

Содержание

6 Filtering rules management interface	3
Universal Locking Rules UI	3
Introduction	3
Installation	3
Configuration	3
.env Configuration	3
Key Installation	4
Roles Management	5
Dictionaries Configuration	6
IGW Profiles Management	10
Web Server for Global Lists Configuration	12
Web-server	12
DSCP Rules	13
ASN Filter	14
IP & ASN Excludes	16
IP Excludes	17
ASN Excludes	19
VIP Subscriber Management	21
ISP Configuration	23
Creating an ISP Profile	23
Editing ISP Profile	24
Deleting ISP Profile	24
Policing Profile	25
WEB and IP Filter	26
Locking Rules List	26
Creating/Editing Locking Rules	26
Deleting the Locking Rule	27
Domain Check	28
Search the Database (among the blocking rules)	29
Whitelist	30
Whitelist rule list	30
Creating/Editing the white list	30
Deleting a white list rule	31
Whitelist operating mode management	32
Database search (global)	32
Task monitoring	33
Logs	33

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

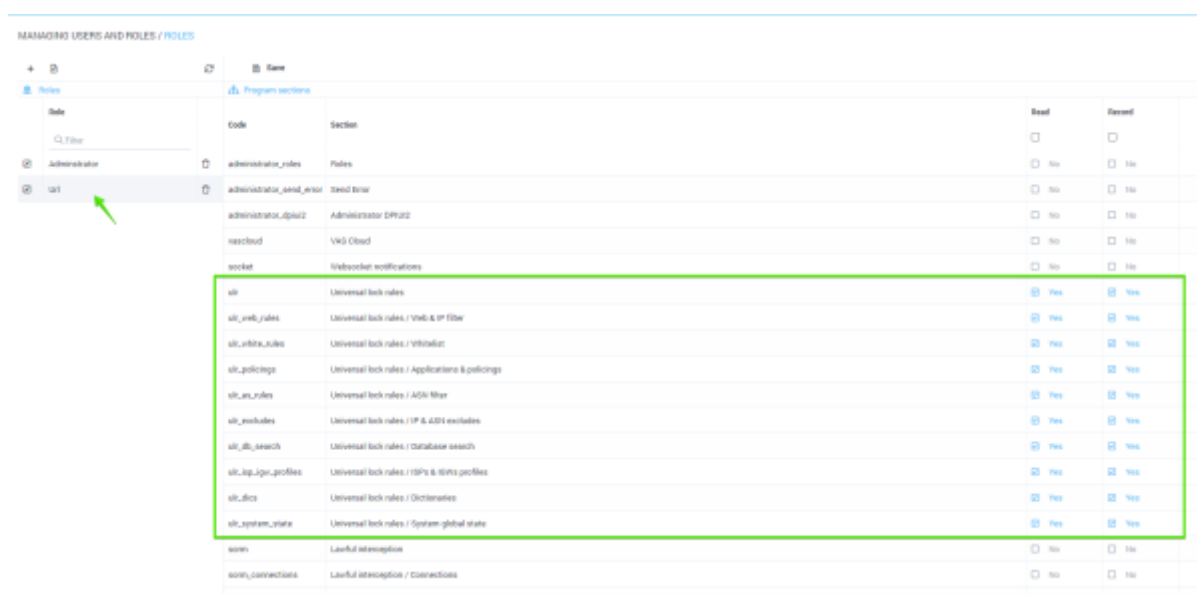
Enter expire date in Y-m-d format:
> 2099-12-31

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:



Code	Section	Read	Write
administrator_roles	Roles	<input type="checkbox"/>	<input type="checkbox"/>
administrator_send_email	Send Email	<input type="checkbox"/>	<input type="checkbox"/>
administrator_dpiui2	Administrator DPIUI2	<input type="checkbox"/>	<input type="checkbox"/>
rescloud	VMD Cloud	<input type="checkbox"/>	<input type="checkbox"/>
socket	Websocket notifications	<input type="checkbox"/>	<input type="checkbox"/>
ulr	Universal lock rules	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
ulr_web_rules	Universal lock rules / Web & IP filter	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
ulr_auth_rules	Universal lock rules / Validation	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
ulr_policies	Universal lock rules / Applications & policies	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
ulr_app_rules	Universal lock rules / ADI filter	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
ulr_modules	Universal lock rules / IP & ADI modules	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
ulr_db_search	Universal lock rules / Database search	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
ulr_log_profiles	Universal lock rules / HTTP & HTTPS profiles	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
ulr_dico	Universal lock rules / Dictionaries	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
ulr_system_state	Universal lock rules / System global state	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
snort	Snort intrusion	<input type="checkbox"/>	<input type="checkbox"/>
snort_connections	Snort intrusion / Connections	<input type="checkbox"/>	<input type="checkbox"/>

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

User name *

ulr_user

Full name *

user

E-mail *

user@user.com

Phone *

+796023...

