G Suite Control Over HTTPS

https://campus.barracuda.com/doc/17106182/

SSL Inspection is a resource intensive feature which is supported by the Barracuda Web Security Gateway as described in Using SSL Inspection With the Barracuda Web Security Gateway. Because of the way Google handles SSL certificates, Barracuda provides a Category Filter on the **BLOCK/ACCEPT > Web App Control** page for Google Consumer Apps, which must be selected in order to identify and to SSL-inspect certain Google domains and sub-domains. This feature requires version 9.1 or higher of the Barracuda Web Security Gateway.

For information about limitations in blocking Google over HTTPS, see Google Restrictions With SSL Inspection.

For Chromebook users with the Barracuda Chromebook Security Extension installed, policies for G Suite web traffic are configured on the Google Admin Console, not on the Barracuda Web Security Gateway. Also note that the settings on the **BLOCK/ACCEPT > Web App Control** and **BLOCK/ACCEPT > Web App Monitor** pages do not apply to Chromebooks running the Barracuda Chromebook Security Extension.

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 Google.com. This article explains how to apply block/allow policies by selecting some or all Google Consumer Apps to be inspected over HTTPS.

How to Block and Allow Google Consumer Apps

Step 1. Enable and Configure SSL Inspection

This is the first step required for SSL inspecting HTTPS traffic.

1. Log into the Barracuda Web Security Gateway web interface as an administrator.
2. On the **ADVANCED > SSL Inspection** page:
    1. For inline deployments on the 910 and above, set **SSL Inspection Method** to **Transparent**.
    2. For forward proxy deployments on the 610 and above, set **SSL Inspection Method** to **Proxy**.
3. In the Inspected Domains field, enter `Google.com` and click **Add**.
4. Install an SSL certificate. There are two recommended options:
    - Select **Create** to generate your own signed SSL certificate and download it to install in or push out to each client browser. If you don't, users will see a warning each time they

browse an HTTPS site when **SSL Inspection** is enabled. For detailed instructions on creating and installing the certificate, see How to Create and Install a Self-Signed Certificate for SSL Inspection.
- Use the Barracuda Default Certificate for SSL Inspection, available on the **ADVANCED > SSL Inspection** page. This is the simpler of the two methods. If you are only using one Barracuda Web Security Gateway (as opposed to clustering two or more systems using Linked Management), the private key is more secure as it never leaves the device. If you have a high availability deployment, you will need to install the same root certificate on each Barracuda Web Security Gateway. For detailed instructions on installing the certificate, see How to Use the Barracuda Default Certificate for SSL Inspection.

Step 2. Block or Allow Google Consumer Apps

The **Google Consumer Apps** content category is used to block or allow traffic from Google domains and sub-domains. You can then create Exceptions to these policies for certain users or groups for 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 example use cases in this article.

How to Block/Allow Google Hangout

To block Google Hangouts, you must block **both** of the following:

- https://plus.google.com/hangouts
- https://plus.google.com

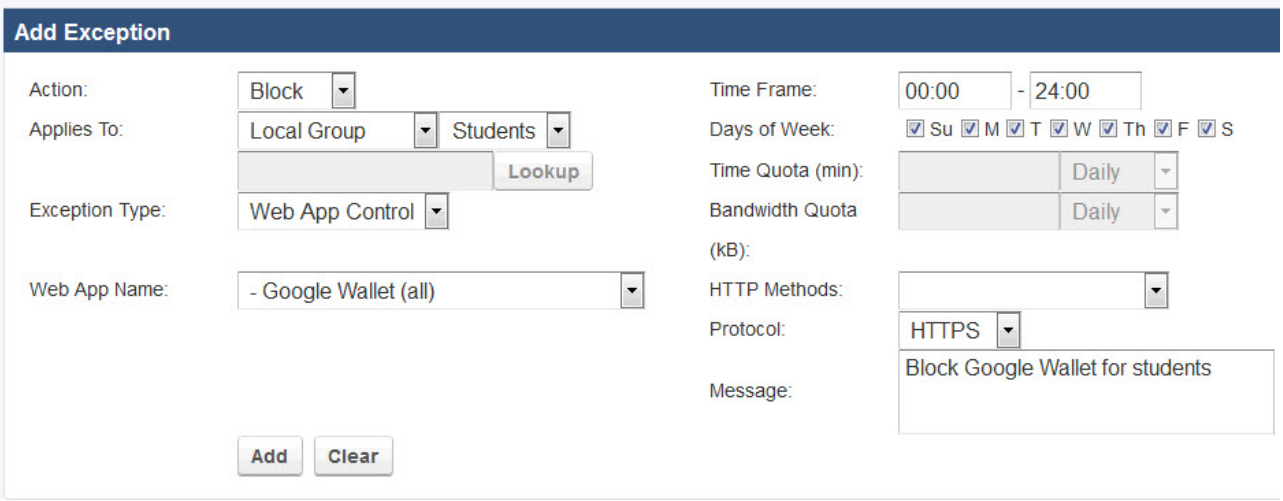
Use Case #1 – Allow Google Consumer Apps, While Blocking Google Wallet Students

