How to Configure URL Filtering in the HTTP Proxy

https://campus.barracuda.com/doc/48203304/

Web filtering allows you to control web access. To limit access to certain types of websites and restrict requests from specific dedicated networks or users, configure URL filtering policies. You can also exempt certain users and IP addresses from filtering, log which requests are allowed and denied, and specify the types of statistics that are generated for the service.

On the Barracuda NextGen Firewall F-Series, you can use one of the following engines for web filtering:

- **Barracuda NG Web Filter** – The Barracuda NG Web Filter requires a subscription. With the Barracuda NG Web Filter, different URL category databases can be stored locally on the Barracuda NextGen Firewall F-Series.
- **Barracuda URL Filter** – The Barracuda URL Filter is included for free with a valid Energize Updates subscription. It uses the same category database as the Barracuda NG Web Filter but does not store a local copy of the database on the Barracuda NextGen Firewall F-Series. Instead, every URL is requested through the cloud and the categories for the URLs are stored on the Barracuda NextGen Firewall F-Series.

You can also configure authentication for the web filter and display blocked URL categories with an external HTTP server.

Before you Begin

Enable the Barracuda Web Filter. For more information, see How to Configure URL Filtering in the Firewall.

Configure Web Filtering

To configure web filtering, complete these steps:

Step 1. Configure Web Filter Settings

You can configure the following settings for the web filter:

URL Filter Policies

Configure each policy to grant or deny access to specific URL categories. To determine the category of a

specific website, go to http://www.barracudacentral.org/lookups. A policy can also be restricted to only certain networks and users that access the HTTP Proxy. If a request matches any networks, user groups, or users that are specified in a policy, the policy is applied to it.

Policies are processed in an order that is determined by their name, which must be numerical. For example, a policy named *0000123* will be listed before a policy named *023*. If you want to add a policy at the top of the processing list, include leading zeroes in its name.

By default, a whitelisting policy named *999999* is included in the table. You can edit, clone, or delete this policy.

To create an URL filter policy:

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > HTTP Proxy > Web Filter Config**.
2. Click **Lock**.
3. From the **Web Filter Type** list, select the filter that you want to use:
   - **Barracuda NG Webfilter** – Requires a subscription.
   - **Barracuda Web Filter** – Included in the Energize Updates subscription.
4. In the **Timeout [s]** field, enter the maximum duration of a URL category lookup.
5. Select the **Enable Custom Categories** check box.
6. In the **Categorization Policies** table, add (click **+**) or edit your URL filtering policy. For more details on the settings that you can configure for the policy, see Categorization Policy Settings.
7. To block requests that exceed the user limit of the URL Filter license, select the **Block If User Limit Exceeded** check box.
8. To block requests when the URL Filter service is down, select the **Block If Service Down** check box.
9. Click **Send Changes** and **Activate**.

Deny Message

To inform users that their URL request has been denied, you can either configure an HTML page locally or specify the URL of an external HTTP server that can display the deny message.

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > HTTP Proxy > Web Filter Config**.
2. In the left menu, select **Deny Message**.
3. Click **Lock**.
4. To configure an HTML page locally:
   1. From the **Notification Method** list, select **Message**.
   2. In the **Displayed Message Text** field, configure the HTML page. To display information about the denied request, use the $$MESSAGE$$ variable.
5. To specify the URL of an external HTTP server for the deny message:
   1. From the **Notification Method** list, select **URL**.

2. In the **Displayed URL** field, enter the URL of an external HTTP server capable of CGI that will display the deny page. In the URL of the message server, you must specify the server protocol and IP address. The port can be optionally specified. For example, `http://msgsrv.com:80`.
3. To append information about the denied request, select **Yes** from the **Append Deny Query** list.

6. Click **Send Changes** and **Activate**.

Exempt Users and IP Addresses

In the whitelist, you can add users or IP addresses that are exempt from filtering.

1. Go to **CONFIGURATION** > **Configuration Tree** > **Box** > **Virtual Servers** > ***your virtual server*** > **Assigned Services** > **HTTP Proxy** > **Web Filter Config**.
2. In the left menu, select **Whitelists**.
3. Click **Lock**.
4. In the **Whitelisted IPs** table, add whitelisted IP addresses.
5. In the **Whitelisted Users** table, add whitelisted users.
6. Click **Send Changes** and **Activate**.

Logging and Statistics

You can enable the logging of denied and/or allowed URL requests, and select the types of statistics data that should be generated for the HTTP Proxy URL filter.

