

URL Filtering in the Firewall

<https://campus.barracuda.com/doc/72516526/>

The firewall offers real-time URL filtering for web and application traffic. URL filtering is handled as part of the application policy. In combination with Application Control, URL filtering can also be enabled on a per-access-rule basis. To use URL filtering, you must have a Barracuda Web Security Subscription.

URL Filter Policies

URL Filter policies define access restrictions for URL categories. To restrict or allow access to specific URL categories and/or websites, create URL policy objects. When applied to an application policy, the URL policy object defines how the application policy handles user access to websites based on the URL Filter policy. When configuring a URL policy object, assign a policy for every URL category with the option of including custom URL block and allow lists. The following actions are available for each URL category:

- **Allow** – Allows access to all URLs defined in the category.
- **Warn** – Users are redirected to a warning page and must click **Continue** to access the website. Set **Warn and Continue override** to configure the timeout after which the user is redirected to the warning page again.
- **Alert** – Users are allowed to access websites in this category, but the action is silently logged. Go to **BASIC > Application Monitor** to see the websites that trigger the alert action.
- **Override** – Users are redirected to the URL Filter Override page and can request temporary access from an administrator to a URL from a denied category.
- **Block** – Blocks access to all URLs defined in the category .

For more information, see [How to Create a URL Filter Policy Object](#).

Configure URL Filtering

To configure URL filtering, apply URL policy objects to application policies. A URL policy object defines the action to be performed by the firewall when your users connect to a website and the application policy applies. The firewall sends the visited URL to a large online database for URL categorization and then performs the action specified in the URL policy object. To use application policies with URL policy objects for web and application traffic, you must also enable URL filtering separately in the matching access rule.

For more information, see [How to Configure URL Filtering in the Firewall](#).

Configure URL Filter Overrides

If the action for the detected URL category is set to override in the URL Filter policy object, the user can request permission for a URL category override. A URL Filter override admin must grant the request and set the duration of the override request. Override requests are granted per URL category.

For more information, see [How to Configure URL Filter Overrides](#).

© Barracuda Networks Inc., 2020 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.