Content Filter

Setting up content filtering and troubleshooting.

Content filtering on the SafeUTM server is implemented based on web traffic data received from the web traffic proxying module. Thus, the content filter allows you to efficiently block access to various internet resources.

The mechanism of content filtering consists in checking the affiliation of the address requested by a website or website page user and its presence in prohibited resource lists. The lists in their turn are divided into categories for easier administration.

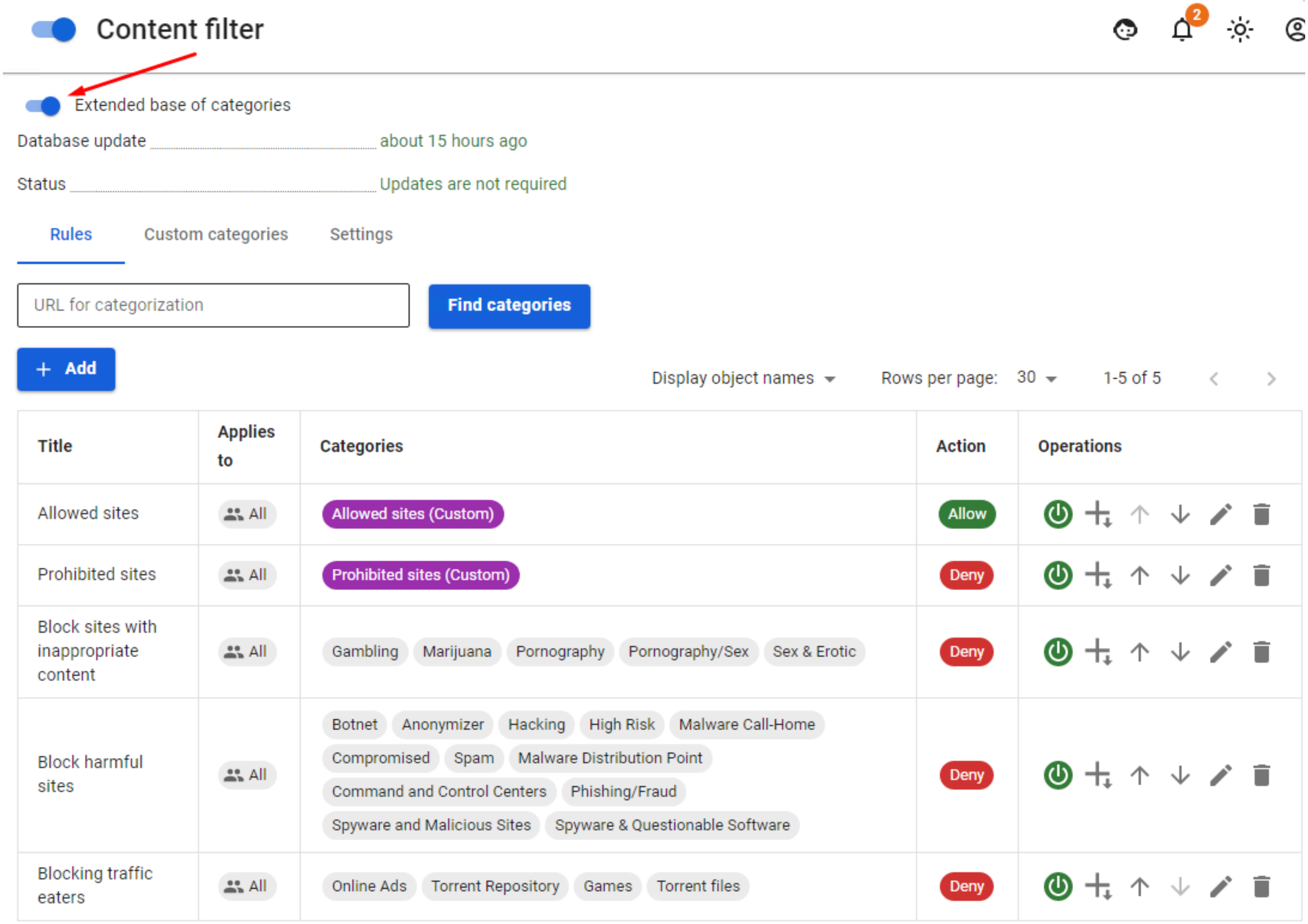
> The content filtering module only works with an active subscription to updates in the Enterprise edition.

