

Creating Block and Accept Policies

<https://campus.barracuda.com/doc/36077742/>

This article discusses filtering options for blocking and allowing various kinds of web traffic. See also [Best Practices in Configuring Policy](#).

To create exceptions to block/accept policies by specific user, group, or time frame, see [Exception Policies](#). For a video of this article content, scroll to the end of the page.

Content filtering

Barracuda web security products employ a comprehensive database of frequently updated categories of website content types. Use the **BLOCK/ACCEPT > Content Filter** page to control user access to categories of websites that should be blocked, warned, monitored, or allowed based on content. When you block a category, you block all HTTP and HTTPS traffic to the associated URLs in that category.

For example, **http://mail.yahoo.com** is categorized as a web-based email site. If you want to block users from accessing their web-based email accounts, block the Web-based Email category.

See [Web Use Categories](#) for a listing and definition of content classification.

Safe Search

Safe Search mode prevents a web search engine from displaying objectionable thumbnail images in search results; only filtered thumbnails are displayed in the search results. To limit Safe Search to specific users, create an exception using the **BLOCK/ACCEPT > Exceptions** page. For details, see [How to Enable SafeSearch](#). The entries in this category include search engines which allow users to enable or disable Safe Search mode for image searches. If you enable Safe Search through the Barracuda Web Security Gateway, users cannot use the search engine settings to override this mode. If you only want to enable Safe Search for certain users, select **Disable** for each search engine listed in the table, or click the **All** link. On the **BLOCK/ACCEPT > Exceptions** page, create an **Enable** exception for the user or group of users for whom you want to enable Safe Search.

Important: Safe Search will not work if the search request is encrypted *unless* the Barracuda Web Security Gateway is configured to inspect or 'scan' SSL traffic. Google Safe Search requires SSL inspection as searches are encrypted. Using Google Safe Search requires enabling the **SSL Inspection** feature, which is available for the Barracuda Web Security Gateway 310 and higher.

See [Using SSL Inspection With the Barracuda Web Security Gateway](#) for details.

Make sure your Barracuda Web Security Gateway is running version 8.1.0.005 or higher before turning on SSL inspection.

Safe Browsing for Schools

- For educational institutions wishing to restrict YouTube access, the procedure to configure the Barracuda Web Security Gateway is detailed in [How to Restrict YouTube Content On Your Network](#). See also the Google article [Manage your YouTube settings](#).
- See [Temporary Access for Education](#) for how to give teachers and students temporary access to websites, for classroom research, that are typically blocked.

Application Filtering

Non Web-Based Applications

Use the **BLOCK/ACCEPT > Applications** page to block or allow specific application traffic over the HTTP (and HTTPS) protocol that is not browser-based. For example: Skype, Pandora, Adobe Acrobat, FTP. This type of filtering does NOT scan for content. If you need to scan and filter content, you must enable [SSL Inspection](#).

Note that the SSL Inspection feature is only available on the Barracuda Web Security Gateway 310 (limited) and higher, and requires more system resources and installation of SSL certificates to configure. The Barracuda Web Security Gateway 410 and higher is required to block/allow specific functions that run within web applications, such as Facebook games or Skype chat. Configure on the **BLOCK/ACCEPT > Web App Control** page.

For a user to download or use an application, the user's application needs to communicate with an external server. When you select to block an application, the Barracuda Web Security Gateway searches for traffic that contains data associated with an application server and then blocks that traffic.

Virtual Machine Support for Application Filtering and Monitoring

The Barracuda Web Security Gateway 610 Vx virtual machine and higher supports application filtering, social media monitoring, and suspicious keyword alerts.

Exceptions to policies can be created for a specific user or group based on bandwidth quotas, time of

day and/or days of the week. For example, you might want to allow employees to access certain applications such as Skype, for example, ONLY during lunch hours. See [Limiting Access by Time frames, Time Quotas and Bandwidth Quotas](#). You can use the applications filter as a pre-emptive measure to protect your network against malware.

Social Media and Other Web-Based Applications

From the **BLOCK/ACCEPT > Web App Control** page you can block or allow specific web-based application traffic. For example: Facebook, LinkedIn, MySpace, Twitter, and others. You can allow or block the entire application or only specific functions that run within these web applications. For example, you might allow Facebook, but want to block Facebook games and Facebook apps to protect against viruses and malware.

