

BLOCK/ACCEPT Order of Precedence - Barracuda Web Security Gateway

<https://campus.barracuda.com/doc/6160461/>

The **BLOCK/ACCEPT** pages in the Barracuda Web Security Gateway web interface provide a wide range of filters that enhance the default spyware and virus detection capabilities of the Barracuda Web Security Gateway. **Note that application filtering is supported by the Barracuda Web Security Gateway appliance but not by the Barracuda Web Security Gateway Vx virtual machine.** See also [Best Practices in Configuring Policy](#) for guidelines on planning and creating your Block/Accept rules, and [Creating Block and Accept Policies](#) for details on filters available.

Order of Precedence of Block/Accept Rules

The Barracuda Web Security Gateway will recognize specific types of block and accept rules in the order they are listed below (from top to bottom). If conflicting rules are created, the rule listed first will be honored. *Allow* rules take precedence over *Block* rules of the same type.

Block/Allow Rule Order of Precedence

The different rules, configured mostly configured under the **BLOCK/ACCEPT** tab, are applied in this order:

1. **BLOCK/ACCEPT> IP Block/Exempt** - Use this section to exempt traffic from all filtering - including spyware filtering - based on IP address criteria. You can exempt certain ports, portions of your network, or external application servers.
2. **BLOCK/ACCEPT > Exceptions:** Applications - Use the **Exceptions** page to manage policy exceptions for specific users or groups. An exception rule grants selected users - local users or groups, domain users or groups, or all users (authenticated or unauthenticated) - exceptions to a Barracuda Web Security Gateway policy for a specific period of time.
3. **BLOCK/ACCEPT> Applications** - Available for Inline deployments only. Use this feature to block or allow specific application traffic. You can select from a pre-defined list of non-HTTP web applications including IM clients, media programs, common PC tools, software updates, and peer-to-peer software. Additionally, *some* applications you select on the **BLOCK/ACCEPT > Web App Control** page, and which communicate over the HTTP/HTTPS protocols, are included in this order of precedence.
4. **Advanced > Temporary Allow List** - This applies to websites which administrators or teachers request to allow for access by students, employees, etc. for a temporary time period, as specified with the [Temporary Access](#) tool.
5. **BLOCK/ACCEPT> Exceptions:** All Web Traffic, URL Pattern, Domains, Category, Web

Application Control

6. **BLOCK/ACCEPT>Mime Type** - Use the MIME Type Blocking page to add standard MIME types to your Block List. You can create a MIME type block list for either unauthenticated or authenticated users. These rules are useful when content is not easily blocked by other methods.

Note the mime type blocking only applies to HTTP responses, and therefore will not be observed for requests that are blocked due to other rules, including category-based content filtering.
7. **BLOCK/ACCEPT>Web Application Control** (*most*) applications; i.e. social media, file sharing, Dropbox, Skype, Google Consumer Apps, etc.
8. **BLOCK/ACCEPT >Domains**, URL Pattern Allowed - Use these pages to specify *Allowed* domains or URL patterns.
9. **BLOCK/ACCEPT >Domains**, URL Pattern Blocked - Use these pages to specify domains or URL patterns. that should be *Blocked*. This blocking filter operates in addition to those defined in other filtering categories.
10. **BLOCK/ACCEPT > Content Filter** - Use the **Content Filter** page to manage your users' Internet access based on the website content being requested. You can apply content category filters to either unauthenticated or authenticated users.

Barracuda Networks does not recommend using IP block/exempt rules for blocking traffic to websites or for specific applications. IP block/exempt rules are generally used to control access to and from particular client computers or external web servers (such as email servers or update servers). However, you can use this feature to control access by specifying destination IP/port combinations. **These rules have precedence over all other block/accept rules.**

© 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.