Best Practices in Configuring Policy

https://campus.barracuda.com/doc/6160388/

Begin creating filtering policies which you can assign to specific users and/or groups by following the best practices listed below. The BLOCK/ACCEPT pages in the web interface provide a wide range of filters that enhance the default spyware and virus detection capabilities of the Barracuda Web Security Gateway. **Note that application filtering is supported by the Barracuda Web Security Gateway appliance, but not by the Barracuda Web Security Gateway Vx virtual machine.**

Users and Groups for Authentication

You can apply domain, IP address, pattern, content, application, and MIME type blocking filters to *authenticated* and/or *unauthenticated* users. The first step in creating your policy should be deciding which categories your users will **not** be allowed to visit (*Adult Content, Game Playing & Game Media, Streaming Media,* etc.). You can later override this policy using exception policies to grant either additional or more restrictive access for individual users or groups. Before you create or modify a filter, make sure to use the drop-down menu on the right side of the web interface page to select which type of user you want the filter applied to (authenticated or unauthenticated).

Use the **USERS/GROUPS** pages to manage users and authentication. See Managing Users and Groups to get started.

Exception Policies for Specific Access

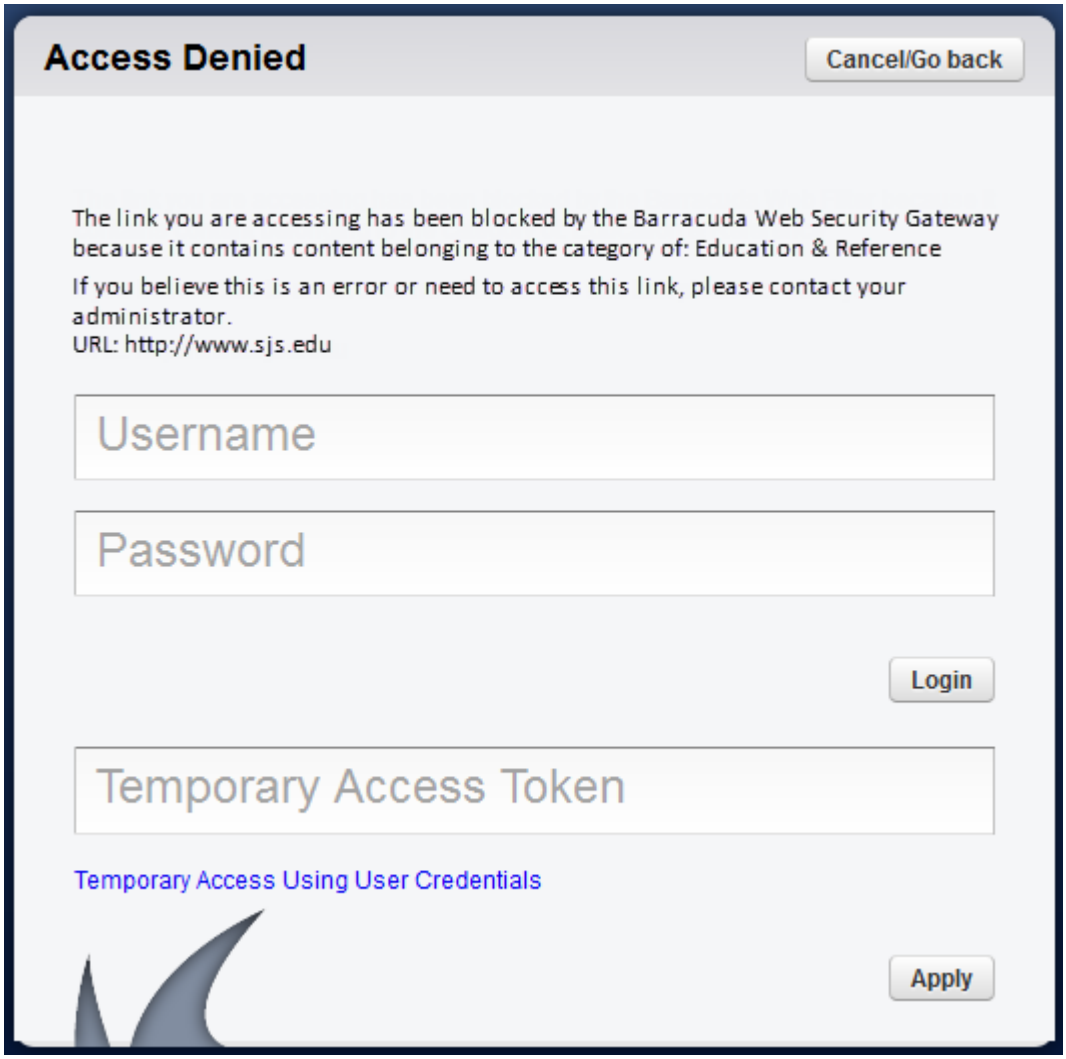
Exceptions are useful for creating policies that allow a subset of your users to access content that is blocked for other users. On the **BLOCK/ACCEPT > Exceptions** page, you can create policies to override filters you have created on a per-user or group basis. For example, if you configure your content filters to block access to auction sites for both *authenticated* and *unauthenticated* users, but a member of your purchasing department requires access to these sites, you can create an exception policy that allows access to only this user. Or you could create an exception for the entire purchasing department (a 'Group') using the LDAP organizational unit in your Active Directory server.

