

How to Configure Offline Firewall Authentication

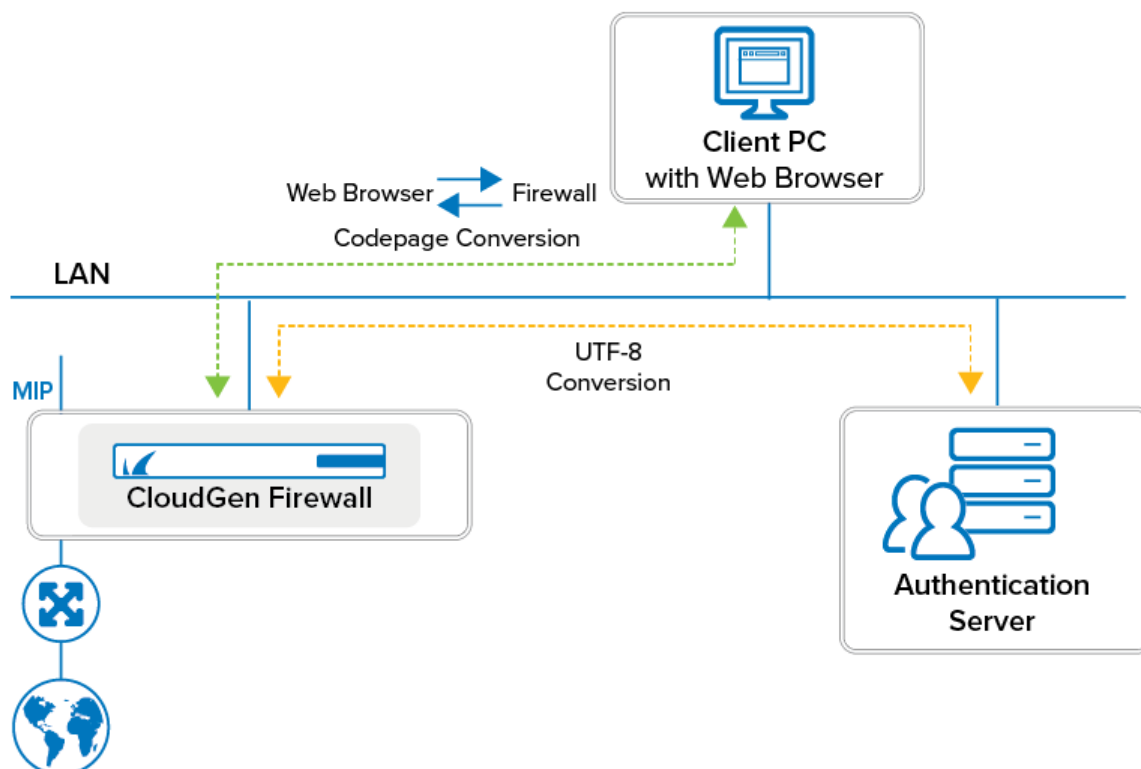
<https://campus.barracuda.com/doc/96026292/>

Offline Firewall Authentication works with all CloudGen Firewall services. The user is authenticated by the fwauth daemon. To implement offline firewall authentication, configure your firewall authentication settings and create an App Redirect access rule with the destination set to an internal firewall IP to let users access the fwauth service. The user can then use the Barracuda CloudGen 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).

Usage of Special Characters and Umlauts in Passwords

When configuring Offline Firewall Authentication, you must consider whether passwords may contain special characters, e.g., € or umlauts. Because characters will be translated between the web browser and the firewall and between the firewall and the authentication service using codepages, it is important to decide which client codepage will be used and which authentication scheme supports the appropriate character conversion.



The following table shows if codepage will be used, under which constraints it will be used, and if special characters will be translated correctly:

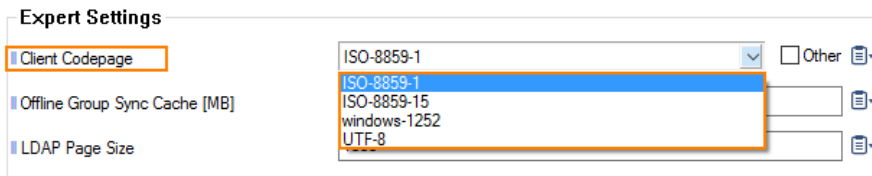
Conversion of special characters	Web Browser > CODEPAGE > Firewall	Firewall > CODEPAGE > Authentication Service	Authentication Scheme
NO	8859-1	UTF-8	Any
YES	8859-15	UTF-8	Any except NGFLocal
YES	UTF-8	UTF-8	Any except NGFLocal
YES	Windows 1252	-	NGFLocal

The codepage in the column *Web Browser > CODEPAGE > Firewall* can be configured.

(Optional) Step 1. Configure the Codepage if Special Characters Must Be Allowed in Passwords

1. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Service > Authentication Service**.

2. Click **Lock**.
3. In the left menu, click **Configuration Mode**.
4. In the left menu, click **Switch to Advanced**.
5. In the left menu, click **Timeouts and Logging**.
6. In the section **Expert Settings**, for **Client Codepage**, select the codepage according to the upper table and that best fits your requirements.