Company *

vasexperts

Position *

ulr

Role

Url

New password

Confirm password

Save

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

SPECTREDM

WEB & IP FILTER

EN -

RULES

WEB & IP FILTER

Add new rule

Check status

Search database

APPLICATIONS & POLICIES

ASN FILTER

IP & ASN EXCLUDES

WHITELIST

IPS & IGMP PROFILES

DATABASE SEARCH

SYSTEM GLOBAL STATE

DICTIONARIES

WEB & IP FILTER

WebtP firewall summary

TYPE	ACTIVE	DISABLED	TOTAL
DN	4	0	4
SD	4	0	4

Last entries in WebtP register

RULE	DATE	TYPE	RESOURCE NAME	RESOURCE VALIDATED	REGULATOR	PERSON
Enabled 1	11.09.2019 07	SD	mail.ru	*mail.ru	REG 1	Tec
Enabled 1	11.09.2019 07	SD	mail.ru	mail.ru	REG 1	Tec
Enabled 1	11.09.2019 07	DN	mail.ru	*mail.ru	REG 1	Tec
Enabled 1	11.09.2019 07	DN	mail.ru	mail.ru	REG 1	Tec
Enabled 1	11.09.2019 07	DN	194.19	194.19	REG 1	Tec
Enabled 1	11.09.2019 07	DN	194.19	*194.19	REG 1	Tec
Enabled 1	11.09.2019 07	SD	194.19	194.19	REG 1	Tec
Enabled 1	11.09.2019 07	SD	194.19	*194.19	REG 1	Tec

14 of 9

<<

<

1

>

>>

SHOW 10

REPORT

Dictionaries Configuration

- Category Dictionary
- Regulators Dictionary



These dictionaries are used for creating/editing locking rules.

Category Dictionary

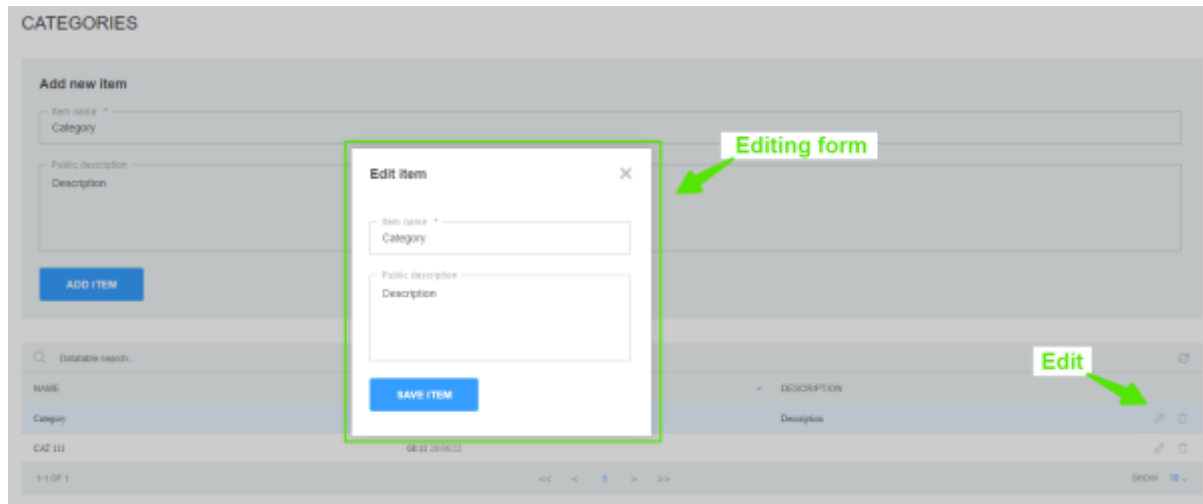
In the Locking Rules management interface go to the Dictionaries → Categories section.

