

Exception Policies

<https://campus.barracuda.com/doc/16679217/>

This article applies to the Barracuda Web Security Gateway running firmware version 7.0 and higher. For examples blocking Google Consumer Apps, see [Google Workspace Control Over HTTPS](#).

Once you have created desired block and accept policies, use the **BLOCK/ACCEPT > Exceptions** page to create exceptions to these rules for specific users or groups so they can override the filters that block, warn or monitor access to applications and websites. You can create exception policies for the following types of filters:

- Domains
- URL Patterns
- MIME types
- Content, including Safe Search
- Applications
- Web 2.0 applications
- Search terms (found anywhere in the URL)
- All web traffic

Exceptions are useful for:

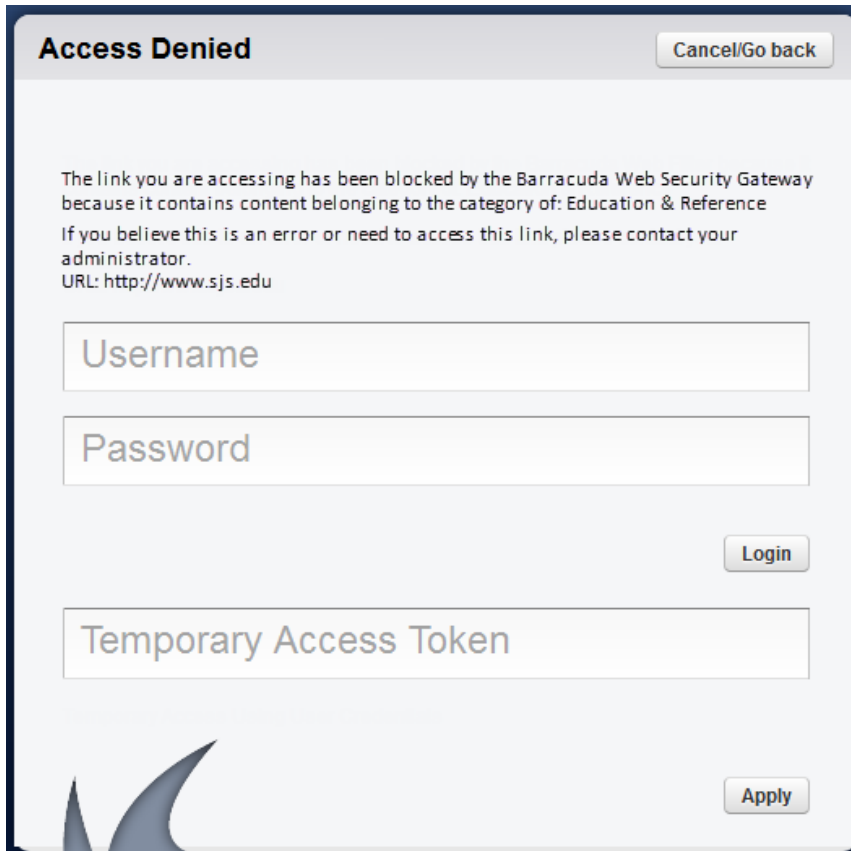
- Creating policies, or rules, that allow a user or a group of users to access content that is blocked for other users.
- Creating policies that block a specific user or group of users from accessing content that is allowed for other groups/users.
- Configuring policies to only apply during certain hours or days of the week.

See examples below.

How Exceptions Work

When a user tries to access content that is blocked by one of the Barracuda Web Security Gateway policies, the user receives a block message. If the user is not authenticated with NTLM and is not using the Barracuda WSA agent, the block page will contain login fields as shown below:

Figure 1. Block page with login fields

A screenshot of a web browser window showing an "Access Denied" dialog box. The dialog has a title bar with "Access Denied" and a "Cancel/Go back" button. The main text explains that the link is blocked by the Barracuda Web Security Gateway due to content in the "Education & Reference" category. It provides a URL "http://www.sjs.edu" and instructions to contact an administrator. Below the text are three input fields: "Username", "Password", and "Temporary Access Token". There is a "Login" button next to the Password field and an "Apply" button at the bottom right.