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

Step 2. Configure the Firewall Authentication Settings

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

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Settings**.
2. In the left menu, click **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**.

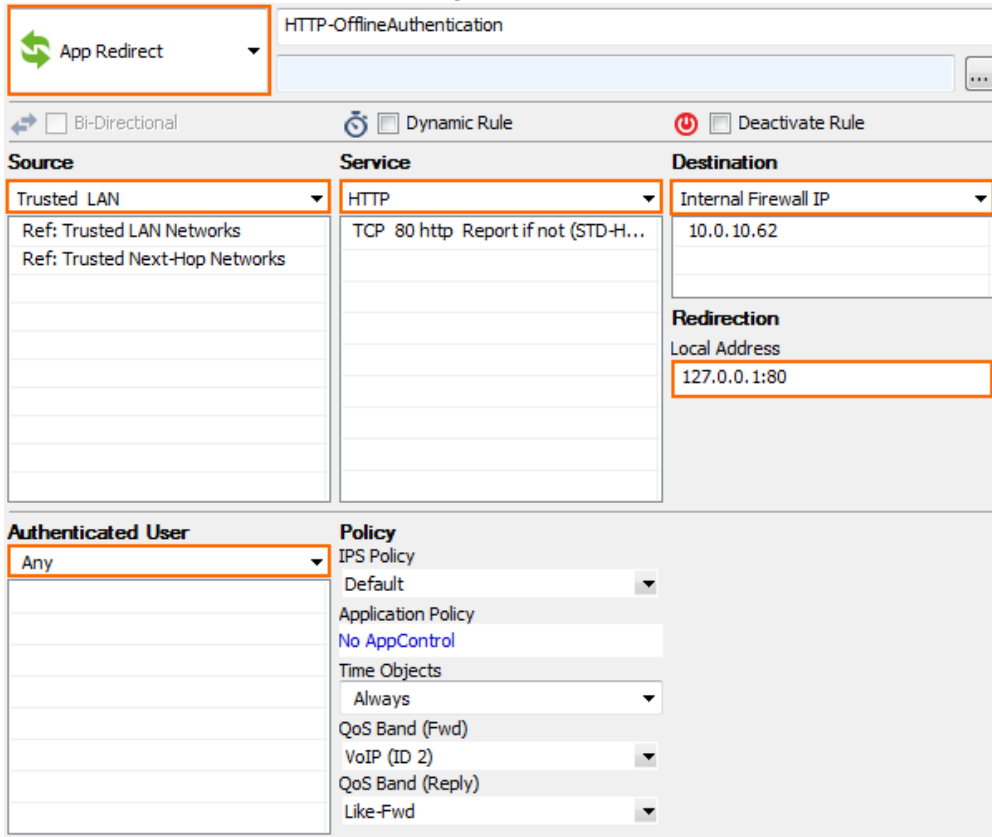
Step 3. Create Access Rules for Offline Authentication

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 > Assigned Services > Firewall > Forwarding Rules**.
2. Click **Lock**.
3. Create an **App Redirect** access rule 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: <port>. Enter the port of the authentication method supporting HTTP: 80, 444, 445, 448 - see list at the top of the page.
- **Authenticated User** - Select **Any**.



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

Source	Service	Destination
Trusted LAN	HTTP	Internal Firewall IP
Ref: Trusted LAN Networks	TCP 80 http Report if not (STD-H...	10.0.10.62
Ref: Trusted Next-Hop Networks		