This scenario allows access to Google Gmail and most other Google Consumer Apps, which are accessed via HTTPS. Exception to this policy is blocking Google Wallet over HTTPS. Since no time frame is specified on the **BLOCK/ACCEPT > Exceptions** page in this example, these policies would be enforced by the Barracuda Web Security Gateway 24/7 if configured as shown here.
Step 1. Configure SSL Inspection as described above.

Step 2. Create the *Block* policy for Google Wallet.

1. On the **BLOCK/ACCEPT > Exceptions** page, in the **Add Exceptions** section, select the *Block* **Action**. See **Figure 1.**
2. Select the type of users you want to block (*Authenticated, Local Group,* etc.) in the **Applies To** field. In this case we've chosen the *Students* Local Group.
3. Select *Web App Control* as the **Exception Type**.

Figure 1: Blocking Google Wallet for the *Students* group



4. In the **Web App Name** box, select Google Wallet (all).
5. From the **Protocol** drop-down, select *HTTPS*.
6. Click **Add**.

Use Case #2 – Restricting Use of Google Mail During Business Hours

This example requires version 9.1 or higher of the Barracuda Web Security Gateway.

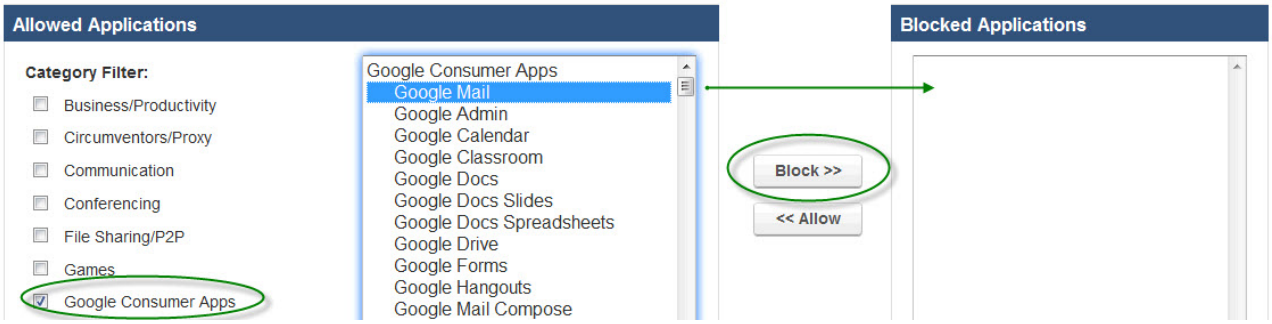
You may want to allow managers access to G Suite business mail, while blocking Gmail access to non-managers. Here are the basic steps.

Step 1. Configure SSL Inspection as described above.

Step 2. Create the Block policy for Gmail.

1. Create a group called *Managers* on the **USERS > USERS/GROUPS** page. Assign appropriate users to this group.
2. Go to the **BLOCK/ACCEPT > Web App Control** page and, in the **Allowed Applications** box, select **Google Consumer Apps** under **Category Filter**.
3. In the list box, you can either select **Google Mail** or **Google Consumer Apps** (to block ALL Google Consumer Apps), and click the **Block** button to move it to the **Blocked Applications**

list box. Click **Save**.



Step 3. Create the Allow policy for business Gmail for *Managers*.

1. Go to the **BLOCK/ACCEPT > Exceptions** page and select the *Allow* action.
2. Select the *Local Group* in the **Applies To** field. In the dropdown to the right, select *Managers.*
3. Select the *Web App Control* **Exception Type**.
4. Select *Google Mail* for the **Web App Name**.
5. In the **Allowed Domains** text box, enter, separating by commas, the Google sub domain(s) from which managers can access Google Mail. This will be the domain(s) with which they log into their business Google accounts.
6. Click the **Add** button to see the exception added to the **List of Exceptions** table below.