> HTTPS sites without traffic decryption are filtered by domain only (not by full URL), **Files** category rules cannot be applied to them either. Create rules for decrypting HTTPS traffic of necessary categories in order to fully filter HTTPS.

Content filter settings and categories

Content Filtering Setup

Go to **Traffic Rules -> Content Filter** and activate the extended content filter database by switching the slide to **Enabled** next to **Extended base of categories**.



Extended base of categories

Database update .... about 15 hours ago

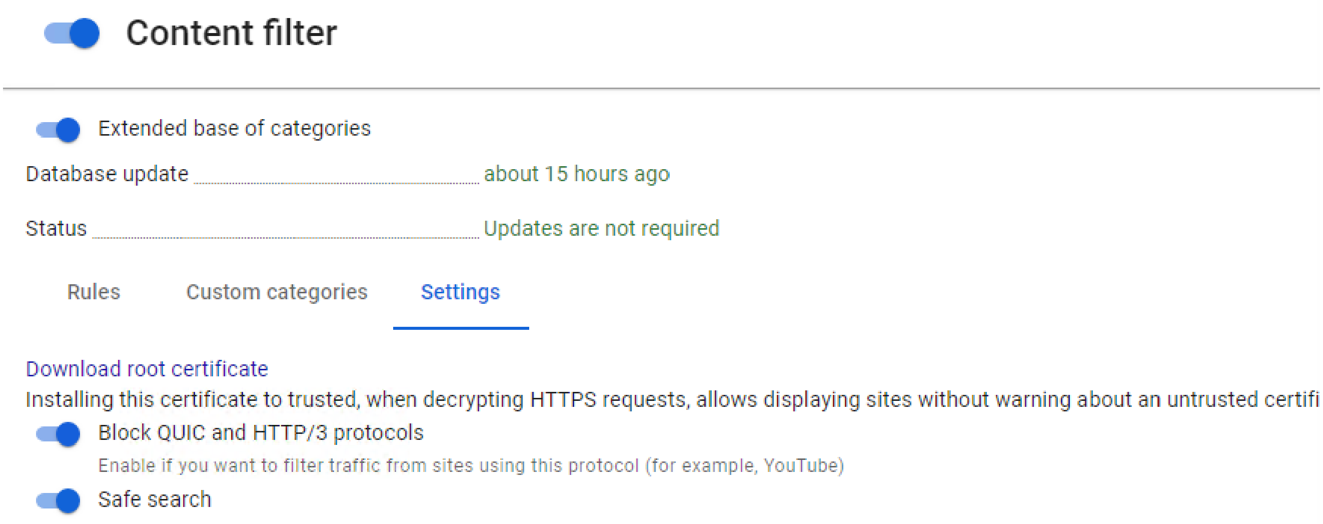
Status .... Updates are not required

Rows per page: 30 1-5 of 5

Title	Applies to	Categories	Action	Operations
Allowed sites	All	Allowed sites (Custom)	Allow	
Prohibited sites	All	Prohibited sites (Custom)	Deny	
Block sites with inappropriate content	All	Gambling Marijuana Pornography Pornography/Sex Sex & Erotic	Deny	
Block harmful sites	All	Botnet Anonymizer Hacking High Risk Malware Call-Home Compromised Spam Malware Distribution Point Command and Control Centers Phishing/Fraud Spyware and Malicious Sites Spyware & Questionable Software	Deny	
Blocking traffic eaters	All	Online Ads Torrent Repository Games Torrent files	Deny	

You can configure additional filtering options in the **Settings** tab:

- **Block QUIC and HTTP/3 protocols.** An experimental protocol used by Chrome browser for access to some resources (e.g. YouTube). It is recommended to be blocked as filtering of resources working under this protocol will not be possible otherwise.
- **Safe search.** Forcibly enables safe search in search engines (Google, Yandex, YouTube, Yahoo, Bing). **In order for this function to work, you need to enable HTTPS filtering by certificate substitution for these resources**.



