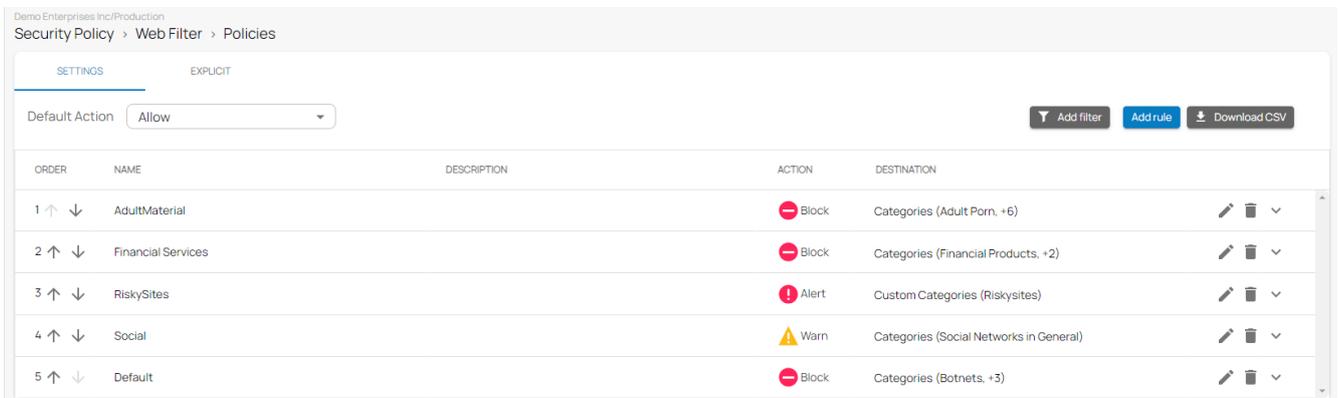


## Web Filter Policies

<https://campus.barracuda.com/doc/98223638/>

The Barracuda SecureEdge Manager allows administrators with appropriate permissions to configure Web Filter policies to protect against potential threats and enforce corporate policies. Barracuda Networks provides a large database, organized in categories, for web filtering. You can either use the provided categories to create rules, or you can specify the domains yourself. Malicious URLs are blocked in the default configuration. For example, web filtering is set to allow all and to block only defined exceptions, whereas the corresponding ACL is set to block all and to allow only defined exceptions.



ORDER	NAME	DESCRIPTION	ACTION	DESTINATION
1	AdultMaterial		Block	Categories (Adult Porn, +6)
2	Financial Services		Block	Categories (Financial Products, +2)
3	RiskySites		Alert	Custom Categories (Risksites)
4	Social		Warn	Categories (Social Networks in General)
5	Default		Block	Categories (Botnets, +3)

A filter rule either blocks or allows a domain, category or custom category from any source, whereas an explicit rule blocks or allows URLs from specified sources. In addition, for the web filter rule, you can now either alert or warn users against suspicious traffic.

The following actions are available for the Web Filter policy :

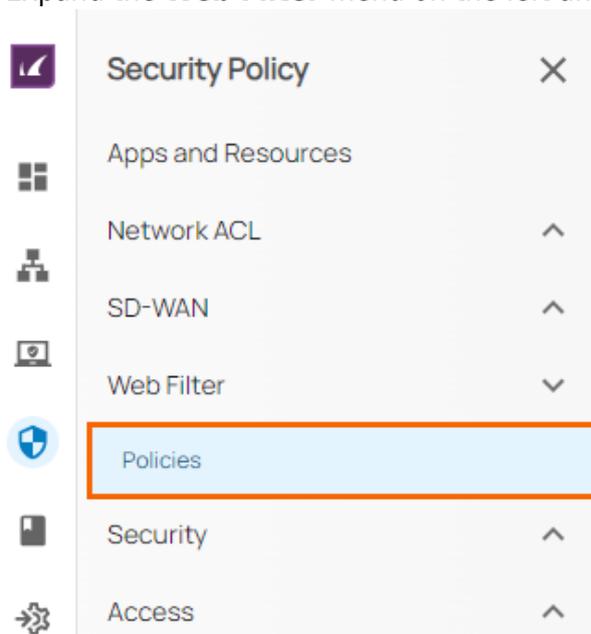
- **Allow** – The user can access the website.
- **Block** – The user is blocked from viewing the website.
- **Alert** – The user is allowed to access websites in this category, but the action is silently logged.
- **Warn** – The user is redirected to a warning page and must click **Continue** to access the requested website. For example, a web filter rule exists with SSL Inspection enabled and with a **Warn** action for different types of selected URL categories (such as social media and lottery). If a user visits a website that matches the filter rule, it allows access to the specific URL categories and/or websites. However, a warning page is shown. When a user clicks **Continue** in the browser, it will implicitly cause a security inspection.

The **Warn** action does not work with any non-SSL-inspectable domains.

For Web Filter policies, wildcards are added implicitly. For example, adding `campus.barracuda.com` will automatically match `www.campus.barracuda.com` (or any other subdomain) even without adding a wildcard.

## Create a Web Filter Policy

1. Go to <https://se.barracudanetworks.com> and log in with your existing Barracuda Cloud Control account.
2. In the left menu, click the **Tenants/Workspaces** icon and select the workspace you want to create a web filter policy for.
3. Go to **Security Policy**.
4. Expand the **Web Filter** menu on the left and select **Policies**.



