4.4. Setup - Traffic Rules

- Firewall
- Application Control
- Content Filter
  - Content Filter
  - Description of Content Filter Categories
  - Setting up HTTPS Filtering
- Traffic Shaping
- Antivirus
- Intrusion Prevention System
- Objects
- Quotas

Firewall

Principle of Operation

One of the main means of traffic management on the server is a firewall. It helps to limit user traffic:

- From LANs to external ones via the server.
- Between different LANs of the server.
- To the SafeUTM server.

The principle of operation for a firewall is as follows: it analyzes headers of packets passing through the server interfaces. This low-level task is solved by a gateway based on the TCP/IP protocol stack. This is why a firewall is well-suited for determining global traffic management rules for network protocols, ports, belonging to certain IP networks, and other criteria based on values of fields in network packet headers.

> The firewall is not designated to solve problems related to controlling access to internet resources based on URL address, domain name, or website content type. These higher-level tasks usually related to web traffic are solved with the help of the **Content Filter** module.

The firewall is configured in the web interface section **Traffic Rules -> Firewall**.

> SafeUTM has pre-configured and automatically enabled system rules. They provide protection for proxy and reverse proxy, mail server services, and others. As a rule, it is not necessary to additionally configure protection for the SafeUTM server with the help of user-defined rules. Use them to filter LAN traffic and publish resources. Even when the user firewall is disabled in the web interface, system rules continue to work.

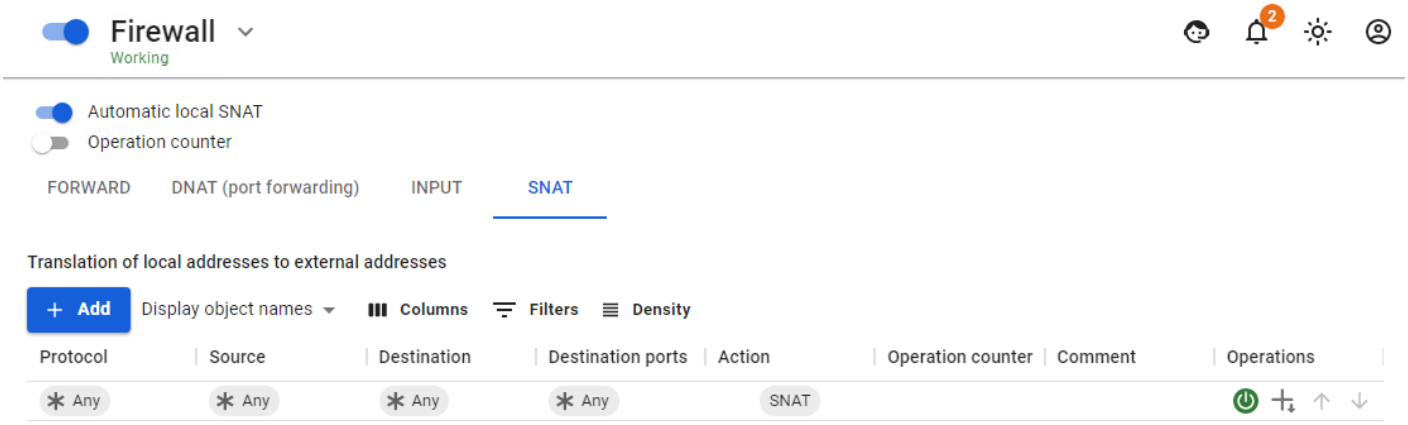
In case incorrect rules have been created (for example, access to the SafeUTM web interface has been prohibited), you can disable the user firewall from the local server menu. To do this, select **Disable user's firewall**, enter **8,** and press **Enter.**

```
Server management

1. Shell
2. Configuring a local network interface
3. Disable access to the web interface from WAN
4. Enable access to the server via SSH from WAN
5. Enable access to the server via SSH from LAN
6. Enable `Allow Internet Access to All`
7. Flush IP bans
8. Disable user's firewall
9. Create new backup
10. Restore backup
11. Enable Remote Assistant
12. Technical support contacts
13. Edit server name
14. Create cluster
15. Rollback to the previous version
16. Reboot
17. Shutdown
18. Exit

Type your choice and press Enter.
# 8
```

Automatic SNAT

NAT (Network Address Translation) is a mechanism in TCP/IP networks that allows you to convert the IP addresses of transit packets. **Read more**.

The **Automatic local SNAT** setting enables the automatic translation of the address for traffic going to the external interface in the firewall if the source is 10.0.0.0/8, 172.16.0.0/12 192.168.0.0/16 and addresses that are registered in the **SNAT** tab if the **SNAT Action** is selected. This way you don't have to create such rules manually and change them when you add or change local networks.



Disable this setting if there is a need for access from external networks (for example, DMZ) to SafeUTM LAN without NAT.

You can create SNAT rules manually for those who need them and disable them (by the "Not SNAT" rule) for those who need to be allowed into the network without network address translation.

Firewall Tables

> Rules in the table have priority from top to bottom (i.e., the upper rule has priority over the lower one).
> Before creating rules for networks, IP addresses, or IP address ranges, first, create them in the **Objects** section.

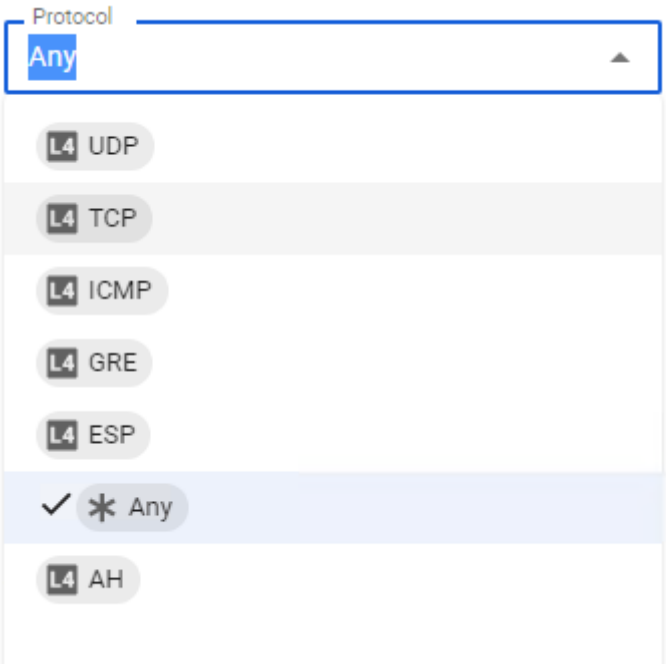
For the convenience of rule management, they are divided into four tables:

- **FORWARD** – rules in this table apply to traffic passing between the server interfaces, (i.e., the internet and LAN, as well as between LANs). This is the main table to which rules that restrict user traffic can be added.
- **DNAT (port redirection)** – the rules of this table are used to redirect ports from the external interface to certain resources in LAN. Such rules are often called port forwarding rules (port forwarding, portmapper).
- **INPUT** – a table for rules of incoming traffic to the server interfaces. As a rule, it is traffic for server services (for example, a mail server).
- **SNAT** – a table of rules for managing the translation of network addresses.

> It is strongly NOT recommended to create a FORWARD or INPUT rule that blocks all traffic.

Protocols

When creating a rule, you need to select the data transfer protocol that the rule you are creating will apply to. If you select **Any** from the list of options, the rule will apply to all traffic.



Descriptions of each protocol from the list

- **UDP** - It is one of the simplest transport layer protocols of the OSI model. Does not guarantee packet delivery. This allows for much more quick and more efficient delivery of data for apps that require high bandwidth or a short data delivery time.
- **TCP** - Performs the functions of a transport layer protocol of the OSI model. Unlike UDP, TCP guarantees packet delivery.
- **ICMP** - It is mainly used to transmit error messages and other exceptions that occur during data transmission.
- **GRE** - This protocol is used to encapsulate the network layer packets of the OSI model into IP packets. The number of the protocol in IP – 47. It is mainly used when creating a VPN (Virtual Private Network).
- **AH** - A protocol protecting transmitted data in IPsec. Provides identification, integrity check, and protection from information reproduction.
- **ESP** - A protocol protecting transmitted data in IPsec. Provides identification, integrity check, and protection from information reproduction. **Unlike the AH protocol, ESP encrypts data**. When working with ESP, both end systems use a common key to encrypt data.

Creating Firewall Rules

To create rules in the desired table, click the **Add** button in the upper left corner of the screen.

Specify the required parameters and actions for the rule and click the **Save** button. The rule will be added to the end of the list. If necessary, change its priority with the buttons.

When creating rules for filtering web traffic from local networks (80, 443 TCP ports), the **Any** object must be specified in the **Incoming interface** field for the rule to work properly. If a different incoming interface is specified, the rule will not process web traffic.

Firewall Rules

By default, **ALLOW** policy is used. If you do not create prohibiting rules, all ports and protocols for users will be allowed.

Firewall rules parameters:

- **Protocol** - Data transfer protocol (UDP/TCP/ICMP/GRE/ESP/AH or **Any**)
- **Source** - IP address of the source (src) of traffic passing through the gateway. IP addresses, IP address ranges, networks, or domains can be specified in the field. Data is taken from **Objects** specified by the user. Users and groups can also be used as a source (when changing their IP addresses, the firewall will automatically take it into account).
- **Destination port** - Specified when creating a rule with TCP/UDP protocols. It can be a single port, a list of ports, or a range of ports defined in **Objects**.
- **Incoming interface** - UTM interface that traffic will come into.
- **Outgoing interface** - UTM interface that traffic will come out of.
- **Time of action** - The duration period of the rule. Time intervals (for example, **working hours)** are specified, which are defined in **Objects**.
- **Action** - Allows or prohibits traffic.
- **Comment** - Any text explaining the purpose of the rule. Maximum 255 characters.

Actions

The values of the Action parameter:

- Deny - Prohibits traffic
- Allow - Allows traffic
- DNAT - Translates destination addresses, thus redirecting inbound traffic. Below, in the field **Change destination IP address,** you can specify one IP address or range (when specifying a range of IP addresses, the packet will be redirected to any of them). Similarly, if you specify TCP or UDP when creating the rule, the field **Change destination port** will appear. With this feature, you can transparently redirect inbound traffic to another address or port.
- Don't use DNAT - Cancels DNAT for traffic meeting the rule criteria.
- SNAT - Translates source addresses
- Don't use SNAT - Cancels SNAT for traffic meeting the rule criteria.

Examples of Rules and Techniques

Port mapping, DNAT, server publishing in LAN

Examples of these settings are described in detail in the corresponding articles in the **Publishing Resources** section.

Blocking various resources by means of a firewall

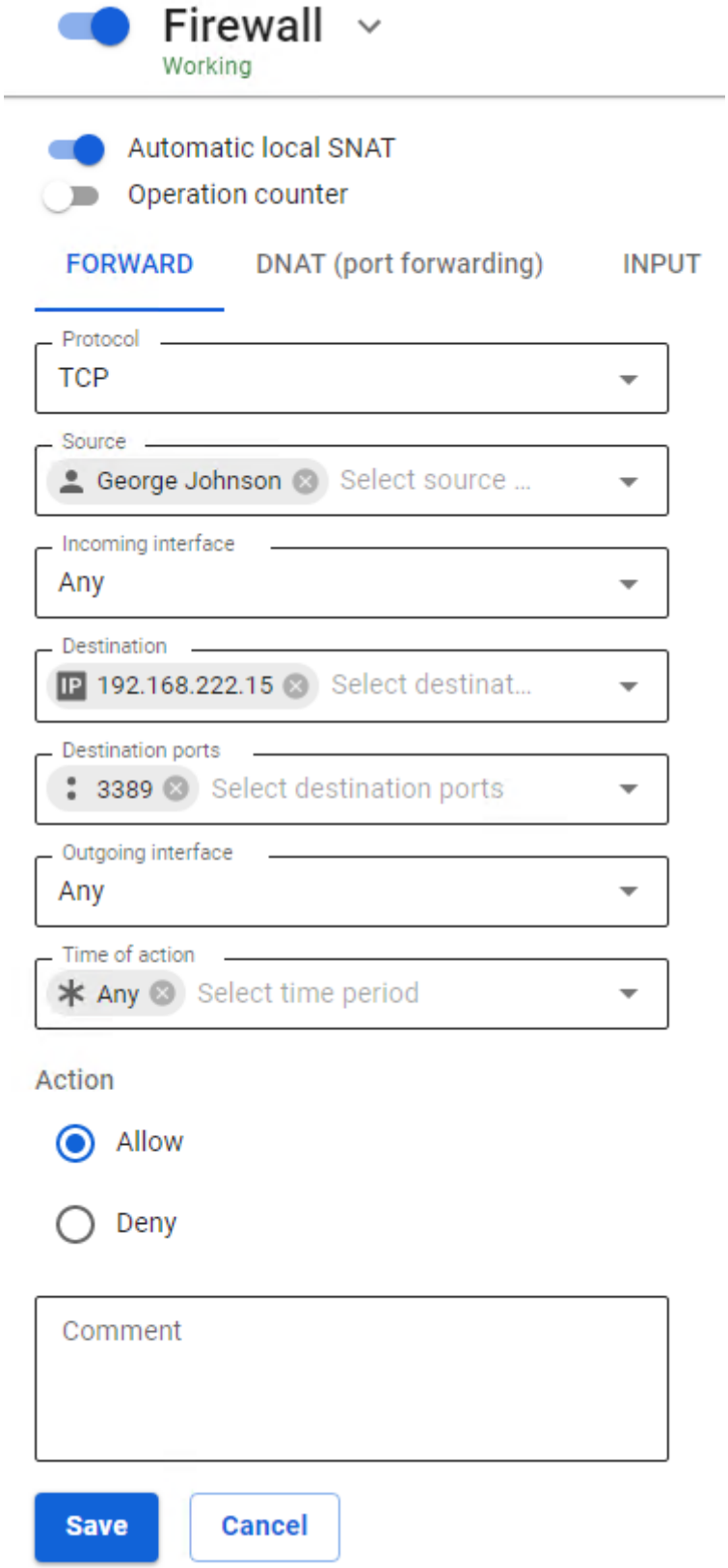
Issues of blocking various resources – remote control software (AmmyAdmin and TeamViewer), messengers, and other software are described in the **Blocking Popular Resources** section.

Access to the terminal server for a specific user

1. In the **Forward** tab, click **Add**
2. Fill in the following fields:

- **Protocol** - select TCP
- **Source** - select a user or user group
- **Destination** - specify the address of the terminal server
- **Destination ports** - specify port 3389

- **Action** - Allow



3. Click **Save**.

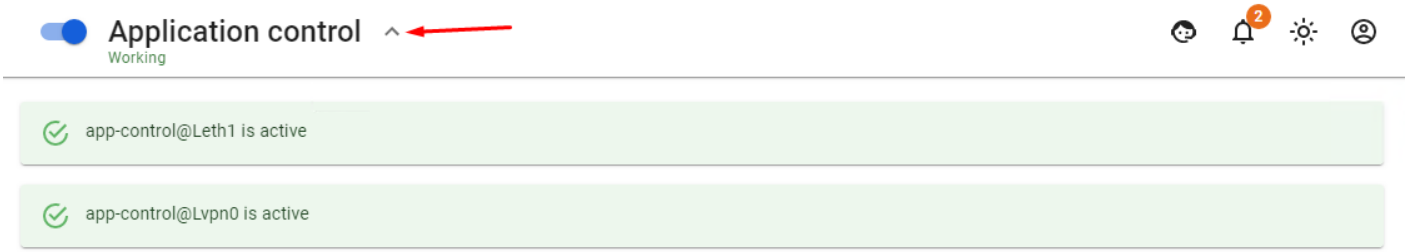
Application Control

The module implements in-depth traffic analysis (Deep Packet Inspection - DPI) to reveal protocols of popular apps (layer-7 filtering).

> App control works only in the Enterprise edition for users with an active subscription to updates and technical support, as well as in the SafeDNS SMB edition with the purchased module. The list of compatible network adapters with which this model works for certain can be seen in the **Installation Process** section.
>
> The **Intrusion Prevention**, **Application Control**, and **Traffic Shaping** rules do not handle traffic between LANs and branch networks.

> See the **Blocking Popular Resources** article to find out how to block remote access software, anonymizers, torrents, and other popular resources.