Content filter

Extended base of categories

Database update .... about 15 hours ago

Status .... Updates are not required

Download root certificate

Installing this certificate to trusted, when decrypting HTTPS requests, allows displaying sites without warning about an untrusted certifi

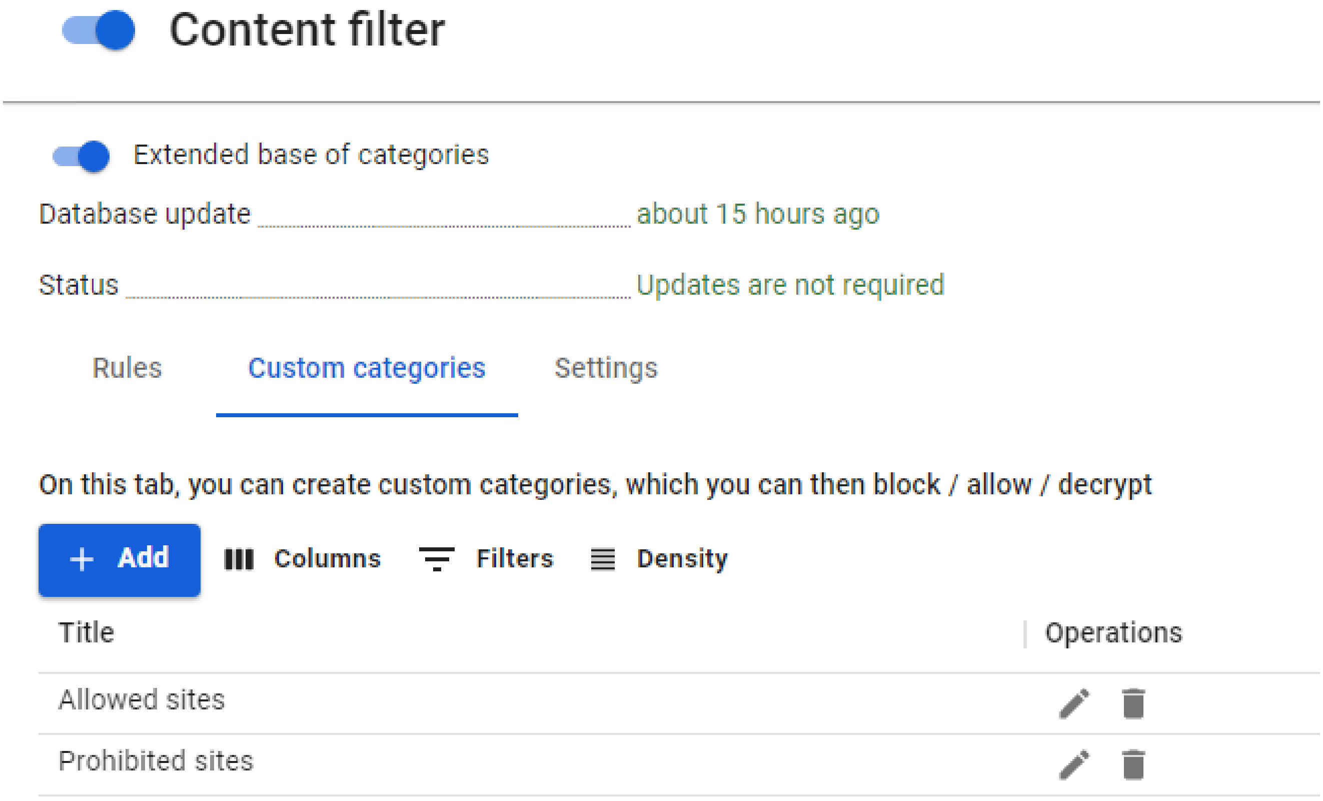
Block QUIC and HTTP/3 protocols

Enable if you want to filter traffic from sites using this protocol (for example, YouTube)

Safe search

Content Filtering Categories

- **Extended base of categories**. Over 140 categories including millions of URLs automatically updated by the server. The status of updates and database usage can be viewed in the **Settings** tab in the Content Filtering section. These categories only work with an active subscription to updates in commercial editions.
- **Custom categories**. You can create your own rules in the tab with the same name.



