Google Restrictions With SSL Inspection

https://campus.barracuda.com/doc/45712185/

Note that you cannot rely solely on the HTTPS Filtering feature to block Google over HTTPS. This is because SSL inspection is required to properly identify some Google domains.

SSL Inspection and Google Consumer Apps

When the SSL Inspection feature is enabled on the Barracuda Web Security Gateway, the administrator has granular control over what applications are blocked or allowed on websites like Facebook, Twitter or Google. In these use cases, administrators can typically apply block/allow policies by specifying domain/sub-domain patterns associated with the website to be inspected over HTTPS. However, with Google consumer apps, there are currently some limitations due to the way in which Google deals with SSL certificates. These limitations, and the Barracuda solution for correct identification and filtering of Google domains and sub-domains over HTTPS, are addressed in this article.

For instructions and examples on how to block Google consumer apps over HTTPS, see G Suite Control Over HTTPS.

To filter Google consumer apps traffic for **Chromebooks**, see How to Get and Configure the Barracuda Chromebook Security Extension. The extension requires upgrading to the Barracuda Web Security Gateway version 11 or above.

Google Restrictions on Identifying Google sub-domains Over HTTPS

Google has been moving more of its services to encrypted (HTTPS) connections for additional security, and is tending towards moving all of their sites to use HTTPS by default. In some cases, when SSL inspecting web traffic to Google sites, the only information the Barracuda Web Security Gateway has to evaluate over the encrypted connection is the IP address and the certificate name, which in most cases, including Google, is a wildcard certificate (*.google.com) identifying the domain name but not the specific host. Additionally, many schools and other institutions still use older versions of Windows and various browsers.

These issues result in limited ability to completely identify certain Google sub-domains, and to apply differentiated policies such as, for example:

- Allow an encrypted connection to Google drive but block the connection to mail.google.com

- Allow an encrypted connection to Google business accounts, but block the connection to Google consumer accounts

Limited Abilities for Some Mobile Devices With SSL Inspection

With the introduction of mobile devices and specialized apps such as the Google Play Store on Android or the Google Drive app for Windows, limitations in SSL inspecting this web traffic are also an issue due to varied support for SSL Inspection tools in these specialized apps. Some versions of the apps support SSL Inspection tools needed to specifically determine the identity of certain Google sites over HTTPS, and some do not. This means that some selective policies based on service can't be applied to that web traffic

These issues are causing difficulties for schools in applying granular policy to student web browsing and to other organizations when applying policies. Google is working to make changes on their side to resolve them.

For schools that have not adopted G Suite for Education, and are not widely using Android-based mobile devices, these issues may not be a problem.

Safe Solutions

Use the Barracuda Chromebook Security Extension

For Chromebook users, you can download the Barracuda Chromebook Security Extension and install it on each device to enforce security policies configured on the Barracuda Web Security Gateway: The extension provides control and visibility over both HTTP and HTTPS traffic, and does not send any user generated traffic through the Barracuda Web Security Gateway, but instead, synchronizes policy and report data between the Chromebook and the Barracuda Web Security Gateway. See How to Get and Configure the Barracuda Chromebook Security Extension. The extension requires upgrading to the Barracuda Web Security Gateway version 11 or above.

Deploy the Barracuda Web Security Gateway in Proxy Mode

This deployment allows for full access to the URL that the user is accessing and can fully identify the resource and make differentiated policy decisions. See Forward Proxy Deployment of the Barracuda Web Security Gateway.

Use the Google Consumer Apps Category Filter

Use the **Google Consumer Apps** content category in the Barracuda Web Security Gateway and create Exceptions to block or allow certain users or groups access to all or some Google Consumer

Apps:

1. From the **BLOCK/ACCEPT > Web App Control** page, in the **Allowed Applications** box, select **Google Consumer Apps** under **Category Filter**.
2. In the list box, you can either select **Google Mail** or **Google Consumer Apps**, and click the **Block** button to move it to the **Blocked Applications** list box. Click **Save**.
3. On the **BLOCK/ACCEPT > Exceptions** page, create block/allow exceptions by user(s) and/or group(s).

See G Suite Control Over HTTPS for examples.