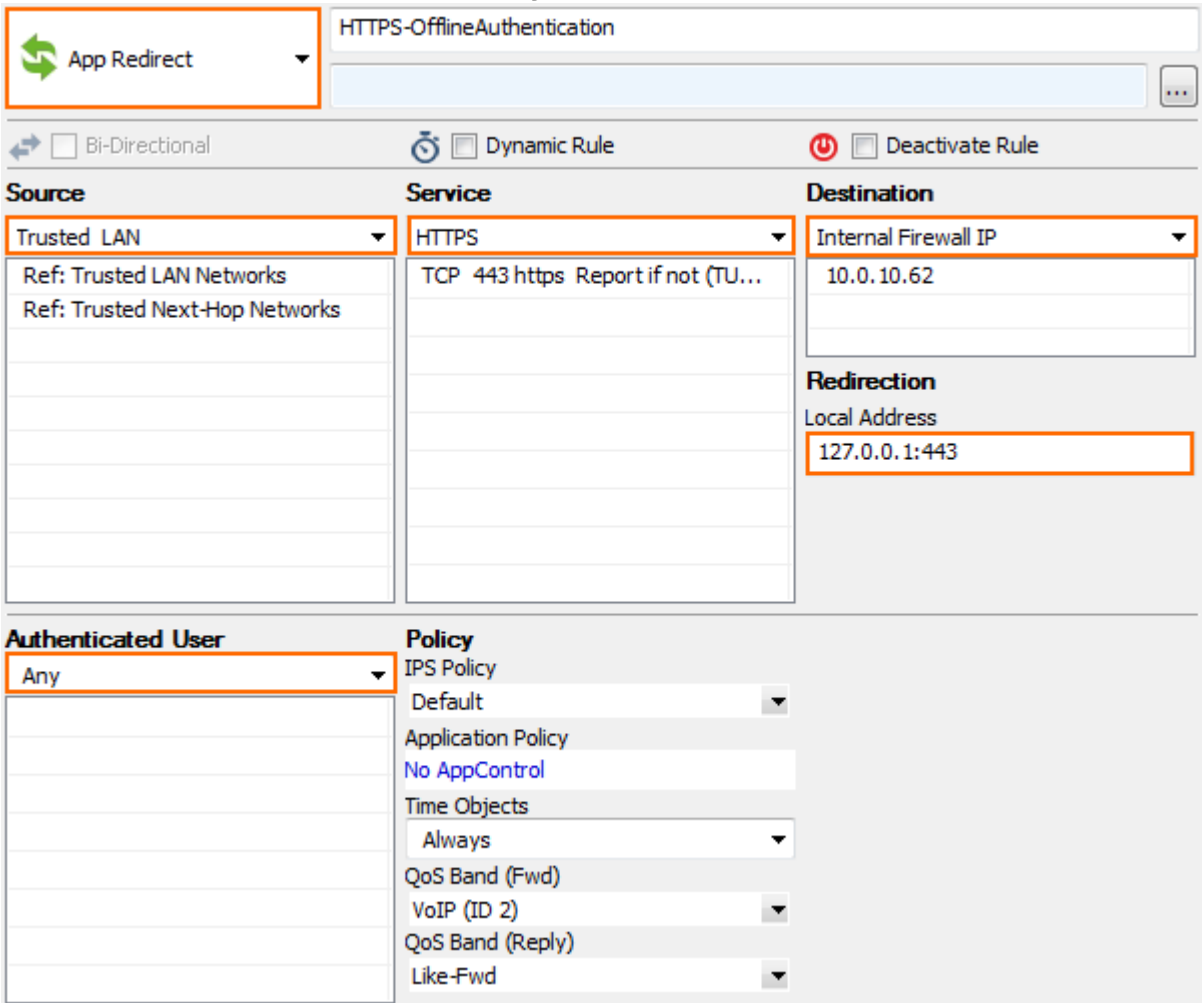


The screenshot shows the configuration for an 'App Redirect' firewall rule. The rule name is 'HTTP-OfflineAuthentication'. The configuration is as follows:

- Source:** Trusted LAN (References: Trusted LAN Networks, Trusted Next-Hop Networks)
- Service:** HTTP (TCP 80 http Report if not (STD-H...))
- Destination:** Internal Firewall IP (10.0.10.62)
- Redirection:** Local Address 127.0.0.1:80
- Authenticated User:** Any
- Policy:**
  - IPS Policy: Default
  - Application Policy: No AppControl
  - Time Objects: Always
  - QoS Band (Fwd):
  - VoIP (ID 2):
  - QoS Band (Reply):
  - Like-Fwd:

4. (optional) Create an **App Redirect** firewall rule for HTTPS traffic:
  - o **Source** - Select **Trusted Networks**, or enter the internal network for the clients who need to authenticate.
  - o **Service** - Select **HTTPS**.
  - o **Destination** - Enter an internal IP used by the firewall service. Do not use the management IP.
  - o **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**.



