Содержание

6 Filtering rules management interface

Universal Locking Rules UI

Introduction

Universal locking rules (ULR) UI is designed to manage filtering rules on multiple DPIs simultaneously using a graphical interface.

Installation

Equipment or virtual machines with the following characteristics are suitable for the subsystem:

1. CPU 2.5 GHz, 2-4 cores
2. RAM from 8 GB (mainly for sphinx)
3. Hard drive (HDD) 50 GB - 250 GB
4. Cent OS 7+ operating system (we do not recommend to not install minimal, because most of the dependencies will have to be installed manually)
5. Network Card (NIC) from 10 Mbps

We recommend Cent OS 7+ operating system. **Do not not install minimal, because most of the dependencies will have to be installed manually.** If you need to install software on Cent OS 6, make sure that supervisor 3+ is installed. If you do not have the package, please contact technical support.

The locking rules management interface is a special section of The VAS Experts DPI Graphical User Management Interface ver.2. The installation is similar to the script of The VAS Experts DPI Graphical User Management Interface ver.2.

Configuration

.env Configuration

The subnet configuration is handled with .env file.

```
/var/www/html/dpiui2/backend/.env
```

The file contents:

```
#Redirect URL for "White list" service
ULR_WHITE_LIST_REDIRECT_URL=https://google.com

#The period after Ulr tasks data is deleted (days)
ULR_QUEUE_DELETE_TASKS_DAYS_INTERVAL=1

#ASN for IP-exception rules
ULR_IP_EXCLUDE_ASN=64401

#The host for blocked resources list deployment. To connect the blocked
resources server.
ULR_BLACK_LIST_DEPLOY_HOST=<IP address or host of global locks web-server>

#The port for blocked resources list deployment. To connect the blocked
resources server.
ULR_BLACK_LIST_DEPLOY_PORT=22

#Username for blocked resources list deployment. To connect the blocked
resources server.
ULR_BLACK_LIST_DEPLOY_USER=default

#Password for blocked resources list deployment. To connect the blocked
resources server.
ULR_BLACK_LIST_DEPLOY_PASS=

#To use sudo for blocked resources list deployment. (0 - do not use, 1 -
use)
ULR_BLACK_LIST_DEPLOY_SUDO=1

#Black lists saving path.
ULR_BLACK_LIST_DEPLOY_PATH=/var/www/html/blacklists/

#Log Detail Level (0 - info, 1 - debug, 2 - tracing).
ULR_LOAD_LOG_LEVEL=0
```

After changing the .env file, you need to run the command

```
php /var/www/html/dpiui2/backend/artisan queue:restart
```

These settings can be added to the configuration in the Administrator → DPIUI2 Server Configuration section in the The VAS Experts DPI Graphical User Interface ver.2.

Key Installation

To use the Universal Locking Rules UI, you need to activate the ULR-license in DPIUI2 with a command:

```
dpiui2 ulr_lic --make=1
```

Next:

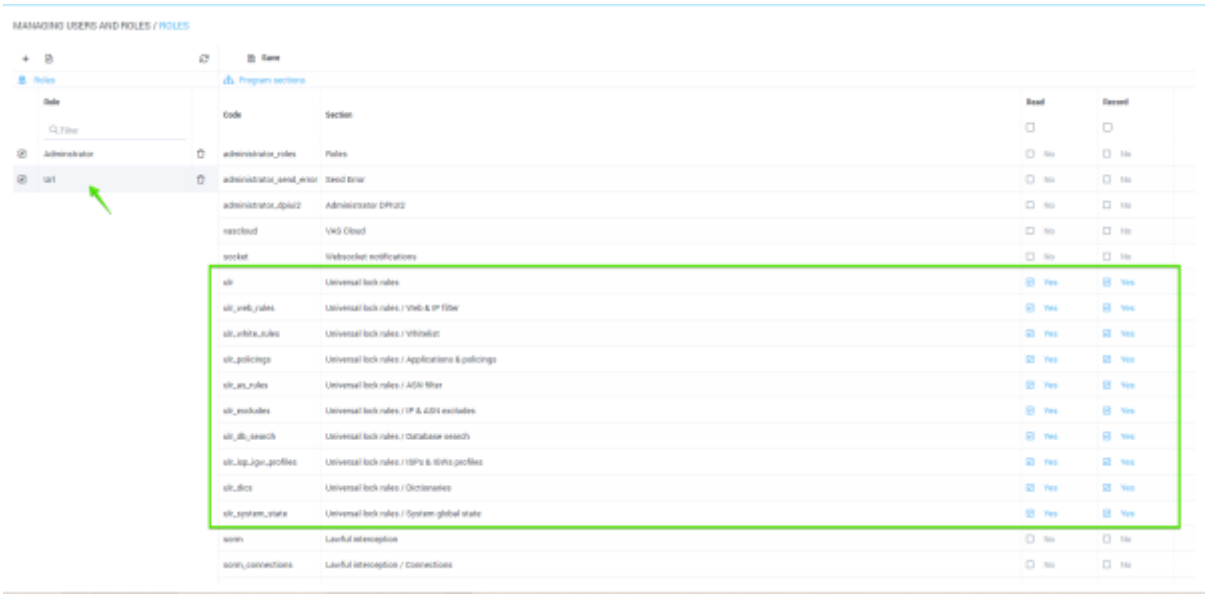
1. Enter license level: standard
2. Enter the license completion date in the Y-m-d format (e.g. 2099-12-31)
3. Enter the license password.

If the data is correct, a success message will be displayed:

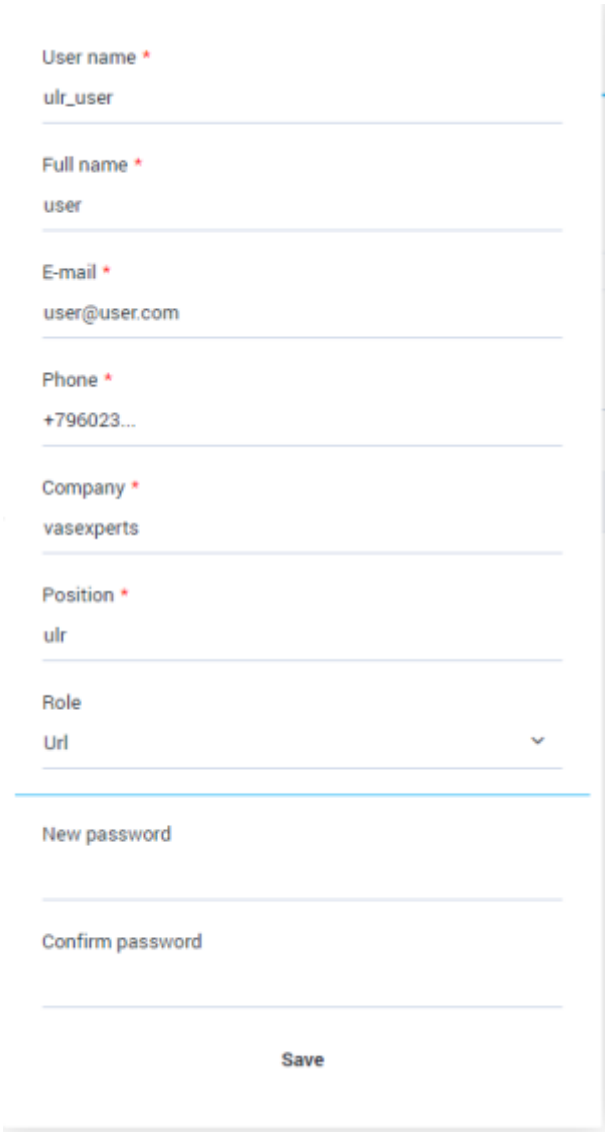
```
dpiui2 ulr_lic --make=1
 Enter level:
 > standard

 Enter expire date in Y-m-d format:
 > 2099-12-31

 Enter password:
 >

stdClass Object
(
    [success] => 1
)
```

Roles Management

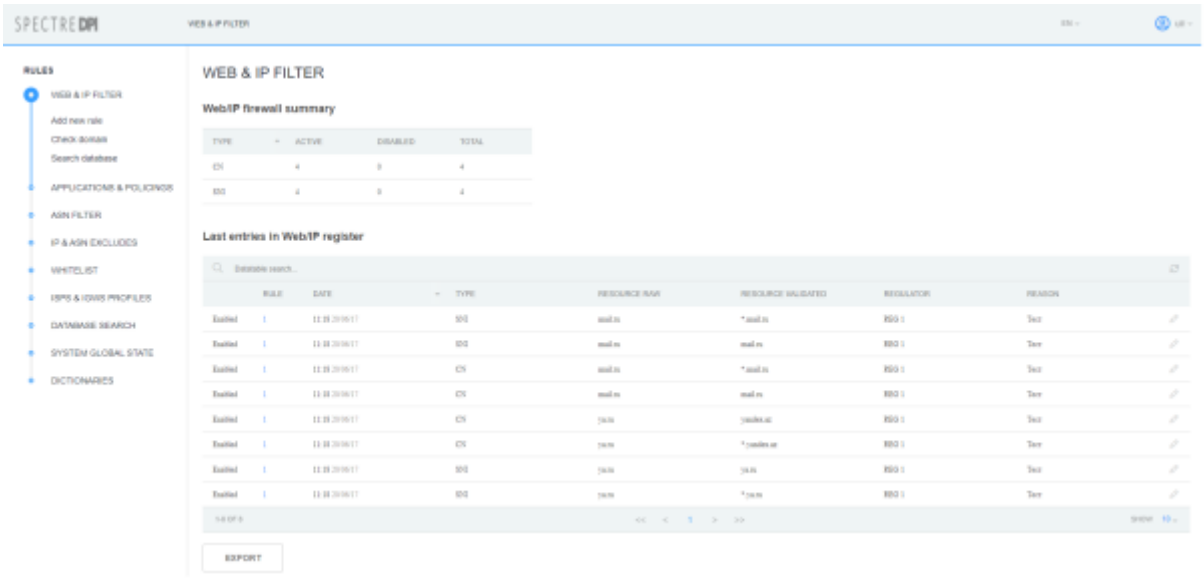
In the DPIUI2 interface visit the Administrator → Roles section. Create a new role and set read and write permissions in the ulr_admin section:



Next, go to the Administrator→ Users section. Create a new user and set him the role that you created earlier.



After the user logs in, he is moved to the locking rules management section.



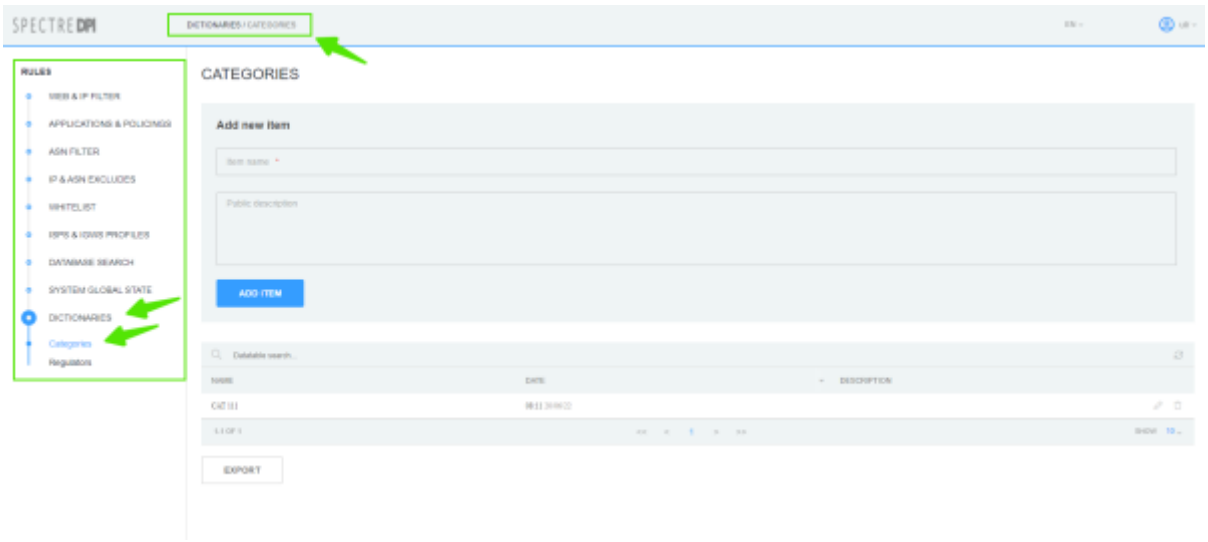
Dictionaries Configuration

- Category Dictionary
- Regulators Dictionary

These dictionaries are used for creating/editing locking rules.

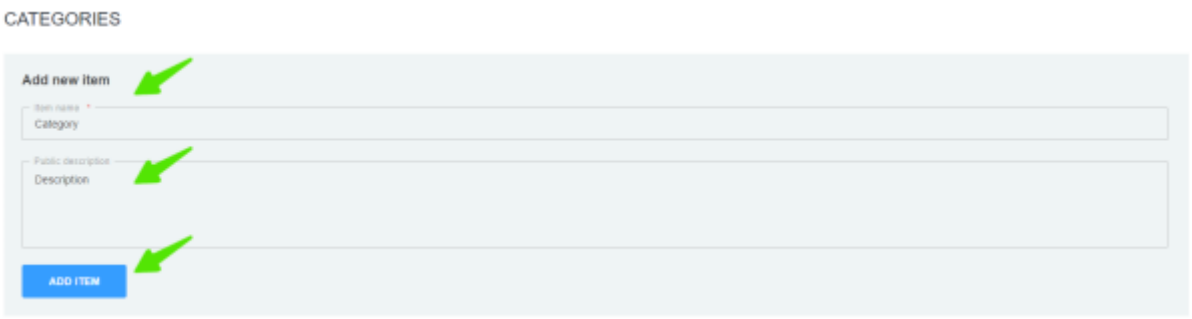
Category Dictionary

In the Locking Rules management interface go to the Dictionaries → Categories section.