The status of the module can be viewed by clicking on the checkmark icon at the top of the screen next to **Application Control:**



How the rule set works:

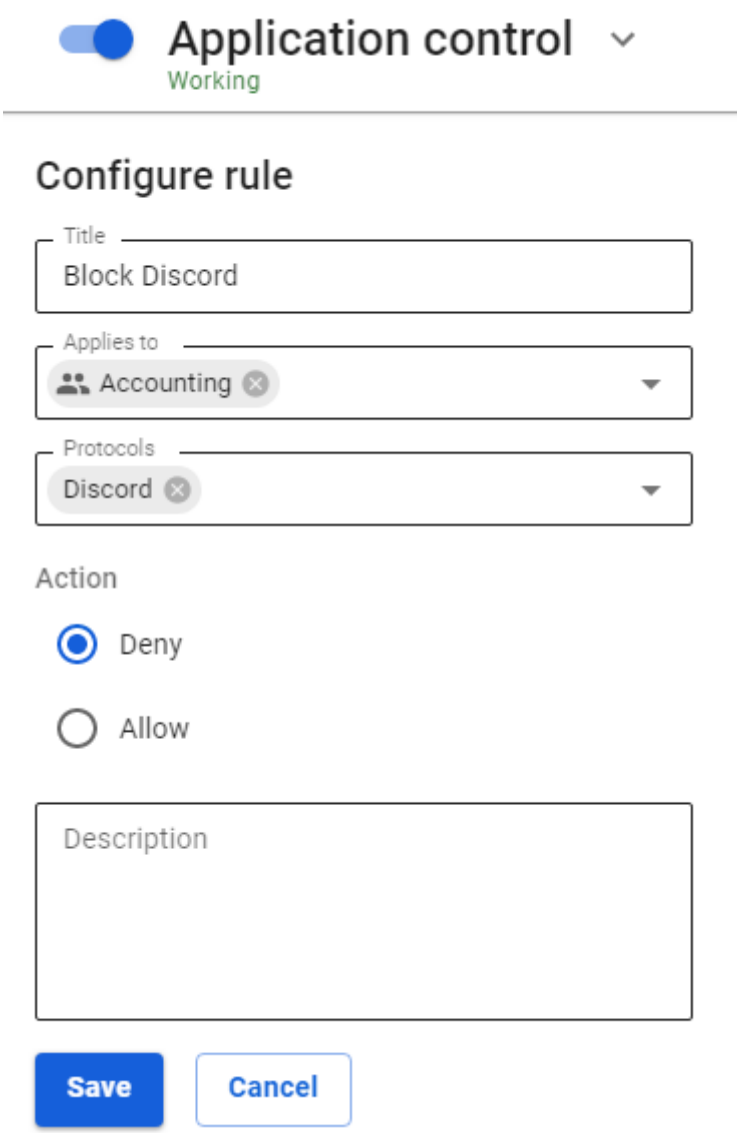
SafeUTM analyzes traffic and looks for a rule that matches this traffic from the list and applies it. If there are several rules in the list with the same conditions ("Applies to" and "Protocols" columns) but different actions (Action column), then the one with the higher priority will be applied.

Creating Rules

Rules are configured in **Traffic Rules -> Application Control**.

To create a new rule, follow these steps:

1. Click **Add** in the left upper corner of the screen.



2. Specify the following parameters:

- **Title** – type in the rule name for the convenience of administration. 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).
- **Protocols** – select (app) layer-7 protocol(s) from the list.
- **Action** – allow or deny the selected protocol.

3. Click **Save**.

Content Filter

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.

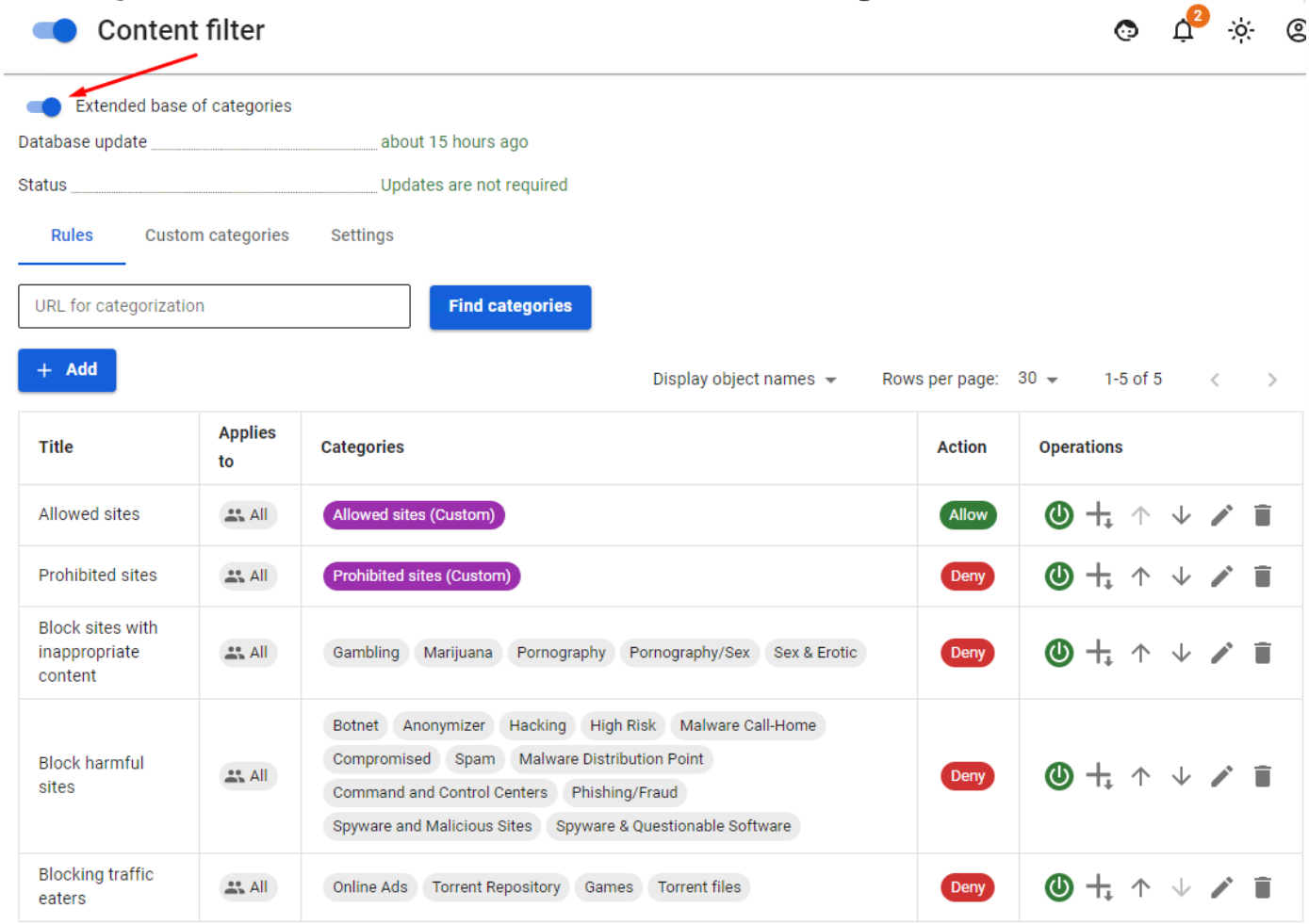
> The content filtering module only works with an active subscription to updates in the Enterprise edition.

> 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

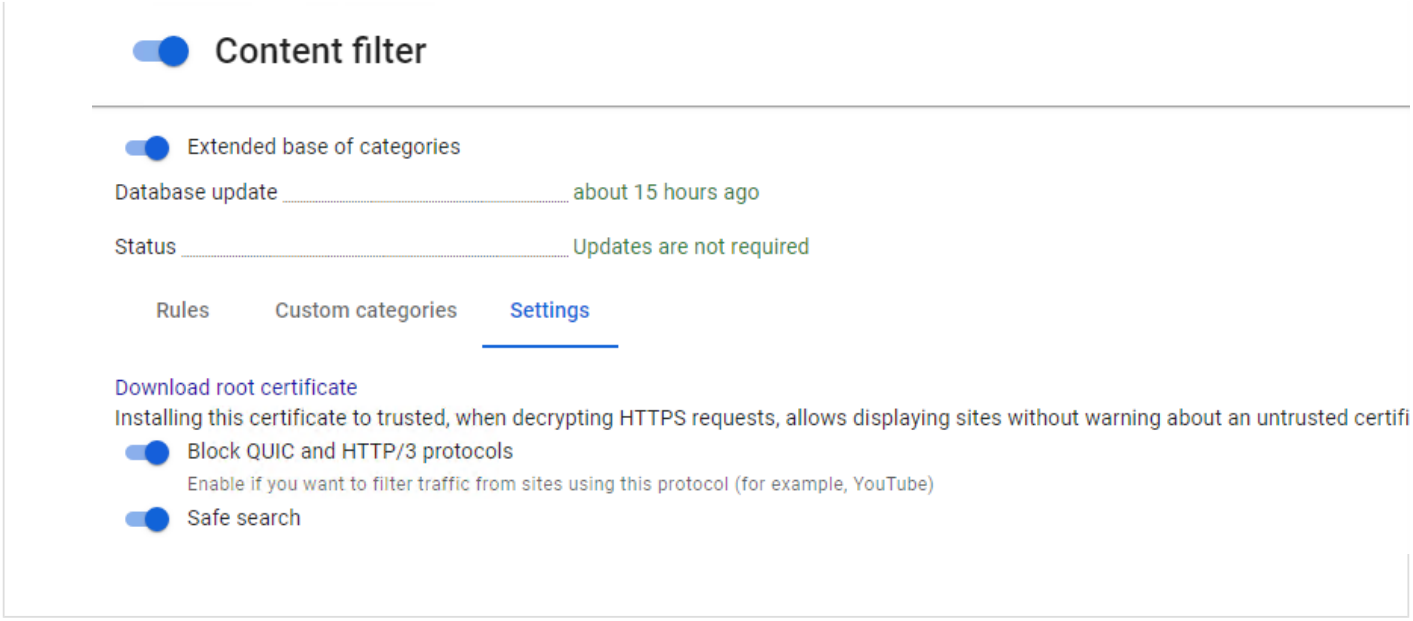
Content Filtering Setup

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**.



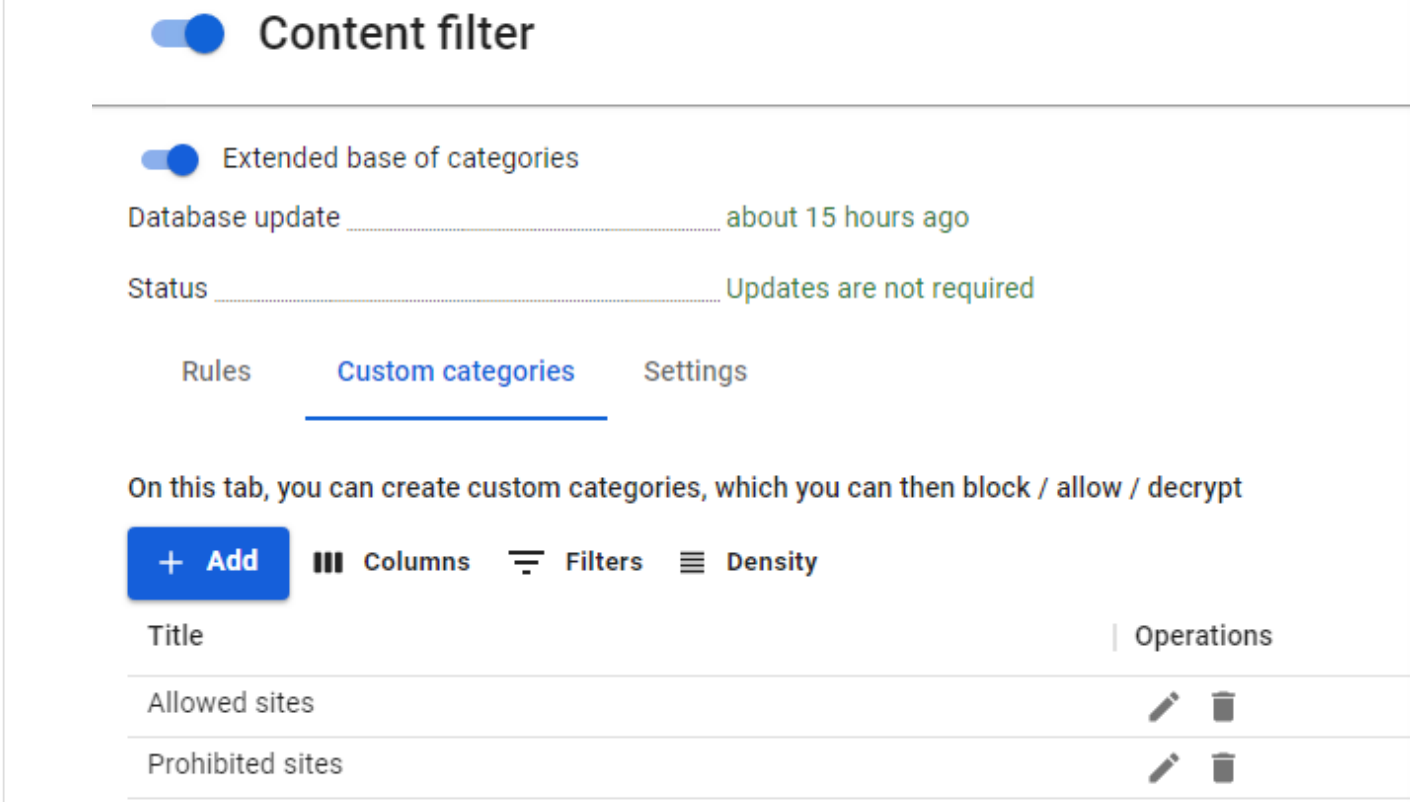
You can configure additional filtering options in the **Settings** tab:

- **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 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.



