How to Configure DNS Filtering and Policies

https://campus.barracuda.com/doc/77401148/

You can configure DNS Filtering policies by outbound IP address (network), which apply to **ALL USERS**, by either:

- Selecting a pre-configured filtering level: High, Medium, or Low as illustrated below, – OR –
- Specifying a custom set of categories of domains

Based on what you select, you can set block/allow policies by content category for web traffic by network IP address. After creating your block/allow policy, you have the option to create exceptions (either *block* or *allow*) for specific domains from that policy. If you want to create policies specific to users or groups, you can use Advanced Filtering Policies if you have a *BCS Plus* subscription.

Best Practices:

- **You can simulate groups** by segregating users by different external IP addresses. This provides the option to apply different policies to different groups. For example, the *Students* group could be assigned a *High* security policy while the *Faculty* group could have a *Low* security policy.
- Group location policies all into one location policy if possible. This facilitates easier management and editing of policies.

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 into 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 grouped at the subcategory level. See Web Use Categories 2.0 for a list of content categories.

Your filtering policy is built using these categories, and you can refine the policy by adding exceptions at the domain level.

Domain look up: To find out which category a domain belongs to, go to the **ACCOUNT SETTINGS** page and use the **Look For Domain Category** feature.

View Configured Filtering Policies

If you have already configured DNS Filtering for a network, the following displays in a table on the **DNS FILTERING** page:

- Name – The name you (optionally) gave to the network when it was added to the system
- Type – Dynamic IP or Static IP
- Outbound IP Address – Identifies the network
- Activity Last Seen – Timestamp of the last traffic seen
- Category Policy – Click to see which content categories are blocked, and to change the selection of categories if needed
- Exception Policy – Click to see block or allow exceptions you created for the list of categories, and to add or delete exceptions

Configure a New Filtering Policy For a Network

There are three ways to assign a filtering policy to a network:

- Select a preset filtering policy that includes various categories of domains
- Copy a custom filtering policy that was assigned to another network
- Create a custom filtering policy for the network you are adding

After reading this section, see Best Practices for Creating DNS Policies for examples.

To get started:

1. Go to the **DNS FILTERING** page.
2. To begin using the wizard, click **Add Location**.
    1. *Optional*: Enter a name you want to use to identify the network. **Note**: If you don't enter a name for the network, BCS will auto-generate a name:
        - In the case of a dynamic (DHCP) address, the auto-generated name will be simply: *Dynamic*.
        - In the case of a manually entered IP address, the auto-generated name will be *Network - ######* where the hashtags are replaced by the IP address provided.
    2. Select one of two methods of how to specify an outbound IP address for clients. Barracuda Content Shield policies that you configure are applied according to the outbound IP address associated with each client.
        - If the outbound IP address for each client is static (remains the same, as opposed to dynamic), choose **Manually configure outbound IP addresses** and continue with step **c**. Barracuda recommends this deployment since it is the most simple.
        – OR –

- If the service provider issues a dynamic IP address (which potentially changes periodically), choose **Automatically update the outbound IP addresses**. This will lead you to the Barracuda Dynamic IP Updater installation at the end of the wizard. The Barracuda Dynamic IP Updater is a tool that installs on a client and runs periodically to inform the BCS DNS proxy server if the outbound IP address for your network has changed. Click **Start** and skip to **Step 3.**

3. If you selected **Manually configure outbound IP addresses**, after clicking **Start**, the **Outbound IP Address** page of the wizard displays. Enter the IP address of the network for outbound web traffic you want to filter with the policies you will create in this wizard. The **Outbound IP Address** (also known as a "public IP address") can commonly be found on the *status* screen or similar screen of most routers.
4. Enter the **Prefix**. The prefix length shows the number of bits set in the subnet mask; for instance, if the subnet mask is 255.255.255.0, then there are 24 bits in the binary version of the subnet mask, so the prefix length is 24 bits.
5. Click **Add Outbound IP Address**. Click **Next**.