1. Go to **CONFIGURATION** > **Configuration Tree** > **Box** > **Virtual Servers** > ***your virtual server*** > **Assigned Services** > **HTTP Proxy** > **Web Filter Config**.
2. Click **Lock**.
3. To configure logging:
   1. Select **Log Policy** in the left menu.
   2. To log denied URL requests, select the **Log Denied URLs** check box.
   3. To log allowed URL requests, select the **Log Allowed URLs** check box.
4. To configure statistics:
   1. Select **Statistics Policy** in the left menu.
   2. Select the check box of each statistics data type that should be generated.
5. Click **Send Changes** and **Activate**.

Additional Scanning with Third Party Software

For additional scanning with third party software products that are installed on the Barracuda NextGen Firewall F-Series (such as virus scanning), you can optionally cascade the redirector.

1. Go to **CONFIGURATION** > **Configuration Tree** > **Box** > **Virtual Servers** > ***your virtual server*** > **Assigned Services** > **HTTP Proxy** > **Web Filter Config**.
2. In the left menu, select **Cascaded Redirector**.
3. Click **Lock**.

4. To specify the cascaded redirector as the primary component in the scanning chain, select the **Cascaded is Primary** check box. The URL request will be routed through the additional scanner before it is routed through the URL Filter.
5. In the **Cascaded Redirector** field, enter the full path to the cascaded redirector in the Barracuda NextGen Firewall F-Series.
6. Click **Send Changes** and **Activate**.

Step 2. Activate the Web Filter

You can limit searches to use Google Safe Search. Google Safe Search is a third party content filtering solution to make using Google safe for children and users who do not want adult or explicit search results included. For more information, see Google Safety Tools .

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > HTTP Proxy > HTTP Proxy Settings**.
2. In the left menu, select **Web Filter**.
3. Click **Lock**.
4. From the **Enable Content Filtering** list, select **Yes**.
5. To activate **Google Safe Search** for the HTTP Proxy service, select the filtering level from the **Google Safe Search** list:
   - **Moderate** – Default setting. Excludes most explicit images from Google Images results but does not filter ordinary web search results.
   - **Strict** – Applies SafeSearch filtering to all search results (i.e. both image search and ordinary web search).
   - **Very Safe Search** – Strictest level for limiting search results and potential exposure to graphic content.
6. If you want to increase the number of simultaneously working redirectors for high traffic processing:
   1. Select **Switch to Advanced View** from the **Configuration Mode** menu.
   2. In the **Number of Redirectors** field, enter the number of simultaneously working redirectors (default: 5).

      If you change the default value for the **Number of Redirectors** setting, specify the same value for the **Max URL Filter Processes** setting for the URL Filter service.
7. Click **Send Changes** and **Activate**.

Configure Web Filter Authentication

1. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > Authentication Service**.
2. In the left menu, select **Webfilter Authentication**.
3. Click **Lock**.
4. From the **Activate Scheme** list, select **Yes** to start the authentication processes.
5. In the **Server Setting** table, add the settings for your web filter servers. For each entry:
   1. Specify the following settings:

- **IP Address** – The IP address of the web filter server.
- **Passphrase** – The password for the web filter server. (If you are using the Barracuda Web Filter, enter the **API Password** that is configured on the **BASIC > Administration** page of the Barracuda Web Filter.)
- **Sync Interval (s)** – The synchronization interval between your Barracuda NextGen Firewall F-Series and your web filter.

2. Click **OK**.

6. In the **Auto Logout After (d)** field, enter the timeout (in days).
7. If you want to enable extensive logging for maintenance purposes, select **Moderate** or **Full** from the **Debug Log** list.
8. From the **Filter Type** list, select the type of authentication that should be synced.
   If you change the default value for the **Number of Redirectors** setting, specify the same value for the **Max URL Filter Processes** setting for the URL Filter service.
9. Click **Send Changes** and **Activate**.

Display Blocked URL Categories Using an External HTTP Server

For URL filtering with the Barracuda NextGen Firewall F-Series and an external HTTP server, the server must act as Common Gateway Interface (CGI). The block web page on the external HTTP server must include a parameter to display the reason why the connection was blocked.

Parameters

You can use the following parameters:

category=[1-63], 99 – Indicates which URL categories caused the block (Category 99 indicates that a category was not found).