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

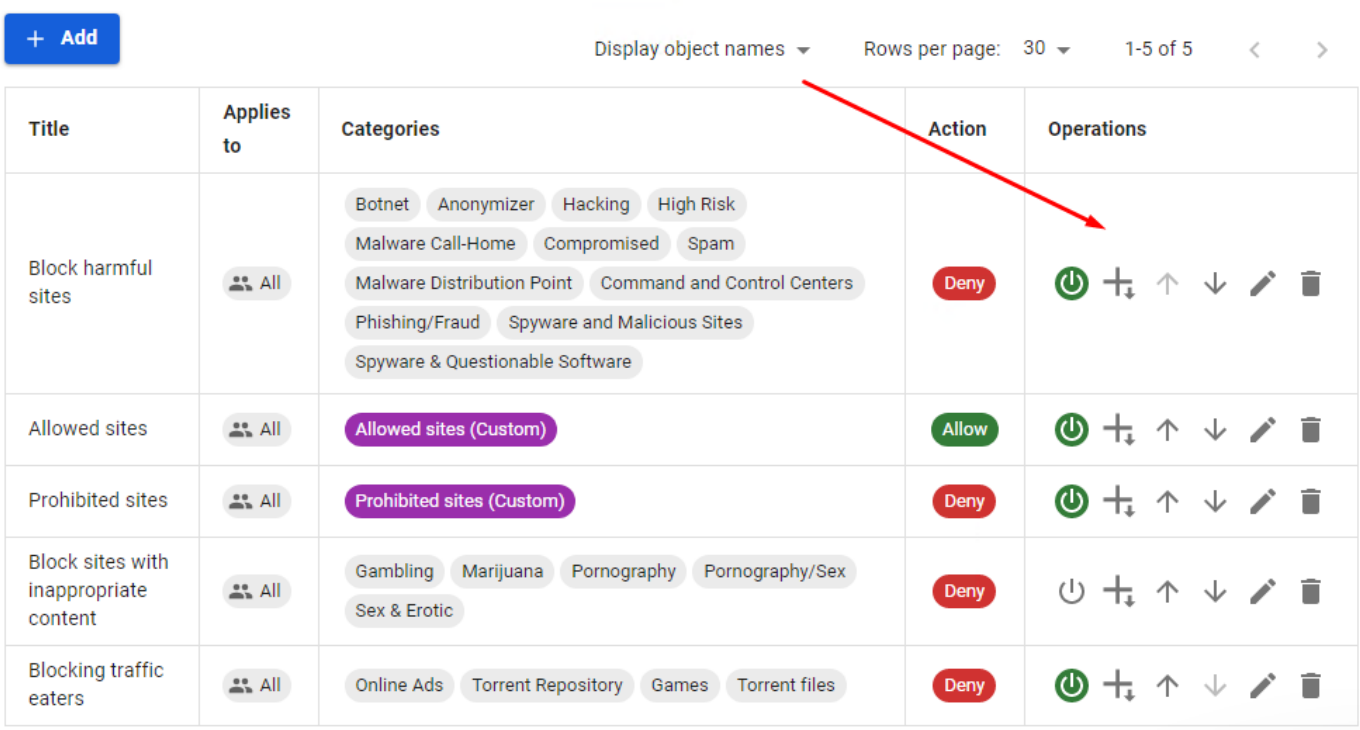
- **Files**. Eight defined categories of files blocked by extension and MIME type. Preset file groups (Executable Files, Archives, Video Files, Audio Files, Flash video, Active-X, Torrent files, and Documents) cannot be edited. Filtering HTTPS traffic for these types of categories is only possible when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

Applying Filtering

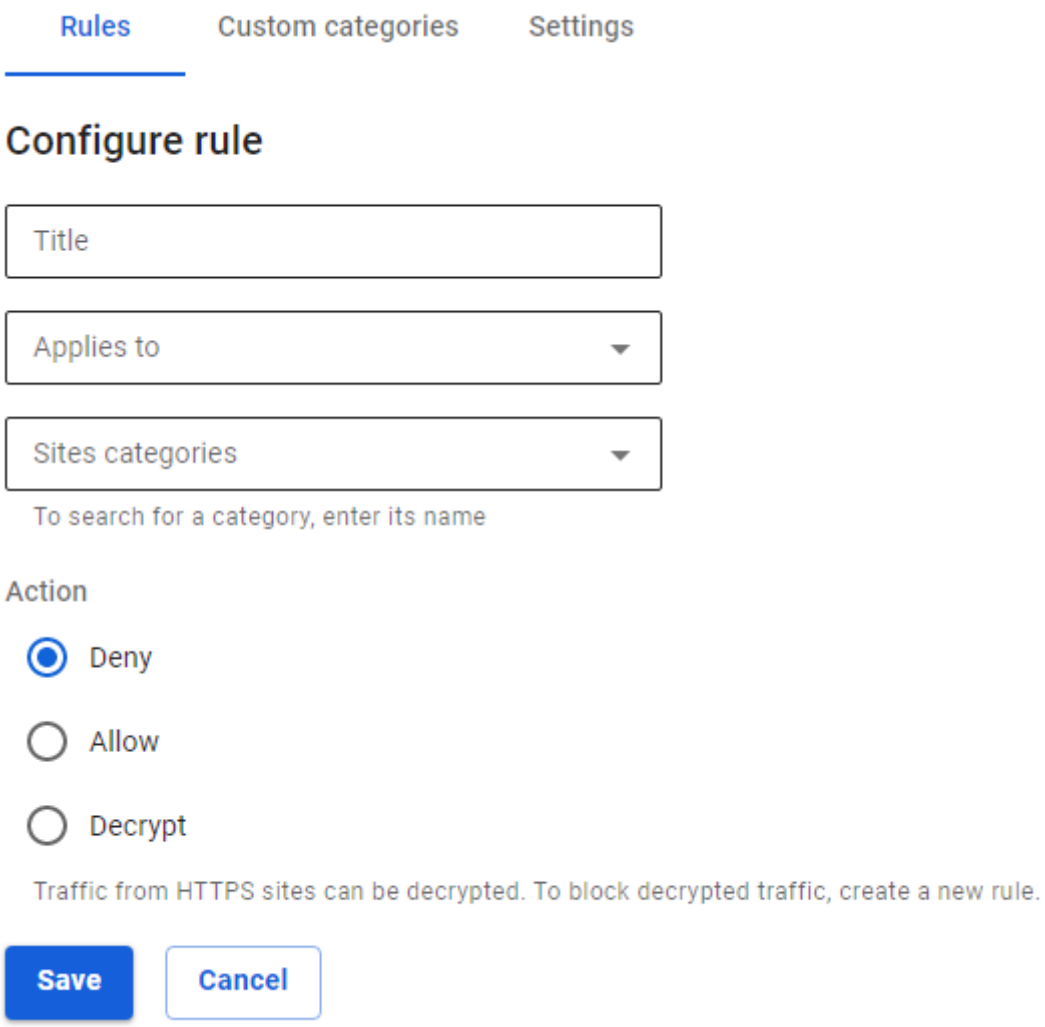
Applying Filtering Rules to Users

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.

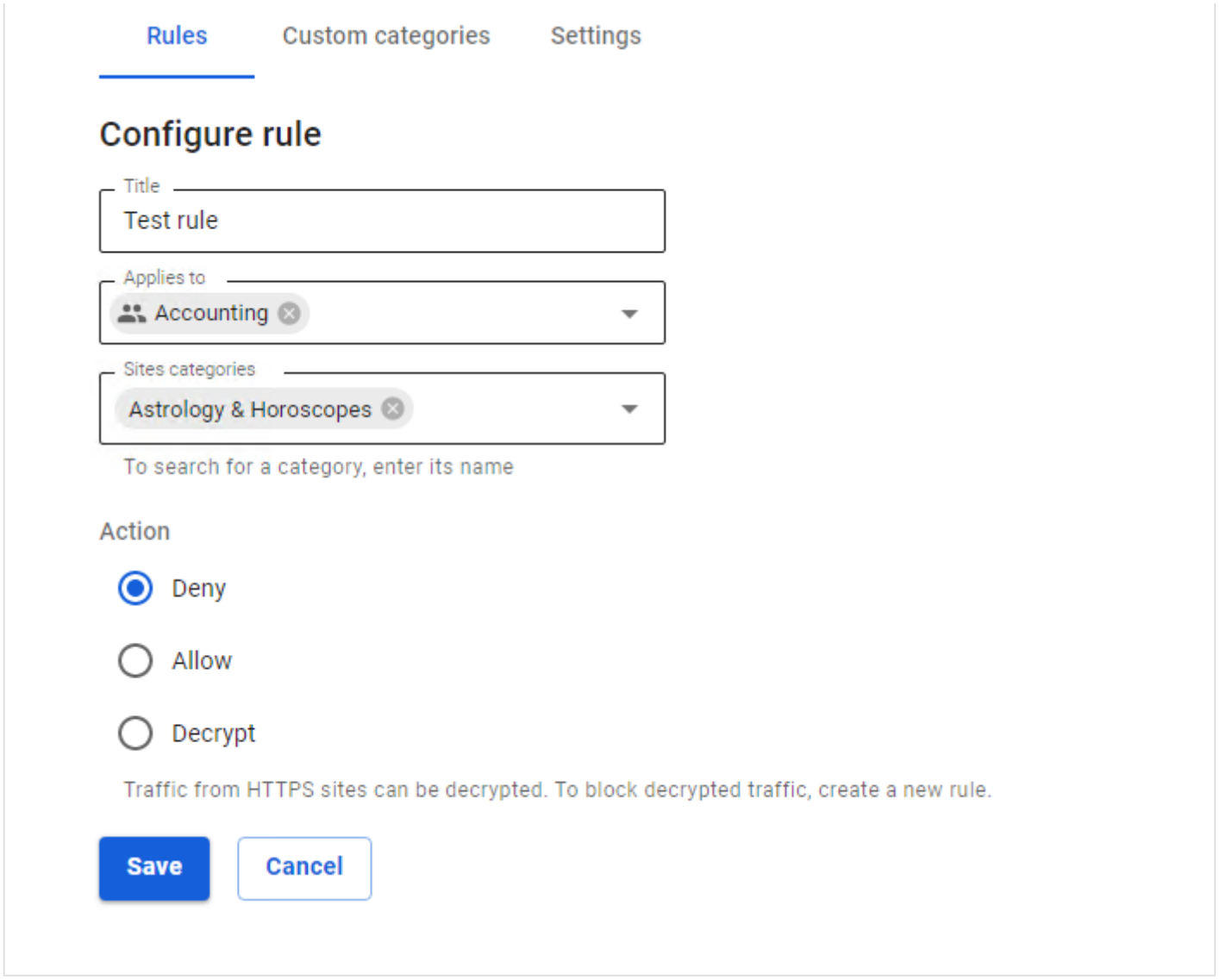


To create a new rule, click on **Add** in the left corner above the table.



Fill in the following fields:

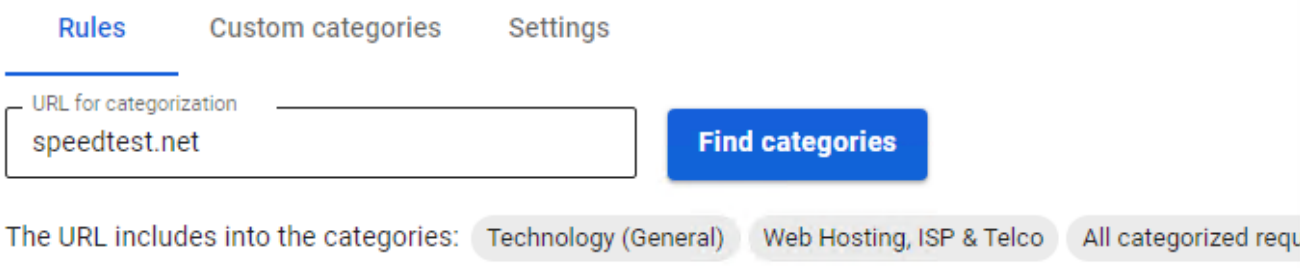
- **Title** – the rule name in the list. Maximum 42 characters.
- **Applies to** – you can select objects of the following types: user, user group, IP address, IP address range, subnet, list of IP addresses, or a special object **Quota Exceeded** (users who exceed traffic quota fall in this object).
- **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.



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.



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.

Description of Content Filter Categories

The article describes in detail the categories of queries to web resources.

Special categories

- **All queries** - all queries to web resources fall under this category.
- **All categorized queries** - all queries to web resources categorized by built-in or custom categories fall under this category.
- **All non-categorized queries** - all queries to web resources that have not been categorized by built-in or custom categories fall under this category.
- **Direct access by IP** - queries to web resources by IP address (http://84.201.128.105 /).

Extended categories

	Category	Description
1	Abortion	Websites, that discuss abortions from medical, legal, historical, and other points of view
2	Abortion - Pro-Choice	Websites advocating the legal right to choose whether or not to have an abortion
3	Abortion - Pro Life	Websites condemning the use of abortion
4	Advocacy Groups & Trade Associations	Websites about industrial shopping groups, lobbyists, unions, professional organizations, and other associations, including communities of like-minded people
5	Agriculture	Websites about science, art, and business related to agriculture (production of grain crops, lifting livestock, products, services, etc.).

6	Alcohol	Websites calling for alcohol consumption (or justifying its use), as well as sites that sell alcoholic beverages, including beer, wine, etc.
7	Anonymizer	Websites designed to bypass network filters. Such resources can be used by company employees to visit prohibited websites
8	Architecture & Construction	Websites about the construction, design of buildings and structures, architecture, as well as organizations or services related to design, construction, and construction design
9	Art	Websites about fine art
10	Arts	Websites about art in general
11	Astrology & Horoscopes	Websites about astrology, horoscopes, as well as predictions on stars or zodiac signs
12	Atheism & Agnosticism	Websites leading anti-religious propaganda or questioning religious, spiritual, metaphysical, or supernatural views
13	Auctions & Marketplaces	Websites about sales of goods and services through ads, online auctions, or other non-traditional channels
14	Banking	Websites of banks and other credit institutions, including websites of Internet banks. This category does not include sites of organizations offering brokerage services
15	Biotechnology	Websites about studies in the field of genetics, as well as sites of research institutes and organizations working in the field of biotechnology
16	Botnet	Websites or compromised web resources on which the software used by hackers for spam mailings and the implementation of various Internet attacks is launched
17	Business/Services	Websites about business and services.
18	Businesses & Services (General)	Websites about business and services. This category includes resources that are not subject to more accurate categorization than business and services

19	Cars/Transportation	Websites about vehicles, including sales, promotion, discussion, manufacturers, and online stores
20	Cartoons, Anime & Comic Books	Websites with animation, cartoon TV shows, and comics
21	Catalogs	Websites with grocery lists and catalogs without the ability to make an online purchase
22	Chat	Online chats
23	Chat/IM	Online chats and messengers
24	Child Abuse Images	Websites with images of physical or sexual violence against children
25	Child Inappropriate	Materials inappropriate for children: tasteless, cruel (including, in relation to animals), toilet humor, etc.
26	Command and Control Centers	Internet servers used to manage botnets
27	Community Forums	Websites of forums, news groups, archives of mailing lists, announcement boards, and similar community resources
28	Community Sites	Social networks, as well as websites of various online communities
29	Compromised	Websites that were compromised by attackers and look like official websites, but actually contain malicious code
30	Computers & Technology	Websites about it, software, Internet, and computers
31	Content Servers	Websites that do not contain navigation elements and are usually used to place images or other media content in order to increase productivity and scalability
32	Contests & Surveys	Websites about online competitions, sales, and lotteries that are created to study consumer preferences, and can also be used as an element of various marketing activities
33	Coupons	Websites offering the acquisition of discount coupons

34	Criminal Skills	Websites providing information on how to commit illegal activity, such as theft, murder, creation of a bomb, opening locks, etc.
35	Criminal Skills/Hacking	Websites providing information about computer hacks
36	Dating & Relationships	Websites about acquaintances, marriage, etc.
37	Download Sites	Websites with software catalogs, including shareware, paid, free, and open-source software
38	Education	Websites related to learning
39	Educational Institutions	Websites of schools, universities, and other educational institutions
40	Educational Materials & Studies	Websites on which academic publications, magazines, research results, curricula, as well as online courses, textbooks, etc. are posted.
41	Entertainment and Videos	Websites with video and entertainment
42	Entertainment News & Celebrity Sites	Websites about news and gossip about celebrities, television shows, films, and show business in general
43	Entertainment Venues & Events	Websites about cultural institutions such as theaters, cinemas, nightclubs, festivals, etc.
44	Fashion & Beauty	Websites about fashion and beauty, including sites related to fashion and containing information about clothes, jewelry, cosmetics, and perfume
45	File Repositories	File sharing sites
46	Finance	Websites, that discuss economic issues, investment strategies, pension, and tax planning
47	Finance (General)	Websites, that discuss economic issues. This category includes resources that are not subject to more accurate categorization than finances.
48	Fitness & Recreation	Websites about fitness and other recreational activities
49	Food & Restaurants	Food sites: from restaurants and cafes to recipes and cooking tips

50	Gambling	Websites calling for participation in gambling (lotteries, casinos, etc.)
51	Games	Websites about computer games, as well as sites with online games
52	Gay, Lesbian, or Bisexual	Websites that discuss non-traditional sexual orientation
53	Government	Websites of state organizations
54	Government Sponsored	Websites of state organizations, including police, fire services, election commissions, research, and programs sponsored by the state
55	Hacking	Websites containing information or utilities that can be used to make online hacks
56	Hate Speech	Websites calling for extremism, discrimination on sexual, racial, religious, and other signs
57	Health	Websites about personal health
58	Health & Medical	Websites about personal health, medical services, medical equipment, procedures, mental health, hospitals, and clinics
59	High Risk	High threat sites
60	Hobbies & Leisure	Websites containing information about various crafts and hobbies, such as collecting, aircraft modeling, etc.
61	Home & Office Furnishings	Websites that include information about furniture manufacturers, and retail stores for the sale of furniture, tables, chairs, cabinets, etc.
62	Home, Garden & Family	Websites about family relationships and the house, including information about education, internal decoration, landscaping, cleaning, family, etc.
63	Home/Leisure	Websites about house and leisure
64	Humor	Websites containing humorous information, such as comics, jokes, funny pictures
65	Illegal Drugs	Websites about narcotic substances, including improper use of drugs

