How to Configure Web Security Policies

https://campus.barracuda.com/doc/98209799/

This article applies to the CloudGen Access agent version 2.0 and higher.

To view and/or edit web security policies you already created, see View Web Security Policies. Note that policies are enforced in the order they are listed on the page: policies above others in the table take precedence.

To create customized policies for a particular user, users, or group(s), you can base policies on either categories of domains or specific domains:

1. Click on the shield icon on the left navigation pane. You'll see the **Web Security** page with a list of any policies you might already have created.
2. Click the **+** on the right side of the screen to begin creating a new policy.
3. In the **Edit Policy** modal, select one or more groups of users if you want the policy to apply to groups.
4. Select one or more users if you want to create a policy for one or more specific users.
   To apply a policy to ***everyone***, do not select any users or groups.
5. Select either the *Block* or *Allow* action.`
6. For **Secure**, select *Categories* if you want the policy to apply based on domain categories visited. Or select *Domains* if you want the policy to apply when one or more specific domains are visited. See the **Creating Policies by Categories** and **Creating Policies by Domains** sections below for more details.

Creating Policies by Categories

If you selected *Categories* in step 6 above, you'll see a list of *Supercategories*. To see the list of categories within each supercategory, click **Expand All**. Now you can either:

- Select each individual category you want to block or allow – Or –
- Click the box in the **Select All** column to the right of the supercategory name to automatically apply your policy to all of the categories within that supercategory.

Click **Collapse All** to just show the supercategories.

At the bottom of the page, configure Feedback Settings (alerts), and then click **Create** at the bottom of the page to save your policy.

Creating Policies By Domains

If you selected *Domains* in step 6 above, you'll see the **Domains** text box. Enter a domain name, and then press **Enter**. You can then add the next domain name, and so on. To remove a domain name, click the **X** to the right of the domain name.

- When you enter a domain name, a wild card is automatically applied to include subdomains and the TLD (for example, .com, .org, .net, .us, .de., etc.)
- For domain-based policies, you cannot add a URL. For example, you could enter `redfin.com`, but `https://www.redfin.com/zipcode/95123` would not be accepted.

At the bottom of the page, configure Feedback Settings (alerts), and then click **Create** at the bottom of the page to save your policy.

Feedback Settings

Configure these settings to determine how the administrator will be alerted to violations to policy, blocked domains, or to track policy related activity.

- **Alert** – CloudGen Access will send an alert via email if a violation to policy occurs.
- **Logs** – The **Activity** page will show policy related activity.
- **Mobile App Notification** – Show a notification on the app if a domain is blocked.

Save Your Policy

To save your policy, click **Create** at the bottom of the page.

Best Practices for Creating Policies

1. Pay attention to policy precedence when you create user and group policies: policies above others in the table take precedence.
2. Barracuda Networks recommends beginning by creating a baseline policy for *everyone* with a

default action of *Allow*. Do this by *not* selecting any users or groups for the policy. This prevents you from accidentally blocking newly discovered websites that may be important to people in your organization, such as new competitors, local government alerts, or breaking weather events. You can later add exception policies as needed. This policy would end up at the bottom of the table, so all policies created after that, or placed above it in the table, would take precedence and/or be exceptions to the *everyone* policy.

3. The next policy you create should be an *everyone* policy that blocks a broad set of categories.

   Important: Be sure to *ONLY* block the **Content Delivery Networks & Infrastructure (CDNs)** category under the **Security** super-category if you understand CDNs, because thousands of websites rely on CDNs to deliver critical website content.

   After you create these two policies, you'll see the second policy you created *above* the first policy in the table. This means that the higher level policy (block) takes precedence over the one(s) below it. See **How Policies Are Applied (Order of Precedence)** below for more information.

4. Finally, create your group and user specific policies. These should be in the table **above** the first general *Everyone* policies you created, and represent exceptions to those policies. Barracuda Networks recommends placing *user* polices at the top of the list (table) and *group* policies near the bottom for easy policy precedence.

Syntax for policies by domains and subdomains

When entering a domain for a policy, do not use wildcards ('*'), or include protocols, such as http:// or https://. When you enter a domain name, a wild card is automatically applied to include subdomains and the TLD.

Correct	Incorrect
mydomain.net, www.mydomain.net	https://www.mydomain.net
www.mail.barracuda.com	*mail.barracuda.com
yourdomain.org	*.yourdomain.org

All subdomains of the domain you enter are automatically included; in other words, subdomains inherit policies applied for a domain, *UNLESS* you create an exception. If you want to create an exception for a particular subdomain, *you must specify that subdomain explicitly.* For example, if you create a *block* policy for **google.com**, all subdomains are included and blocked. Here are more examples of how exceptions work with domains and subdomains:

Policy	Results

BLOCK google.com BLOCK server1.mail.google.com	http://google.com/ BLOCKED (matches google.com), and blocks ALL Google subdomains http://mail.google.com/ ALLOWED (matches mail.google.com) http://server1.mail.google.com/ BLOCKED (matches server1.mail.google.com) http://server2.mail.google.com/ ALLOWED (matches mail.google.com)
BLOCK www.abc.com	http://abc.com ALLOWED (doesn't match www.abc.com)
BLOCK abc.com	http://www.abc.com BLOCKED (inherits policy from abc.com domain)
ALLOW abc.com BLOCK z.abc.com	http://z.abc.com BLOCKED (matches z.abc.com) http://y.abc.com ALLOWED (inherits policy from abc.com)

How Policies Are Applied (Order of Precedence)

Policies are applied in the order in which they appear in the table. Each policy takes precedence over the policies listed *below* that one. For example, you may create a *group* policy that blocks YouTube.com for *everyone* or for a specific group of users. If you want to create a separate policy allowing one user to access YouTube.com, and that user is part of the group for which you created the *block* policy, you must place the policy for the user above the policy for the group. If you place the policy for that user *below* the group policy, then YouTube.com would be blocked for that user as well.

> Barracuda Networks 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 policies that block categories of websites, you can choose a supercategory to block, or you can drill down and block websites at the category level. See Web Use Categories for a list of content categories.

Modifying, Moving or Deleting a Group or a User Policy

- To edit a policy: At the right of a table row for a policy, click the 3 dots ( ) for a drop-down and click *Edit*.
- To delete a policy: At the right of a table row for a policy, click the 3 dots ( ) for a drop-down and click *Delete*.
- To MOVE a policy up or down in the table to change order of precedence, click the 8 dots () to the left of the **Action** (Allow or Block), and use the hand icon to drag the policy up or down in the table.

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. 8 Dots.png