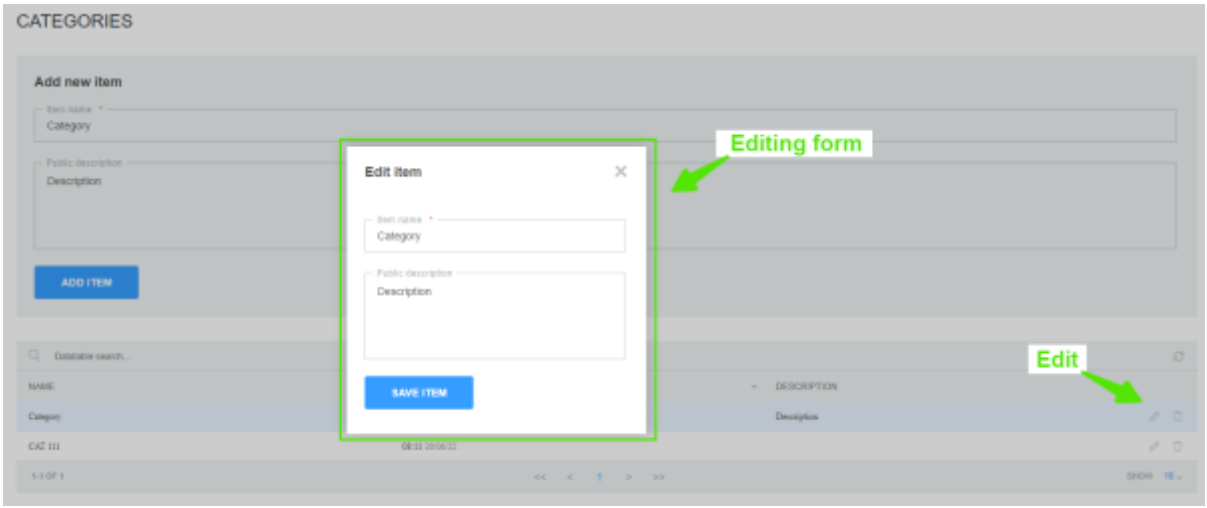
Creating

Fill in the form with category name and description and click the "Add" button.



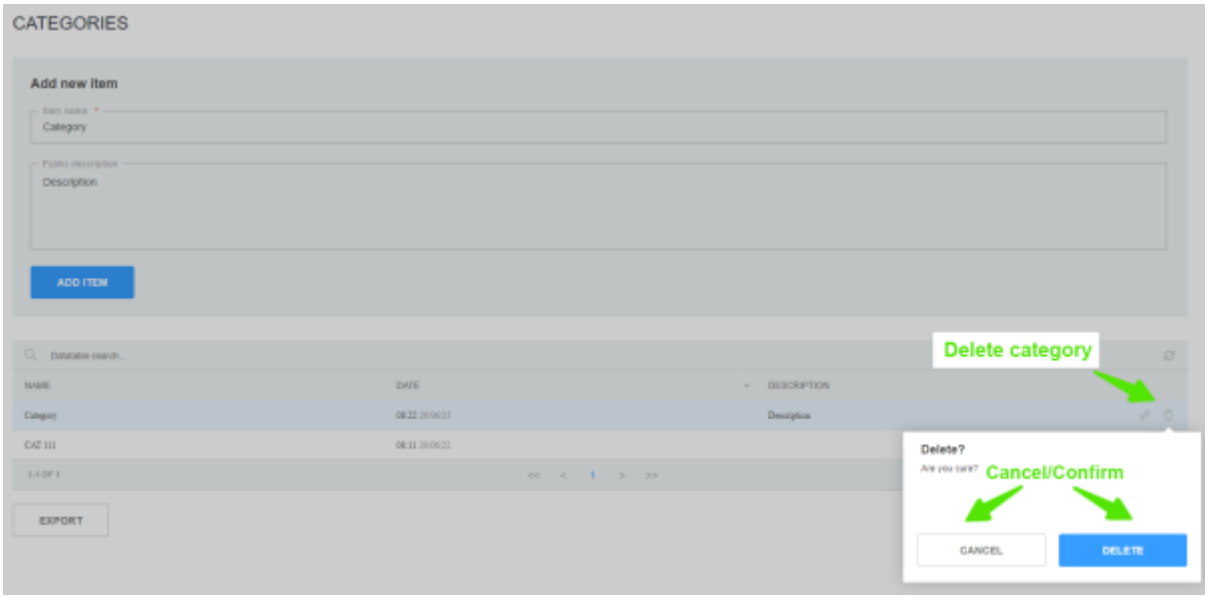
Editing

To edit: click on the category editing button in the categories table. In the form, change the name and/or description of the category, then click the "Save" button.



Deleting

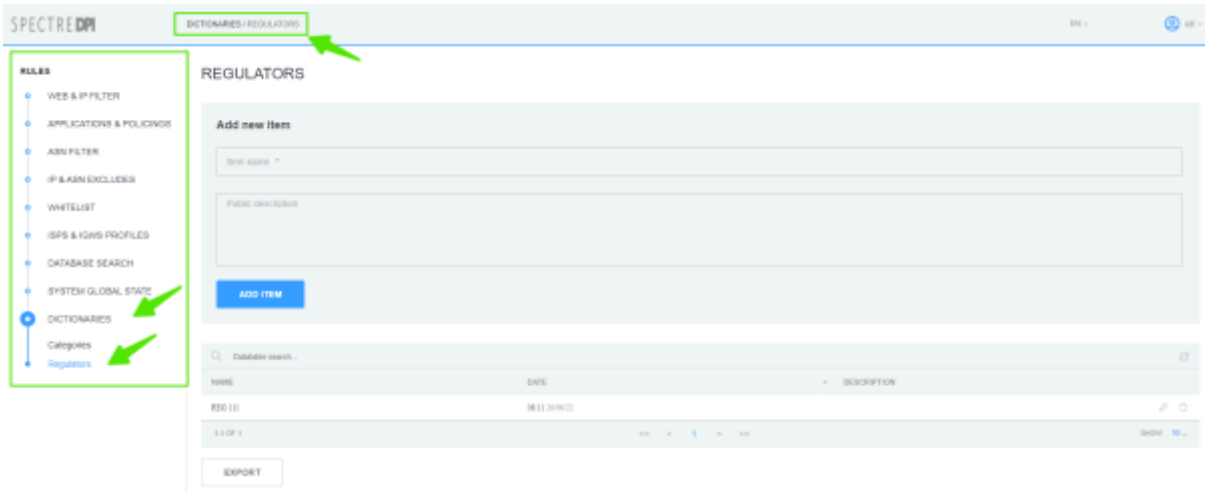
Click on the delete category button in the categories table. In the pop-up window confirm or cancel the action.



Attention: Before deleting a category, make sure there are no rules referring to this category!

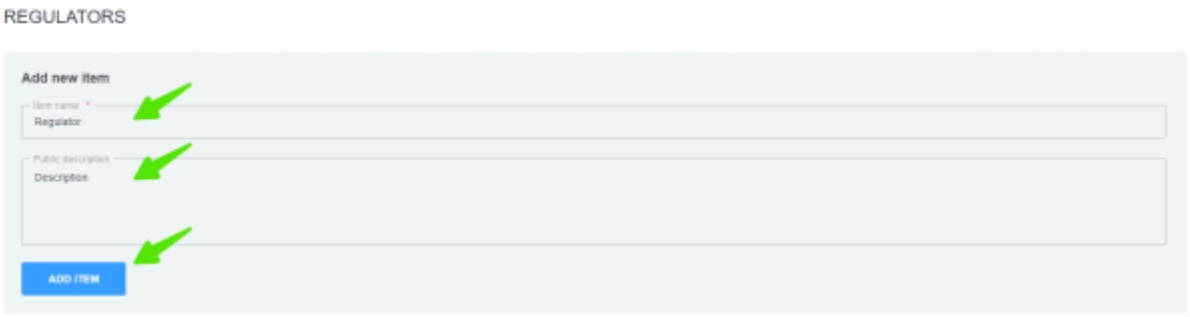
Regulators Dictionary

In the Locking Rules management interface go to the Dictionaries → Regulators section.



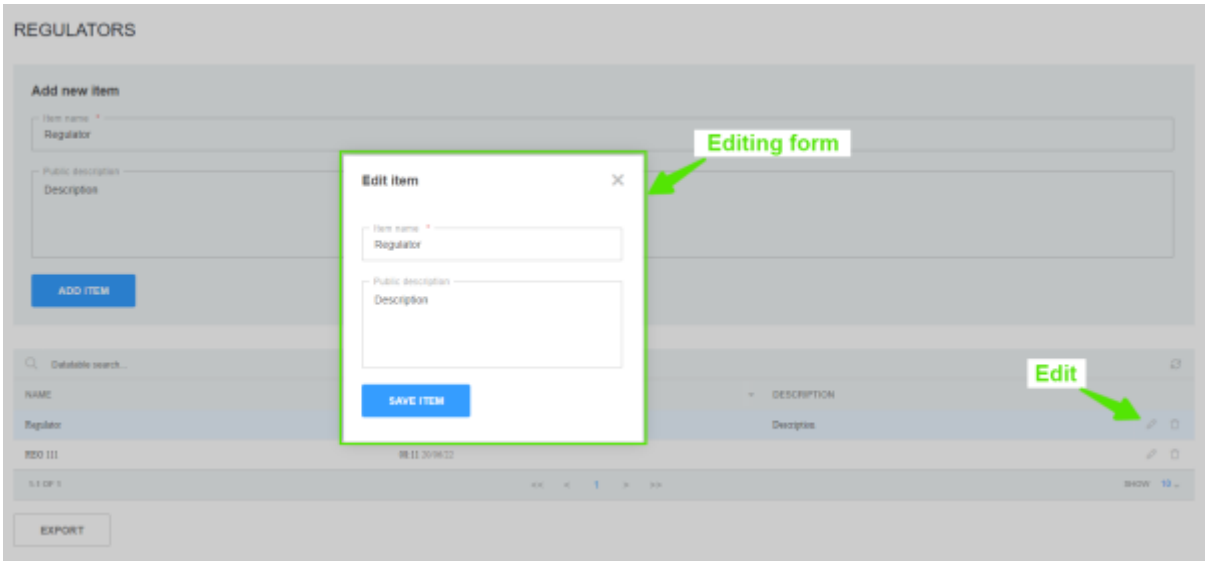
Creating

Fill in the form with regulator name and description and click the "Add" button.



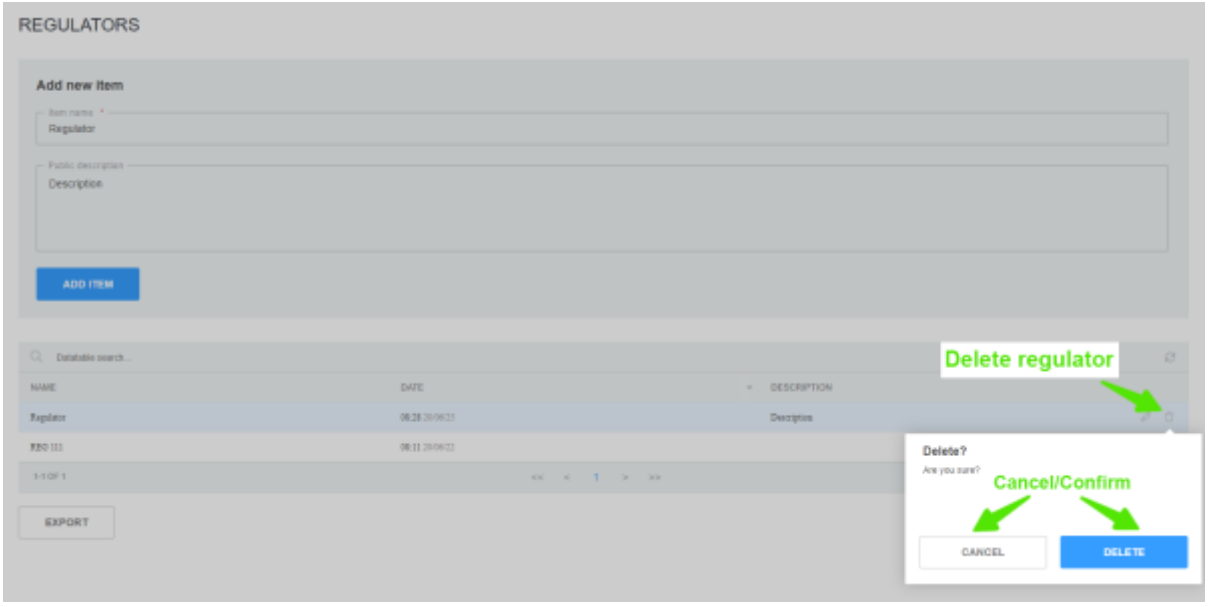
Editing

To edit: click on the regulator editing button in the regulators table. In the form, change the name and/or description of the regulator, then click the "Save" button.



