Captive Portal and Barracuda Content Shield

https://campus.barracuda.com/doc/93194530/

BCS Plus subscriptions support Captive Portal implementations, and all traffic is logged in BCS.

For hotel or Internet cafe guests, or employees who bring personal devices to work, a **Captive Portal** application gives the administrator control over user access to the Internet or other networks. When using a captive portal, the BCS agent automatically presents the captive portal login page as set up by the administrator for the network. The **Captive Portal** feature is always enabled and does not require configuration in BCS.

Example use cases of captive portal include:

- Hotel or Internet cafe guests tend to be unauthenticated and will browse based as 'guests' based on policies you create in your application for unauthenticated users.
- BYOD (bring your own device) users, such as employees, can typically use their LDAP credentials to log into the portal and continue to browse based on policies you apply, using your Captive Portal application, to authenticated users. You can typically also configure so that these users can browse as guests (unauthenticated) when using these devices.