Content filter

Extended base of categories

Database update .... about 15 hours ago

Status .... Updates are not required

On this tab, you can create custom categories, which you can then block / allow / decrypt

Title	Operations
Allowed sites	✎ 🗑
Prohibited sites	✎ 🗑

- **Special**. Includes four categories – all queries, all categorized queries, all non-categorized queries, and queries with direct access by IP addresses.

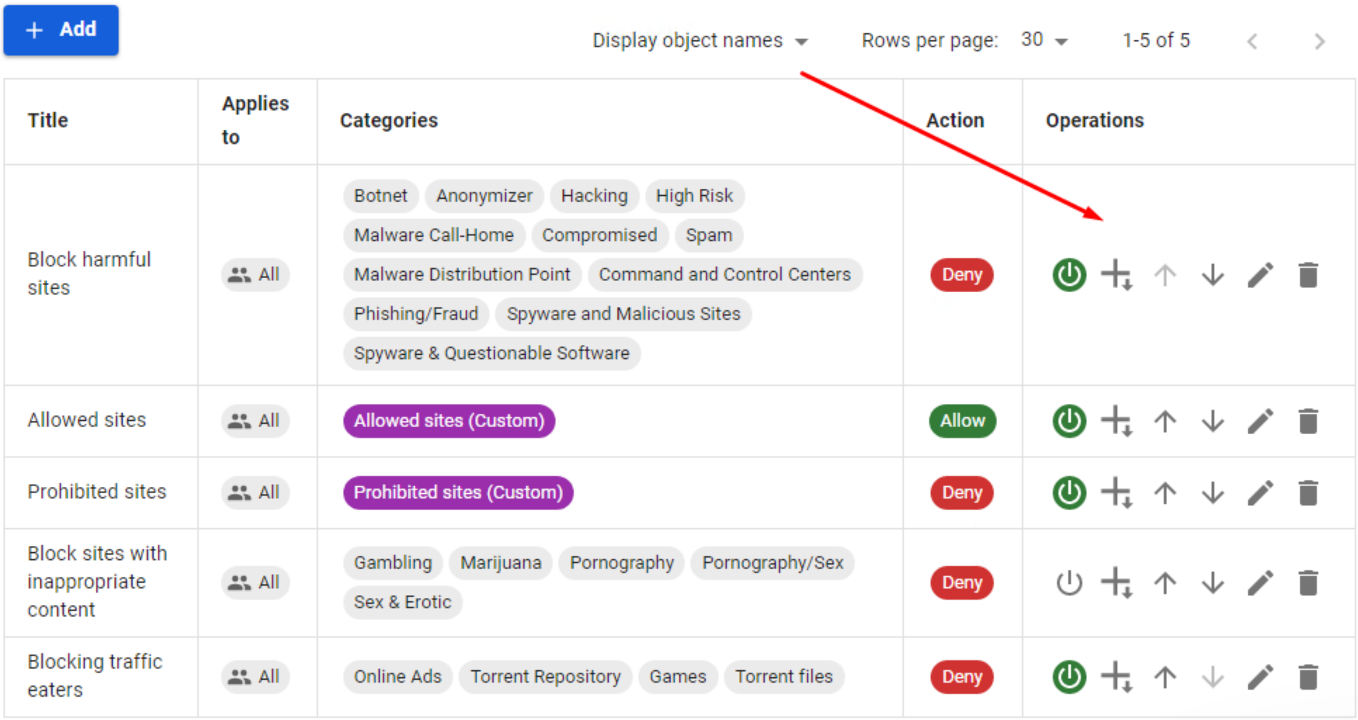
- **Files**. Eight defined categories of files blocked by extension and MIME type. Preset file groups (Executable Files, Archives, Video Files, Audio Files, Flash video, Active-X, Torrent files, and Documents) cannot be edited. Filtering HTTPS traffic for these types of categories is only possible when it is decrypted.