Deleting

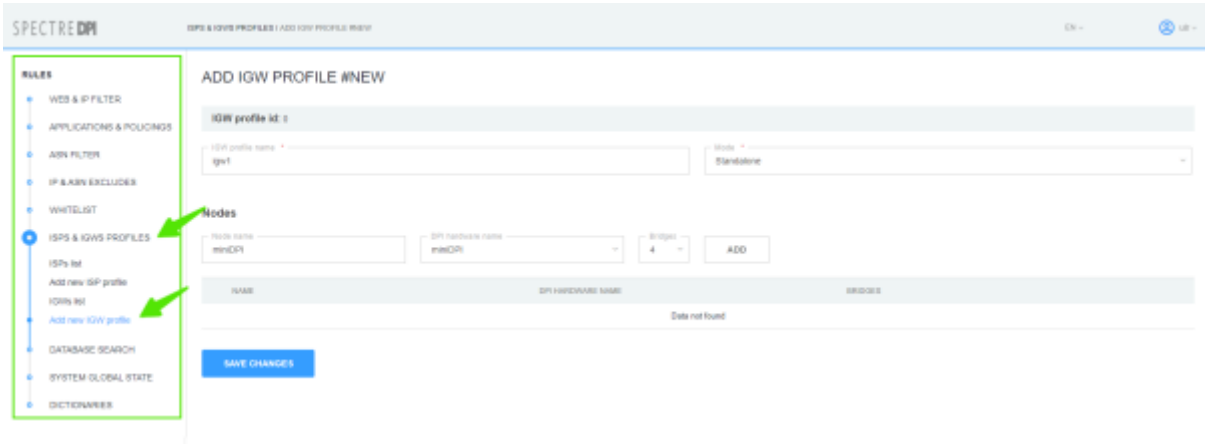
Click on the delete regulator button in the categories table. In the pop-up window confirm or cancel the action.



Attention: Before deleting a regulator, make sure there are no rules referring to this regulator!

IGW Profiles Management

Change to the section "ISPS & IGWS Profiles" → "IGWs List".



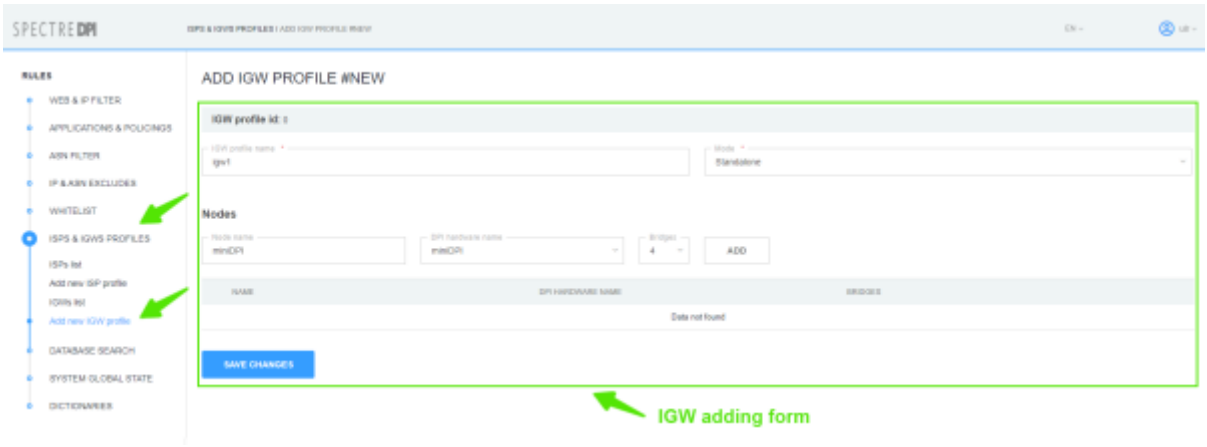
Creating

To create new IGW profile change to the section "ISPS & IGWS Profiles"→"Add new IGW profile".

In the form specify:

- Profile name;
- Operation mode (Standalone/Cluster)

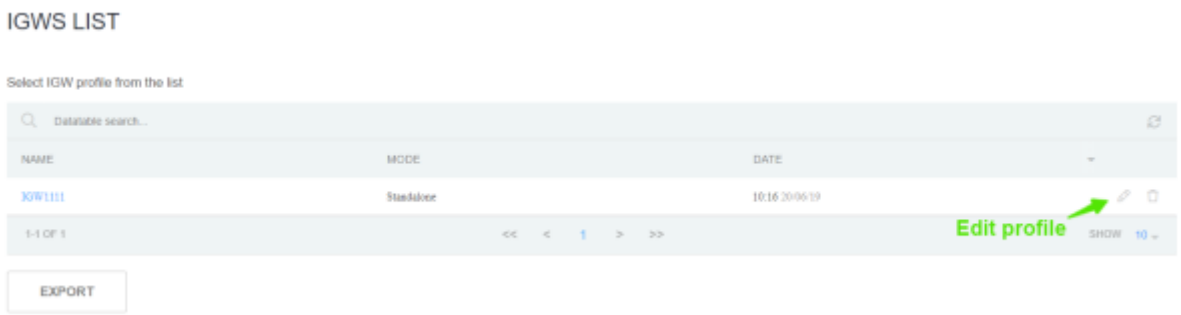
- Nodes for the profile (Node name, DPI from the list of available equipment and number of bridges)



Before creating IGW profile add FastDPI server in the main section of DPIUI 2 Administrator -> Devices

Editing

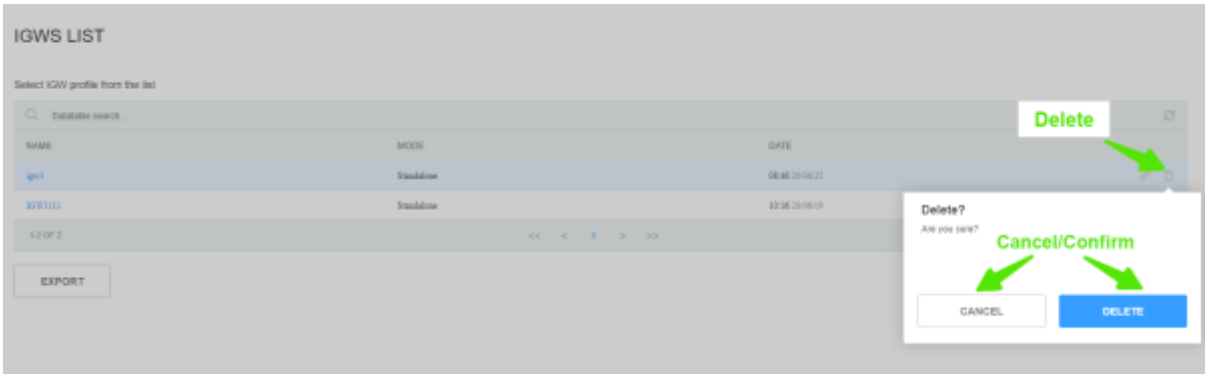
In the "ISPS & IGWS Profiles" → "IGWs List" section click the button "Edit profile".



The IGW profile creation/editing form will open. Make the changes you need and click "Save Changes".

Deleting

In the "ISPS & IGWS Profiles" → "IGWs List" section click the button "Delete" and confirm/cancel the operation.



Attention: Before deleting a profile, make sure there are no ISP profiles referring to this category!

Web Server for Global Lists Configuration

Web-server

1. Prepare a machine with CentOS7+ installed

2. Create a sudo user without password as described in Dpiui2: DPI connection details section

3. Run the script:

```
rpm --import http://vasexperts.ru/centos/RPM-GPG-KEY-vasexperts.ru
rpm -Uvh http://vasexperts.ru/centos/6/x86_64/vasexperts-repo-1-0.noarch.rpm
yum install dpiutils -y
yum install httpd -y
yum install unzip -y

mkdir /var/www/html/blacklists
chmod -R 777 /var/www/html/blacklists

echo "
<VirtualHost *:80>
    DocumentRoot \"/var/www/html/blacklists\"

    <proxy *>
    Order deny,allow
    Allow from all
    </proxy>
</VirtualHost>
" > /etc/httpd/conf.d/bl_lists.conf

firewall-cmd --permanent --add-port=80/tcp
firewall-cmd --reload
```

```
systemctl enable httpd.service
systemctl restart httpd.service
```

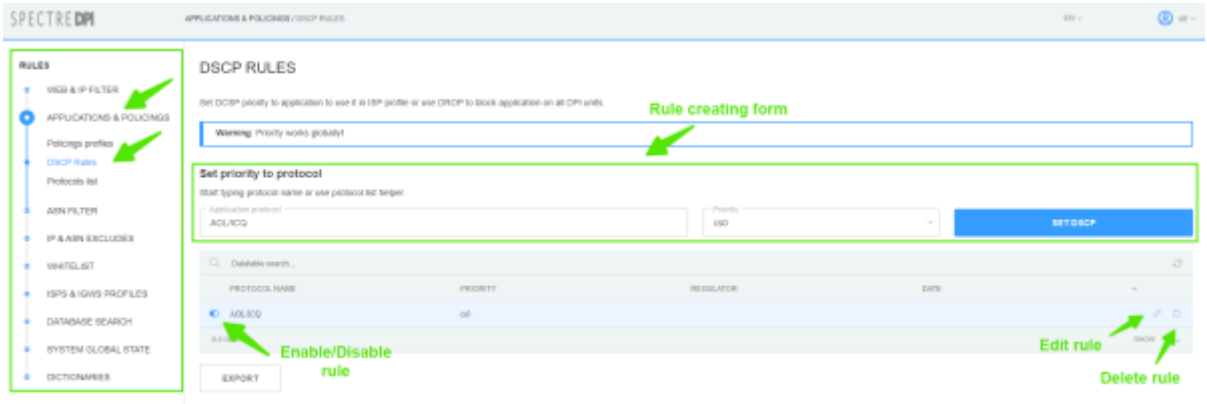
4. In dpiui2 configuration specify the web-server access parameters in ULR settings section

5. Specify the path to Custom lock list in the settings of all connected FastDPI servers:

```
# URL dictionary for blocking by HTTP (custom_url_black_list)
custom_url_black_list=http://<IP address of Web-server>/blacklist.dict

# Names dictionary for blocking HTTPS protocol by certificate
(custom_cname_black_list)
custom_cname_black_list=http://<IP address of Web-server>/blacklistcn.dict

# IP addresses dictionary for blocking HTTPS by IP (custom_ip_black_list)
custom_ip_black_list=http://<IP address of Web-server>/blacklistip.dict

# Host names dictionary for blocking HTTPS by SNI (custom_sni_black_list)
custom_sni_black_list=http://<IP address of Web-server>/blacklistsni.dict
```

DSCP Rules

Change to "Applications and policings" section → "DSCP Rules".



Creating

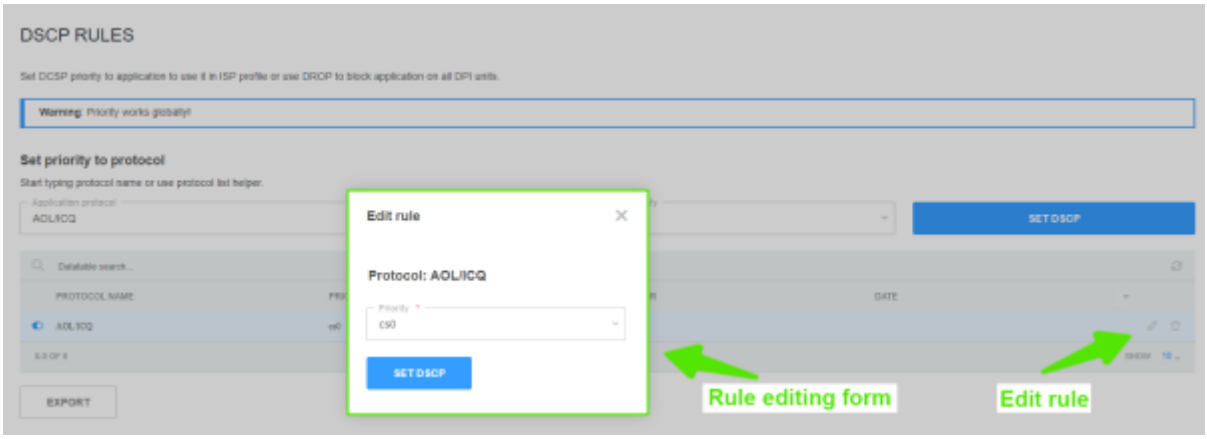
In the form of rule creating:

- Enter the name of application protocol and choose one from the list;
- Choose the priority from the list.

Save the rule by clicking on "Set DSCP" button.

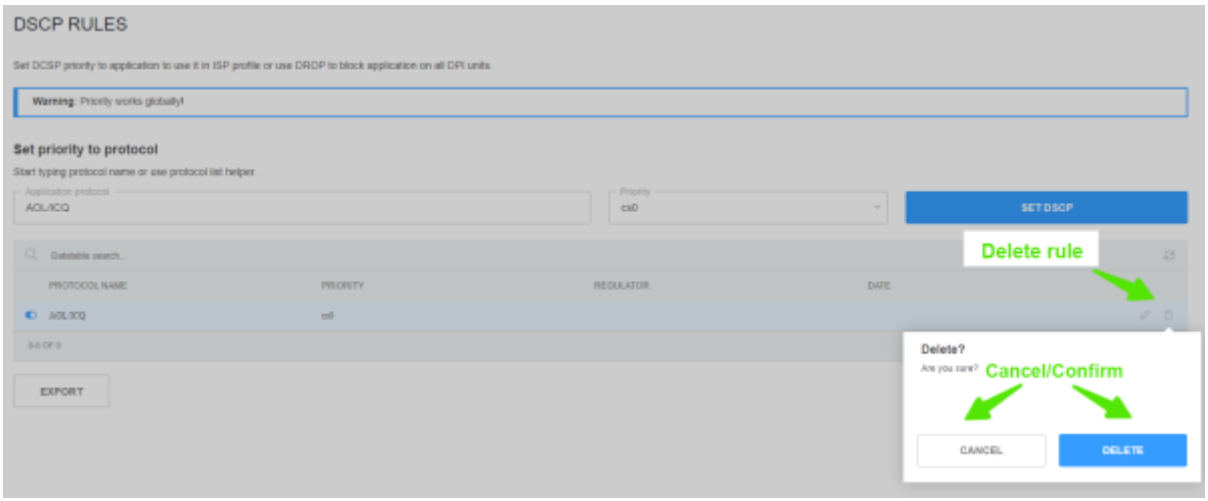
Editing

In the list of DSCP rules click on "Edit rule" button. In the popup editing form set the necessary priority and save changes by clicking on "Set DSCP" button.