66	Image Search	Websites and search engines used to search for images and return results containing miniatures of the latter
67	Information Security	Websites of organizations providing information security services
68	Instant Messenger	Websites of instant messages, as well as websites used for advertising instant messengers on them
69	Insurance	Websites about all types of insurance, including medical, state, property insurance, etc.
70	Internet Phone & VoIP	Websites allowing to make calls via the web or programs of software products that are designed to make calls via the Internet
71	Job Search	Websites about the search for work, including recruiting agencies
72	Kid's Pages	Websites designed for young children (up to 10 years old), including games and entertainment pages
73	Legislation, Politics & Law	Websites on legislation, politics, parties, elections, their results, and opinions
74	Lingerie, Suggestive & Pinup	Websites with photos and videos that depict women in sexy provocative clothes, for example, in lingerie
75	Literature & Books	Websites on which literature is presented, including fiction and documentary novels, poems, and biographies
76	Login Screens	Websites that are used for a single authentication and access to a wide variety of services. For example, systems such as Yahoo or Google
77	Malware Call-Home	Malicious event when active malware on a computer attempts to contact a remote “home” server
78	Malware Distribution Point	Websites with viruses, exploits, and other malicious programs
79	Manufacturing	Websites about business related to industrial production

80	Marijuana	Websites on which information about marijuana, its cultivation, or smoking is presented, including sites about the legal use of marijuana, for example, in medicine
81	Marketing Services	Websites of advertising and marketing agencies
82	Mature	Mature content
83	Medium Risk	Websites that pose the average threat
84	Military	Websites sponsored by the armed forces and other state military institutions
85	Miscellaneous	Websites that cannot be unambiguously attributed to any of the categories
86	Mobile operators paid sites	Paid websites of mobile operators
87	Mobile Phones	Websites of mobile phone manufacturers, including sites selling mobile phones and accessories for them
88	Motorized Vehicles	Websites about transport with engine
89	Music	Websites about music. Internet radio, files in mp3 format, information about music groups, clips, etc.
90	Nature & Conservation	Websites with environmental information, ecology, etc.
91	News	News web resources. Online publications of newspapers, magazines, news feeds
92	No Content Found	Websites with unrecognizable content, which does not allow categorization of them
93	No Known Risk	Websites that do not pose threats and do not fall into other categories
94	Non-profits	Websites of nonprofit organizations
95	Non-traditional Religion & Occult	Websites about religions that are not in the mainstream or not included in the top10 of world religions (folk religions, mysticism, cults, and sects)

96	Nudity	Websites containing erotic materials (partial or complete exposure), excluding pornographic materials
97	Nutrition & Diet	Websites with information about healthy diets, weight loss, weight loss programs, and food allergies
98	Online Ads	Web pages strictly about advertising, banners, or popup windows with advertising
99	Online Financial Tools & Quotes	Websites containing information about financial quotes, as well as tools for financial analysis and budget planning, such as mortgage calculators, software for tax reporting, etc.
100	Online Information Management	Websites about programs for managing personal information, for example, applications for managing tasks, calendars, address books, etc.
101	Online Shopping	Online stores and other sites offering things online
102	Online Stock Trading	Websites of brokerage companies that carry out online securities, etc.
103	Parked	Websites that are used as “plugs” for acquired but not used domain names
104	Parks, Rec Facilities & Gyms	Websites about parks and other zones intended for wellness activities, such as swimming, skateboarding, mountaineering, etc.
105	Pay to Surf	Websites of companies offering to view advertising in their specialized applications
106	Peer-to-Peer	Peering networks sites
107	Personal Pages & Blogs	Personal and lifestyle content
108	Personal Storage	Websites for storing personal files
109	Personal Webpages	Personal pages, including blogs and other means of exchange of news, opinions, and information about the author, as well as home and family pages
110	Pets & Animals	Websites containing information, products, and services for pets

111	Pharmacy	Websites containing information about drugs (including legal narcotic substances), as well as their use
112	Philanthropic Organizations	Websites with information about charitable institutions and other non-profit philanthropic organizations
113	Phishing/Fraud	Websites used for fraud are also known as phishing. Usually, they look like official web pages of financial or other institutions with the aim of unauthorized access to confidential information, for example, CVV codes of bank cards
114	Photo Sharing	Websites on which users can place digital photos, as well as search for images, exchange them, etc.
115	Physical Security	Websites related to products and services regarding security, with the exception of computer security
116	Piracy & Copyright Theft	Websites that provide access to an illegal content, for example, pirated software (Warez), pirated films, music, etc.
117	Politics and Law	Websites on politics and legislation
118	Pornography	Websites containing images or videos with a demonstration of sexual intercourse or a naked body
119	Pornography/Sex	Websites containing images or videos with a naked body
120	Portal Sites	Web resources that provide access to custom-made personal portals, including yellow pages and other catalogs
121	Possible Risk	Websites with the possibly risky contents
122	Private IP Address	Websites served on private IP addresses reserved for use within organizations and houses
123	Product Reviews & Price Comparisons	Websites designed to help customers compare shops, products, and prices, but not selling online
124	Profanity	Websites containing episodic or serious swearing or blasphemy

125	Professional Networking	Websites of social networks focused on professionals and building business relations
126	R-Rated	Websites, the content of which must contain material intended only for an adult audience. There can be sexual topics or training materials
127	Real Estate	Websites about real estate issues (purchase, sale, rent, etc.)
128	Redirect	Websites that redirect visitors to other resources
129	Reference Materials & Maps	Websites containing reference materials and data sets: atlases, dictionaries, encyclopedias, census, etc.
130	Religion	Websites about a specific religion
131	Religions	Websites about the main world religions, as well as general religious and theological topics
132	Remote access	Websites that provide remote access to private computers and networks, intranet resources (files and web applications)
133	Restaurants	Restaurant websites
134	Retirement Homes & Assisted Living	Websites about nursing houses and thematic communities, including patient care and hospice assistance
135	School Cheating	Websites with answers to tests, ready-made works, step-by-step solutions to problems, and similar resources
136	Search Engines	Search systems that search for websites, news groups, pictures, and other content
137	Self-help & Addiction	Websites offering information and assistance in alcohol, drug, gaming dependencies, as well as eating disorders (anorexia, etc.)
138	Sex & Erotic	Websites offering products and services related to sex, but not containing naked nature and other candid images
139	Sex Education & Pregnancy	Websites with teaching materials and clinical explanations about sex, safe sex, pregnancy, childbirth, etc.

140	Shipping & Logistics	Websites on stock management, including transportation, warehouse, distribution, storage, execution, and delivery of orders
141	Shopping	Online shopping and purchases
142	Sites from the list of the Ministery of Justice	Additional blocklist for specific regions
143	Social and Affiliation Organizations	Websites of social and affiliated organizations
144	Social Networking	Websites of social networks - communities in which people are "friends"
145	Software, Hardware & Electronics	Site about computer equipment, software, peripherals, data networks, and electronics, as well as manufacturers of appropriate goods and services
146	Spam	Websites advertised using spam
147	Sport and Recreation	Websites about training and competitions in martial arts: boxing, struggle, fencing, etc.
148	Spyware & Questionable Software	Websites with software sending information to the central server, including spy software and keyboard spies
149	Spyware and Malicious Sites	Websites that are spying, sending information about the visitor to a special address
150	Streaming & Downloadable Audio	Storage sites broadcasting music or other audio content (can consume the entire available bandwidth of the company's channel)
151	Streaming & Downloadable Video	Storage sites broadcasting videos, including streaming (can consume the entire available bandwidth of the company's channel)
152	Supplements & Compounds	Websites containing information about vitamins and other substances of unregulated turnover
153	Swimsuits	Websites containing images of people in bathing suits. Images of costumes themselves do not fall into this category

154	Technology (General)	Websites about web design, standardization on the Internet (for example, RFC), protocol specifications, news, and other wide discussions of technology
155	Television & Movies	Websites about television shows and films, including reviews, programs, plots, discussions, trailers, marketing, etc.
156	Text Messaging & SMS	Websites designed to exchange short text messages (SMS) between a web page and a mobile phone
157	Tobacco	Websites about tobacco products (cigarettes, cigars, vapes, etc.)
158	Torrent Repository	Websites that host torrent files that allow you to download potentially large files via P2P networks
159	Toys	Websites of toy manufacturers, as well as marketing resources and online toy stores
160	Translator	Dictionaries and translators from foreign languages
161	Travel	Websites about travel information and tourism, as well as online orders of plane tickets, hotels, cars, etc.
162	Unknown Sites	Websites without category
163	Unreachable	Websites that display errors such as “The connection time expired”, “the address is not found”, etc.
164	Violence	Websites about dubious actions, such as violence and aggression
165	Weapons	Websites about weapons
166	Web Hosting, ISP & Telco	Websites offering web-hosting services, blogging blogs, Internet providers, and telecommunication companies
167	Web-based Email	Services providing web access to mailboxes
168	Web-based Greeting Cards	Websites that allow users to send and accept postcards online

169	Wikis	Websites and resources of communities creating information documents available for editing for all participants

Setting up HTTPS Filtering

HTTPS traffic filtering provides the possibility for further processing of websites accessible via HTTPS.

Filtering is implemented by several methods:

- Analysis of Server Name Indication (SNI) headings. Thanks to this method, it is possible to analyze the domain to which the client connects without certificate substitution and interference with HTTPS traffic. Domains specified in the certificate are also analyzed.
- SSL-Bump Method. Filtering occurs by substitution on the fly of the certificate used to sign the requested site. The original site certificate is substituted by a new one signed by the SafeUTM root certificate instead of a certificate authority. Thus, the traffic transmitted over a secure HTTPS connection becomes available for processing by all modules provided by SafeUTM, namely by the content filter (it is possible to categorize the full URL of the query and MIME-type content), ClamAV, as well as external ICAP services.

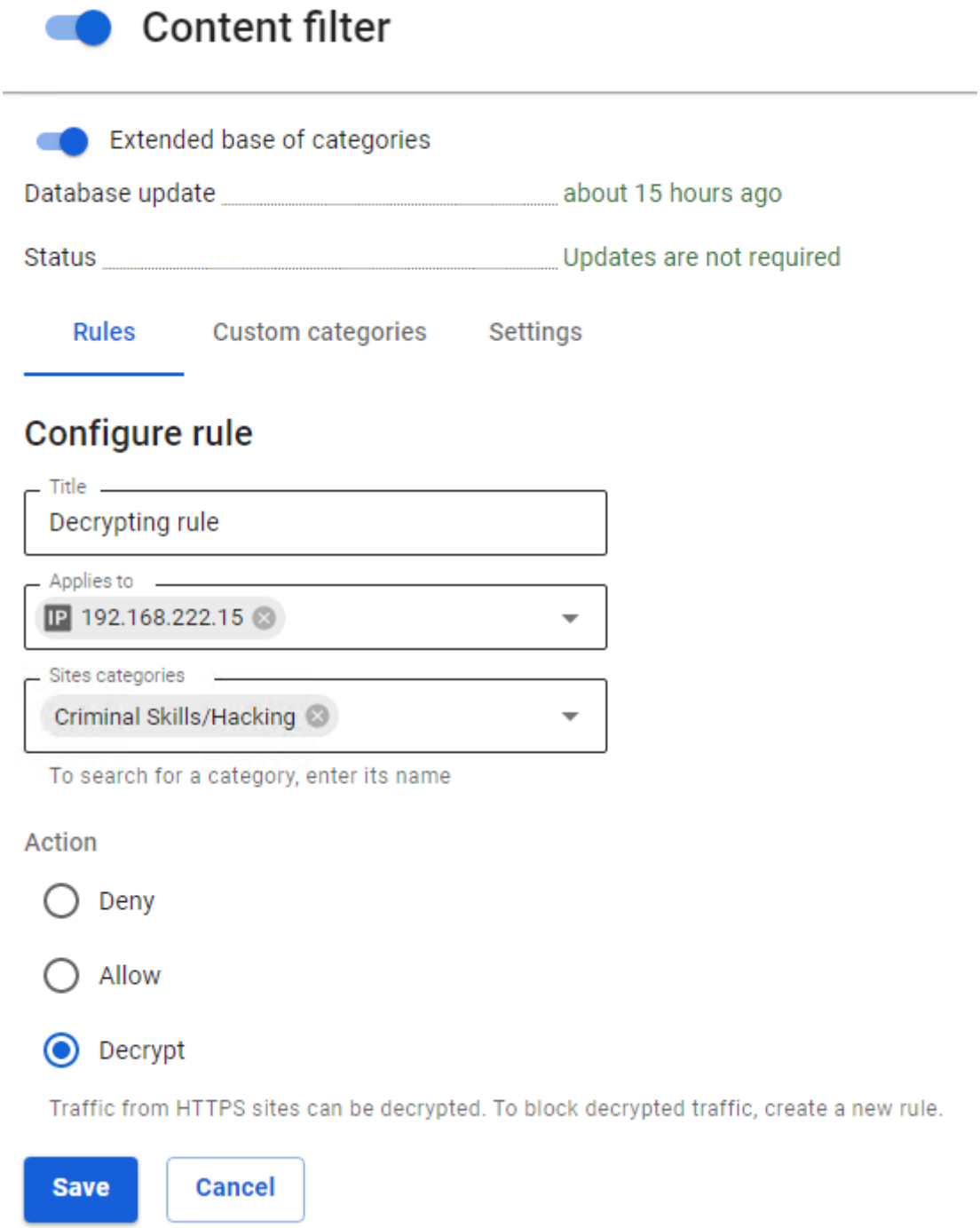
> The specifics of implementing HTTPS traffic filtering with certificate substitution require configuring both sides of the connection – the SafeUTM server and each user’s workstation in the local network.

Setting up SafeUTM Server

By default, the server performs HTTPS filtering without certificate substitution by analyzing SNI and domains in the certificate.

HTTPS traffic decryption is configured in **Rules -> Content Filter -> Rules** using the rules created by the admin with the action **Decrypt**.

An example of a decryption rule can be seen below:

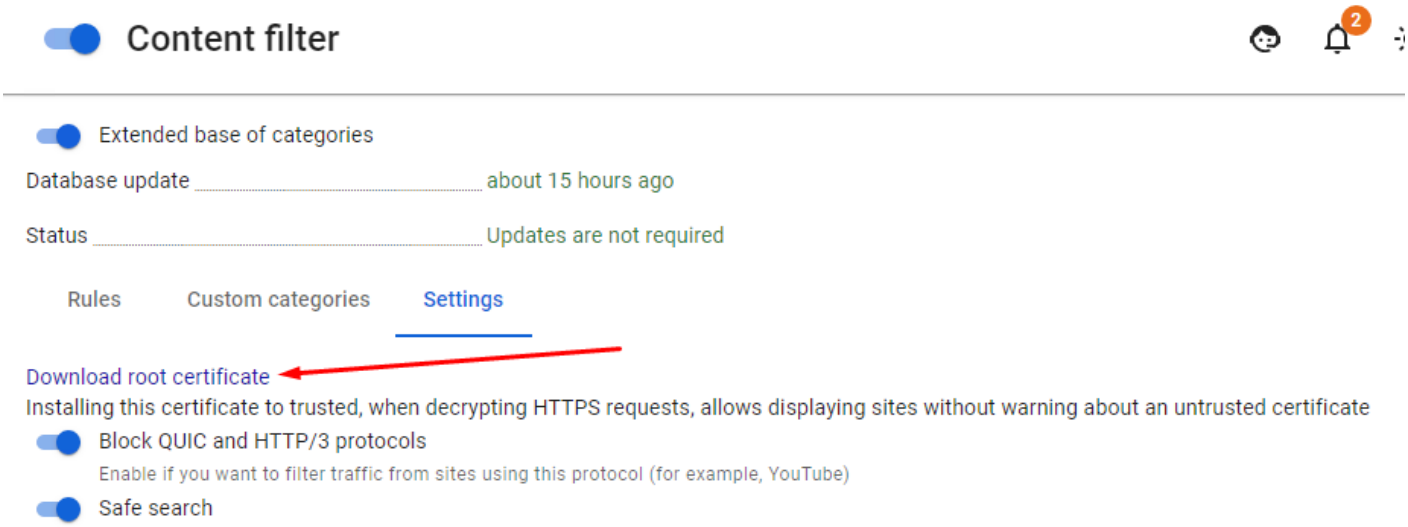


Setting up the User's Workstation

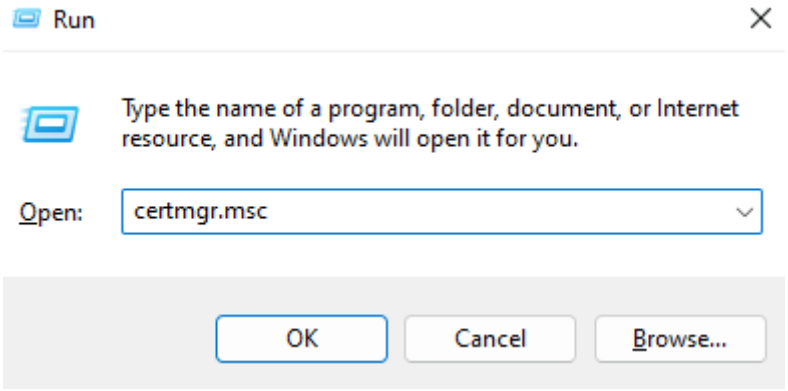
When the HTTPS traffic decryption option is enabled, the browser and other network software (for example, antiviruses, IM clients, etc.) on the user's workstation will require explicit confirmation to use a substitute certificate created and issued by the SafeUTM server. To improve the user's convenience, the SafeUTM server's root certificate should be installed in the workstation's operating system and made trusted. The root SSL certificate is available for download from the section **Traffic Rules -> Content Filter -> Settings**.