Applying Filtering

Applying Filtering Rules to Users

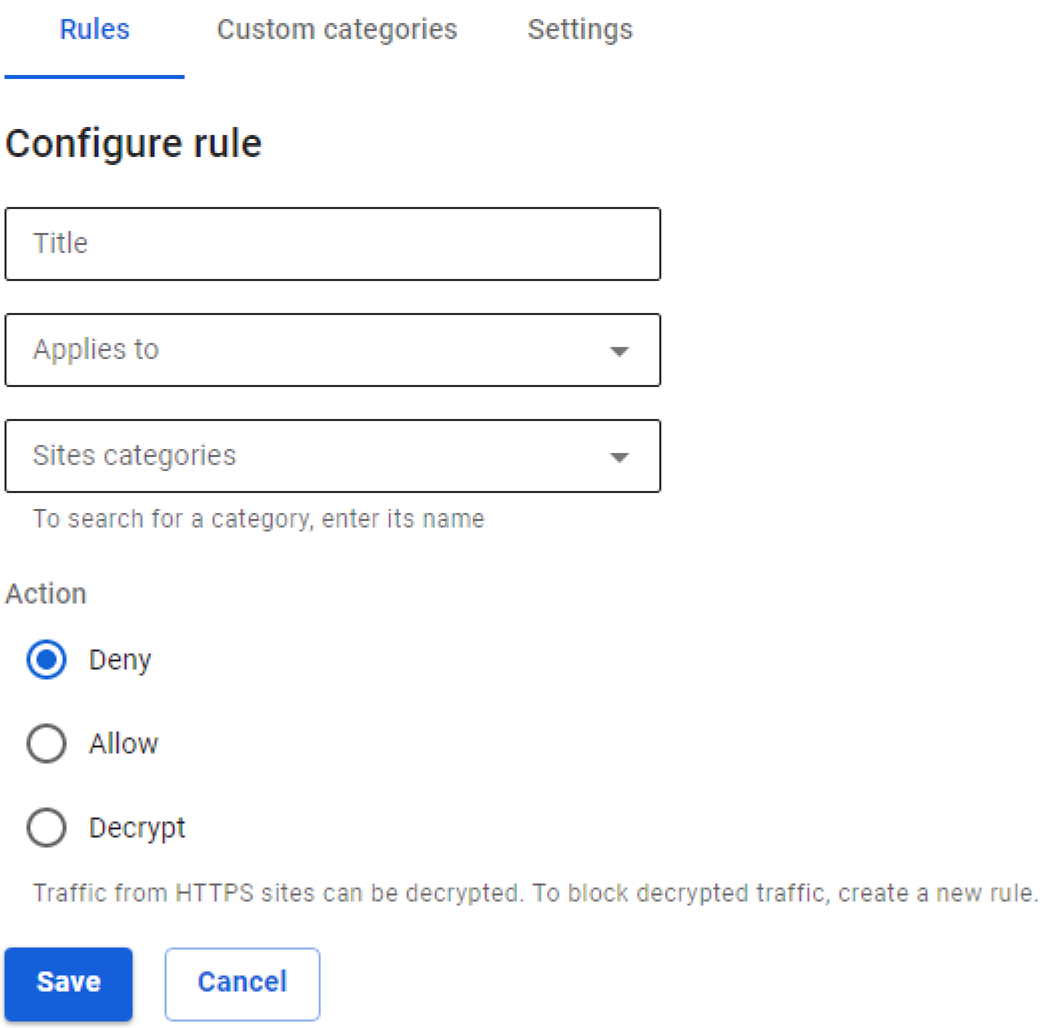
The rules are applied from top to bottom according to the order in the table until the first match. Thus, if the higher-level rule allows a certain resource for a specified user group, the lower-level rules will not be applied to it. This way more flexible filtering settings can be created, excluding desired users by higher-level rules from blocking rules. HTTPS decryption rules apply in a similar way.

Rules can be enabled, disabled, changed in priority, edited, and deleted in the **Operations** column. Content filtering rules are applied immediately after they are created and enabled.