Creating

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

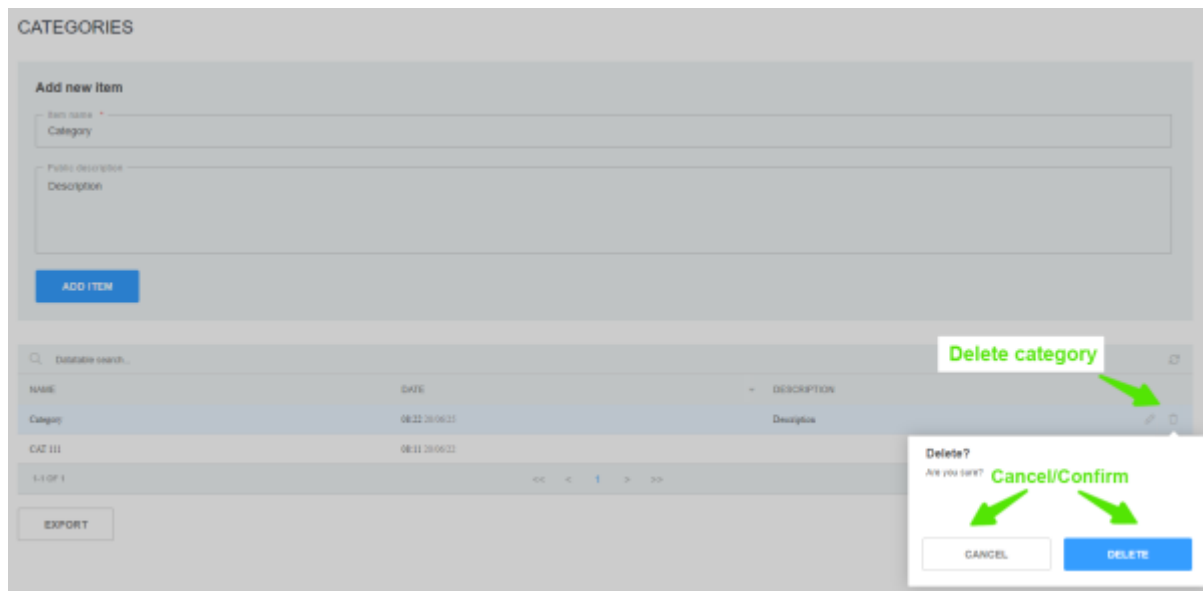
Editing

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

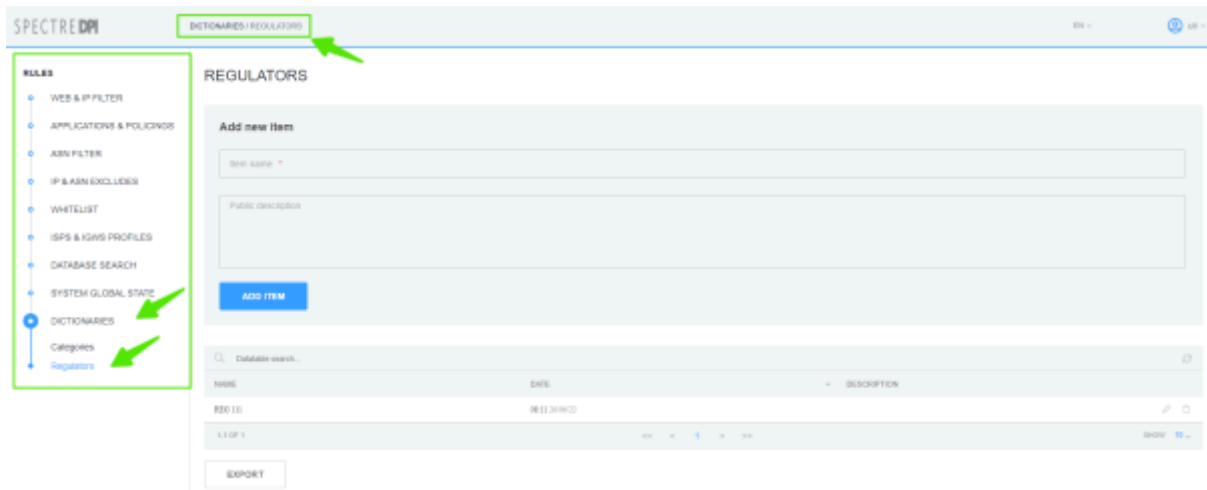
Click on the delete category button in the categories table. In the pop-up window confirm or cancel the action.



