Firewall Authentication and Guest Access

https://campus.barracuda.com/doc/17530/

If you are not using the Barracuda DC Agent to authenticate users, you can use inline or offline firewall authentication. Knowing which users are associated with an IP address makes the firewall user aware. This allows you to create policies based on the user. The following types of firewall authentication methods are available:

Inline Authentication

Inline Authentication requires an HTTP/HTTPS connection as the authentication requests are injected into the data stream. The firewall redirects the first HTTP/S request of an unauthenticated user to the internal authentication server. This server generates the authentication request by sending an HTTP 401 status code (Server Auth) to the client browser. Before users can access the original resource, they must authenticate themselves in a pop-up window.

For more information, see How to Configure Inline Firewall Authentication.

Offline Authentication

Offline Authentication works with all protocols (for example, POP3). Before users can access resources, they must log into the firewall via a web browser. Their authentication is verified by the **fwauth** daemon. After users authenticate themselves, they must also leave the web browser open. Otherwise, their connection is terminated after a (configurable) refresh timeout.

For more information, see How to Configure Offline Firewall Authentication.

Authentication Client

If you have the Barracuda Network Access Client installed, you can use a built-in authentication client to avoid users having to log in every time they start their computer. This utility is available for Microsoft Windows and is started automatically when configured. The Authentication Client keeps the user logged in as long as the application is running in the background.

For more information, see How to Enable Personal Access Using the Authentication Client.

Guest Access

You can set up a confirmation page or ticketing system to temporarily grant guests access to your network. Before guests can access the network, they must either enter a username and password created by the ticket admin or agree to a message on the confirmation page. Guest Access times out after configurable amount of time, forcing the user to reauthenticate.

For more information, see:

- How to Configure Guest Access with a Confirmation Page
- How to Configure Guest Access with the Ticketing System
- How to Manage Guest Tickets - User's Guide

Customizing Firewall Authentication HTML Files

The HTML pages used for offline firewall authentication can be customized to your personal preferences. These customized HTML files are uploaded to the firewall and used instead of the default files. Customized files are not included in PAR files and not synced to the HA partner.

For more information, see How to Customize Firewall Authentication HTML Files.