Title	Applies to	Categories	Action	Operations
Block harmful sites	All	Botnet Anonymizer Hacking High Risk Malware Call-Home Compromised Spam Malware Distribution Point Command and Control Centers Phishing/Fraud Spyware and Malicious Sites Spyware & Questionable Software	Deny	⏻ + ↑ ↓ ✎ 🗑
Allowed sites	All	Allowed sites (Custom)	Allow	⏻ + ↑ ↓ ✎ 🗑
Prohibited sites	All	Prohibited sites (Custom)	Deny	⏻ + ↑ ↓ ✎ 🗑
Block sites with inappropriate content	All	Gambling Marijuana Pornography Pornography/Sex Sex & Erotic	Deny	⏻ + ↑ ↓ ✎ 🗑
Blocking traffic eaters	All	Online Ads Torrent Repository Games Torrent files	Deny	⏻ + ↑ ↓ ✎ 🗑

To create a new rule, click on **Add** in the left corner above the table.



Rules | Custom categories | Settings

Configure rule

Title

Applies to ▾

Sites categories ▾

To search for a category, enter its name

Action

● Deny

○ Allow

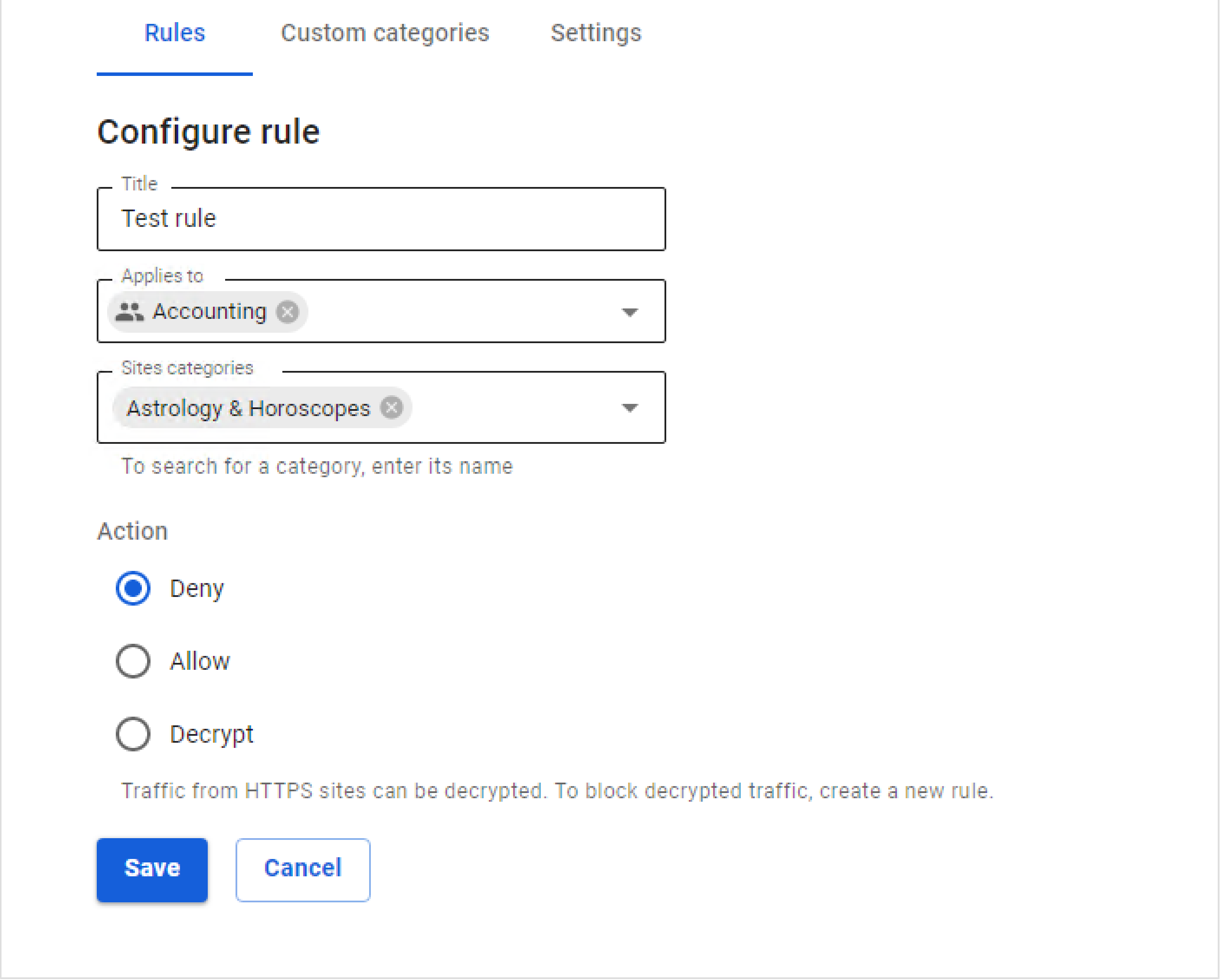
○ Decrypt

Traffic from HTTPS sites can be decrypted. To block decrypted traffic, create a new rule.

Save | Cancel

Fill in the following fields:

- **Title** – the rule name in the list. Maximum 42 characters.
- **Applies to** – you can select objects of the following types: user, user group, IP address, IP address range, subnet, list of IP addresses, or a special object **Quota Exceeded** (users who exceed traffic quota fall in this object).
- **Sites Categories** – user, special, and advanced web-resource categories.
- **Action** – the action of this rule towards web requests. You can prohibit, allow or decrypt HTTPS traffic.