Access Denied Cancel/Go back

The link you are accessing has been blocked by the Barracuda Web Security Gateway because it contains content belonging to the category of: Education & Reference
If you believe this is an error or need to access this link, please contact your administrator.
URL: <http://www.sjs.edu>

Username

Password Login

Temporary Access Token

Apply

If an exception policy exists for the blocked content, the user can enter their username and password (LDAP credentials, if configured) for the account that was assigned to the exception policy. The block page also includes a **Temporary Access Token** field where a student can enter a code they've been given by a teacher to allow temporary access to a particular website or category of websites for classroom research. See [Temporary Access for Education](#) for details. After the user enters the correct account information, the Barracuda Web Security Gateway applies the effective policy for that authenticated user.

Policy Alerts

You can configure the Barracuda Web Security Gateway to send an email alert to one or more email addresses when a content filter rule is triggered more than a specified number of times. For example, say you block the *Propriety* and *Commerce* categories on the **BLOCK/ACCEPT > Content Filter** page and one or more authenticated users browses sites under those categories (such as *Adult Content* and *Shopping* content types respectively). A Policy Alert email can be sent at a predefined interval (hourly, etc.), summarizing the top number of users violating the *block* policy for these categories.

Where to configure Policy Alerts

- See the **BLOCK/ACCEPT > Exceptions** page to enable/disable and configure policy alerts, and to specify the action, user(s) or group(s) to include as well as the content category and threshold for when to send alerts.
- You can alternatively specify the email addresses to which policy alerts should be sent by *role* using the **ADVANCED > Delegated Admin** page.
- Configure policy alerts format (HTML, PDF, etc.) and frequency of notification emails from the **BLOCK/ACCEPT > Configuration** page.

Limiting Access by Time frames, Time Quotas and Bandwidth Quotas

Use the **Time Quota** and **Bandwidth Quota** exception types on the **BLOCK/ACCEPT > Exceptions** page to assign browsing limits by domain, URL, content category and/or application to specific groups or individual users. Time based quotas can be based upon periods of time or a calculation of time used. Periods of time are exact, for example: 1-2 pm; however, if you choose to limit time by calculation, the user's session time logic is used to determine the amount of time spent. For more information about how session times and browse times are calculated, see [Reporting](#).

The bandwidth quotas are based on the amount of transferred data. Bandwidth quotas include both download and upload traffic. The *Allow* and *Monitor* actions are available for both time and bandwidth quotas. When groups are used, quotas are applied to each individual within the group, not the group as a whole.

Quotas can be configured to be in effect during the **Time Frame** you specify.

Exceptions for MIME Types or Domains

When you select the **Exception Type** as either *MIME Type* or *Domain*, note that you can only specify **one** MIME Type or domain per exception. If you want to create exceptions for more than one MIME type or domain, you must create a separate exception for each type or domain.

Examples of Using Exceptions

After you create an exception for an application that is blocked, it may take up to 30 minutes

for that exception to take affect. This behavior is most likely to be seen when the application traffic had started before the exception was applied.

Example 1 - Limit access to job search websites

Your organization configures their content filters to block access to Job Search and Career Development sites like Monster.com. However, your Human Resources department requires access to such sites. In this case, you would do the following to create the policy:

1. Go to the **USERS/GROUPS > Local Groups** page. Enter *HR* in the **Group Name** field group and click **Add**. Assign appropriate users to this group from the **USERS/GROUPS > Account View** or **New User s** page.
2. **Create** a *Block* policy for *Authenticated* users on the **BLOCK/ACCEPT > Content Filter** page.
3. On the **BLOCK/ACCEPT > Exceptions** page, select *Allow* for the **Action**.
4. Select *Local Group* for **Applies To**, and **select** *HR* from the dropdown to make an exception for the *HR* Group.
5. Select the *Content Filter* **Exception Type**.
6. Select *Job Search and Career Development* in the **Content Type** dropdown.
7. Click the **Add** button to create the policy.

