

RV315W VPNルータでのコンテンツフィルタリングの設定

目的

コンテンツフィルタリングの設定により、管理者は不要なWebサイトをブロックできます。コンテンツフィルタリングは、URLおよびキーワードに基づいてWebサイトへのアクセスをブロックできます。

この記事では、RV315W VPNルータでのコンテンツフィルタリングの設定方法について説明します。

該当するデバイス

- ・ RV315W

[Software Version]

- ・ v1.01.03

コンテンツフィルタリングの設定

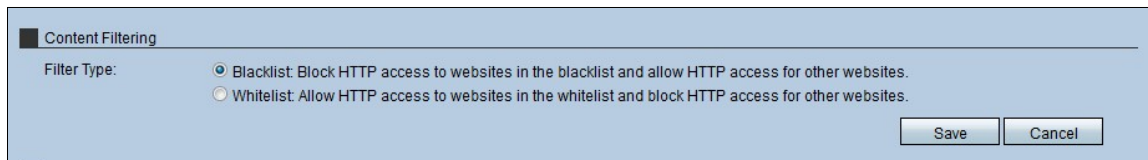
ステップ1: Web構成ユーティリティにログインし、[Security] > [Content Filtering]を選択します。[コンテンツフィルタリング]ページが開きます。

The screenshot shows the 'Content Filtering' configuration page. It includes sections for 'Filter Type' (Blacklist/Whitelist), 'Add Content Filtering Rule' (with fields for URL/Keyword and File Type), 'Content Filtering Rules' (a table listing rules), and 'Import Content Filtering Rules' (with a file selection field).

Type	Value
Blacklist	www.example2.com
Blacklist	Text File (.bt)

コンテンツのフィルタリング

[コンテンツフィルタリング(Content Filtering)]セクションでは、管理者がWebページへのアクセスの観点から、ネットワーク内でホストが動作するパラメータを選択できます。



The dialog box titled "Content Filtering" has a "Filter Type:" label. It contains two radio button options: "Blacklist: Block HTTP access to websites in the blacklist and allow HTTP access for other websites." (which is selected) and "Whitelist: Allow HTTP access to websites in the whitelist and block HTTP access for other websites." At the bottom right, there are "Save" and "Cancel" buttons.

ステップ1: ホストが使用するフィルタの種類ラジオボタンをクリックします。フィルタには2つのタイプがあります。

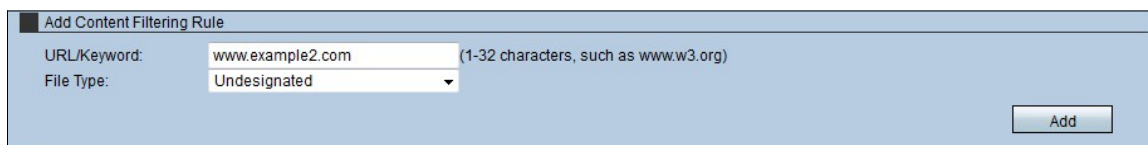
- ・ ブロックリスト: ブロックリスト上のWebサイトへのHTTPアクセスを拒否し、他のWebサイトへのHTTPアクセスを許可します。
- ・ 許可リスト: 許可リストのWebサイトへのHTTPアクセスを許可し、他のWebサイトへのHTTPアクセスをブロックします。

[詳細については、用語集を参照してください。](#)

ステップ2:[Save(保存)]をクリックして設定を保存します。

コンテンツフィルタリングルールの追加

ステップ1:[URL/キーワード(URL/Keyword)]フィールドに、ルールに適用するURLまたはキーワードを入力します。URLに一致するか、キーワードを含むWebサイトのURLはすべてブロックまたは許可されます。



The dialog box titled "Add Content Filtering Rule" has two input fields. The first is "URL/Keyword:" with the value "www.example2.com" and a note "(1-32 characters, such as www.w3.org)". The second is "File Type:" with a dropdown menu showing "Undesignated". An "Add" button is located at the bottom right.