Other reasons include:

- **urlfd_not_running –** The URL Filter Daemon is not running.
- **urlfd_read_error –** Could not read from URL Filter Daemon.
- **no_more_memory –** Machine is running out of memory.
- **udp_not_received** – Could not receive an answer for the requested URL. Please try later.
- **filter_timeout –** Could not receive an answer for the requested URL. Please try later.
- **request_not_correct** – The proxy has sent an incorrect request.
- **black_list** – This site is on the BLACK LIST.
- **no_category –** This domain is in no category.
- **timestamp_not_active** – Sorry, but at this time the access is blocked.
- **user_limit_exeeded** – Sorry, but the URL Filter user limit exceeded.
- **user** – If applicable, the user that requested the blocked website.
- **peerip** – Client IP that requested the blocked website.

url=www.[url].com – The URL of the blocked page.

Examples

Example 1

Example 1 shows how a parameter line that is included in a custom block page can look. In the example, www.msgsrv.com is the external HTTP server displaying the customized block page:

```
www.msgsrv.com/block_page?filter_timeout&url=www.forbidden.com
www.msgsrv.com/block_page?categories=1,6,35& url=www.forbidden.com
```

Example 2

Example 2 shows how a blocked URL is displayed together with the user ID and IP address:

```
} [category] => 35,67 [urlfilter] => 1 [url] => www.gotomeeting.com [user] =>
jdoe [peerip] => 10.0.10.20 ) request_uri:
/?category=35,67&urlfilter=1&url=www.gotomeeting.com&user=jdoe&peerip=10.0.10
.20
```

Categorization Policy Settings

The following table provides more detailed descriptions for settings that you can configure for URL Filter Policies:

Section	Settings
Categorization Policy Configuration	• **Category Policy** – From this list, select *Whitelisting* or *Blacklisting* to specify if the categories that are added to this policy are allowed or blocked. • **Categories** – In this table, add the types of websites to be blocked or allowed. • **Exempted Categories** – In this table, add the types of websites that are exempt from the category policy.

Domain Exceptions Handling	• **Domain Whitelist** – In this table, add domains that are always granted access, notwithstanding the domain's categorization. Subdomains are not included into the list automatically; you must specify them explicitly instead. For each entry, specify the following settings: ◦ **Domain Whitelist** – The domain name or a term in the URL. (When entering the domain name, do not specify the protocol identifier. For example, enter *www.domain.com* instead of *http://www.domain.com/*) ◦ **Search String** – If the filter should search URLs for the name or term that is entered in the field, select this check box. • **Domain Blacklist** – In this table, add the names of domains that are always denied access, notwithstanding the domain's categorization. Subdomains are not included into the list automatically but must be specified explicitly instead. For each entry, specify the following settings: ◦ **Domain Blacklist** – The domain name or a term in the URL. (When entering the domain name, do not specify the protocol identifier. For example, enter *www.domain.com* instead of *http://www.domain.com/* .) ◦ **Search String** – If the filter should search URLs for the name or term that is entered in the field, select this check box.
Network and User Restrictions	• **Affected Networks** – In this table, add networks to which the category policy will be applied. To apply the category policy to all networks, leave this table blank. • **Affected Groups | Affected Users** – In these tables, add users and groups to which the category policy will be applied. To apply the category policy to all groups or users, leave these tables blank. Group and user names may contain space characters and are case-insensitive. The syntax of group and user names depends on the authentication method used: ◦ For MSNT or RSAACE, the **Affected Groups** settings do not apply because these authentication methods do not provide group names. ◦ RADIUS servers provide group names that must be entered exactly as they are provided. ◦ LDAP and MSAD provide distinguished names that must be entered exactly as they are provided. For example, *CN=Group,OU=Unit,DC=Company,DC=com*. If values have been specified for all three parameters in the **Network and User Restrictions** section, they will be linked with OR, and access to a requested URL will be granted or denied according to the default policy and on the basis of the first value applying.
Time Settings	• **Use Local Time** – To use the time settings of the system to determine when to apply time restrictions, select this check box. To explicitly specify a time zone, clear this check box. • **Time Zone** – From this list, you can select the time zone that is used to determine when to apply time settings. To select a time zone from this list, you must clear the **Use Local Time** check box. • **Time Settings** – To select days and times during which the URL filter should be activated or deactivated, click **Always** and then select the required times from the **Time Interval** window. By default, the category policy is always active. If time restrictions apply to a profile, the label of the **Always** button changes to **Restricted!**