In order to install the root certificate, you need to follow these steps:

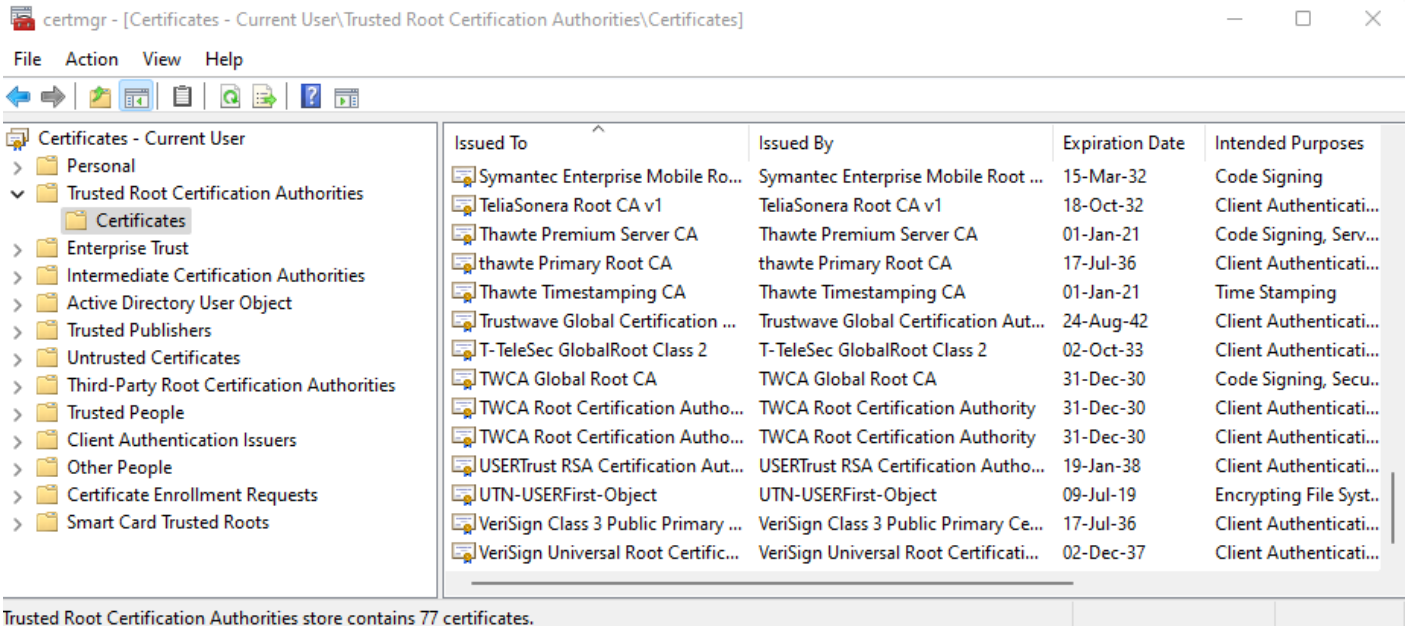
1. Download the root SSL certificate by opening the SafeUTM web interface section **Traffic Rules -> Content Filtering -> Settings**:



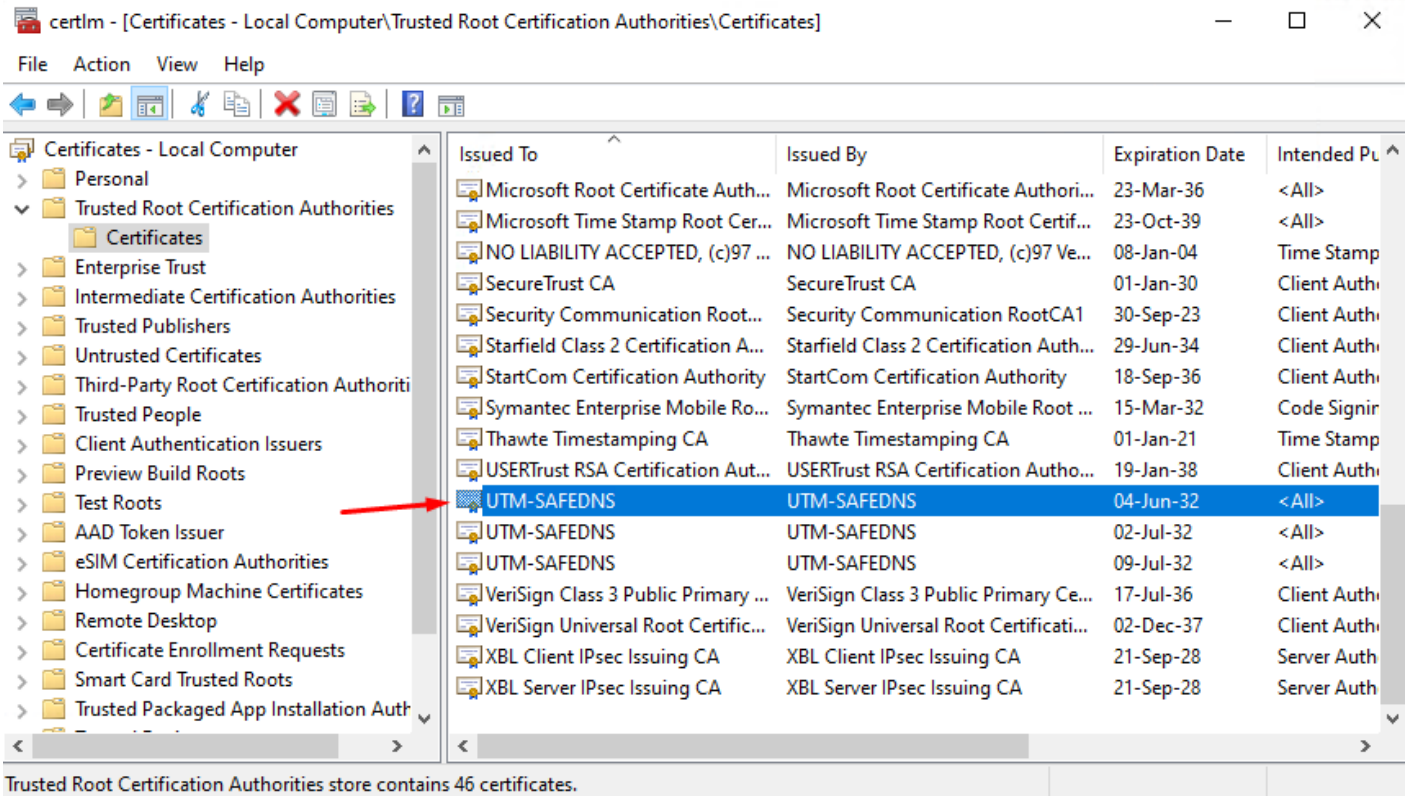
2. Open the certificate management center on the workstation **Start -> Run** by executing the command **certmgr.msc** in the dialog:



3. Select the section **Trusted Root Certificates -> Certificates**:



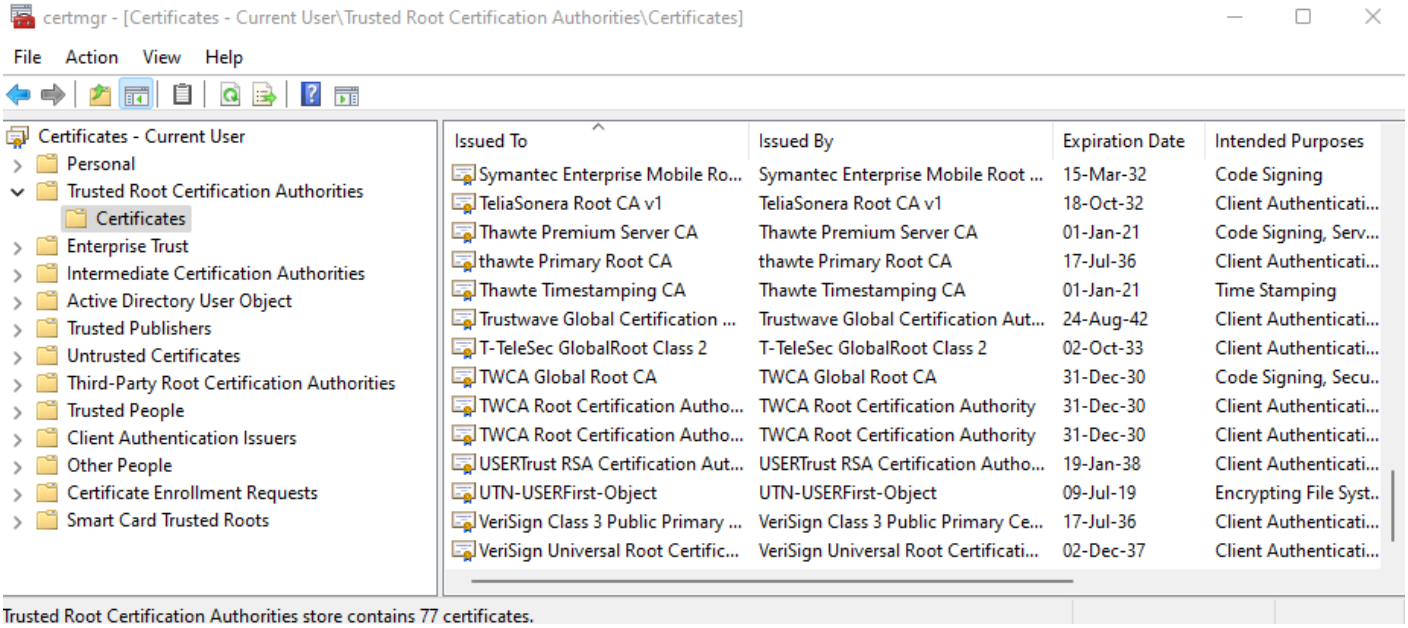
4. In the right part of the window, right-click and select action **All Tasks -> Import...** The Certificate Import Wizard will open. Follow the wizard's instructions to import the SafeUTM server's root certificate. The imported certificate will appear on the list in the right part of the window:



Adding Certificate via Microsoft Active Directory Domain Policies

In networks where users are managed using Microsoft Active Directory, you can install a SafeUTM certificate for all users automatically using Active Directory. To do this, follow these steps:

1. Download the root SSL certificate by opening the SafeUTM interface section **Access rules -> Content Filtering -> Settings**:



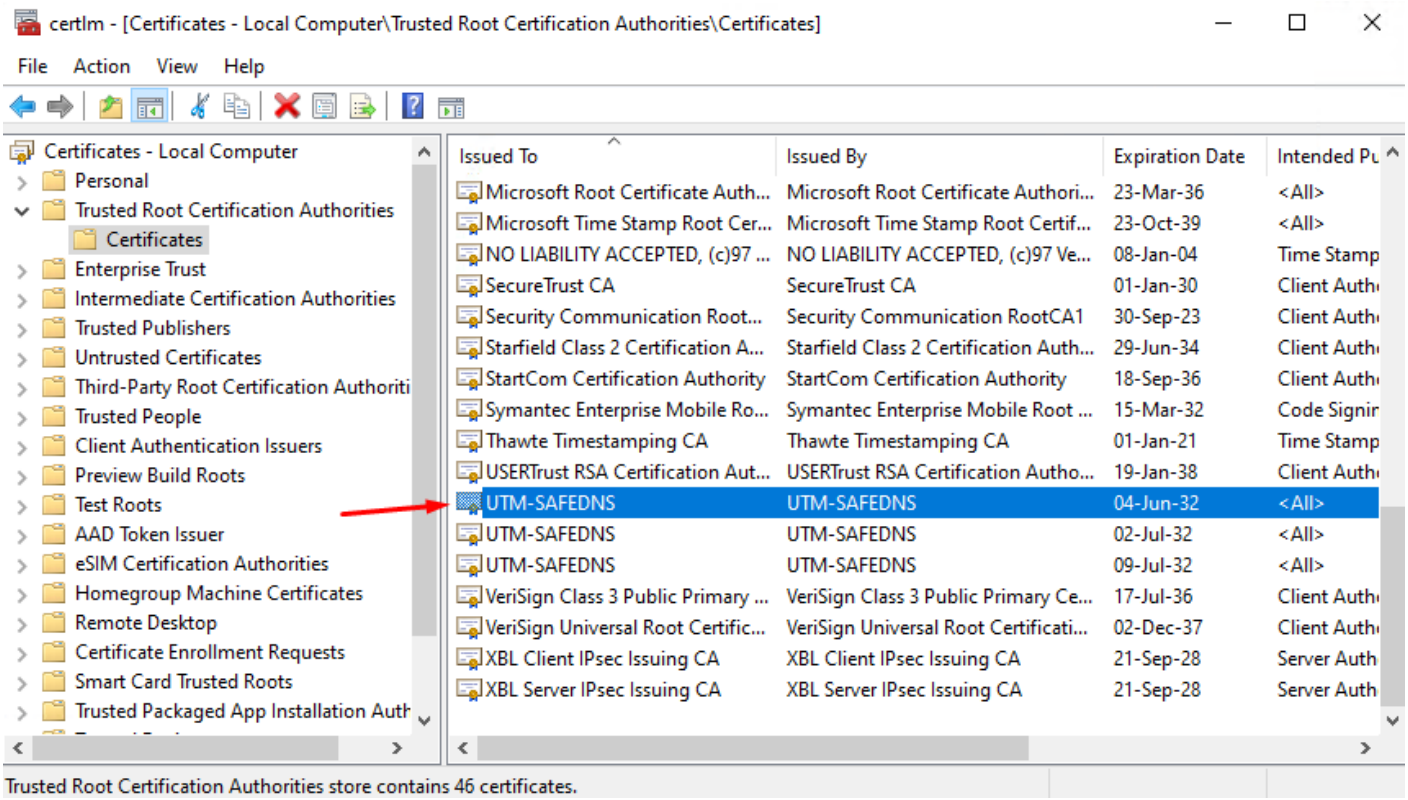
2. Log in to the domain controller with administrator privileges.

3. Launch the group policy management snap-in by executing the command **gpmc.msc**.

4. Find **the domain policy** used on users' computers in **Group Policy Objects** (Default Domain Policy in the screenshot). Right-click on it and select **Change**.

5. In the group policy management editor that opens, select: **Computer Configuration -> Policies -> Windows Configuration -> Security Settings -> Public Key Policies -> Trusted Root Certificate Authorities**.

6. Right-click on the list that opens, select **Import...** and import the SafeUTM key.



7. After restarting workstations or executing the command **gpupdate /force** on them, the certificate will appear in the local certificate stores and the required level of trust will be established for it.