As another example, you may want to block the IRC application because this type of application can present a security risk to the network. An infected PC may communicate with the "hacker" through an IRC channel, and the hacker can send commands to the channel instructing bots to launch an attack. IRC could also be used by a disgruntled employee to launch attacks on other networks or to communicate sensitive information outside of the network.

You can also use the application blocking feature when you hear about a virus spreading over a specific IM service or tool. In this case, you can proactively protect your network from the infection by blocking that particular service until the threat has been resolved.

Web Application Monitoring

Use this feature to capture and archive chat, email, user registrations and other social media interactions. The archiving repository can be your Barracuda Message Archiver, your Microsoft Exchange Server journaling tool or, for example, a system administrator email address.

For example, you might want to allow users in the organization to use Facebook to view and make status updates and use chat, but you want to capture the content. You might also want to block games, shares and other Facebook apps to protect your network from viruses and malware.

To configure Web Application Monitoring, you'll want to first set up your block/accept policies for web-based applications. Here's the process for this example:

1. From the **BLOCK/ACCEPT > Web App Control** page, in the Application Navigator, check Facebook to allow some or all Facebook applications.
2. Select the *Facebook* actions to block and allow and save your changes. In this example, you'd leave chat and status update in the **Allowed Applications** list, moving other applications you want to block, such as shares, games and other apps, to the **Blocked Applications** list. Save your changes.
3. From the **BLOCK/ACCEPT > Web App. Monitor** page, enable the application actions whose content you want to archive. In this example, you would enable *Facebook Wall Posts, Chat*

Message and *Private Message*. Once you enable any actions on the page, the Barracuda Web Security Gateway will capture the content from each action, package it as an SMTP message and email it to the **Notification Email Address** you specify.

Domain filtering

Use the **BLOCK/ACCEPT > Domains** page to block list (block), warn, monitor or allow list (allow) traffic to specific domains and subdomains. Use domain Allow Lists to allow access to domains that belong to categories that are generally blocked. Note that domains that are on your Allow List ARE subject to the MIME type blocking rules you create (see below). Use domain Block Lists to restrict access to domains in addition to those specified in other filtering categories.

Tip

To control access to a domain and all its associated URLs, make sure you enter the domain identifier. For example, **www.example.com** will control access only to the specific URL but example.com will control access to all URLs under the domain.

URL pattern filtering

Use the **BLOCK/ACCEPT > URL Patterns** page to enter regular expressions or keywords that, if matched to a URL, will block, warn, monitor, or allow that URL. For more information about using regular expressions, refer to [Regular Expressions](#). Note that URLs that are on your Allow List ARE subject to the MIME type blocking rules you create (see below).

Tip

Run a test on your regular expressions with special characters before you encode them in a pattern filter.

Examples:

Example 1 - Block all of Facebook except for ONE particular page.

1. Configure SSL Inspection on the Barracuda Web Security Gateway. See the **ADVANCED > SSL Inspection** page.
2. Go to the **BLOCK/ACCEPT > Web App Control** page and block Facebook as follows:
 1. Check *Social Media* under **Allowed Applications**.
 2. In the drop-down below that box, select *Facebook all functions*.

3. Click the **Block** button on the right side of the page.
4. Click **Save**.
3. Go to the **BLOCK/ACCEPT > Exceptions** page. Create an exception as follows:
 1. Select *Allow* for the **Action**.
 2. Select the appropriate group for **AppliesTo**.
 3. Select *URL Patterns* for **Exception Type**.
 4. In the **URL Pattern** field, paste the Facebook page URL you want to ALLOW. For example: **https://www.facebook.com/thenameofyourpage.html**
 5. Configure other Exception rules as desired, such as Time Frame (to Allow), etc.
 6. Click **Add**.

Example 2 - Block all websites that contain "porn" in the URL

1. Go to the **BLOCK/ACCEPT > Exceptions** page. Create an exception as follows:
 1. Select *Block* for the **Action**.
 2. Select the appropriate group for **AppliesTo**.
 3. Select *URL Patterns* for **Exception Type**.
 4. In the **URL Pattern** field, enter **porn**
 5. Configure other Exception rules as desired, such as Time Frame (to Allow), etc.
 6. Click **Add**.

