RUTX10 Web Filter

The information in this page is updated in accordance with firmware version **RUTX_R_00.07.06.10**.

□

Contents

- 1 Summary
- 2 Site Blocking
- 3 Proxy Based Content Blocker
- 4 Troubleshooting

Summary

The **Web Filter** service provides you with the possibility to set up lists of wanted or unwanted websites (Blacklists or Whitelists). This chapter is an overview of the Cloud Solutions section for RUTX10 devices.

If you're having trouble finding this page or some of the parameters described here on your device's WebUI, you should **turn on "Advanced WebUI" mode**. You can do that by clicking the "Advanced" button, located at the top of the WebUI.

Site Blocking

The **Site Blocking** service provides you with the possibility to create a Blacklist or Whitelist that filters out which websites a user on the local network can access.

The figure below is an example of the Site Blocking page and the table below provides information on the fields contained in that page:

Field	Value	Description
Enable	off | on; default: **off**	Turns Site Blocking on or off.
Mode	Whitelist | Blacklist; default: **Whitelist**	Mode of operation. • **Whitelist** - allow every site included in the list and block everything else. • **Blacklist** - block every site included in the list and allow everything else.

Network	All LAN interfaces, Hotspot (where supported); default: All LAN interfaces	Network for which the site blocking service is activated. Can be enabled for custom LAN interfaces.
Hosts list	text file; default: **none**	Provides a possibility to upload a text file containing a list of hosts instead of adding hosts individually via the WebUI. Different hosts must be separated by line breaks (one host per line) in the text file.
Hostname	host; default: **none**	Website name. The formats accepted are either *www.website.com* or *website.com*, i.e., the protocol and subdomains can't be specified. The rules will also be applicable for the subdomains of the specified site.
off/on	off | on; default: **on**	Turns an entry of the list to an active or inactive state. Inactive entries are not considered to be a part of the list until they are activated.

Proxy Based Content Blocker

Proxy Based Content Blocker works in a similar manner to Site Blocking, except with Content Blocker you have the ability to filter out content with more versatility by using the **asterisk** (*) symbol instead of different extensions and phrases.

For example, instead of having to block multiple domains like *website.com*, *website.net*, *website.org* you can simply create an entry called *website.**, which would block all websites whose names begin with *website.*

Note: Proxy Based Content Blocker cannot be used to block HTTPS websites. For HTTPS, use Site Blocking instead.

The figure below is an example of the Proxy Based Content Blocker page and the table below provides information on the fields contained in that page:

Field	Value	Description
Enable	off | on; default: **off**	Turns Proxy Based Content Blocker on or off.
Mode	Blacklist | Whitelist; default: **Blacklist**	Mode of operation. • **Whitelist** - allow every site included in the list and block everything else. • **Blacklist** - block every site included in the list and allow everything else.
URL content	host; default: **none**	Website name or part of a website's name. The asterisk (*) symbol stands for anything so it can be used to block different variations of one website. For example: • The entry '*website.**' would block: - website.**com** - website.**net** - website.**org** - etc.

Troubleshooting

Users often find that the Web Filter service doesn't seem to function as expected. In most cases the issue lies not with the functionality of Web Filter itself. Here are some steps to ensure you are using/testing Web Filter correctly (applies to both "Site Blocking" and "Proxy Base URL Content Blocker"):

- **Reload your browser**. After adding new hostnames to the list, make sure you re-launch your web browser. Web browsers cache previously accessed information so the reason why some sites added to the list don't filter out properly is because the content of those sites had been downloaded and cached prior.
  Or you can test immediately after adding new entries to the list with your web browser's non-caching mode. For example, Google Chrome's "Incognito" mode (**Ctrl + Shift + N**) or Mozilla Firefox's "Private" mode (**Ctrl + Shift + P**).
- **Multiple network interfaces**. If your PC has multiple sources for Internet connectivity, make sure it uses the router as its default Internet gateway.
- **Multiple domains**. Popular sites like Google, Youtube, Facebook, etc. often use multiple domain names. Therefore, sometimes it may be necessary to block more than one domain in order to successfully block a single website.
- **Mobile websites**. If you're testing Web Filter via a mobile phone, keep in mind that by default mobile devices connect to mobile versions of websites (that usually have names beginning with **m.**) when they are available. Therefore, it is necessary to also add the mobile hostname as well as the regular one.
- **Grammar mistakes**. Make sure you have entered the desired hostnames correctly. Often sites aren't blocked because of simple grammar mistakes like typing **.comm** instead of*.com*, **ww.** instead of *www.* or other general misspellings. If a site is not being blocked properly, check that entry in the Web Filter list.