Rules | Custom categories | Settings

Configure rule

Title: Test rule

Applies to: Accounting

Sites categories: Astrology & Horoscopes

To search for a category, enter its name

Action

● Deny

○ Allow

○ Decrypt

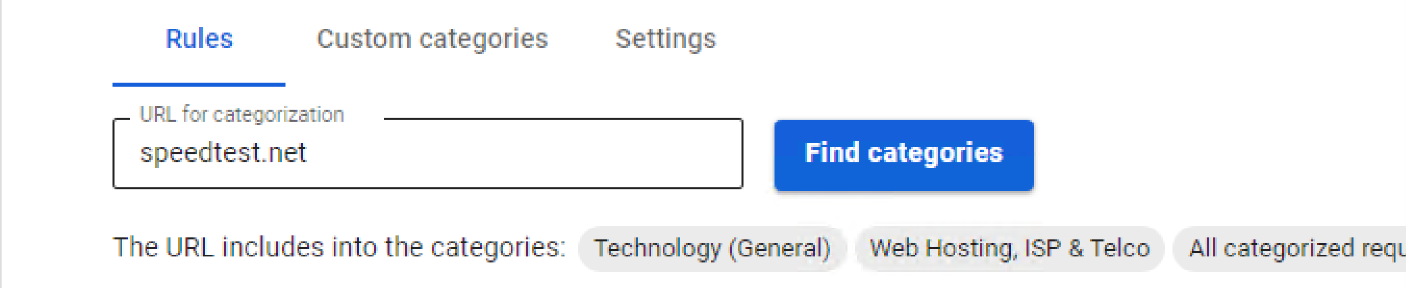
Traffic from HTTPS sites can be decrypted. To block decrypted traffic, create a new rule.

Save | Cancel

Diagnostics

If content filtering rules are not working, check the following parameters in the settings:

1. The IP address of the user’s computer must correspond to their address in authorization (section **Monitoring – Authorized users**), and the user must be in the group to which the rule applies.
2. The IP address of the user and the resource to which they access must not be included in the proxy server exceptions.
3. Check if the resource to which you are accessing is categorized correctly in the field **URL for Categorization** in the **Rules** tab.



Rules | Custom categories | Settings

URL for categorization: speedtest.net

Find categories

The URL includes into the categories: Technology (General) | Web Hosting, ISP & Telco | All categorized requ

If the site is incorrectly categorized, please use the **SafeDNS feedback form**.

4. VPN functions or plug-ins are not used in the user’s browser or computer; third-party proxy servers are not set.

Revision #5
Created 25 August 2022 01:40:43 by Val Redman
Updated 13 October 2022 15:01:52 by Val Redman