5. The **Policies** window opens. To create a new rule, click **Add Rule**.

Demo Enterprises Inc/Production  
 Security Policy > Web Filter > Policies

SETTINGS      EXPLICIT

Default Action: Allow

ORDER	NAME	DESCRIPTION	ACTION	DESTINATION	
1 ↑ ↓	AdultMaterial		Block	Categories (Adult Porn, +6)	✎ ✖
2 ↑ ↓	Financial Services		Block	Categories (Financial Products, +2)	✎ ✖
3 ↑ ↓	RiskySites		Alert	Custom Categories (Risksites)	✎ ✖
4 ↑ ↓	Social		Warn	Categories (Social Networks in General)	✎ ✖
5 ↑ ↓	Default		Block	Categories (Botnets, +3)	✎ ✖

6. The **Add New Rule** window opens.
7. In the **SETTINGS** tab, specify values for the following:
  - o **Name** – Enter a unique name.
  - o **Description** – Enter a brief description.
  - o **Action** – Select the action. You can choose between **Allow**, **Block**, **Alert**, and **Warn**.  
 If you select **Action** = **Block**, you are provided with the option to silently block the rule:
    - **Silent** – Click to enable/disable. By default, **Silent** field is disabled.
 If you select **Action** = **Allow** or **Alert** or **Warn**, the **Silent** field is disabled.

- **Type** – Select the type. You can choose between **Category**, **Domain**, and **Custom Category**.
  - If you select **Category**, expand the category and click on the specific sub-categories you want to allow/block. Additionally, you are also provided with option **Select All** to select all sub-categories.
  - If you select **Domain**, enter one or more domains and click **+**.
  - If you select **Custom Category**, select a custom category from the drop-down menu, or type to search.

Add New Rule ×

Name *	AdultMaterial
Description	Blocksites
Action *	<input type="radio"/> Block
Silent	<input type="checkbox"/>
Type *	Category

Categories Select All

^ Adult material (3 out of 7 selected) -

Adult Magazine Or News + **Adult Porn** X Adult Search Or Links + Fetish +

**Nudity** X Sexual Expression(Text) + **Sexual Services** X

▼ Adult recreation (0 out of 7 selected) □

▼ Business (0 out of 12 selected) □

▼ Commerce and shopping (1 out of 6 selected) -

8. Scroll down to add more categories and click **Save**.

After the configuration is complete, you can see a new policy has been created on the **Policies** page with all your selected categories and sub-categories. For example, in this case, expand **Adult Material** and verify your categories and sub-categories.

Demo Enterprises Inc/Production  
 Security Policy > Web Filter > Policies

SETTINGS    EXPLICIT

Default Action:

ORDER	NAME	DESCRIPTION	ACTION	DESTINATION
1	AdultMaterial		Block	Categories (Adult Porn, +6)

Adult Material:

Commerce and Shopping:

Illegal or Improper:

Society and Lifestyle:

## Edit an Existing Web Filter Policy

1. Go to <https://se.barracudanetworks.com> and log in with your existing Barracuda Cloud Control account.
2. In the left menu, click the **Tenants/Workspaces** icon and select the workspace you want to edit a web filter policy for.
3. Go to **Security Policy**.
4. Expand the **Web Filter** menu on the left and select **Policies**.
5. The **Policies** window opens. Click on the pencil icon next to the rule you want to edit.

Demo Enterprises Inc/Production  
 Security Policy > Web Filter > Policies

SETTINGS    EXPLICIT

Default Action:

ORDER	NAME	DESCRIPTION	ACTION	DESTINATION
1	AdultMaterial		Block	Categories (Adult Porn, +6)
2	Financial Services		Block	Categories (Financial Products, +2)

6. The **Edit Rule** window opens. Edit the value you are interested in.
7. Click **Save**.

## Remove an Existing Web Filter Policy

1. Go to <https://se.barracudanetworks.com> and log in with your existing Barracuda Cloud Control account.
2. In the left menu, click the **Tenants/Workspaces** icon and select the workspace you want to remove a web filter policy for.
3. Go to **Security Policy**.
4. Expand the **Web Filter** menu on the left and select **Policies**.
5. The **Policies** window opens. Click on the trash can icon next to the rule you want to remove.

Demo Enterprises Inc/Production  
 Security Policy > Web Filter > Policies

SETTINGS      EXPLICIT

Default Action:

ORDER	NAME	DESCRIPTION	ACTION	DESTINATION
1 ↑ ↓	AdultMaterial		Block	Categories (Adult Porn, +6)
2 ↑ ↓	Financial Services		Block	Categories (Financial Products, +2)

6. The **Delete Rule** window opens.

## Delete Rule

Are you sure you want to delete this rule?

Cancel

Ok

7. Click **OK** to confirm.

## Select the Default Action

You can configure web filtering either to allow or block traffic by default. In addition, you can now set **Default Action** to **Alert**.

1. Go to <https://se.barracudanetworks.com> and log in with your existing Barracuda Cloud Control account.
2. Go to **Security Policy**.
3. Expand the **Web Filter** menu on the left and select **Policies**.
4. In the **SETTINGS** section, select the **Default Action**.

SETTINGS

Default Action:

ORDER	NAME	DESCRIPTION	ACTION	SOURCE	DESTINATION
-------	------	-------------	--------	--------	-------------

## Further Information

- For more information on User and Groups, see [How to Connect Microsoft Entra ID with Barracuda Cloud Control](#).

## Figures

1. WebFilterPoliciesPage.png
2. gotoWebFilterPolicies.png
3. wf-addrule.png
4. WebfilterPolicy-Addrule.png
5. PoliciesPage.png
6. Edit-WebFilterpolicies.png
7. Del-Policies.png
8. DeleteRule.png
9. acl\_def\_90.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.