ステップ2:[ファイルの種類]ドロップダウンリストから、デバイスがフィルタするファイルの種類を選択します。

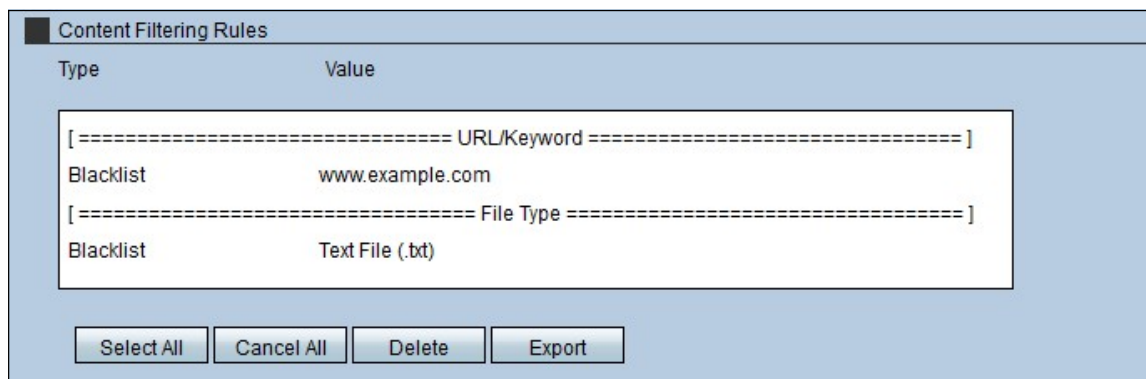
- ・ Undesignated – ユーザーがファイルを含むWebサイトにアクセスした場合に、未指定ファイルのアクセスまたはダウンロードを許可または拒否します。
- ・ テキストファイル(.txt) : テキストファイルを含むWebサイトにユーザーがアクセスした場合に、テキストファイルのアクセスまたはダウンロードを許可または拒否します。
- ・ Wordファイル(.doc/.docx) : ユーザーがWordファイル(.doc/.docx)を含むWebサイトにアクセスするときに、Wordファイル(.doc/.docx)のアクセスまたはダウンロードを許可または拒否します。
- ・ Excelファイル(.xls/xlsx) : ユーザーがExcelファイル(.doc/.docx)を含むWebサイトにアクセスするときに、Excelファイル(.xls/xlsx)へのアクセスまたはダウンロードを許可または拒否します。
- ・ PDFファイル : ユーザーがWordファイルを含むWebサイトにアクセスした場合に、Wordファイル(.xls/xlsx)へのアクセスまたはダウンロードを許可または拒否します。
- ・ 画像ファイル(.jpg/.bmp/.gif/.png) : ユーザーが画像ファイルを含むWebサイトにアクセスする場合に、画像ファイル(.jpg/.bmp/.gif/.png)のアクセスまたはダウンロードを許可または拒否します。
- ・ その他のファイル : ユーザーがファイルを含むWebサイトにアクセスするときに、他のファイルのアクセスまたはダウンロードを許可または拒否します。これらの他のファイルは

、別のオフィスプログラムまたはプラットフォームのファイルである可能性があります。

ステップ3:[Add]をクリックして、フィルタを追加します。この情報は、コンテンツフィルタリングルールテーブルに表示されます。

コンテンツフィルタリングルール

コンテンツフィルタリングルールテーブルを使用すると、管理者は既存のルールに対してアクションを実行できます。



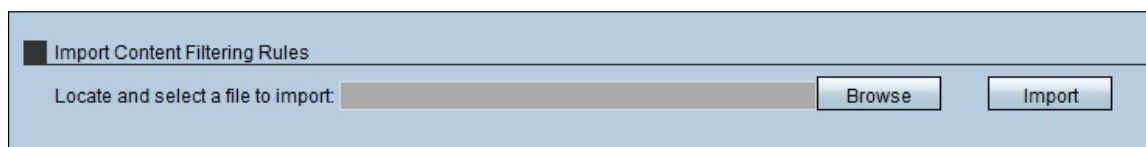
ステップ1:RV315Wのすべてのルールを削除するには、[すべて選択(Select All)]をクリックし、[削除(Delete)]をクリックします。

ステップ2:RV315Wのすべてのルールをキャンセルするには、[すべてキャンセル]をクリックします。

ステップ3：すべてのルールをRV315WからローカルPCにエクスポートするには、[すべて選択(Select All)]をクリックし、次に[エクスポート(Export)]をクリックします。

コンテンツフィルタリングルールのインポート

[Import Content filtering rules]領域では、管理者が他のデバイスの既存のルールをRV315Wにインポートできます。



ステップ1:[参照]をクリックして規則ファイルを検索します。

ステップ2：ファイルを選択し、[Import]をクリックして、別のデバイス(PC)からRV315Wにルールをインポートします。