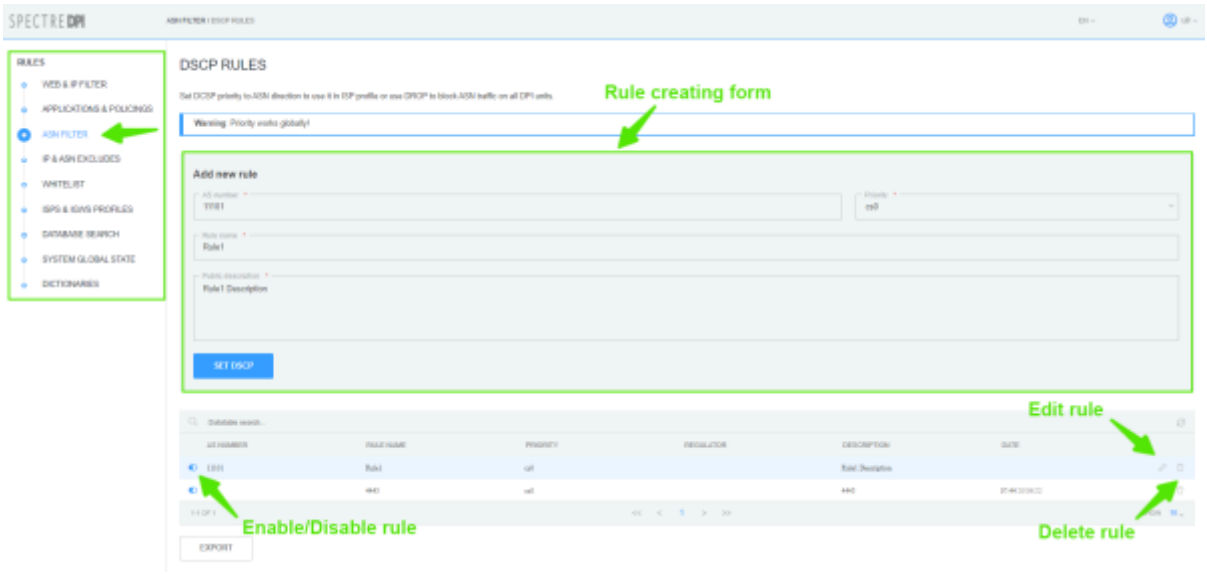
Deleting

In the DSCP rules list click the button “Delete rule” and confirm/cancel the operation.



ASN Filter

Change to the "ASN Filter" section.



Creating

In the form of rule creating:

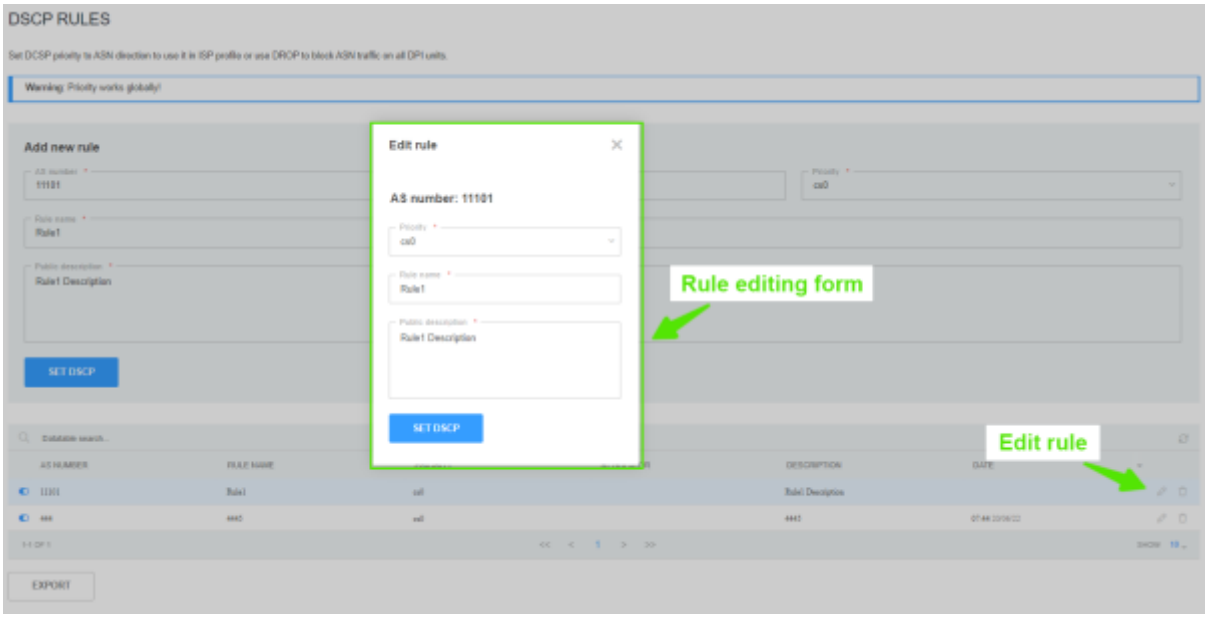
- Specify the number of AS;
- Choose the priority from the list;
- Enter the rule name;
- Enter the rule description.

Save the rule by clicking on "Set DSCP" button.

Editing

In the list of DSCP in ASN direction rules click on the "Edit rule" button. If necessary, in the popup editing form:

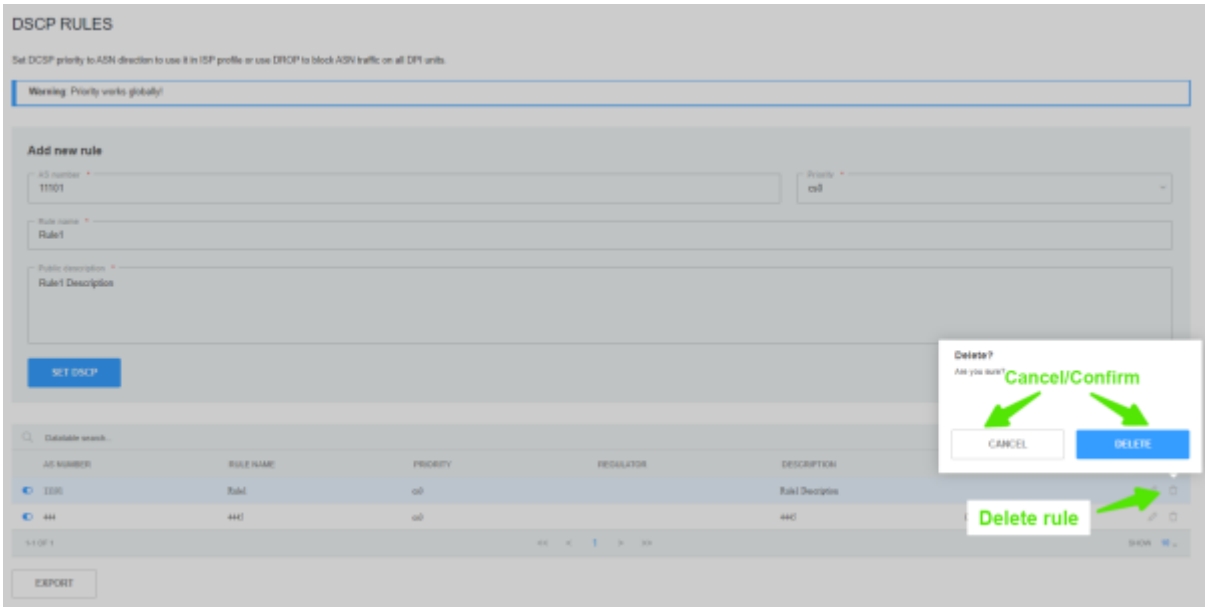
- choose the priority from the list;
- Enter the rule name;
- Enter the rule description.



Save the changes by clicking on "Set DSCP" button.

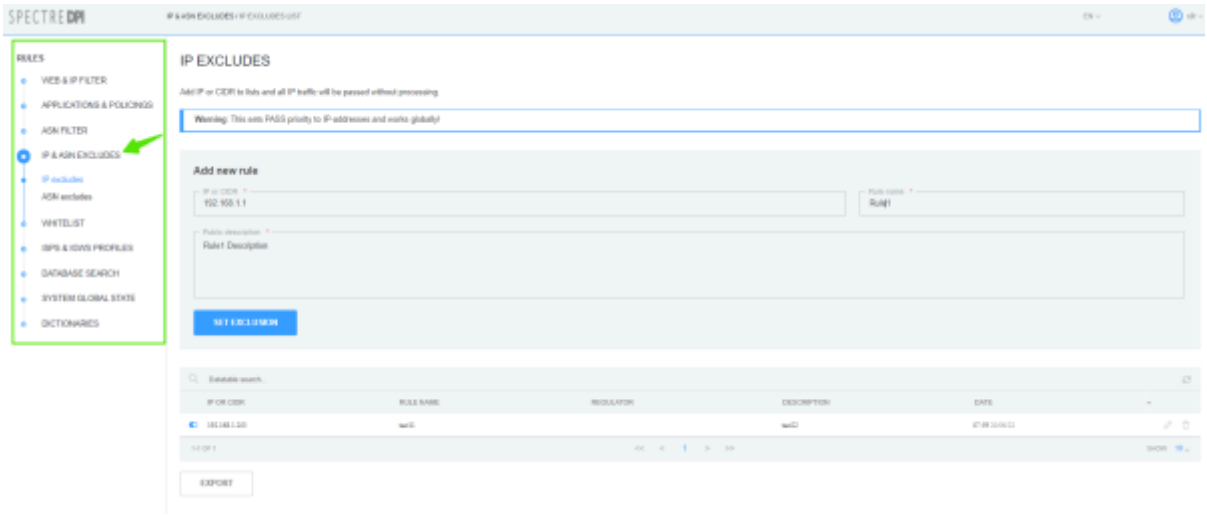
Deleting

In the list of DSCP in ASN direction rules click the button “Delete rule” and confirm/cancel the operation.



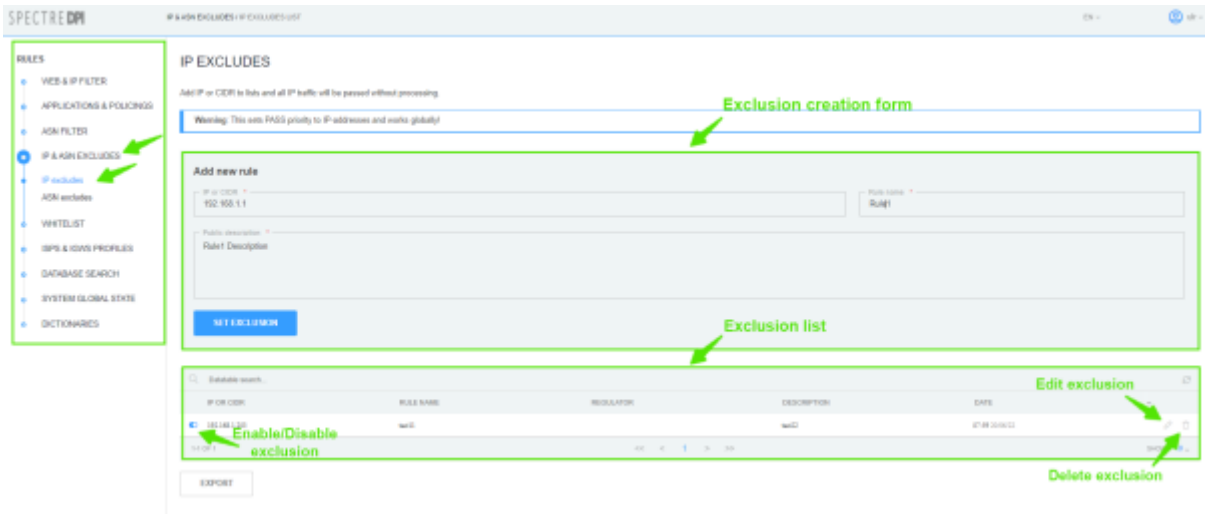
IP & ASN Excludes

Change to the "IP & ASN Excludes" section.



IP Excludes

Change to the "IP & ASN Excludes" section → "IP Excludes".