3. For **Category Policy**, select a filtering strategy depending on your organization's requirements. See Best Practices for Creating DNS Policies.
   1. Begin by selecting either a *Recommended default* policy, or a *Custom* policy to start from scratch.
      Recommended default and *Custom* policy options are:
      - Low – includes domains categorized under Security, Illegal Activity, Violence, Pornography, and Adult Content
      - Medium – includes domains categorized under Security, Illegal Activity, Violence, Media Sharing, and Pornography
      - High – includes domains categorized under Security, Illegal Activity, Violence, Gaming, Media Sharing, and Pornography
      - Custom – includes domains categorized under whichever categories you select on the page
        Note: You can modify any level by selecting or de-selecting any category. Or, you can select any supercategory if you want to include all categories in that supercategory.
   2. Review the set of content categories. All domains in the categories that are checked will be blocked for this network. Add or remove categories per your organization's requirements. You can also create exceptions to these policies by domain.
   3. Click **Next**.
4. For **Exceptions**, you have the option to create exceptions for specific domains from the policy you just created.
   1. To *Allow* traffic from a domain that belongs to a category you configured to *block* as a general policy, enter the domain name in the **Allow Domains** text box, and then click **NEXT.** Note that the **'*'** wildcard is built-in. So, for example, if you enter mydomain.com, all subdomains (users.mydomain.com, etc.) will be included. Likewise, if you add a subdomain, all TLDs will be included.
   2. When you are finished creating exceptions, click **Next**.
   3. To remove a domain exception later, click the **EXCEPTIONS** in the row of the table for that policy and, in the popup, delete the domain and click **NEXT**.

      For more about creating exceptions to policy, see How to Create Exception Policies

for DNS Filtering.

5. On the **Configure DNS** page of the wizard, note the IP addresses of Barracuda DNS nameservers. You must specify these IP address as the Primary and Alternate (or Secondary) DNS Nameservers on any of the following:
   1. Your network router
   2. Your client machines
   3. Your Barracuda Firewall (or other firewall solution)
6. Click **Add** on the wizard to add the network. That network location is then listed in the table. For more information on configuring the Barracuda DNS nameservers for your clients, see How to Configure Barracuda DNS Nameservers for Barracuda Content Shield. If you selected **Manual** for **Outbound IP Address** in step 2b, this concludes the wizard.
7. If you selected **Automatic** for **Outbound IP Address** in step 2b, click **Add**. The Dynamic IP Updater page displays.
   Download the Windows Dynamic IP Updater installer and key files, and use these to perform the installation on **a system that is always connected to your network.** The Windows Dynamic IP Updater only needs to be installed on ONE Windows machine in the network, and will run periodically to inform the BCS DNS proxy server if the outbound IP address for your network has changed.

Note: To edit the **Network Name**, click More Options ( ) at the far right of the entry for that outbound IP address in the table and click **Edit .** To change either the IP address or the mask, you must replace the settings by clicking on the Remove icon ( ), and re-entering the desired IP address *AND* mask.

Copy Policy From Existing Network

When you create a new network, you can copy the policy and exception configurations you specified when defining earlier networks. To copy policy from a network you previously defined, f ollow the instructions in Configure a New Filtering Policy For a Network above, with the following modifications:

- Step 3: In the **Category Policy** window, under **Custom Policies** , select the name of the network from which you want to copy the policy.
- Step 4: In the **Exceptions** window, under **Custom Policies** , select the name of the network from which you want to copy the policy.

For both of these steps, you can accept the policies and exceptions that are copied or use them as a starting point and make changes from there.

Adjust Filtering Policy for a Network/Location

After you have created and tested DNS 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

To edit or delete policies or exceptions:

1. Go to the **DNS FILTERING** page.
2. Locate the entry in the table with the **OUTBOUND IP ADDRESS** for the network (Location) for which you want to update policy, and click on **CATEGORIES** .
3. In the **Category Policy** popup, you can:
    1. Add or remove categories to block for the selected policy in the **Category Policy** dropdown, – OR –
    2. Select a different pre-configured policy set from the dropdown, – OR –
    3. Switch between custom policies you have configured.

    4. Click **Save**.

4. Optionally click **Exceptions** in the **Exception Policy** column to add or delete exceptions to the existing policy. As with Category policies, you can either edit the existing set of exceptions, or use the **Exception Policy** dropdown to switch to another set of exceptions, or create a new set.
5. Click **Save** .
   For more information about exception policies, see How to Create Exception Policies for DNS Filtering.

Figures

1. dots.png
2. deleteException.png