Possible Problems and Troubleshooting

- Some browsers, such as Mozilla Firefox, do not use the system certificate store, in which case it is necessary to add a SafeUTM certificate to the browser’s trusted certificates. In Firefox, you can also set the parameter **security.enterprise_roots.enabled** (in **about:config**) to **true** for trusting system certificates.
- If the local machine uses an antivirus that checks HTTPS traffic using certificate substitution, sites may not open because of double certificate substitution. HTTPS traffic check must be disabled in the antivirus settings.
- With SNI filtering enabled, the server will not allow non-HTTPS traffic through the HTTPS port. Thus, problems with programs trying to do this may occur. In order for them to run, is necessary to allow bypassing the proxy server to the resources they require.
- When blocking HTTPS resources, in order to display the blocking page, it is necessary to set up trusting the UTM root SSL certificate even if only SNI filtering is enabled, as in case the resource opened via HTTPS is blocked, SSL-bumping with UTM SSL-certificate replacement will be applied for the possibility of replacing the resource content with the page about it being blocked by the server.

Traffic Shaping

This service is designed to limit the external incoming traffic speed for network users.

> **Intrusion prevention**, **Application control** rules, and **Traffic Shaping** do not handle traffic between local networks and branch networks.

Setting up Traffic Shaping

To create the rule, go to **Traffic Rules -> Traffic Shaping** and click on **Add**.

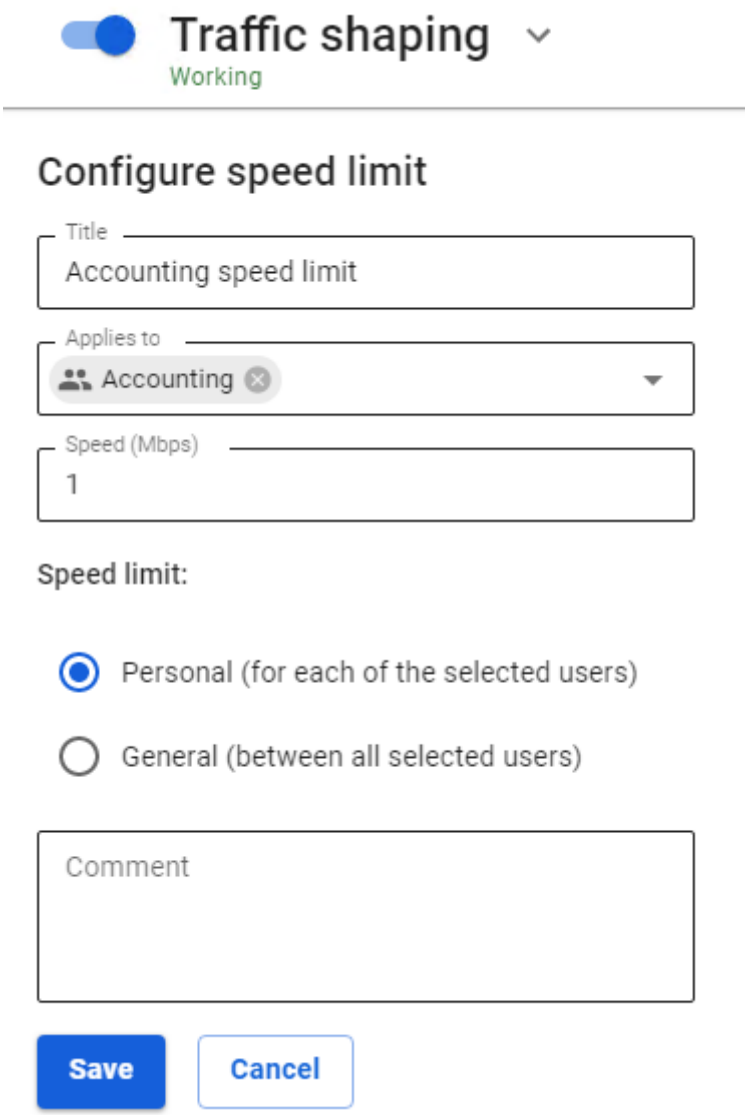
Next, fill in the following fields:

- **Title** – enter the rule name, for example, the **Accounting speed limit**. Maximum 40 characters.
- **Applies to** – select an individual user or group from the drop-down list.
- **Speed (Mbps)** – the speed limit for selected users.

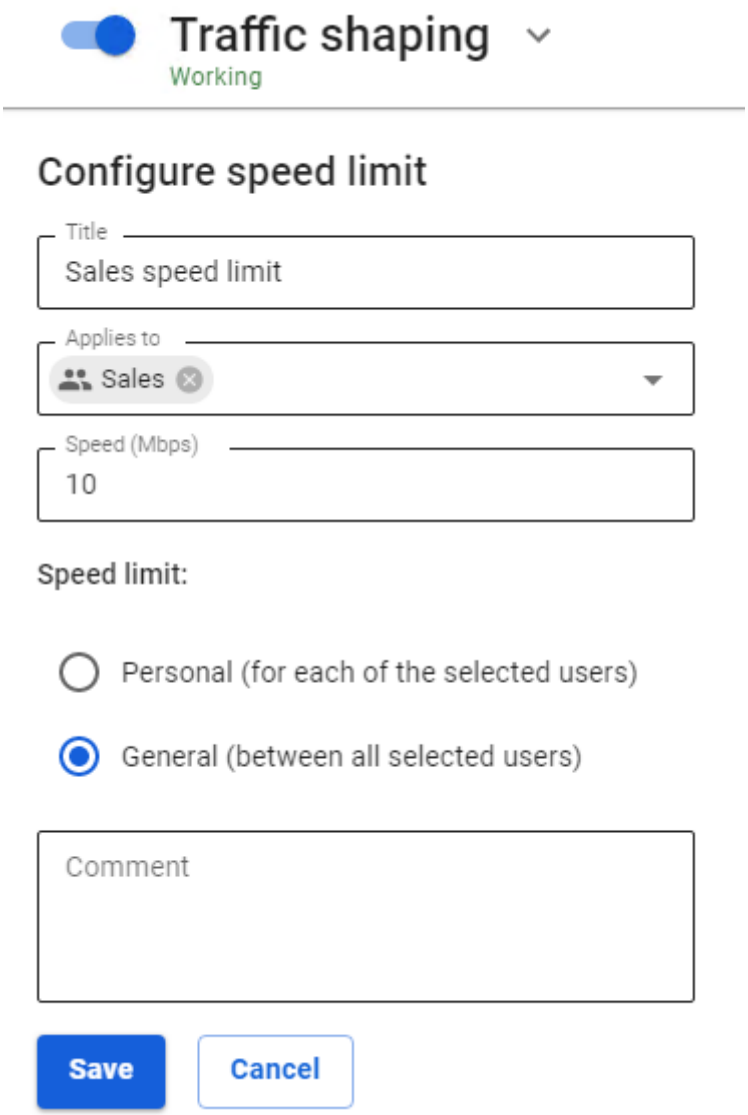
There are two types of speed limits for ease of configuration. They can be applied for users, groups, IP addresses, or a special object **Quota Exceeded** (users who exceed traffic quota fall in this object).

- **Personal** – the speed will be limited for each of the selected users.
- **General** – the speed will be limited and shared among all the selected users.

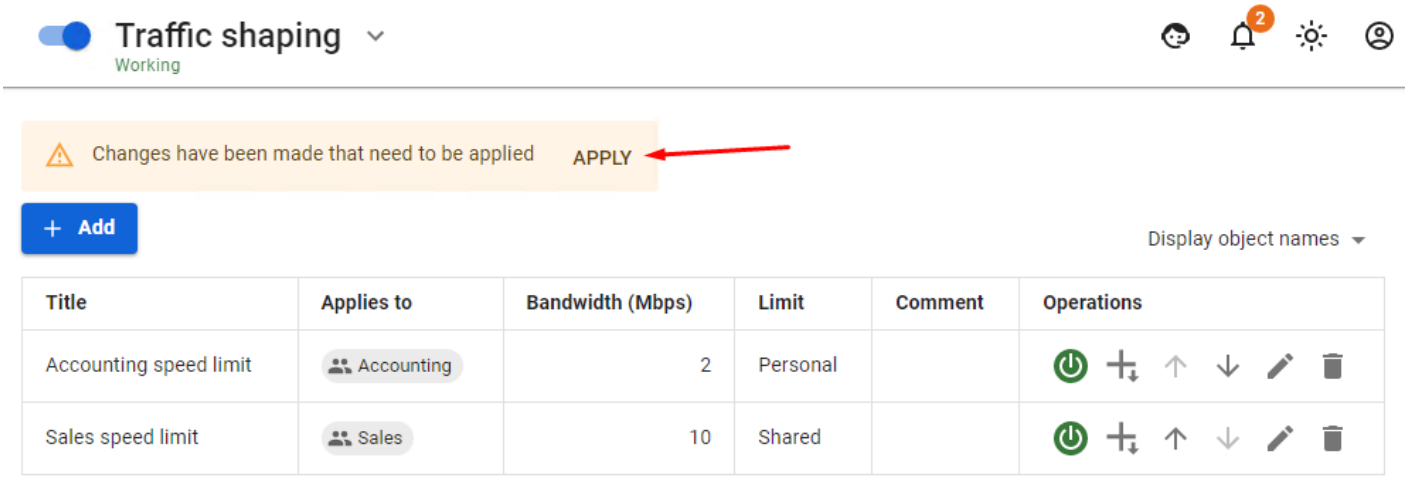
For example, when selecting a personal speed limit, as in the screenshot below, the speed limit for each manager will be 1 Mbps.



If the general speed limit is selected, as in the following example, the channel width for the entire accounting department will be 10 Mbps.



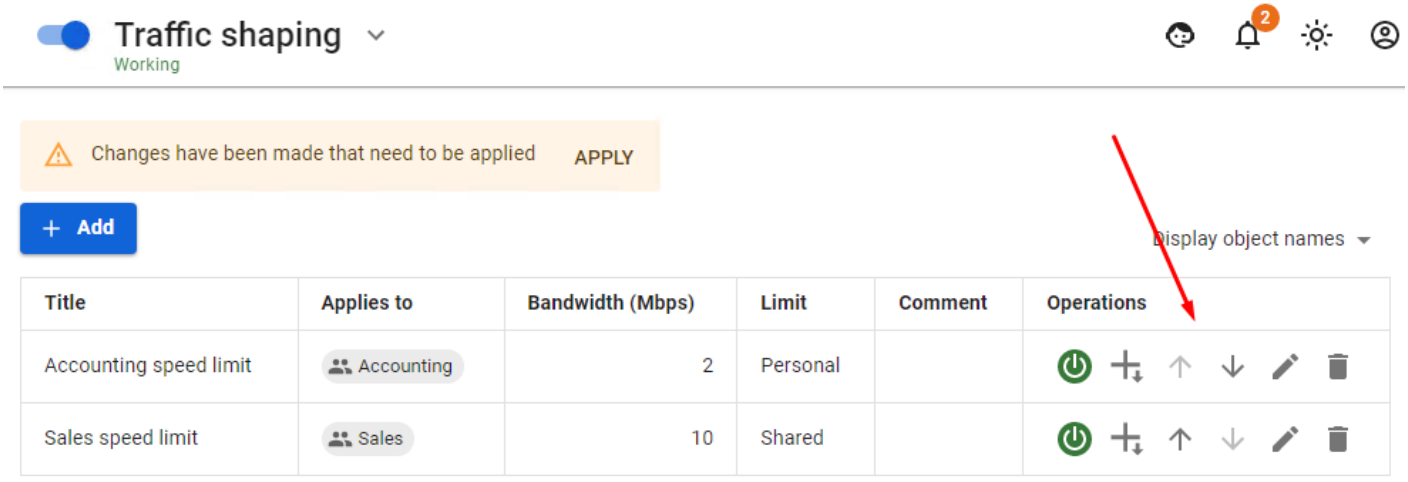
When adding or editing a rule, in order to save and apply it, click on **Apply** above the rules list. The settings will be applied.
Also, do not forget to move the slider in the upper part of the screen near **Traffic Shaping** to **Enabled** in order for the module to work.



If you don't click on **Apply** button above the list of rules and leave the section **Traffic Shaping**, then the created rule will be saved, but will not be applied. To apply the rule, go back to the **Traffic Shaping** section and click on **Apply**.

Also, saved but not applied rules will be lost in the following cases:
- When restarting the server.
- In case of switching to another node.
- When the traffic shaping service is restarted or stopped (in cases when the service has failed or when a technical support employee is working with the service).

You can enable and disable the rule, change its priority, and edit or delete it using the buttons in the **Operations** column.



Order of Rule Application

Rules are applied from top to bottom in their order in the table until the first match. That is, if the user is in several groups simultaneously, the rule that is higher in the rules list applies to them.

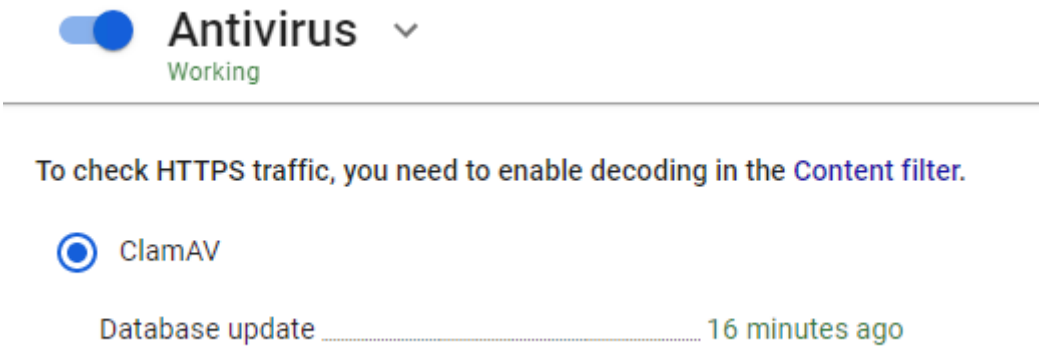
Features

When users connect to SafeUTM from the internet via VPN, the traffic speed to the local network behind SafeUTM may be limited for them according to the Traffic Shaping rules for the end device in the local network.

When users log in from the local network via VPN the Traffic Shaping rules will not apply to them.

Antivirus

For ease of administration, the optimal performance settings of the antivirus module and antivirus filtering settings are pre-configured in the product and do not require manual configuration. If necessary, the settings are optimized in SafeUTM version updates.



The antivirus module is connected to a proxy server and a content filter, so it filters web traffic when the following conditions are met:

- The web resource is not in the proxy server's exclusion lists for its intended purpose.
- The user to whom the traffic is incoming is not included in the proxy server exceptions by source.
- The HTTPS site is checked only if the HTTPS traffic is decrypted by a content filter.

Checking Antivirus Work

You can try downloading test files from the site: **https://www.eicar.org/?page_id=3950**.

If configured correctly, the browser will display an access error.