Creating

In the form of rule creating:

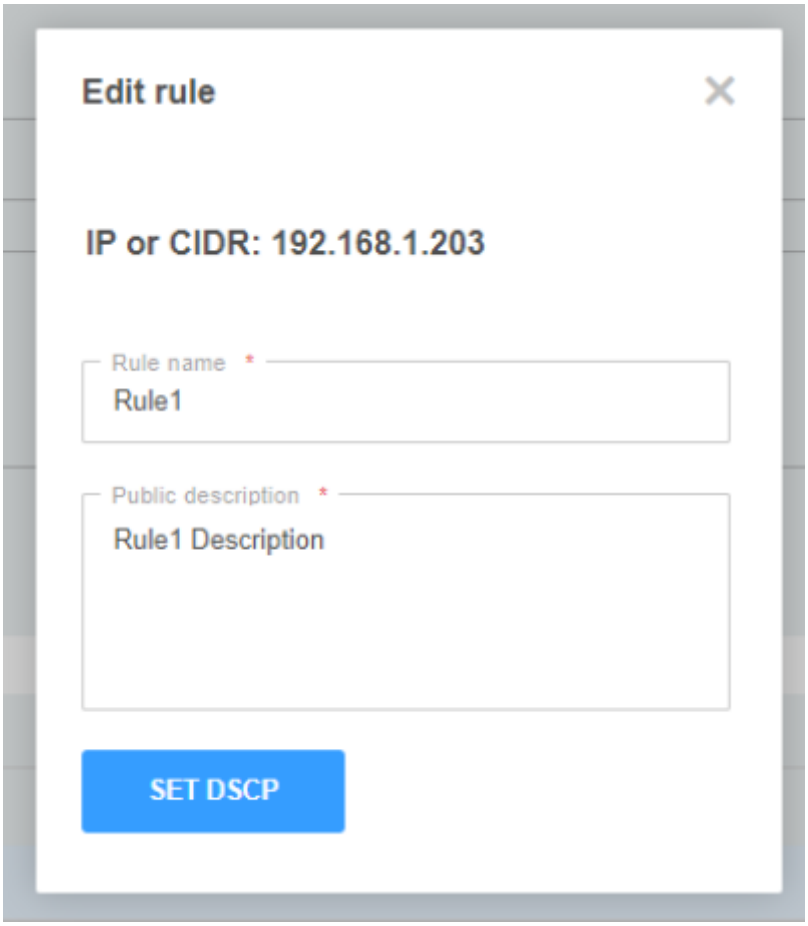
- Specify IP/CIDR;
- Enter the rule name;
- Enter the rule descriptuin;

Save the rule by clicking on "Set exclusion" button.

Editing

Click on the button "Edit exclusion". In the form of rule editing you can change:

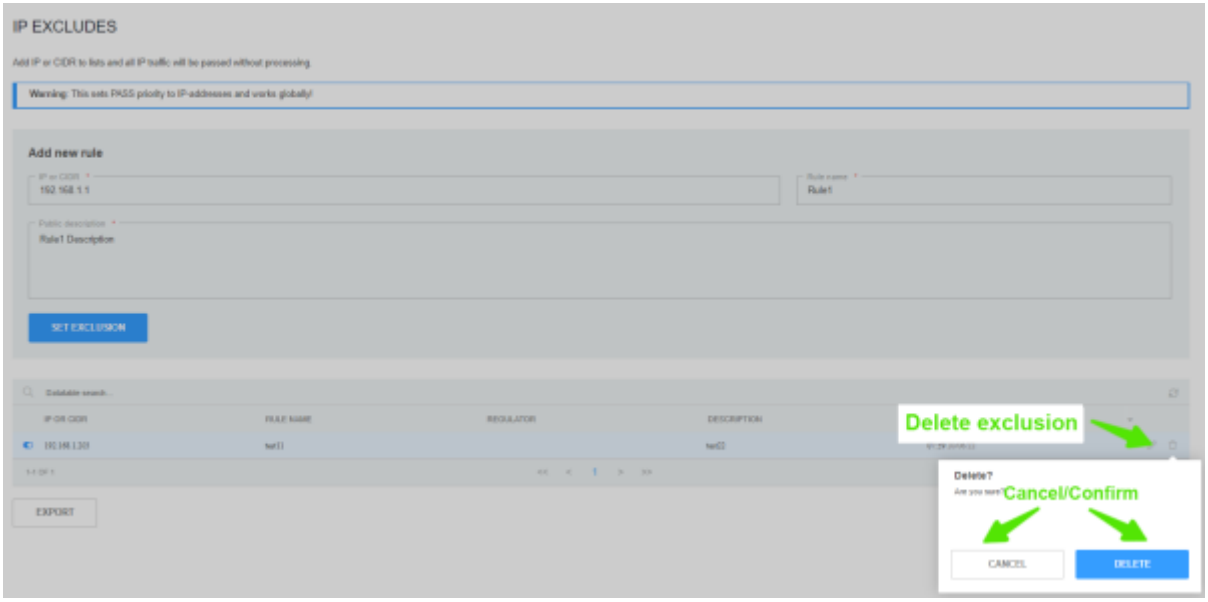
- name of the rule;
- its description.



Save the changes by clicking on "Set DSCP" button.

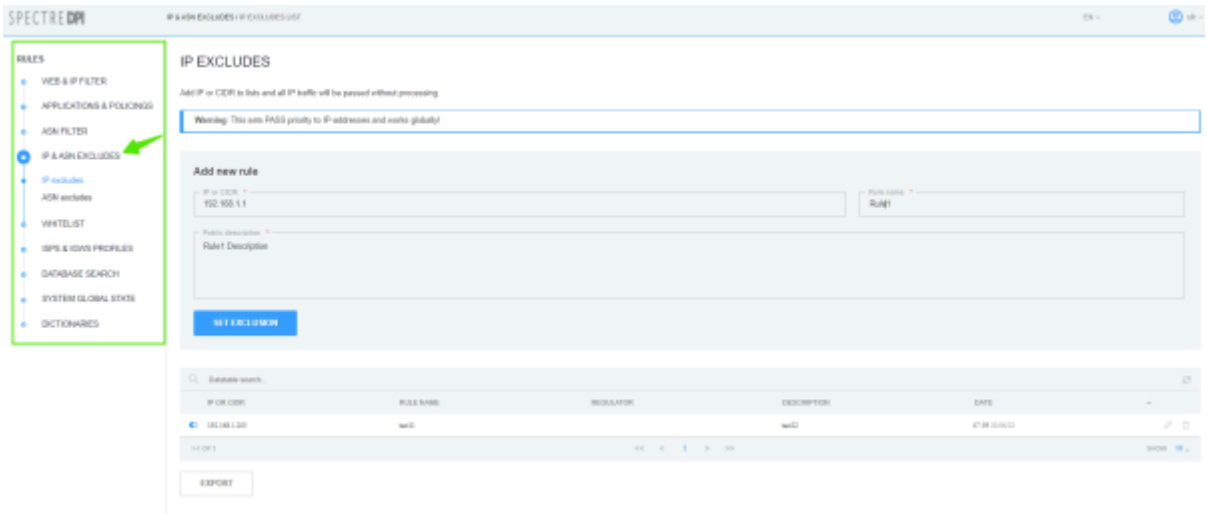
Deleting

In the list of exclusions click the button “Delete exclusion” and confirm/cancel the operation.



ASN Excludes

Change to the "IP & ASN Excludes" section → "ASN Excludes".



Creating

In the form of rule creating:

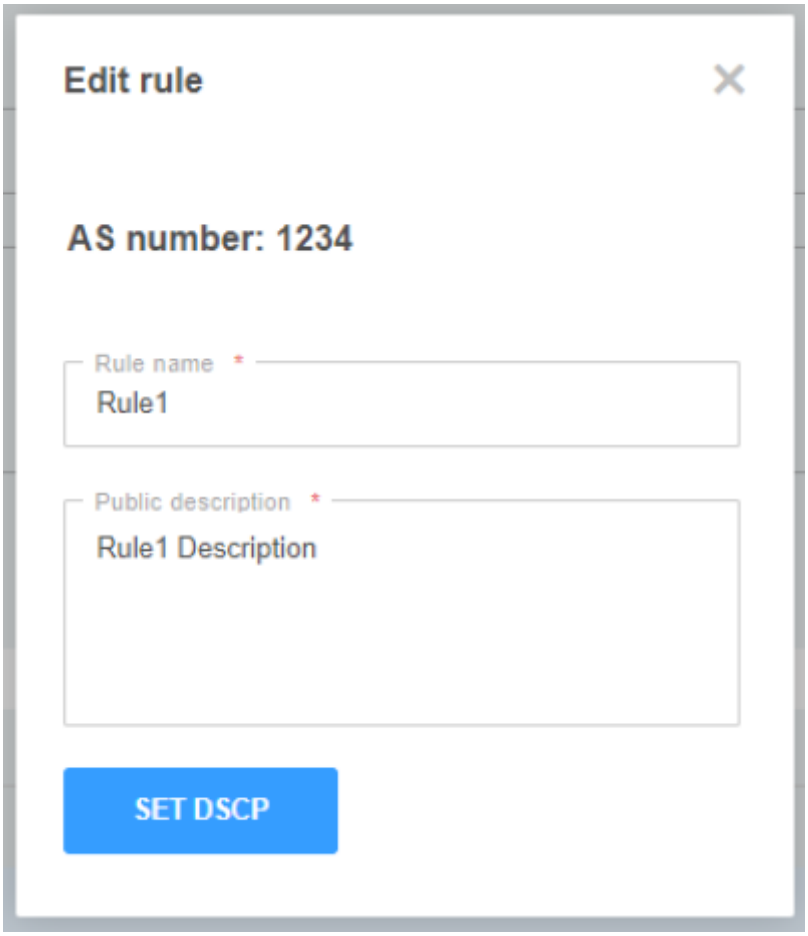
- Specify AS number;
- Enter the rule name;
- Enter the rule descriptuin;

Save the changes by clicking on "Set Exclusion" button.

Editing

Click on the button "Edit exclusion". In the form of rule editing you can change:

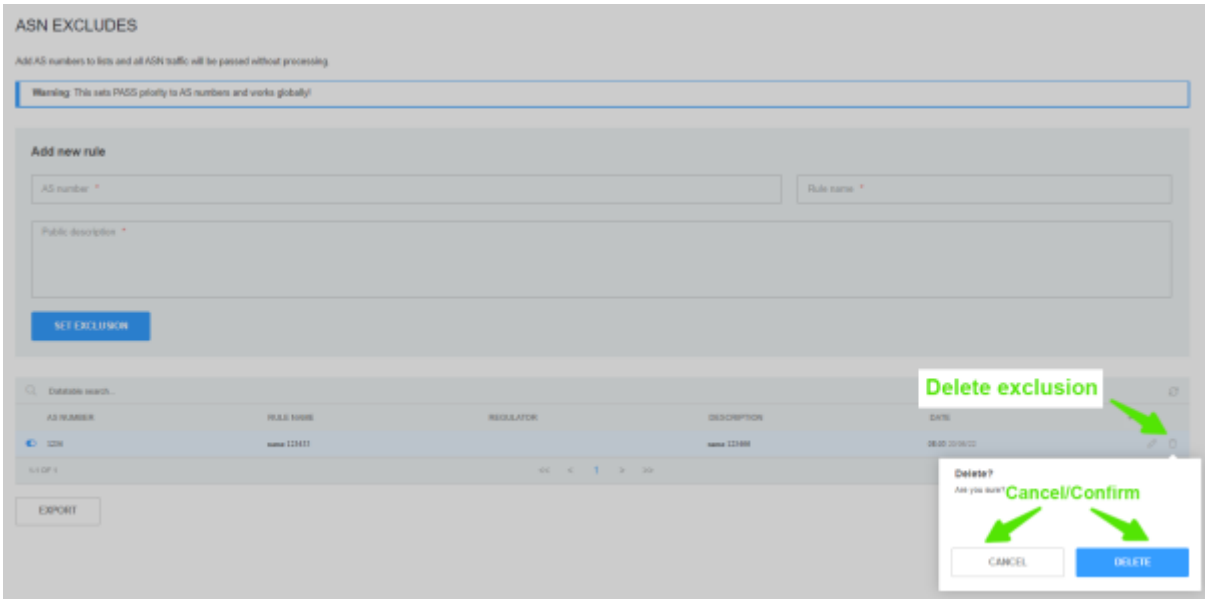
- name of the rule;
- its description.



Save the changes by clicking on "Set DSCP" button.

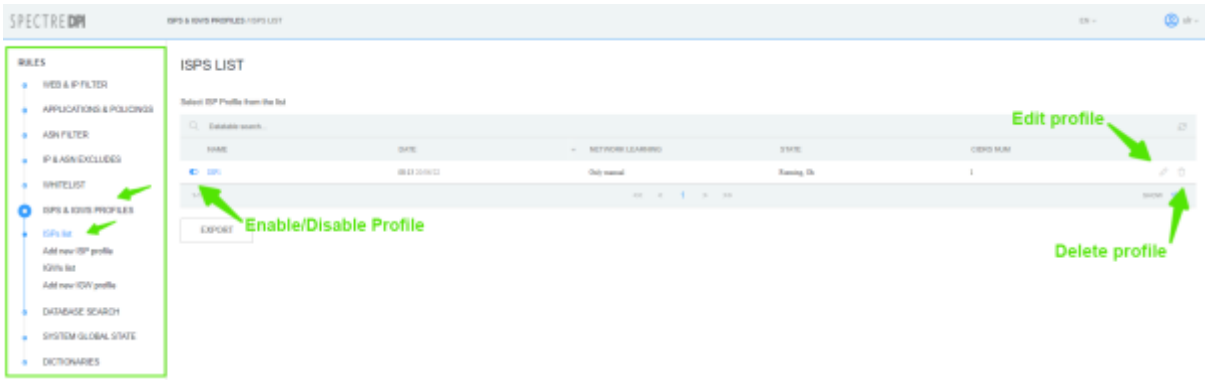
Deleting

In the list of exclusions click the button “Delete exclusion” and confirm/cancel the operation.



ISP Configuration

Change to the "ISPS & IGWS Profiles" → "ISPs List".