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

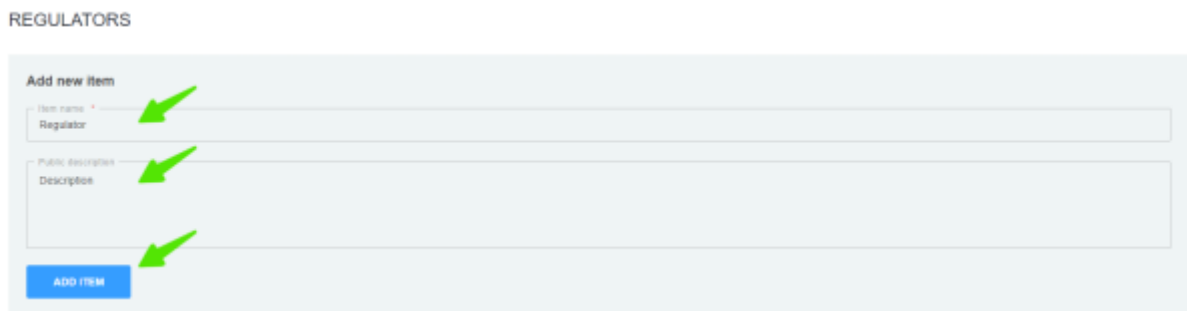
Regulators Dictionary

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



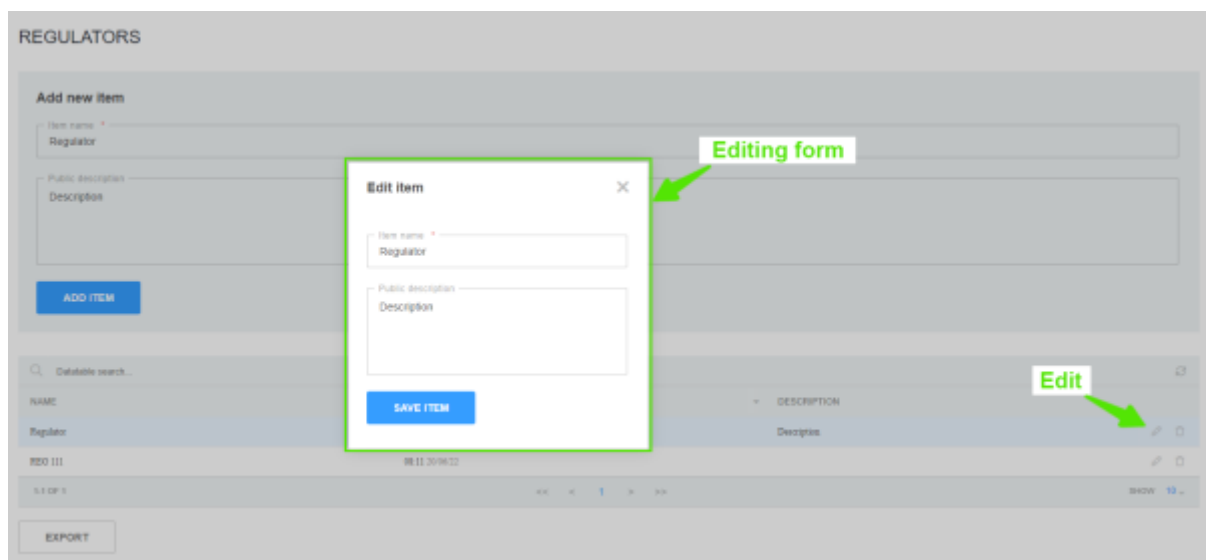
Creating

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



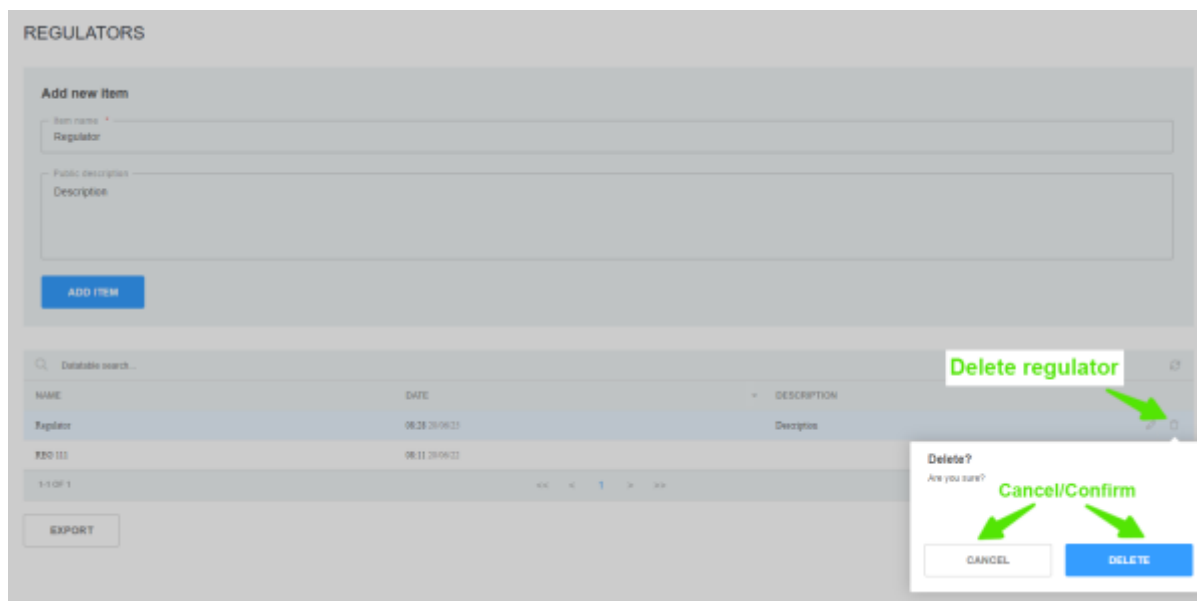
Editing

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

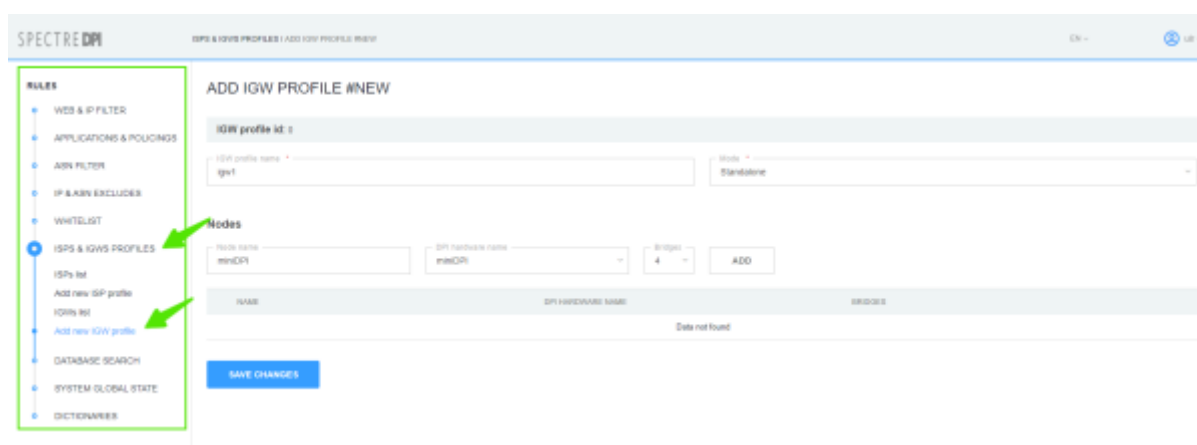
Click on the delete regulator button in the categories table. In the pop-up window confirm or cancel the action.



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)

ADD IGW PROFILE #NEW

IGW profile id: 1

IGW profile name: Mode:

Nodes

Node name: DPI hardware name: Bridges:

NAME	DPI HARDWARE NAME	BRIDGES
Data not found		

IGW adding form



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".

