Captive Portal Terms and Conditions Page

https://campus.barracuda.com/doc/35160119/

For hotel or Internet cafe guests, or employees who bring personal devices to work, the **Captive Portal** feature gives you control over user access to the Internet or other networks. When enabled, this feature presents a ‘terms and conditions’ page to which the user must agree before getting access to browse the web. The **Captive Portal** feature can be enabled and configured on the **BLOCK/ACCEPT > Configuration** page.

Example use cases:

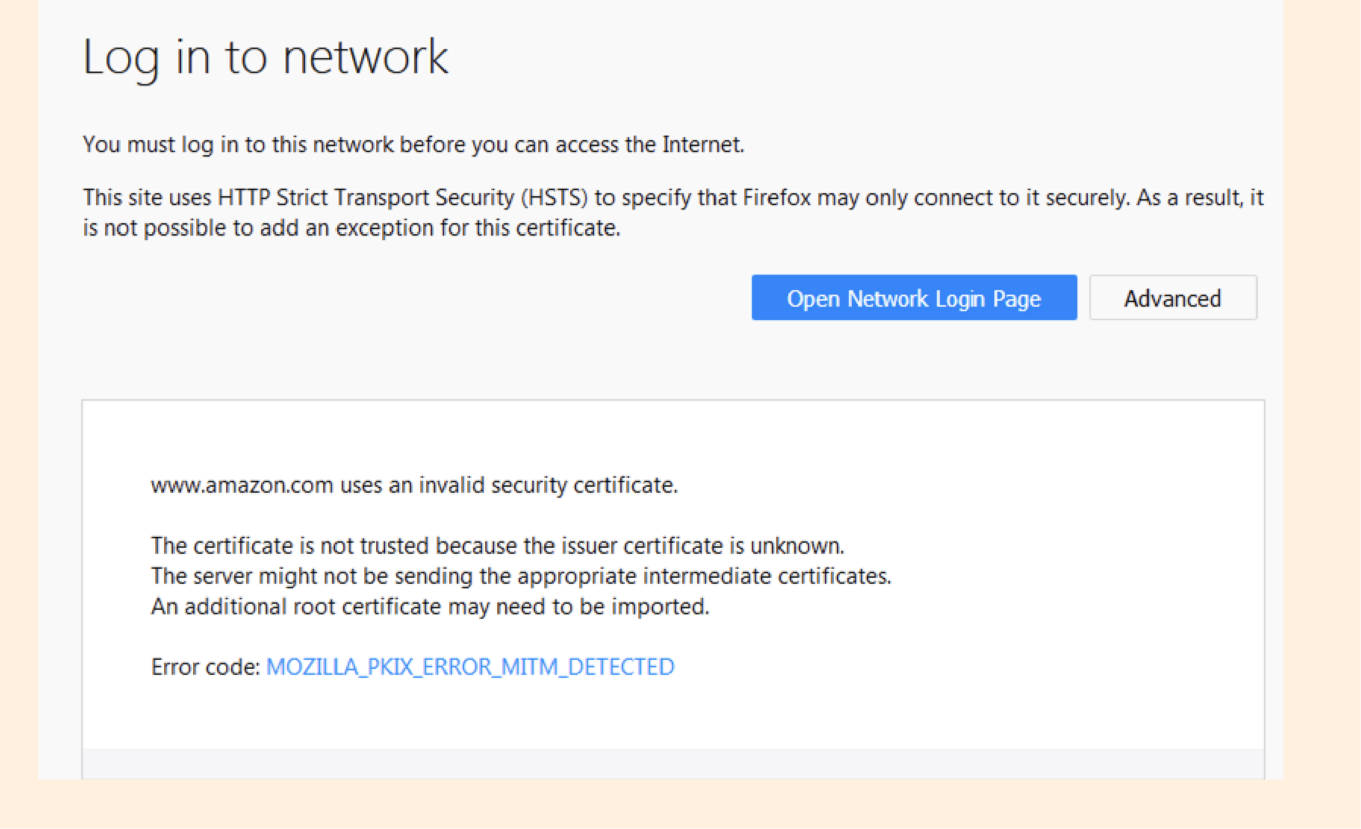
- Hotel or Internet cafe guests tend to be unauthenticated and will browse based as 'guests' based on policies you create for unauthenticated users.
- BYOD (bring your own device) users, such as employees, can use their LDAP credentials to log into the portal and continue to browse based on policies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

User Experience and Authentication

With **Captive Portal** enabled, the first request from every user will be served a splash page displaying customized terms and conditions, which you configure on the **BLOCK/ACCEPT > Block Message** page. Once the user agrees or, for LDAP users, logs in, the page is not presented again for the duration of the browsing session and the user can view content that is not blocked for that user based on Captive Portal settings and block/accept policies. These settings allow for applying this feature to certain IP groups and unauthenticated ('guest') users. You can apply different policies depending on whether the user identifies with LDAP credentials or as a guest. Exclusions for IP groups are also configurable.

Note that all traffic is logged, and the session will time out automatically in 24 hours.

When the **SSL Inspection** feature is enabled on the Barracuda Web Security Gateway, the SSL certificate needs to be imported into the users' browsers to avoid certificate errors when they browse HTTPS sites. A common use case is users who bring their own devices for use on the local network. If the SSL certificate is not imported into the device browser, the user will be redirected to the Captive Portal login page and see the following error message:



Log in to network

You must log in to this network before you can access the Internet.

This site uses HTTP Strict Transport Security (HSTS) to specify that Firefox may only connect to it securely. As a result, it is not possible to add an exception for this certificate.

www.amazon.com uses an invalid security certificate.

The certificate is not trusted because the issuer certificate is unknown.
The server might not be sending the appropriate intermediate certificates.
An additional root certificate may need to be imported.

Error code: MOZILLA_PKIX_ERROR_MITM_DETECTED

Figures