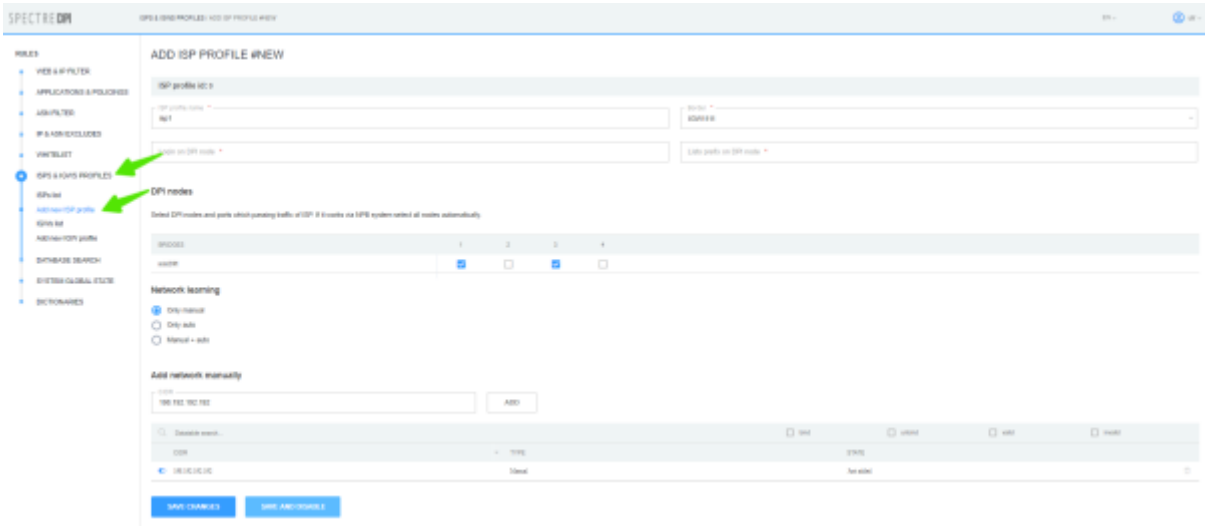


Creating an ISP Profile

To create new IGW profile go to the "ISPS & IGWS Profiles" section → "Add new ISP Profile".

In the form specify:

- Name of ISP profile;
- Choose the border from the list;
- Login to be used on the DPI node;
- Prefix for lists on the DPI node (it will be used as the name of service profile on the node);
- Choose bridges of the border;
- Choose Network training to get the addresses of this profile;
- Specify address/networks of the ISP (if necessary).



Click on the button "Save changes" or "Save and Disable/Enable".

After creation the ISP profile is enabled by default. Only enabled profiles are uploaded to DPI nodes.

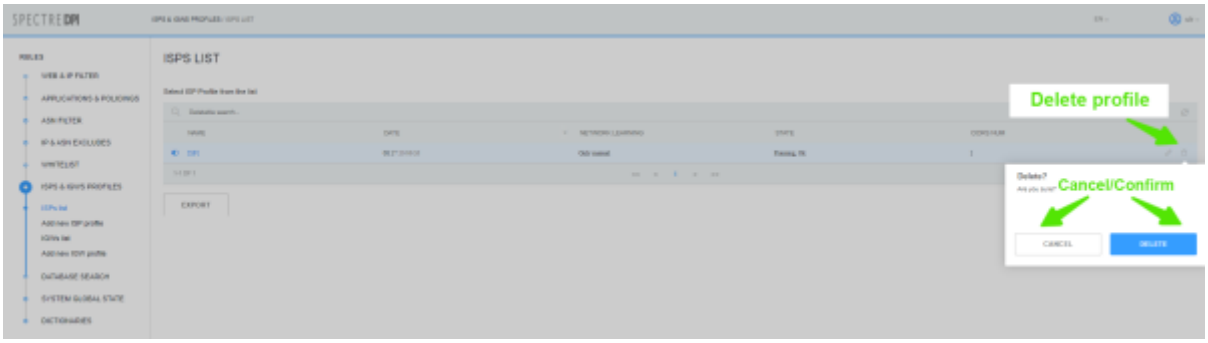
Editing ISP Profile

In the "ISPS & IGWS Profiles" section → "ISPs list" click on the button "Edit Profile".

A modal form for creating/editing ISP profile will pop up; make the chenges you need and click on the "Save changes" or "Save and Disable/Enable" button.

Deleting ISP Profile

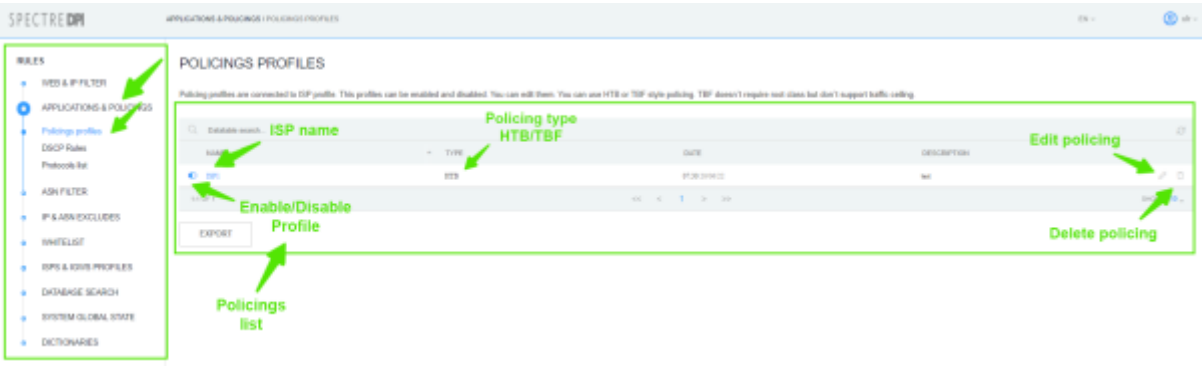
In the "ISPS & IGWS Profiles" section → "ISPs List" click on the "Delete" button and confirm/cancel the action.



Attention: Before deleting the profile, make sure there are no rules referring to this profile!

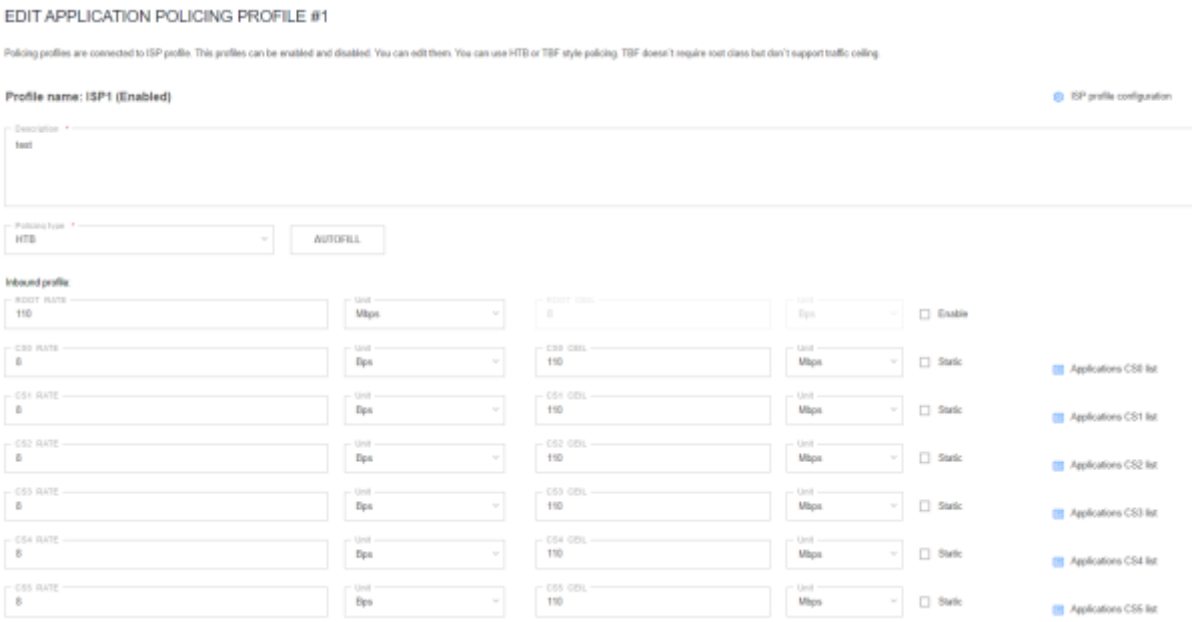
Policing Profile

Chenge to the "Applications and Policings" prfoile → "Policings Profiles".



Editing Policing Profile

Click on the "Edit policing" button.



In the popup editing form:

- Enter policing description;
- Choose policing type TBF/HTB (form with class values will look different depending on the type selected)

You can use configuration autocomplete:

- For HTB type: rate=8Bps, ceil=value that was specified in autocomplete form;
- For TBF type: rate=value that was specified in autocomplete form.

Th save the changes click on the button "Save profile" or "Save and disable/eneble".

Thy policing profile is disabled by default.

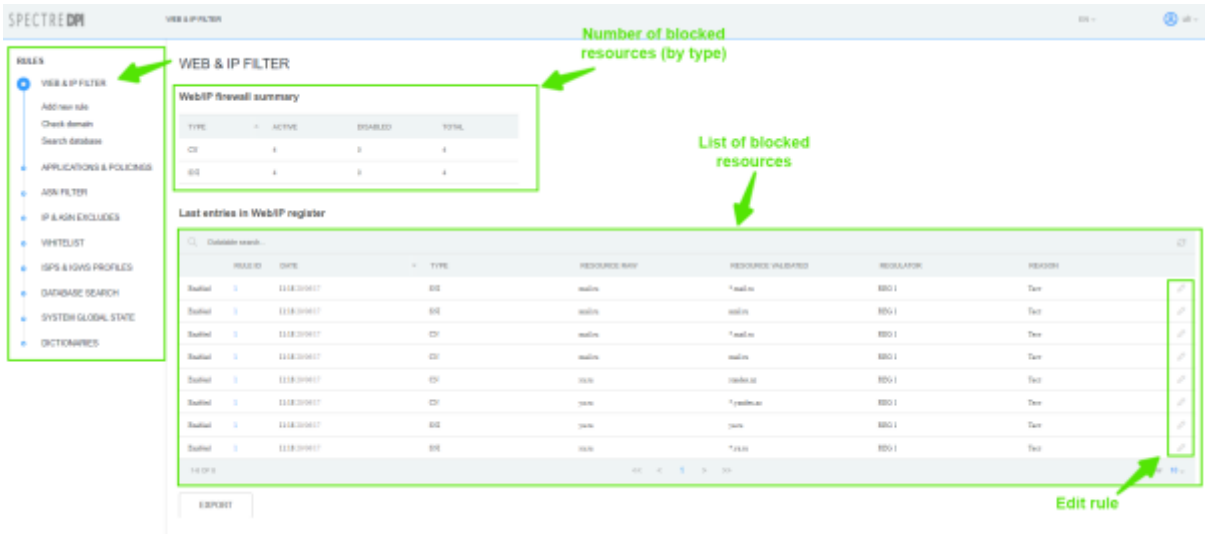
Deletenig Policing Profile

There are two ways to delete the profile: by clicking "Delete profile" button in the list of policing profiles or the same button on Editing Profile page.

WEB and IP Filter

Locking Rules List

Change to the "WEB and IP Filter" section.

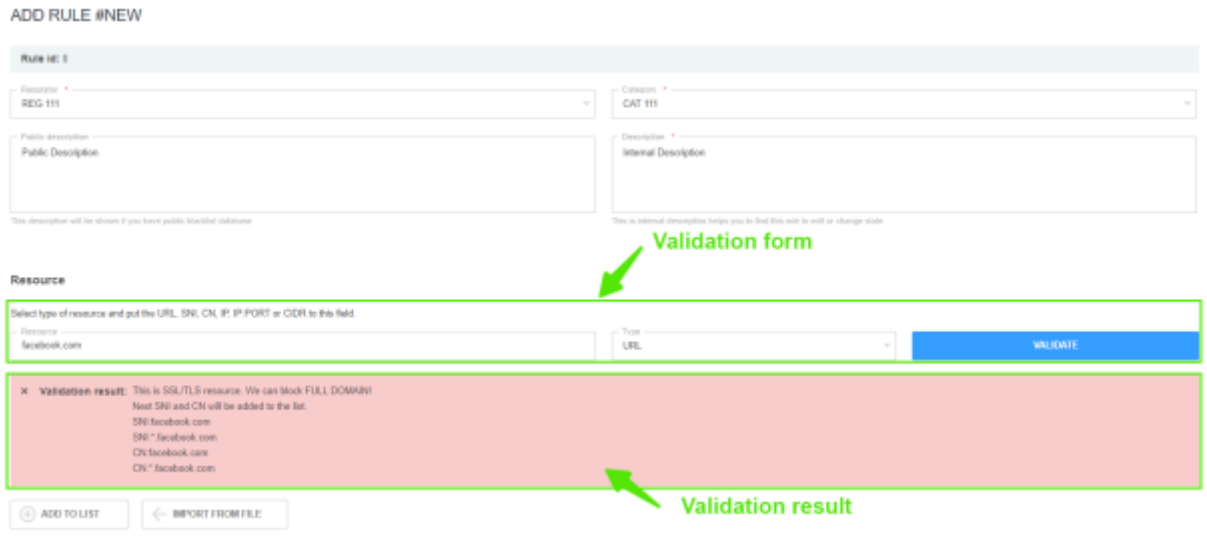


Creating/Editing Locking Rules

- To create new locking rule for a resource, change to the "WEB and IP Filter" section → "Add new rule";
- To edit an existing rule change to the "WEB and IP Filter" section and click on "Edit rule" button.