Sometimes spyware applications use different hostnames but the same domain name, so the URLs appear to be from different hosts. In this case you can enter the domain name as a pattern to block all URLs on that domain.

Example 3 - Allow access to *example.com* but block *maps.example.com*

Follow instructions in the above examples to create an Exception. In this case, specify *example.com* as an *Allowed* URL pattern and specify *maps.example.com* as a *Blocked* URL pattern.

Exceptions for Domains

On the **BLOCK/ACCEPT > Exceptions** page, when you select the **Exception Type** as *Domain*, note that you can only specify **one** domain per exception. If you want to create exceptions for more than one domain, you must create a separate exception for each one.

Custom categories filtering

Use the **BLOCK/ACCEPT > Custom Categories** page to create a custom filter, which can consist of the domain names or built-in web content categories you select. Custom categories are used in the same way as the built-in filters:

- You can apply a custom category to either authenticated or unauthenticated users.
- You can define a user- or group- specific exception rule to a custom category policy.

After you define a custom category, allow between five and ten minutes for the Barracuda Web Security Gateway to compile and then fully activate the new category. To verify that a newly created custom category is active, you can use the **Content Filter Lookup** facility in the **BLOCK/ACCEPT >Content Filter** page, as described in the online help for the **BLOCK/ACCEPT > Custom Categories** page.

MIME type blocking

Use the **BLOCK/ACCEPT > MIME Blocking** page to specify standard MIME types that you want to block. Note that websites that are on your Allow List ARE subject to the MIME type blocking rules you create. Many organizations choose to block Internet radio and streaming media because they add load to the internal network, as well as executable files because they can install viruses and various other malware. Some examples of MIME Type blocking:

- To block Internet radio, which uses MPEG (.mpg, mpeg, or .abs) or Microsoft audio (.wav) files, enter **audio/x-mpeg** or **audio/x-wav** as blocked MIME types.
- To block streaming media, which uses MPEG video, enter **video/mpeg** or **video/x-msvideo** as blocked MIME types.
- To block access to executables (.exe), enter **application/octet-stream** as a blocked MIME type.

For more examples of MIME types, click **Help** on the **BLOCK/ACCEPT > MIME Blocking** page.

Exceptions for MIME types

On the **BLOCK/ACCEPT > Exceptions** page, when you select the **Exception Type** as *MIME Type*, note that you can only specify **one** MIME Type per exception. If you want to create exceptions for more than one MIME type, you must create a separate exception for each type.

IP-based exemption

If you want to exempt certain clients or sub-networks from all filtering (including spyware filtering), you can use the **BLOCK/ACCEPT > IP Block/Exempt** page and specify the source IP address for those clients under IP and Port Exemptions. For example, if you want to exempt an executive's client machine from all filtering, you can do so using the IP address of the client. Similarly, if you want to exempt certain external devices (such as trusted servers outside the protected network), from all

filtering, you can specify the destination IP address and specific port under **IP and Port Exemptions**.

Exempted IP addresses will bypass the following block filters:

- Content filtering
- IM blocking
- All types of download blocking

Exempted IP Addresses will bypass ALL filters including spyware and virus filters.

IP-based blocking

To block *ALL* IP-based URLs, set **Block IP Based URLs** to Yes on the **BLOCK/ACCEPT > URL Patterns** page. The default and recommended value for this setting is *No*.

If you want to block certain clients or sub-networks from all access, you can use the **BLOCK/ACCEPT > IP Block/Exempt** page and specify the source IP address for those clients under **IP and Port Exemptions**. For example, if you want to block traffic from a suspicious client machine or email servers or internal web servers, you can do so using the IP address of the client. Similarly, if you want to block certain external devices, you can specify the destination IP address and specific port under **IP and Port Exemptions**. Note that when the Barracuda Web Security Gateway is deployed as a forward proxy, IP block/accept rules based on request destination are not applied.

This video describes how to block or exempt traffic by IP address in the Barracuda Web Security Gateway.



© Barracuda Networks Inc., 2022 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.