Use Case #3 – Blocking Personal Gmail, While Allowing Business Gmail Access to All Users

This example requires version 9.1.0 of the Barracuda Web Security Gateway.

Suppose you want to allow access for *Authenticated Users* to G Suite business mail 24/7, but block personal gmail during business hours.

Step 1. Configure SSL Inspection as described above under Enable and Configure SSL Inspection.

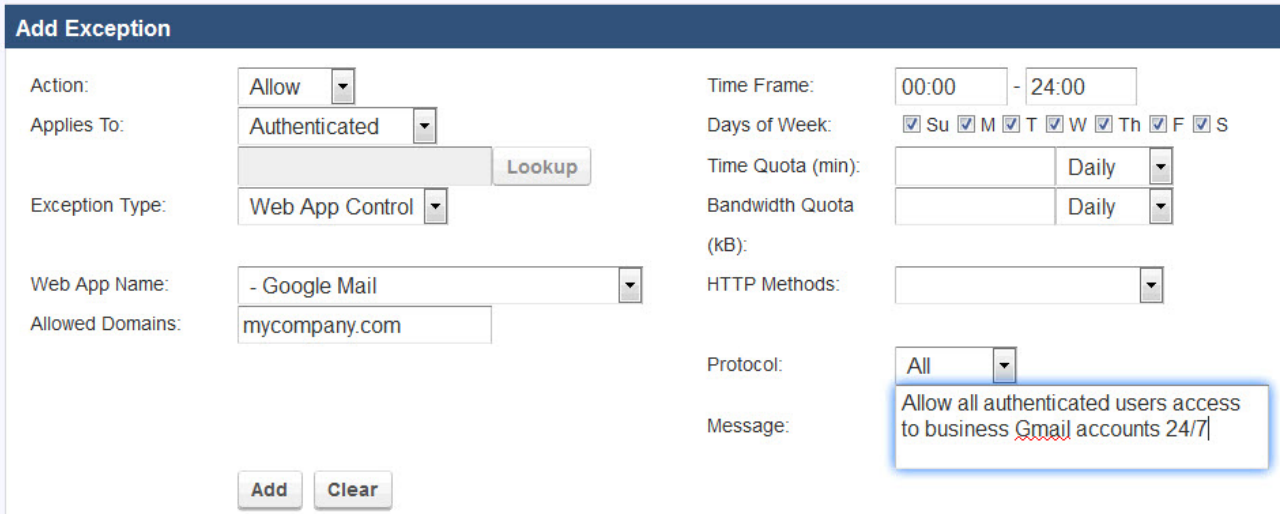
Step 2. Create the block policy for Gmail.

1. Go to the **BLOCK/ACCEPT > Web App Control** page and, in the **Allowed Applications** box, select **Google Consumer Apps** under **Category Filter**.
2. In the list box, select **Google Mail**, and click the **Block** button to move it to the **Blocked Applications** list box. Click **Save**.

Step 3. Create the Allow policy for business Gmail for *Authenticated Users* 24/7.

1. Go to the **BLOCK/ACCEPT > Exceptions** page and select the *Allow* action.

2. Select *Authenticated* in the **Applies To** field.
3. Select the *Web App Control* **Exception Type**.
4. Select *Google Mail* for the **Web App Name**.
5. In the **Allowed Domains** text box, enter, separating by commas, the Google sub-domain(s) from which users can access their business Google Mail accounts. This example uses `mycompany.com` and limits authenticated users to only access Gmail accounts with logins from that domain.
6. Click the **Add** button to see the exception added to the **List of Exceptions** table.



Step 4. Create the Allow policy for personal Gmail account access OUTSIDE of business hours.

1. Follow #1-4 in **Step 3** above.
2. Select a **Time Frame** of Monday - Friday, 17:00 - 08:00 (or whatever constitutes hours *outside* of typical business hours).
3. Click the **Add** button to see the exception added to the **List of Exceptions** table.

Figures

1. ExceptionGoogleWallet.jpg
2. BlockGoogleConsumerAppsGoogleMail.jpg
3. ExceptionGoogleBusMail.jpg