Intrusion Prevention System

Intrusion detection and prevention system

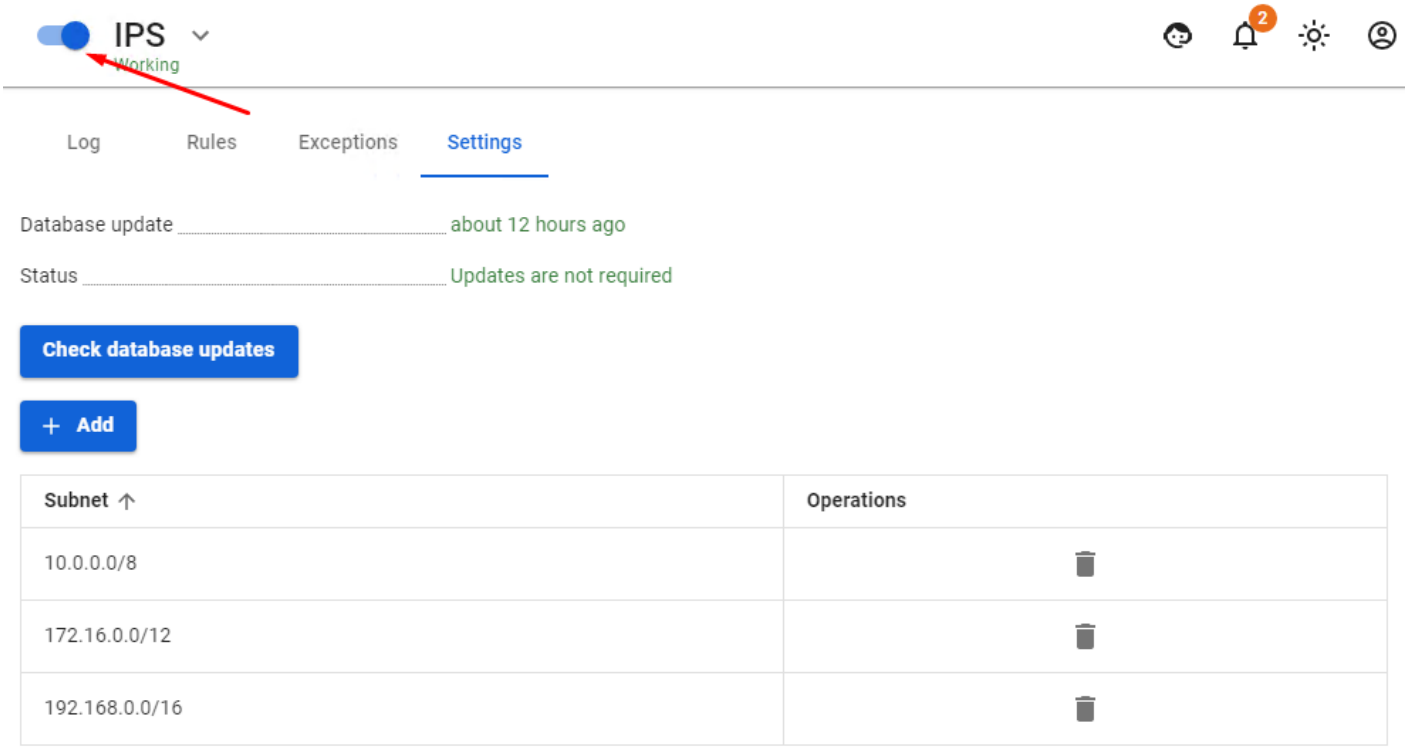
> The intrusion detection and prevention system is only available in the **Enterprise edition of SafeUTM** for users with an active subscription to updates.
>
> **Intrusion prevention system, Application control** rules, and **Traffic shaping** do not handle traffic between local networks and branch networks.

The intrusion prevention system (IDS/IPS, Intrusion detection system / Intrusion prevention system) is designed to detect, log and prevent malicious attacks on the server, integrated services (mail, website, etc.), and local network protected by an internet gateway.

Traffic blocking rules include blocking the activity of Trojans, spyware, botnets, p2p clients and **torrent trackers**, viruses, **TOR** network (used to bypass filtering rules), anonymizers, etc.

You can configure the service in **Traffic Rules -> IPS.**

By moving the switch (to the left of the section name) to the left or to the right you can turn on/off the intrusion prevention service respectively.



In order to add a rule, click on **Add** and add local networks serviced by UTM in the field **Subnet**. As a rule, these are networks of local UTM interfaces, as well as networks of your enterprise's local

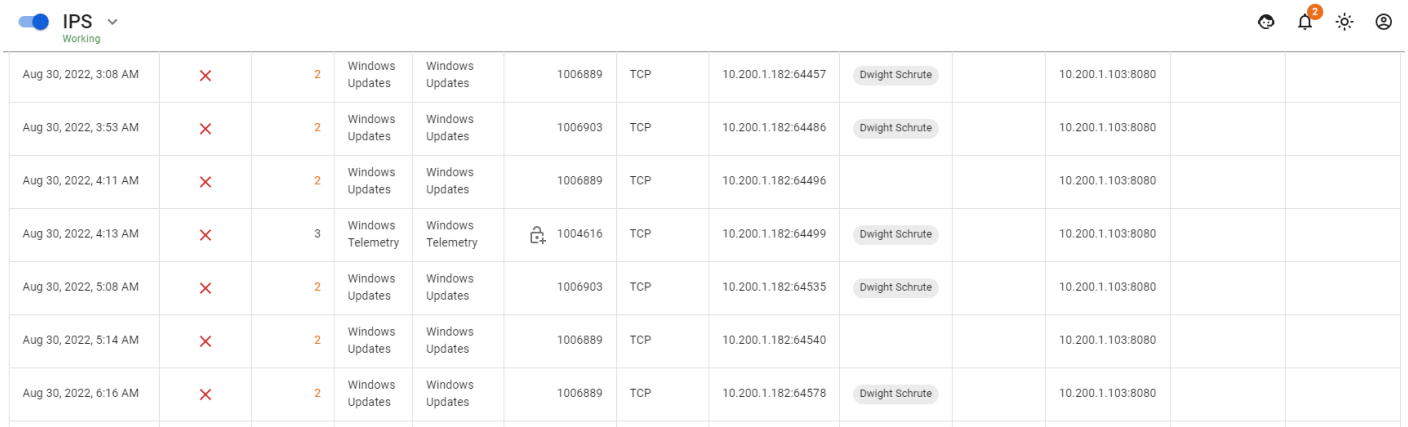
network’s remote segments routed to them.

> Under no circumstances should you specify networks belonging to external UTM network interfaces and external networks. The networks specified here participate in the rules of the intrusion prevention service as local ones characterizing traffic to/from local networks. Local inter-segment traffic is not excluded from the system checks.

When using the intrusion prevention system, **it is not recommended** to use internal DNS servers for the network computers, as the system analyzes DNS queries passing through it and thus determines infected devices. In the case of using an internal AD domain, it is recommended to specify the SafeUTM DNS server on computers as the only DNS server, and specify the Forward zone for the local domain in DNS server settings.

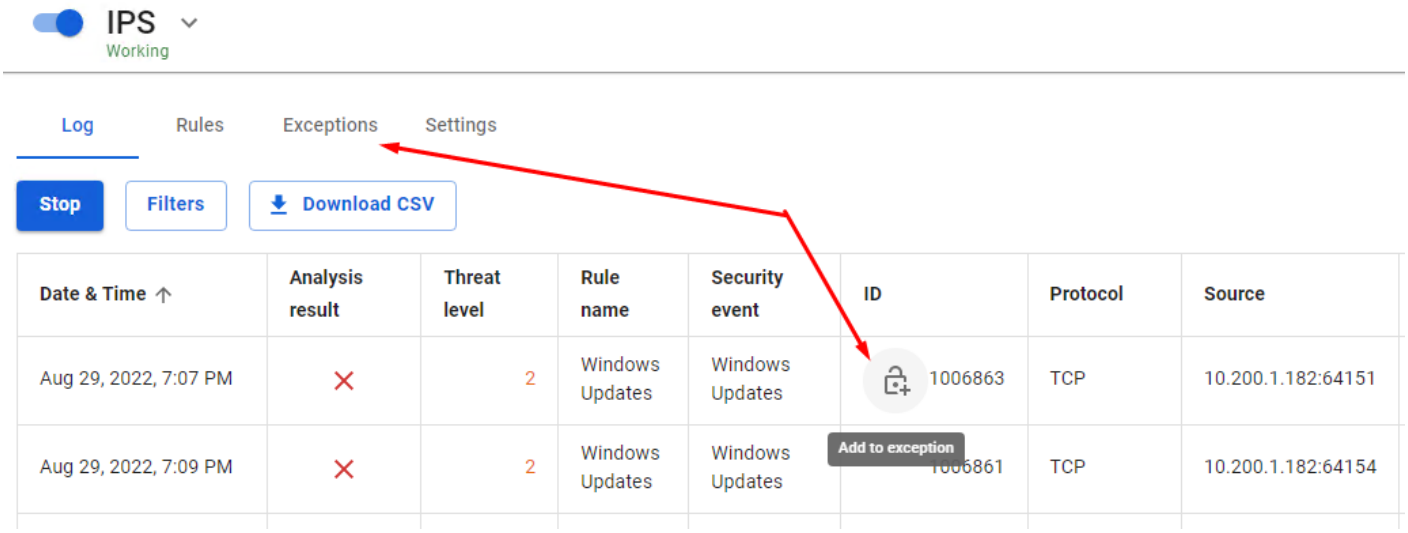
Log

In the **Log** subsection, you can view the intrusion prevention system warning logs.



- **Analysis Result** field displays the system’s action, Blocked — the package is blocked, any other information in the field means Allowed, informing.
- In the field **Threat level** the following values can be displayed:
  - 1 - critical
  - 2 - dangerous
  - 3 – warning
  - 4 - not recognized
  - 255 - not classified

When you hover over the ID column in the line with the rule, the **Add to exception** button (+) will appear, clicking on which the signature will be added to the exclusions:

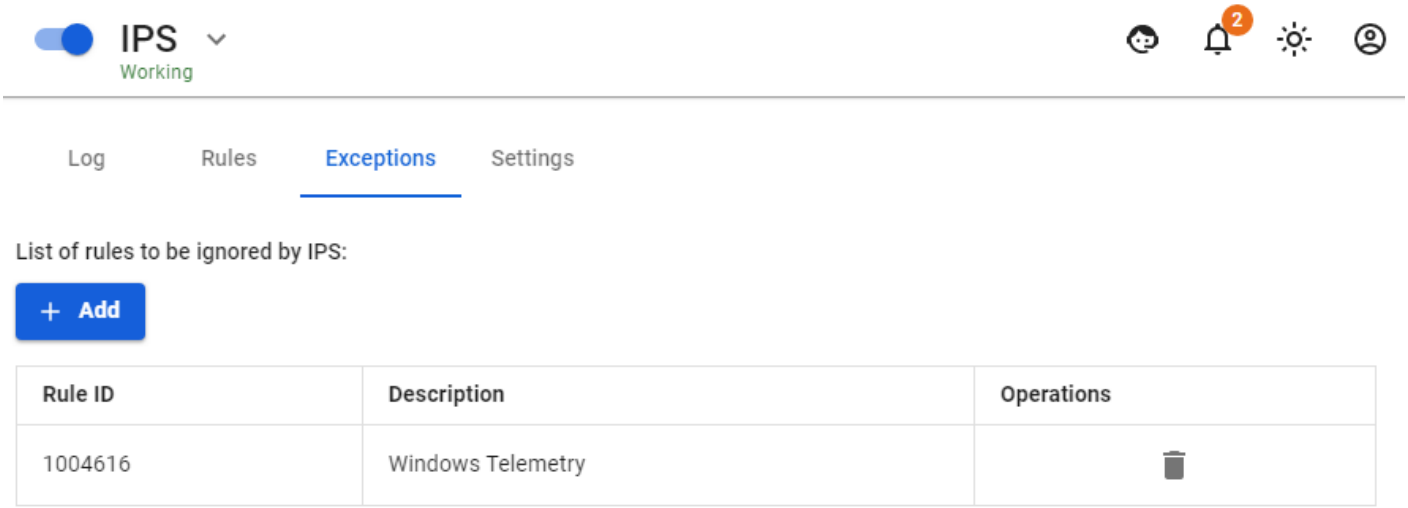


Rules

In the **Rules** tab, groups of rules of the intrusion prevention system are available to view and be enabled/disabled. When enabling/disabling a group of rules, the settings are applied instantly without the need to restart the service.

Exceptions

You can disable certain rules of the intrusion prevention system in case of false positives and for other reasons.



In the **Exceptions** tab, you can add the rule ID (its number, see log analysis example below).

Attention! Over time the rules IDs may change when databases are updated.

Log Analysis Example

In the **Rules** tab, you can open the found group and find the triggered rules in it using its ID.

You can analyze the IP address with which a suspicious connection was attempted via **whois**.

Technical Requirements

The intrusion prevention system requires significant computing resources to operate. Multicore (4 or more cores) processors are preferred. The minimum amount of RAM to use the system is 8Gb.

After turning on the system it is advisable to control that your processor power is sufficient to inspect traffic passing through the gateway.

Objects

In the section **Traffic rules -> Objects**, you can create objects to be used in the rules of firewall, content filter, application control, and routing.

Object types with examples are described in the table below:

Object Types

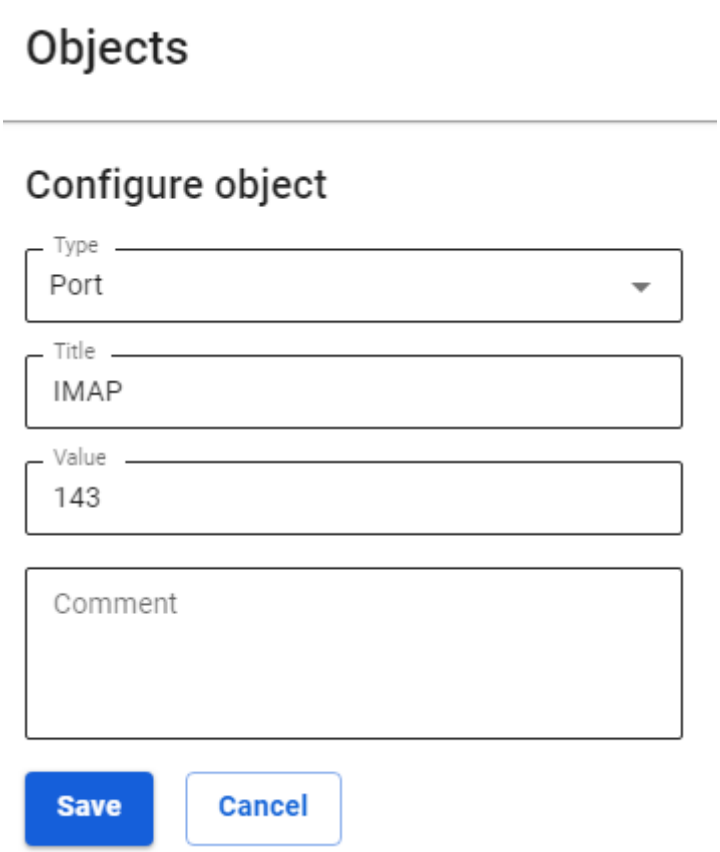
Name	Description	Data Example
IP-address	IPv4 IP address.	10.0.0.1
IP Range	IP address range from the first to the last in the range.	10.0.0.1-10.0.0.25
Subnet	The logical block of IP addressing. The routing prefix is expressed in CIDR notation.	10.0.0.0/24
Domain	A symbolic name used to identify objects on the internet.	google.com
Port	Port number from 1 to 65535.	3389
Port Range	Port range from the first to the last in the range.	1024-65535
Time	Time Range	Mon 9 am – 6 pm
Addresses	A list of objects that may include an IP address, IP address range, subnet, and domain.	10.0.0.1, 10.0.0.4, 10.0.0.126
Port list	Port list.	25, 110, 143, 445, 465, 587, 993, 995
Schedule	List of time ranges	Mon 9am – 12pm; Tue 1pm – 6pm

Creating Objects

To create an object, follow these steps:

1. Go to **Traffic Rules -> Objects** and click on (**+**) in the upper right corner of the screen.

2. Select the type, name, and value of the object. Optionally, you can specify an arbitrary comment no longer than 128 characters



3. Click on **Save**.

> To create object groups, first, you need to create the objects.

Objects like **IP address** and **Port** can be created directly when creating firewall rules by entering a required IP address or port in the corresponding fields.

Quotas

In SafeUTM, it is possible to use traffic limits for users.

For each quota, you can define its validity period (hour, day, week, month, quarter). It can be assigned to users or groups in the user tree in a separate tab **Quota**. Also in this tab, you can increase and view available traffic for the current period of time and find out when the quota will be reset.

If the quota is assigned to a group, then by default it is assigned to all users of the group, as well as to nested groups. The quota inherited from the group can be changed in the priorities of the nested user or group.

> If the quota is exceeded, users get into the object **Quota Exceeded**. **However, by default, no limits apply to such users.** This is why you need to create a restricting rule for the object **Quota Exceeded** in one or more SafeUTM modules (firewall, content filter, application control, speed limit).