App Redirect

HTTPS-OfflineAuthentication

Bi-Directional  Dynamic Rule  Deactivate Rule

| Source  | Service                            | Destination          |
|---|------------------------------------|----------------------|
| Trusted LAN   | HTTPS                              | Internal Firewall IP |
| Ref: Trusted LAN Networks<br>Ref: Trusted Next-Hop Networks | TCP 443 https Report if not (TU... | 10.0.10.62           |

**Redirection**  
Local Address  
127.0.0.1:443

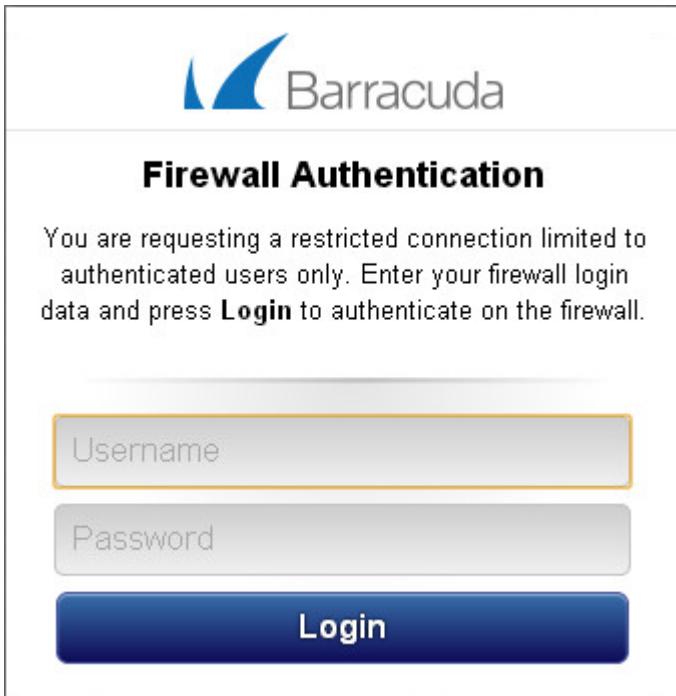
| Authenticated User | Policy                              |
|--------------------|-------------------------------------|
| Any                | IPS Policy<br>Default               |
|                    | Application Policy<br>No AppControl |
|                    | Time Objects<br>Always           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

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

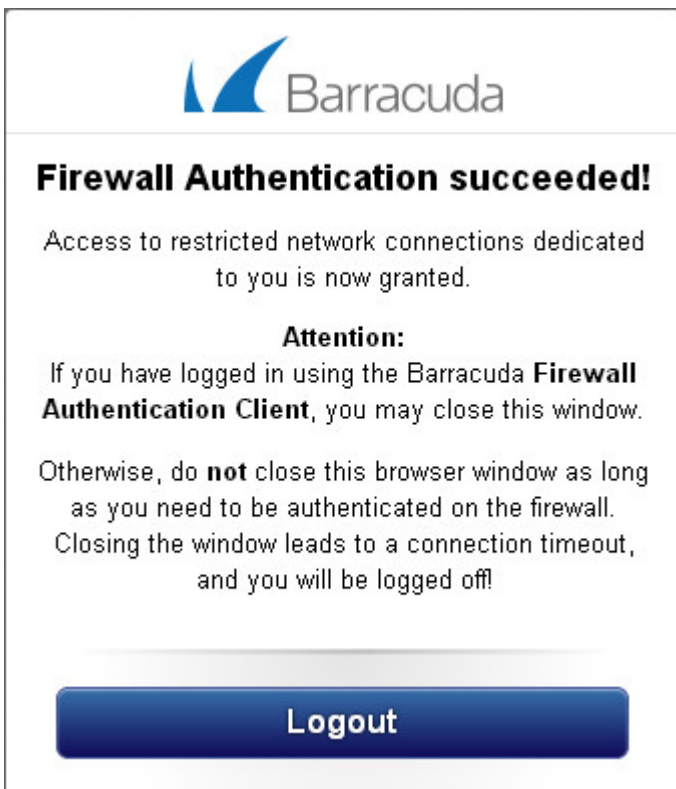
After implementing offline authentication, you can use it to log into the Barracuda NextGen Firewall F-Series.

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



The image shows a login screen for Barracuda Firewall Authentication. At the top is the Barracuda logo. Below it is the heading "Firewall Authentication". The text reads: "You are requesting a restricted connection limited to authenticated users only. Enter your firewall login data and press **Login** to authenticate on the firewall." There are two input fields: "Username" and "Password". Below the fields is a blue button labeled "Login".

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



The image shows a success message for Barracuda Firewall Authentication. At the top is the Barracuda logo. Below it is the heading "Firewall Authentication succeeded!". The text reads: "Access to restricted network connections dedicated to you is now granted." There is an "Attention:" section that says: "If you have logged in using the Barracuda **Firewall Authentication Client**, you may close this window." Below that, it says: "Otherwise, do **not** close this browser window as long as you need to be authenticated on the firewall. Closing the window leads to a connection timeout, and you will be logged off!" At the bottom is a blue button labeled "Logout".

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

© 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.