Example 2 - Block all of Facebook except for ONE particular page

1. Configure SSL Inspection on the Barracuda Web Security Gateway. See the **ADVANCED > SSL Inspection** page.
2. Go to the **BLOCK/ACCEPT > Web App Control** page and block Facebook as follows:
 1. Check *Social Media* under **Allowed Applications**.
 2. In the drop-down below that box, select *Facebook all functions*.
 3. Click the **Block** button on the right side of the page.
 4. Click **Save**.
3. Go to the **BLOCK/ACCEPT > Exceptions** page. Create an exception as follows:
 1. Select *Allow* for the **Action**.
 2. Select the appropriate group for **Applies To**.
 3. Select *URL Patterns* for **Exception Type**.
 4. In the **URL Pattern** field, paste the Facebook page URL you want to ALLOW. For example: **https://www.facebook.com/thenameofyourpage.html**
 5. Configure other Exception rules as desired, such as Time Frame (to Allow), etc.
 6. Click **Add**.

Example 3 - Limit access to chat sites to 30 minutes per day during business hours

1. First create a block policy for this content category on the **BLOCK/ACCEPT > Content Filter** page.
2. Next, on the **BLOCK/ACCEPT > Exceptions** page, create an *Allow* action for a time quota of 30 minutes for a particular user or group between the hours of 6:00 (6am) and 18:00 (6pm) for the *Content Filter* **Exception Type** and the *Gaming Content Type*, and check each box for

Monday - Friday.

Note: Exceptions are applied in the order in which they are listed in the table on the **BLOCK/ACCEPT > Exceptions** page; i.e., exceptions are applied from the top-down and will stop processing rules once a match is made. For example, if you want to block access to all web traffic for unauthenticated users but allow access to selected websites, first create the *block* exception and then create the *allow* exception. You can re-order exception rules once they are created by dragging and dropping exceptions in the table.

Example 4 - Allow limited access to gaming sites during lunch time

1. Create a block policy on the **BLOCK/ACCEPT > Content Filter** page for the Game Playing category.
2. On the **BLOCK/ACCEPT > Exceptions** page, create an *Allow* action for a particular user or group between the hours of 12:00 (12pm) and 1:00 (1pm) for the *Content Filter Exception Type* and the *Gaming Content Type*. To prevent excessive bandwidth usage (uploading or downloading), begin by creating a *Block* policy on the **BLOCK/ACCEPT > Content Filter** page for the Streaming Media category.
3. On the **BLOCK/ACCEPT > Exceptions** page, create an *Allow* action for a particular user or group for the *Content Filter Exception Type* and the *Streaming Media Content Type*, which includes the following:
 - Audio or video streaming services
 - Internet TV and radio
 - Webcam services
 - VoIP (Voice over IP) or telephone services via your computer

Specify the bandwidth limit to allow for these types of traffic in kb and select Daily, Weekly or Monthly from the drop-down. Use the **BASIC > Reports** page to create reports on time and/or bandwidth usage by user, group, application, content type, domain or URL.

Google Consumer Accounts - Creating Policies and Exceptions

Google has some restrictions when applying policy to HTTPS traffic for some Google consumer accounts applications. The Barracuda Web Security Gateway version 9.1 and above offers a Google Consumer Accounts **Category Filter** on the **BLOCK/ACCEPT > Web App Control** page which you can use to create block/allow policies. This category allows you to specify some or all Google Consumer Accounts apps when creating policy. See [Google Workspace Control Over HTTPS](#) for examples of creating policies and exceptions for these apps. For details about Google restrictions related to SSL filtering, see [Google Restrictions With SSL Inspection](#).

If you are running the Barracuda Web Security Gateway version 10.1 or above, for blocking Google sites for Chromebook users, see [How to Get and Configure the Barracuda Chromebook Security Extension](#).

Safe Browsing / Safe Search - Limiting to Specific Users

If you have disabled the Safe Browsing feature on the **BLOCK/ACCEPT > Content Filter** page, all users will be able to browse freely with the listed search engines. If you enabled Safe Browsing, users will *not* see search engine content that contains objectionable thumbnail images in the search results; only filtered thumbnails are displayed in the search results. For instructions on limiting safe browsing to a group such as, for example, students, see [How to Enable SafeSearch](#).

Figures

1. Block Page Login BWSG.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.