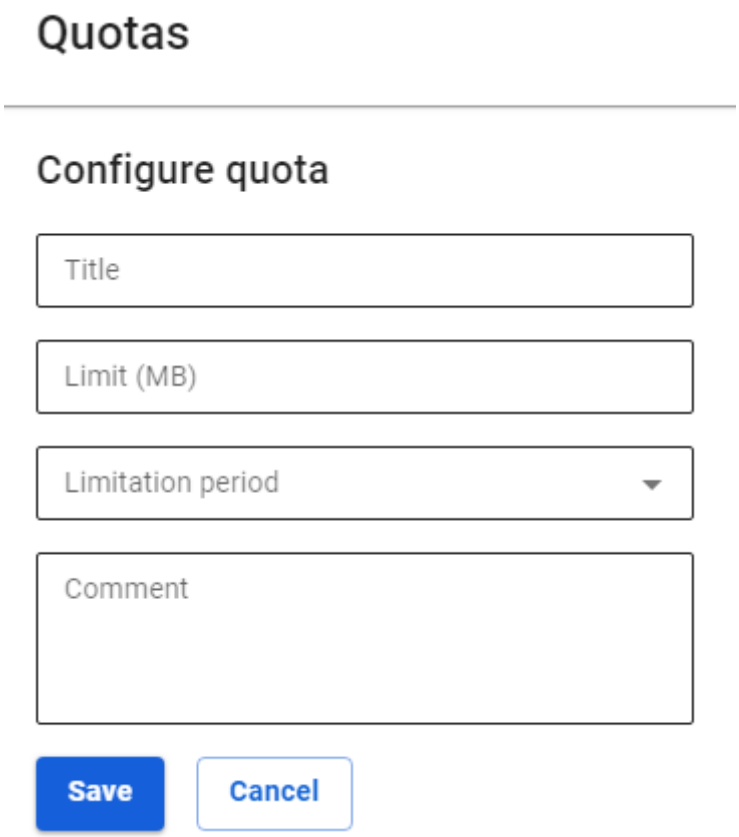
Setting up Quota

In order to set up the quota, follow these steps:

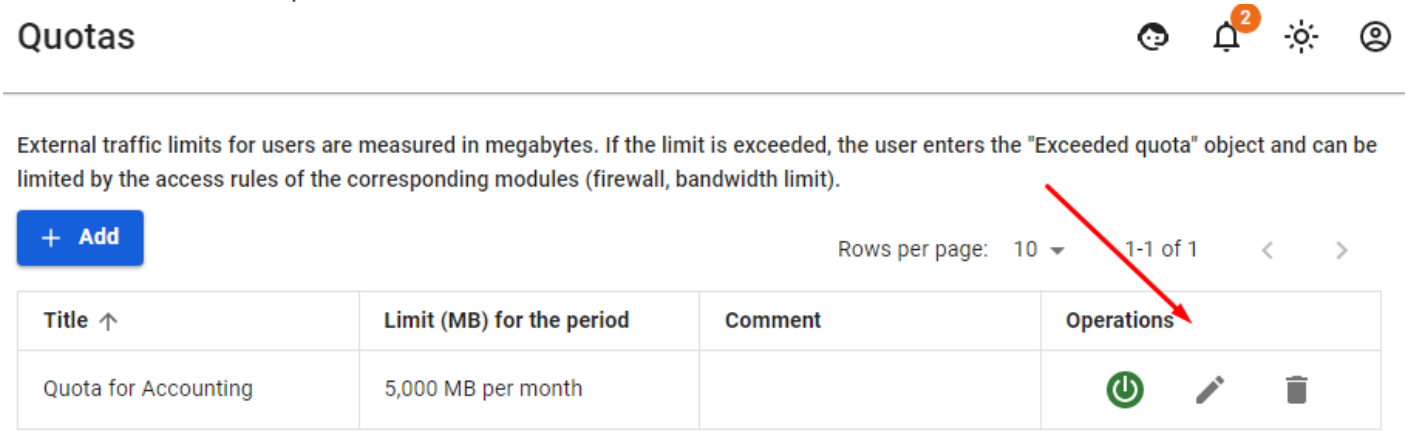
1. Go to **Traffic Rules -> Quotas** and click on **Add**.
2. Fill in the required fields in the quota addition form:

- **Title** – enter a custom quota name.
- **Limit (Mb)** – set a limit of megabytes of traffic for the selected period.
- **Limitation period** – select the validity period for which the quota will be allocated.
  - Hour - each hour
  - Day - from 12:00 am to 11:59 pm
  - Week - from 12:00 am Monday to 11:59 pm Sunday
  - Month - from 12:00 am on the 1st day of the month to 11:59 pm on the last day of the month
  - Quarter - beginning of quarters: January 1, April 1, July 1, October 1

- Check that all the data have been entered correctly and click on **Save**.



You can manage the quota using the buttons in the **Operations** column. You can enable, disable, edit and delete the quota.

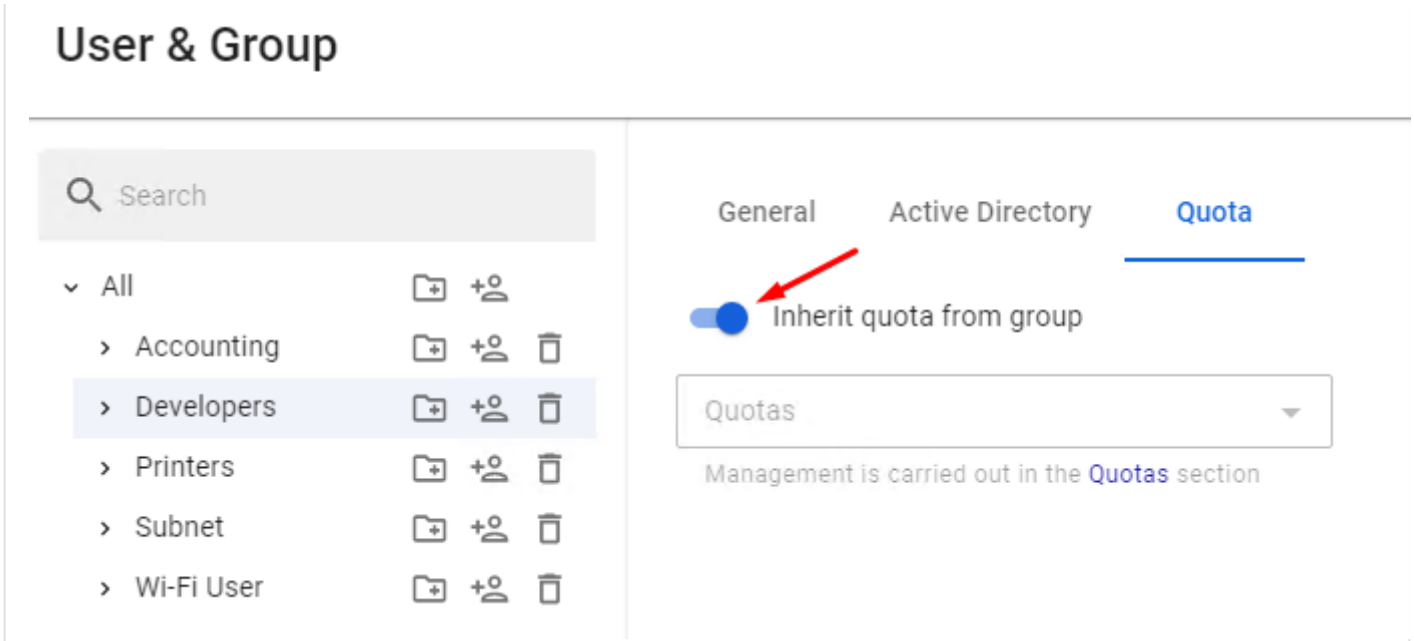


Setting up User and Group

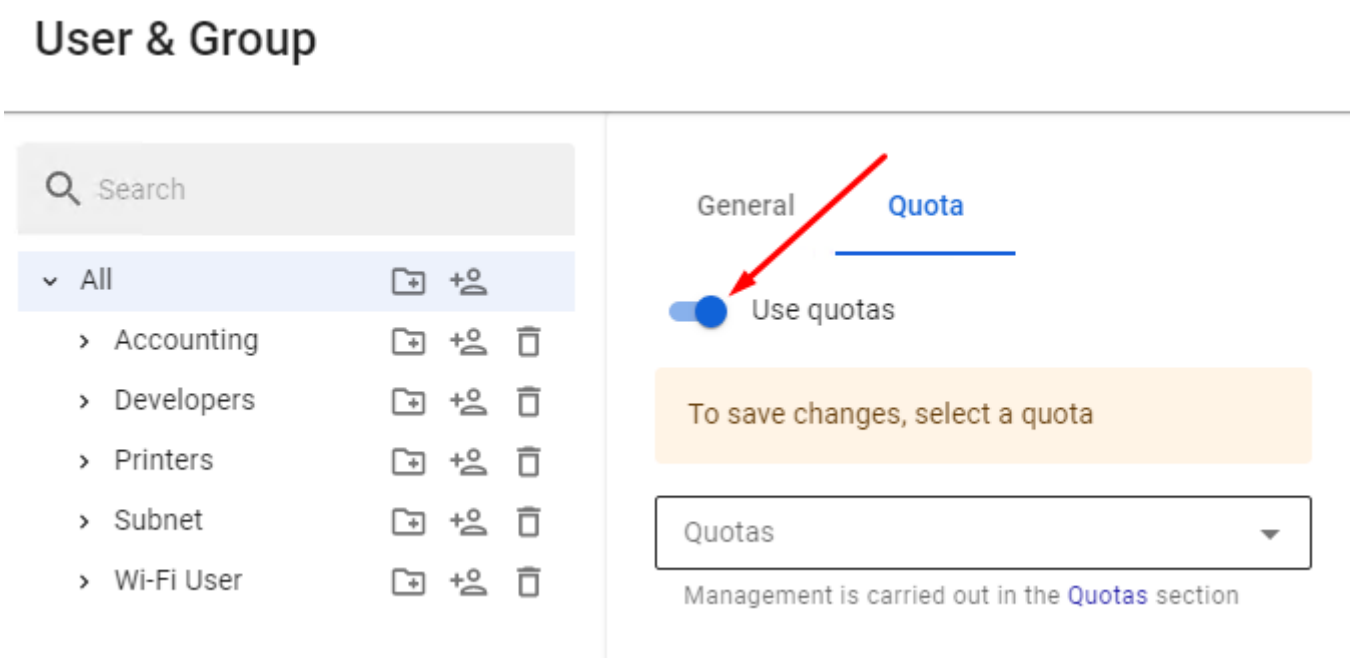
Setting up Group

The created quotas can be applied for groups of users in the tab **Quota**.

You can inherit a quota from the higher-level group, or select another quota by deactivating **Inherit quota from group** switch and selecting the required quota.

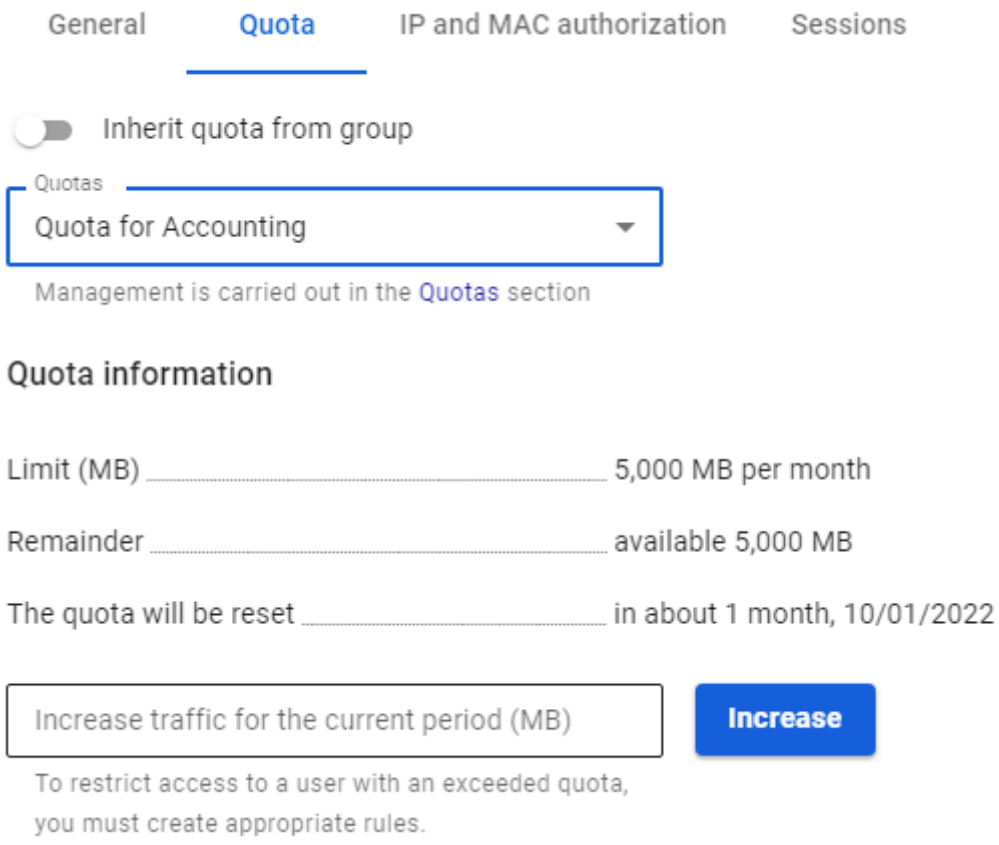


The group **All** has a separate switch **Use quotas**. This parameter allows you to extend the use of quotas to all users.



Setting up Users

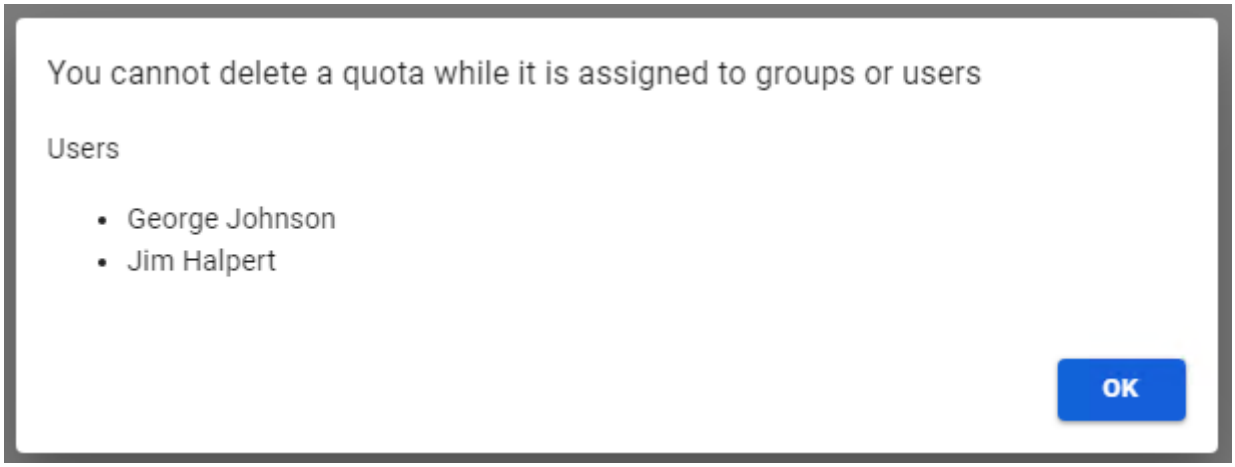
The created quotas can be applied to users. You can manage quotas in the **Quota** tab of the selected user.



In this tab, you can set up inheritance from the group to which the user belongs, or allocate a personal quota to them.

If the quota is allocated to a user, you can view the information about it, i.e. the validity period, available traffic, and the date of quota reset. Here you can also increase it by specifying the required number of megabytes and clicking on **Increase**.

! In order to delete a quota, you need to disable it for all users and groups. Otherwise, if you try to delete it, a window will appear prohibiting such action. The window can be seen in the screenshot below:



Example of Setting up Actions When Quota Is Exceeded

In the example below, we will consider a case when the users having exceeded the quota (those who have fallen into Quota Exceeded object) will be denied access to all social media and video hosting services along with the speed limited to 4 Mbps. However, one user will be allowed access even in case they exceed the quota, as the employee is a marketing specialist.

1. First, you need to create a quota with a limit of 2,000 Mb per day.
2. In all groups and all users in **Quota,** the tab turns the switch to the **Inherit quota from group** to the ‘enabled’ position. It needs to be done only if you changed the switch position because by default all groups and users are created with the switch in the ‘enabled’ position.
3. Assign the created quota to the group **All** (all other groups and users will inherit the assignment of this quota).
4. Create a rule in the **content filter** to restrict access to social networks and video hosting services for users who have exceeded the quota.
5. Create a rule that allows one of the users' access to social networks even if they have exceeded the quota.
6. Create a rule that **limits the speed** for all users that is in the object **Quota Exceeded** down to 4 Mbps.