Exception policies are applied in the order in which they are listed in the table on the **BLOCK/ACCEPT > Exceptions** page of the web interface. You can drag and drop exceptions to re-order them in the table. See Exception Policies for details.

Block Pages and Authorized Logins

When a user tries to access content that is blocked by one of the assigned filters, the user receives a block message (see Figure 1 below) that may contain login fields, depending on how you configure authentication on your Barracuda Web Security Gateway. If you want to hide the login fields because you have not created any exception policies that allow users to bypass the block filter, go to the **BLOCK/ACCEPT > Configuration** page and change the **Enable Login Override of Block Pages** setting to *No*. Note that remote users who access the Barracuda Web Security Gateway via the Remote Filtering (WSA) feature or via the Barracuda Safe Browser on their mobile devices will *not* see login fields on block pages.

Figure 1: Block Message with Login Fields



The Barracuda Web Security Gateway will recognize specific types of block and accept rules in the order they are listed (from top to bottom). If conflicting rules are created, the rule listed first will be

honored (see **1.Exceptions** below) . After exceptions, allow lists for URLs and domains take precedence over block lists, followed by the block rules for applications and content filter categories. On the application and content filter pages, the *Allow* setting really means "don't match/ignore". Unmatched requests are allowed by default.

Barracuda recommends setting **Enable Typosquatting Protection** to **Yes** on the **BLOCK/ACCEPT > Configuration** page so that the Typosquatting Protection feature will prevent users from visiting sites using misspelled names of popular sites, and thereby possibly encountering viruses and malicious downloads. See Typosquatting Protection for details.

Custom Categories

When the custom category a URL belongs to is set to *Allow*, that means that the custom category will not cause a block, but the URL is still checked against other categories. If the URL belongs to a blocked category, then that URL is blocked.

This rule can be overridden by one of the following:

- Using the **Recategorize Domains** option when creating the custom category on the **BLOCK/ACCEPT > Custom Categories** page.
- Creating an exception (**BLOCK/ACCEPT > Exceptions** page) for the custom category to make sure the rule configured for the custom category will take precedence.
- Note also the local recategorization option that might affect whether a custom category applies.

Block/Allow Rule Order of Precedence

The rules you configure under the **BLOCK/ACCEPT** tab are applied in a specific order, and it is important to understand that order before creating policies. See BLOCK/ACCEPT Order of Precedence for details.

Figures

1. Block Page Login BWSG.png