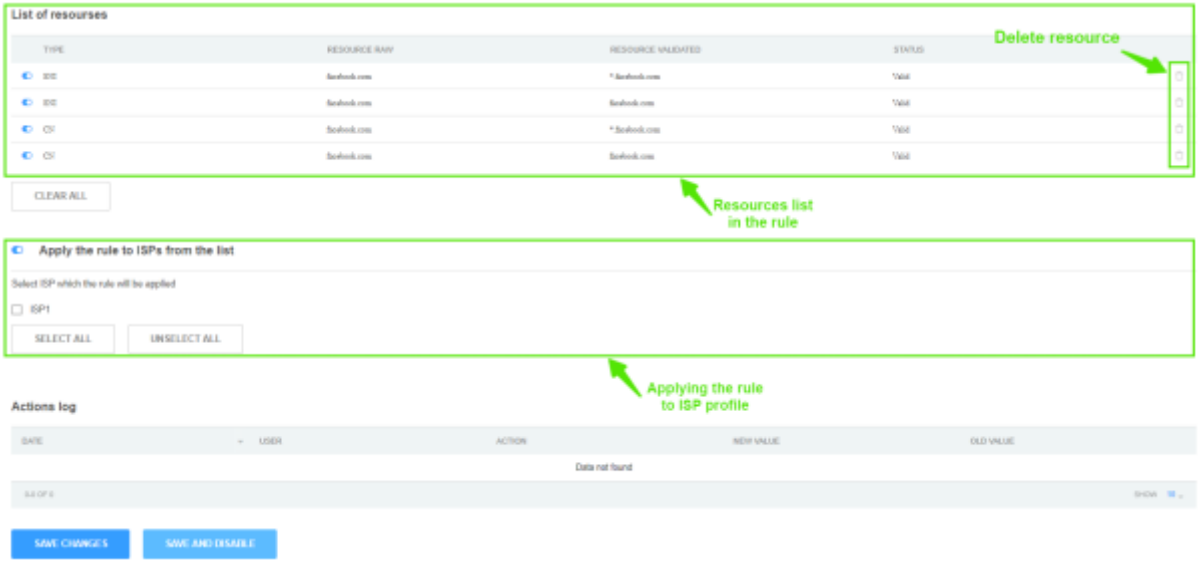
In the popup form:

- Choose the regulator;
- Choose the category;
- Enter rule public description;
- Enter rule hidden description;



In the resource validation form, enter the resource and choose its type:

- If it is not nesessary to validate the resourse, just click on "Add to the list" button;
- Click on the "Check" button. Information about the resource will be displayed. It can be added to the rule locking list. To do this, click the "Add to List" button.

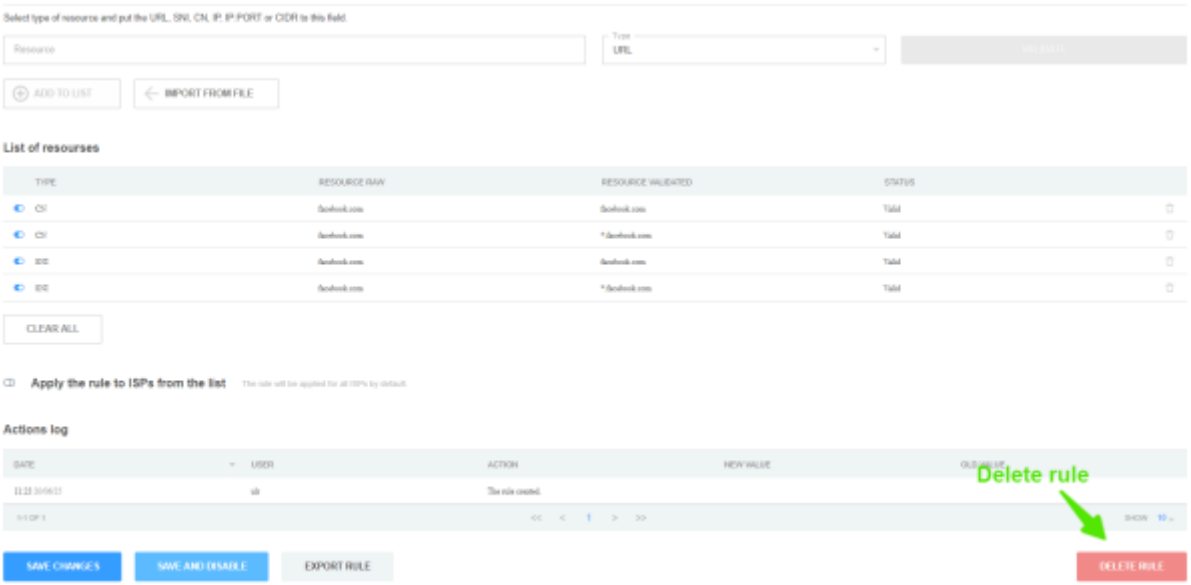


In the subsection for binding rules to ISP profiles:

- If the option "Apply the rule to ISP from the list" is **disabled,** such rule will be global. Resources from this rule will be included in the global lists of blocked resources.
- If the option "Apply the rule to ISP from the list" is **enabled,** such rule will be applied only to those ISP profiles, which are noted in this rule. Resources from this rule will be included in the locking lists for these ISP profiles.

Deleting the Locking Rule

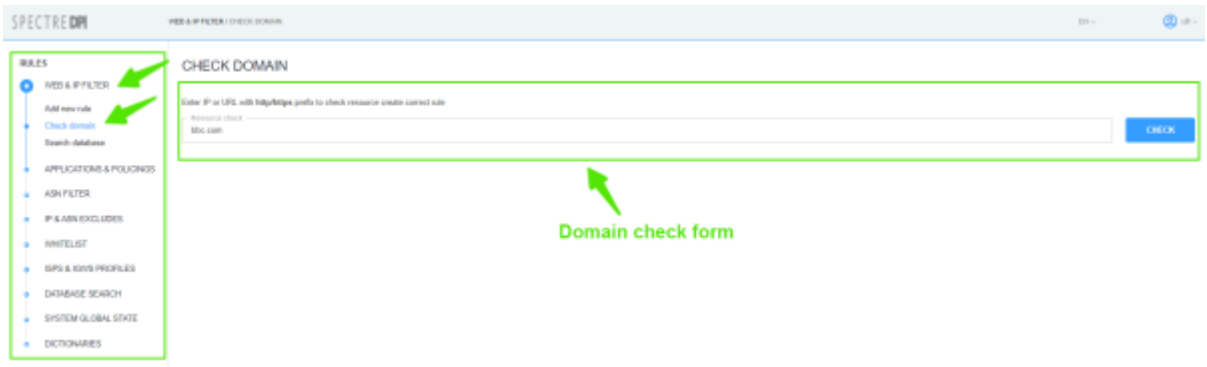
Change to the "WEB and IP Filter" section and click on the "Edit the rule" button.



Attention: Before deleting a rule, make sure it does not refer to any ISP profile.

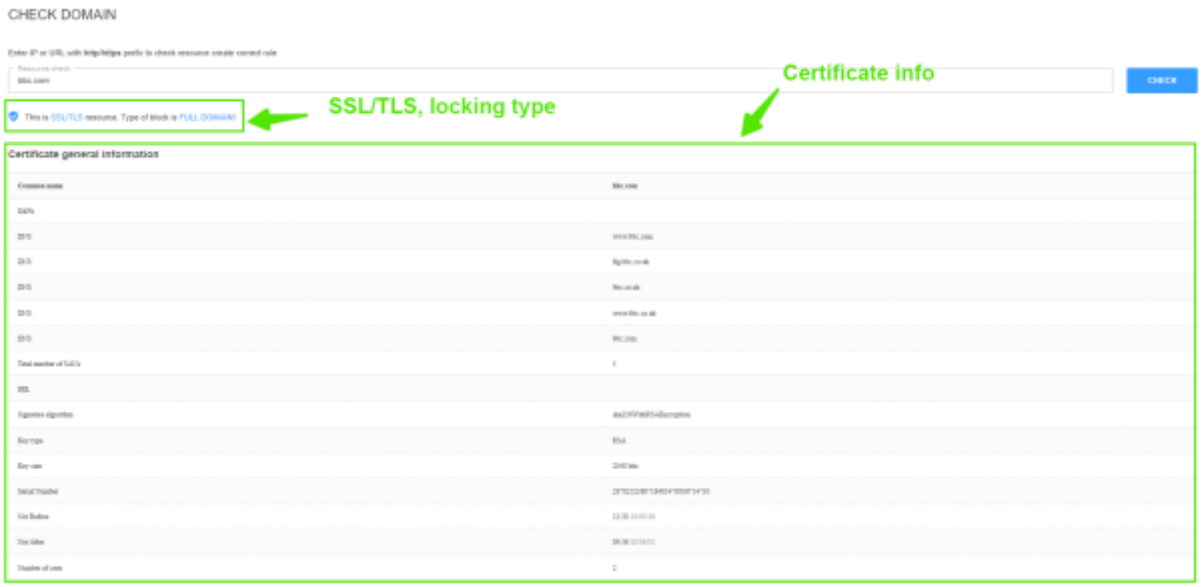
Domain Check

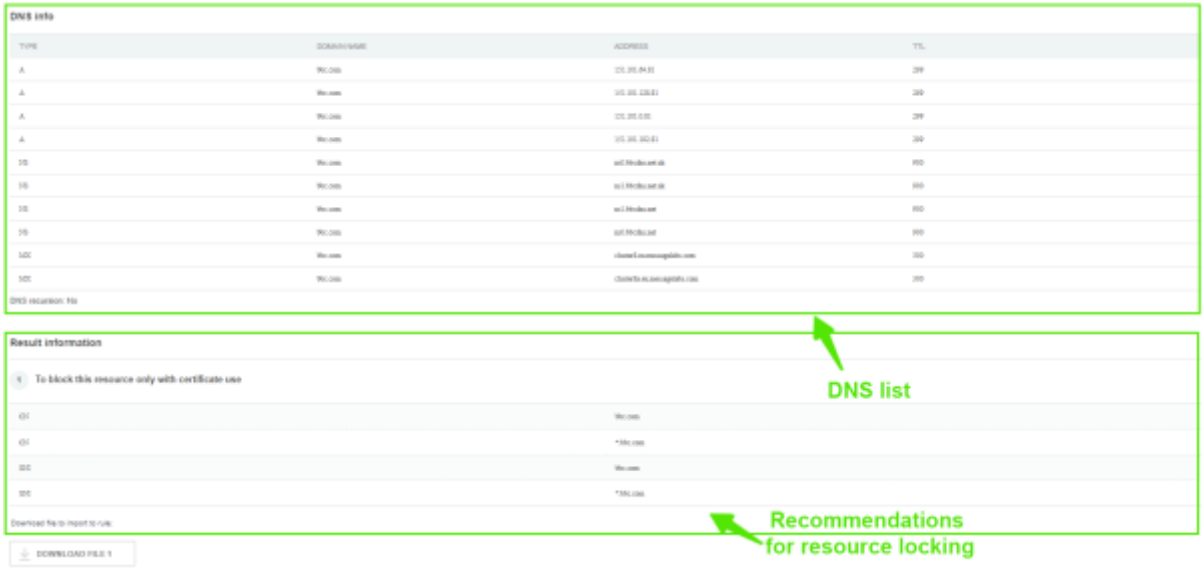
Change to the "WEB and IP Filter" section → "Check domain".



In the "Resourse Check" field type in the URL of resourse to be checked. Then click on the "Check" button. Information about the specified resource will be displayed below the form:

- SSL/TLS, locking type;
- Certificate information;
- DNS list;
- Recommendations about the values to use to lock this resource.



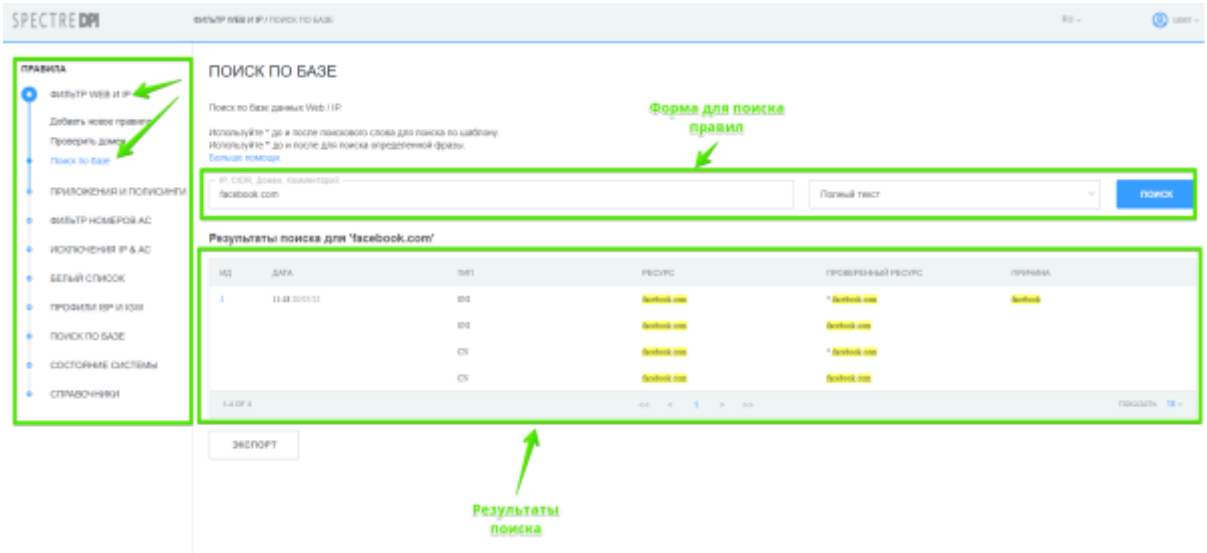


Search the Database (among the blocking rules)

Change to the "WEB and IP Filter" section → "Search Database".

In the "IP, CIDR, Domain, Notes" field enter the value in accordance with the prompts at the top of the page. Then choose type of search: Full Text, By Resources or By Description. Click on "Search" button.

