

How to Configure Advanced Filtering Policies

<https://campus.barracuda.com/doc/78810197/>

Barracuda Content Shield (BCS) provides visibility into customer web activity while enforcing access policies across all users and devices. With more than 170 URL categories, BCS does more than protect your customers from malicious websites; it also ensures that you're protecting their employees from accessing sites that would violate company policy, norms, and standards.

With BCS Plus, you can either use preset filtering policies or create customized policies for a particular user or group, and base policies on either categories, domains, or URLs.


Configuring Local or LDAP Users and Groups

If you have not already done so, you can either manually add local users and groups, or synchronize your LDAP / AD services with the BCS service – this enables you to apply policies by users and / or groups. To connect to your LDAP, see [LDAP Active Directory and BCS](#). Or you can choose to [Manually Configure Local Users](#) and groups.

Updates to policies may take up to 15 minutes to take effect.

To create rules:

1. Click **Manage** for the account for which you want to configure rules/policies.
2. Click on **Advanced Filtering** in the left pane.
3. On the **Advanced Filtering** page, click **Add Rule**. Click in the text box at the top of the popup to select one or more users or groups.
4. Select an **Action** of *Block* or *Allow*.
5. Select a rule **Type** of either *Categories*, *Domains*, or *URLs*.
6. Check each category for which you want the rule to apply, or enter the target domain or URL.
7. Click **Save**.

After you have created rules for users and/or groups, you can create a new rule by clicking More Options () in the table row for that user or group, and then click **Create Rule** in the drop-down.

Traffic that is affected by Advanced filtering policies is logged in the [Web Filtering Logs](#).

Barracuda recommends testing your initial selection of block/allow policies using various domains that you know you want blocked, and/or that you know your organization needs to


access, and then make updates to your policies as needed.

How Domains Are Categorized

Barracuda Networks uses one of the most extensive web content definition databases, covering some of the highest risk websites on the Internet. The websites in the Barracuda Networks database are organized into content categories (subcategories) which are grouped by supercategories. When you create rules that block categories of websites, you can choose a supercategory to block, or you can drill down and block websites at the subcategory level. See [Web Use Categories](#) for a list of content categories.

Viewing Configured Filtering Policies

If you have already configured Advanced Filtering policies by user or group, the following displays in a table on the **Advanced Filtering** page in a separate section for each user or group. You can click the blue chevron to expand or hide the policies for each user or group.

- Order - The order in which the rule is applied, relative to other rules you have created. (0=first, 1=second, etc.). You can click More Options () in the table and select *Move to Top* or *Move to Bottom* to change the order in which the rules are applied.
- Action - *Block* or *Allow*
- Type - How the rule is defined; either by categories, domains, or URLs
- Rule - Lists values included in the rule

Deleting a Group

At the right of a table row for a group, click More Options () for a drop-down and click **Delete**.

Adjusting Policies for Users and Groups

After you have created and tested Advanced Filtering policies, you may need to adjust settings according to the needs of your organization based on the following (or other) reasons:

- Changes in browsing or business policies of your organization
- Need for access to some domains that are included in a category that you need to block, in

general

Figures

1. dots.png
2. dots.png
3. dots.png

© Barracuda Networks Inc., 2020 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.