

Content Filtering Configuration on the RV315W VPN Router

Objective

Content filtering configuration allows an administrator to block unwanted websites. Content filtering can block access to websites based on URLs and keywords.

This article explains how to configure Content Filtering on the RV315W VPN Router.

Applicable Device

- RV315W

Software Version

- v1.01.03

Content Filtering Configuration

Step 1. Log in to the web configuration utility and choose **Security > Content Filtering**. The *Content Filtering* page opens:

Content Filtering

Filter Type: Blacklist: Block HTTP access to websites in the blacklist and allow HTTP access for other websites. Whitelist: Allow HTTP access to websites in the whitelist and block HTTP access for other websites. Save Cancel

Add Content Filtering Rule

URL/Keyword: (1-32 characters, such as www.w3.org)
File Type: Add

Content Filtering Rules

Type	Value
Blacklist	www.example.com
Blacklist	Text File (.bt)

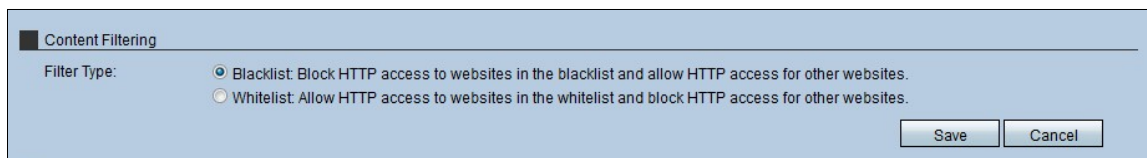
Select All Cancel All Delete Export

Import Content Filtering Rules

Locate and select a file to import: Browse Import

Content Filtering

The Content Filtering section allows the administrator to choose the parameters under which the host works in the network in term of access to the webpages.



Step 1. Click the radio button for the type of *Filter Type* that the hosts will use. There are two types of filters:

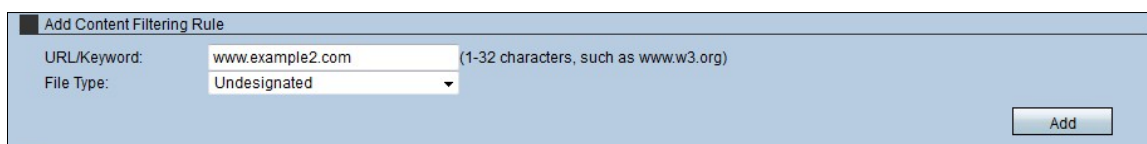
- Block list — Denies HTTP access to websites on the block list and allows HTTP access to other websites.
- Allow list — Allows HTTP access to websites on the allow list and blocks HTTP access to other websites.

[See glossary for additional information.](#)

Step 2. Click **Save** to save the settings.

Add Content Filtering Rule

Step 1. In the *URL/Keyword* field, enter the URL or Keyword that applies to the rule. Any website URL that matches the URL or contains the keyword is blocked or allowed.



Step 2. From the *File Type* drop-down list, choose the type of file that the device has to filter.

- Undesignated— Allows or denies the access or download of undesignated files when the user accesses a web site that contains them.
- Text File (.txt) — Allows or denies the access or download of text files when the user accesses a web site that contains them.
- Word File (.doc/.docx) — Allows or denies the access or download of word files (.doc/.docx) when the user accesses a web site that contain them.
- Excel File (.xls/xlsx) — Allows or denies the access or download of excel files (.doc/.docx) when the user accesses a web site that contains them.
- PDF File — Allows or denies the access or download of word files (.xls/xlsx) when the user accesses a web site that contains them.
- Picture File (.jpg/.bmp/.gif/.png) — Allows or denies the access or download of picture files (.jpg/.bmp/.gif/.png) when the user accesses a web site that contains them.
- Other File — Allows or denies the access or download of other files when the user accesses a web site that contains them. These other files could be files of a different office program or platform.

Step 3. Click **Add** to add the filters. This information will be displayed in the Content Filtering Rules Table.

Content Filtering Rules

The content filtering rules table allows the administrator to perform actions on the existing rules.



The screenshot shows a web interface titled "Content Filtering Rules". It features a table with two columns: "Type" and "Value". The table contains two rows of data, each enclosed in a dashed box. The first row shows a "Blacklist" type with the value "www.example.com" under the "URL/Keyword" header. The second row shows a "Blacklist" type with the value "Text File (.txt)" under the "File Type" header. Below the table, there are four buttons: "Select All", "Cancel All", "Delete", and "Export".

Type	Value
Blacklist	www.example.com
Blacklist	Text File (.txt)

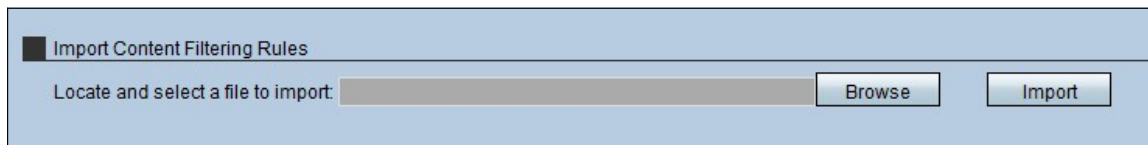
Step 1. To delete all the rules on the RV315W, click **Select All** and click **Delete**.

Step 2. To cancel all the rules on the RV315W, click **Cancel All**.

Step 3. To export all the rules to a local PC from the RV315W, click **Select All** and then **Export**.

Import Content Filtering Rules

The Import Content filtering rules area allows the administrator to import existing rules of other devices to the RV315W.



The screenshot shows a web interface titled "Import Content Filtering Rules". It features a text input field with the placeholder text "Locate and select a file to import:". To the right of the input field are two buttons: "Browse" and "Import".

Step 1. Click **Browse** to search for the rule file.

Step 2. Choose the file and click **Import** to import the rules from another device (PC) to the RV315W.