Firewall Authentication and Guest Access

https://campus.barracuda.com/doc/72516504/

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:

Captive Portal

The captive portal intercepts unauthorized users HTTP or HTTPS connections and redirects them to a login page. After successful authentication the user is forwarded to the original destination.

For more information, see How to Configure the Captive Portal.

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