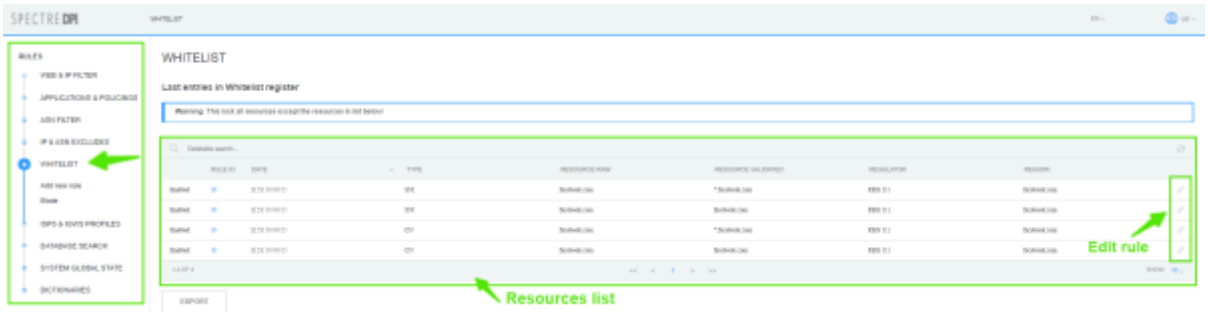
As a result, all blocking rules that match the selected search parameters will be displayed.



Whitelist

Whitelist rule list

Change to the "Whitelist" section.

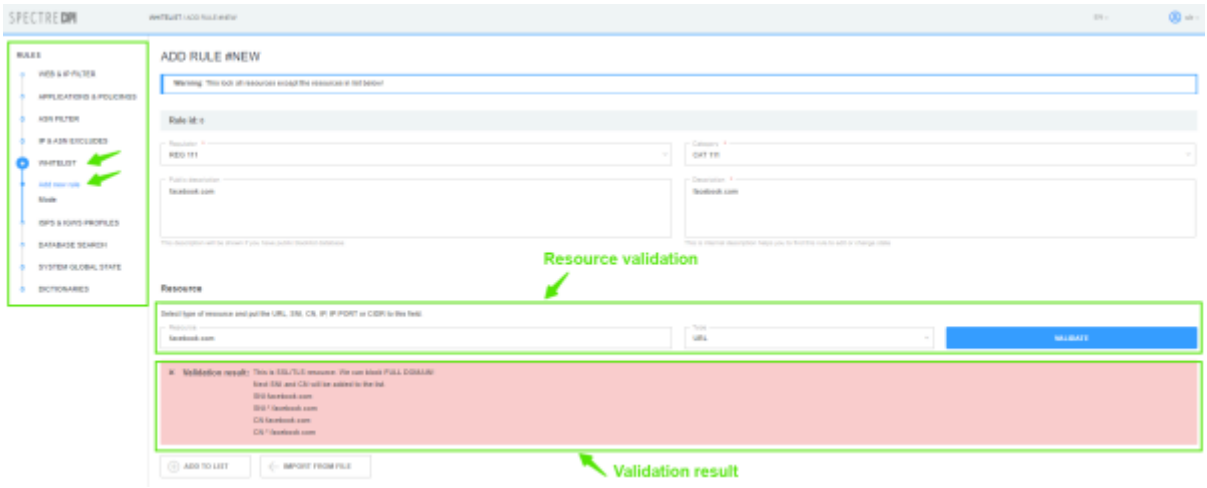


Creating/Editing the white list

- To create a new white list rule change to the "Whitelist" section → "Add new rule";
- To edit an existing rule change to the "White list" section and click on the "Edit rule" button.

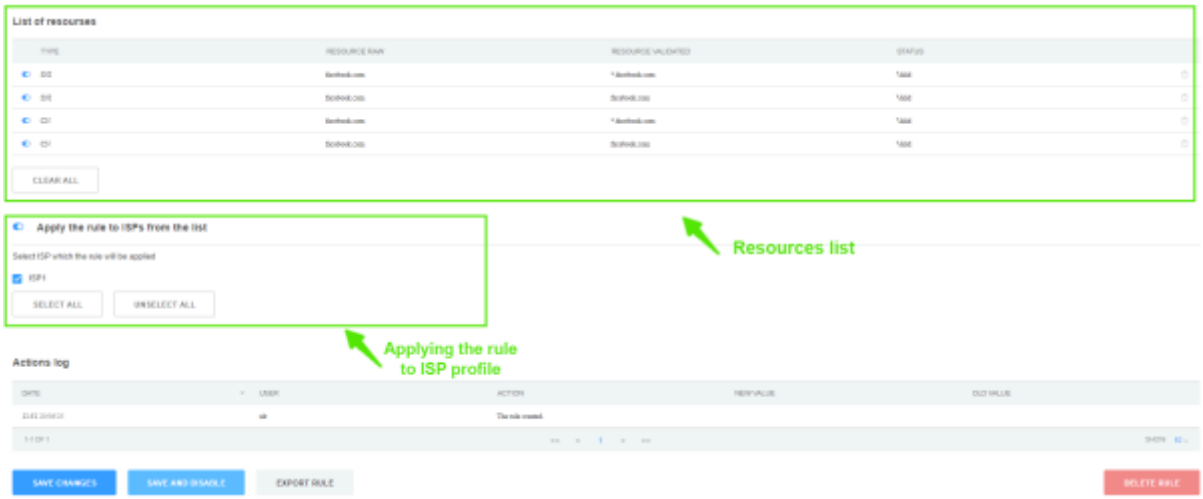
In the popup form:

- Choose the regulator;
- Choose the caregory;
- Enter rule public description;
- Enter rule hidden description;



In the resource validation form, enter the resource and choose its type:

- If it is not nesessary to validate the resourse, just click on “Add to the list” button;
- Click on the “Check” button. Information about the resource will be displayed. It can be added to the rule locking list. To do this, click the “Add to List” button.

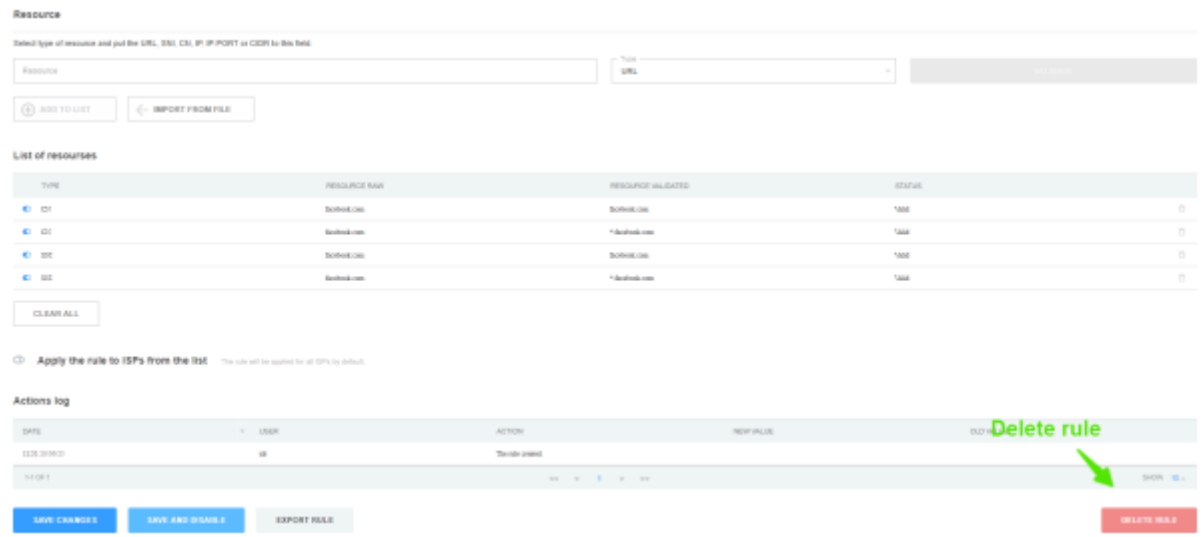


In the subsection for binding rules to ISP profiles:

- If the option “Apply the rule to ISP from the list” is **disabled,** such rule will be global. Resources from this rule will be included in the global lists of blocked resources.
- If the option “Apply the rule to ISP from the list” is **enabled,** such rule will be applied only to those ISP profiles, which are noted in this rule. Resources from this rule will be included in the locking lists for these ISP profiles.

Deleting a white list rule

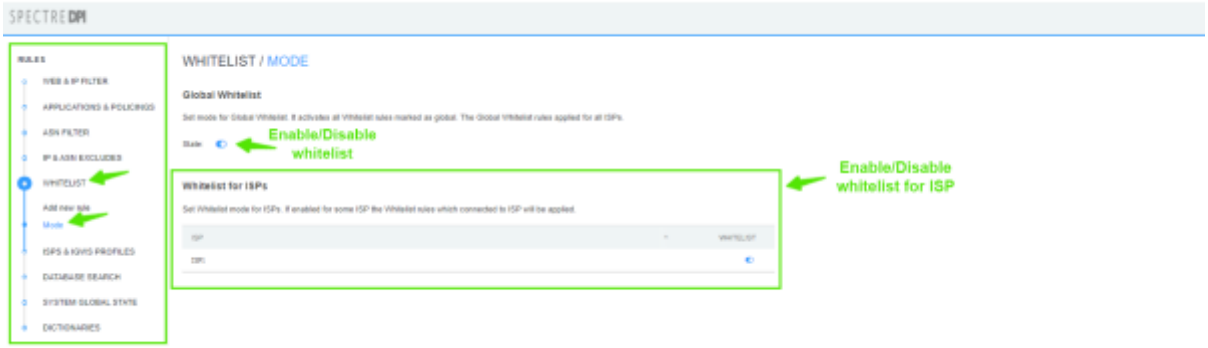
Change to the “Whitelist” section and click on the “Edit the rule” button.



Attention: Before deleting a rule, make sure it does not refer to any ISP profile.

Whitelist operating mode management

Change to the “Whitelist” section → "Mode".



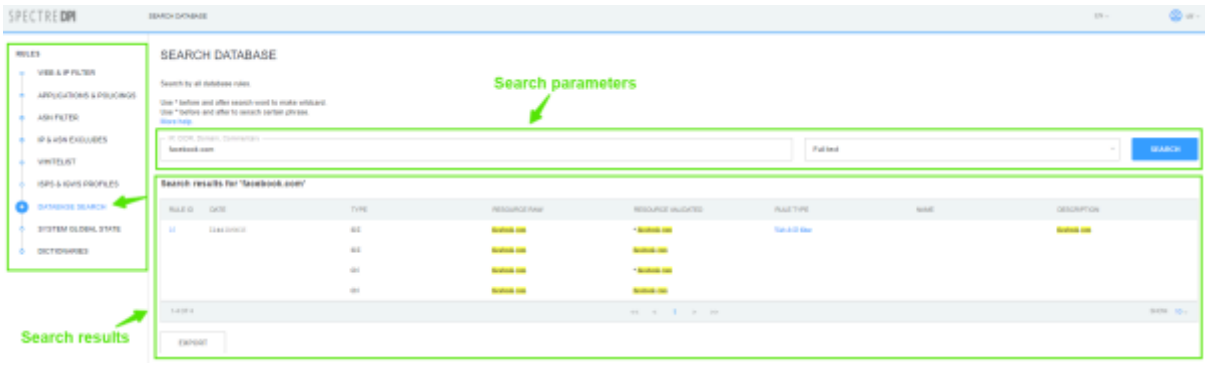
- With the global whitelist mode enabled, the whitelist service is applied to all ISP profiles and resource lists are formed only from global whitelist rules;
- When the whitelist mode is enabled for a separate ISP profile, the service is applied only to ISP which has it enabled. The lists are formed only from white list rules which refer to this ISP profile;
- If both mode are enabled, global and separate ISP rules lists are concatenated. For other ISPs, the whitelist service is used with only the global whitelist rules.

Database search (global)

Change to the "Database search" section.

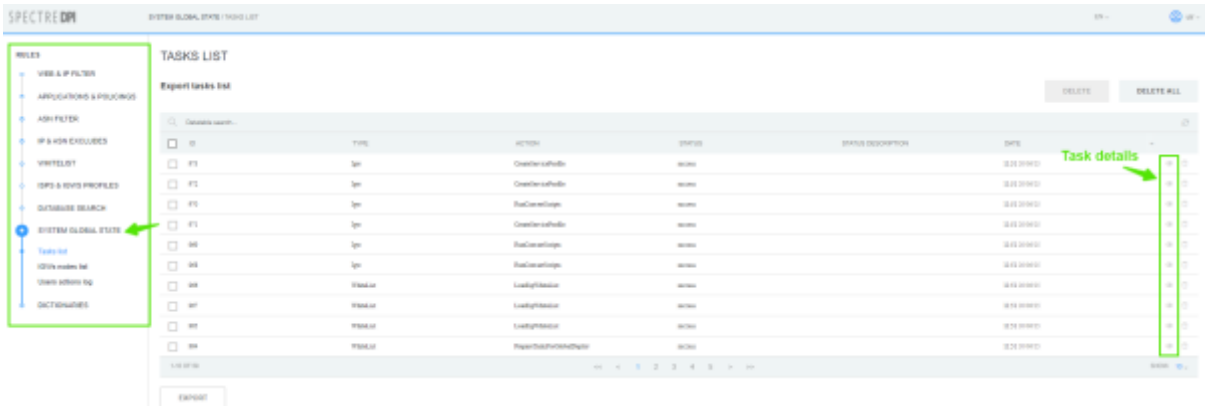
In the "IP, CIDR, Domain, Comment" field enter the value in accordance with the prompts at the top of the page, choose search type: Full Text, By Resources or By Description. Click on “Search” button.

As a result, all blocking rules (with type specified) that match the selected search parameters will be displayed.



Task monitoring

Change to the "State of the system" section.



This section displays the task queue, status and time.

To see the details of the task, click on "Task Details".

Logs

The logs for this section are stored in files:

```
/var/www/html/dpiui2/backend/storage/logs/ulr*.log
```

Log detail level is specified with ULR_LOAD_LOG_LEVEL option in the .env configuration file.