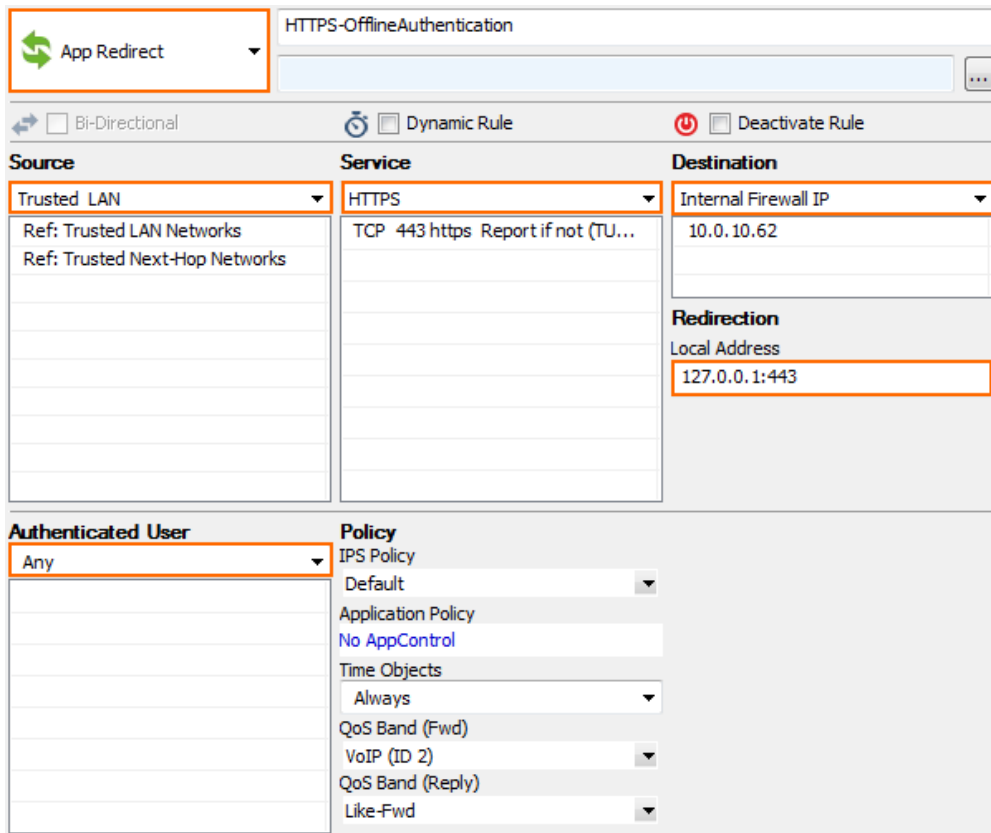
Redirection
Local Address: 127.0.0.1:80

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** access 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: <port>. Enter the port of the authentication method supporting HTTP: 443, 444, 445, 448 - see list at the top of the page.
- **Authenticated User** - Select **Any**.



The screenshot shows the configuration page for an 'App Redirect' rule named 'HTTPS-OfflineAuthentication'. The rule is currently inactive, as indicated by the red power button icon. The configuration is as follows:

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

Below the main configuration, the 'Authenticated User' is set to 'Any' and the 'Policy' is configured with the following settings:

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

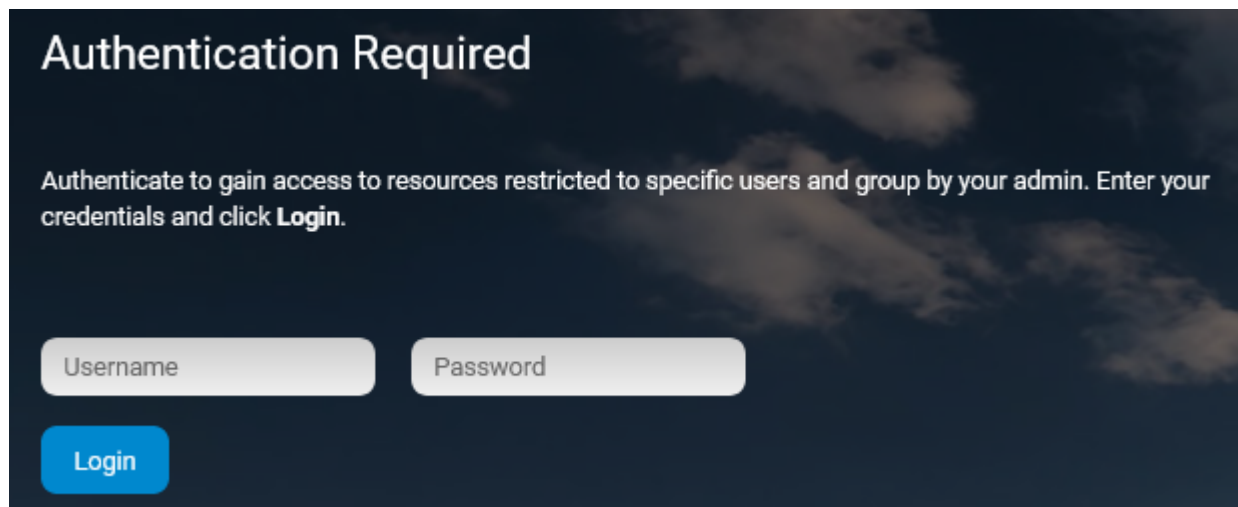
The 'Redirection' section shows the 'Local Address' as 127.0.0.1:443.

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

Step 4. Authenticate to the Barracuda CloudGen Firewall

After implementing offline authentication, you can use it to log into the CloudGen Firewall.

1. Go to **http://<IP address used as destination in the access rule>**
2. On the login screen, enter your user credentials, and click **Login**.

A screenshot of the Barracuda CloudGen Firewall authentication page. The background is a dark blue sky with white clouds. The title "Authentication Required" is in white at the top. Below it, a message in white text says: "Authenticate to gain access to resources restricted to specific users and group by your admin. Enter your credentials and click **Login**." There are two light gray input fields: "Username" and "Password". Below the "Username" field is a blue "Login" button.

Authentication Required

Authenticate to gain access to resources restricted to specific users and group by your admin. Enter your credentials and click **Login**.

Username Password

Login

Keep the authentication page open for as long as you need to be connected to the Barracuda CloudGen Firewall. 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. code_page.png
2. client_code_page.png
3. FWAuth_OFF01.png
4. FWAuth_OFF02.png
5. cgf_auth.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.