IGWS LIST

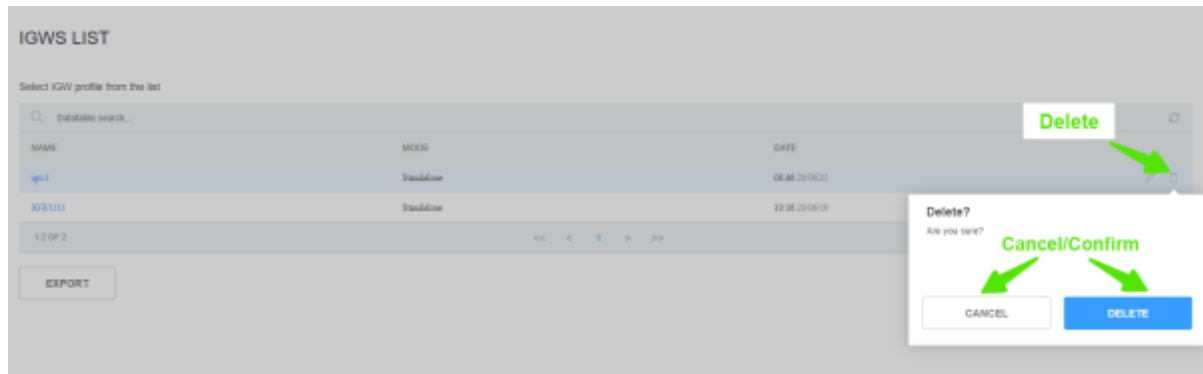
Select IGW profile from the list

<input type="text" value="Database search..."/>			
NAME	MODE	DATE	
IGW1111	Standalone	10:16 20/05/19	<input type="button" value="Edit profile"/> <input type="button" value="SHOW"/> <input type="button" value="10"/>
1-1 OF 1			
<input type="button" value="EXPORT"/>			

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

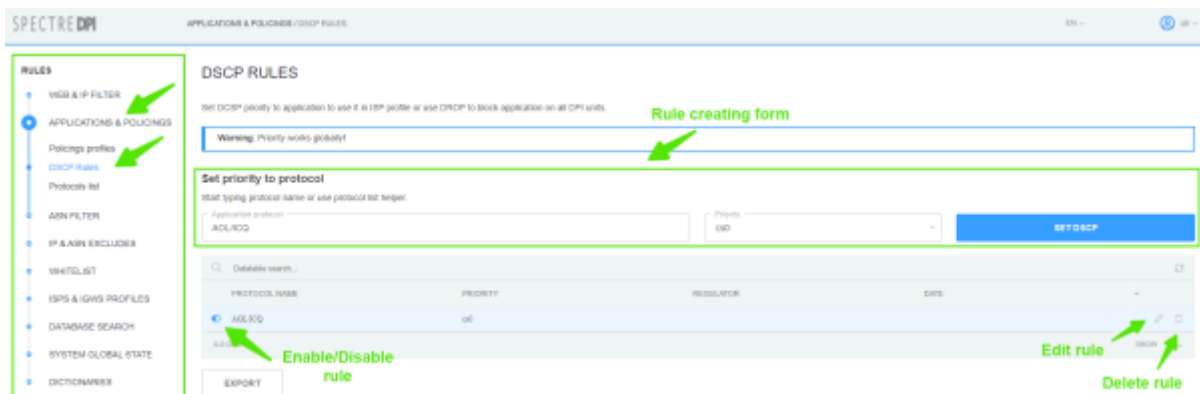
# Names dictionary for blocking HTTPS protocol by certificate
(custom_cname_black_list)
custom_cname_black_list=http://<IP address of Web-server>/blacklistcn.dict

# 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

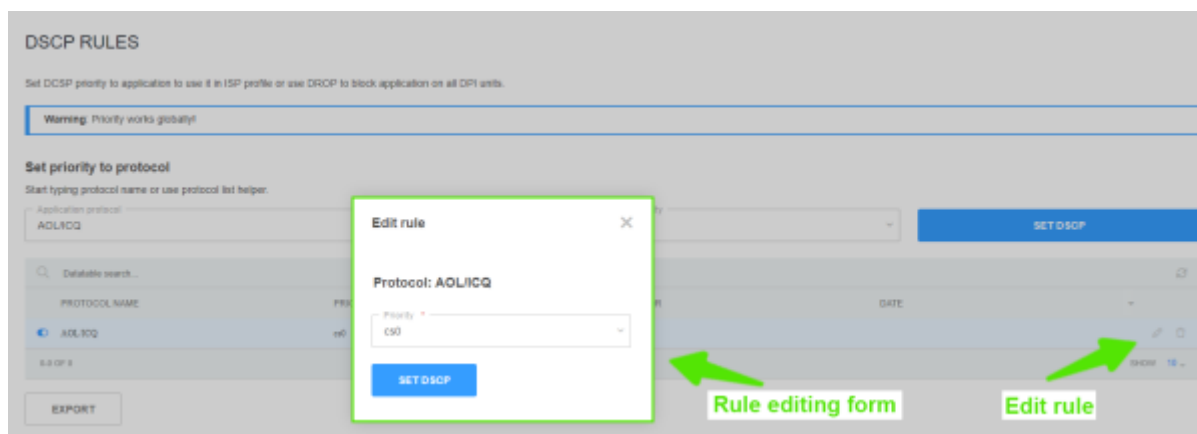
In the form of rule creating:

- 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.

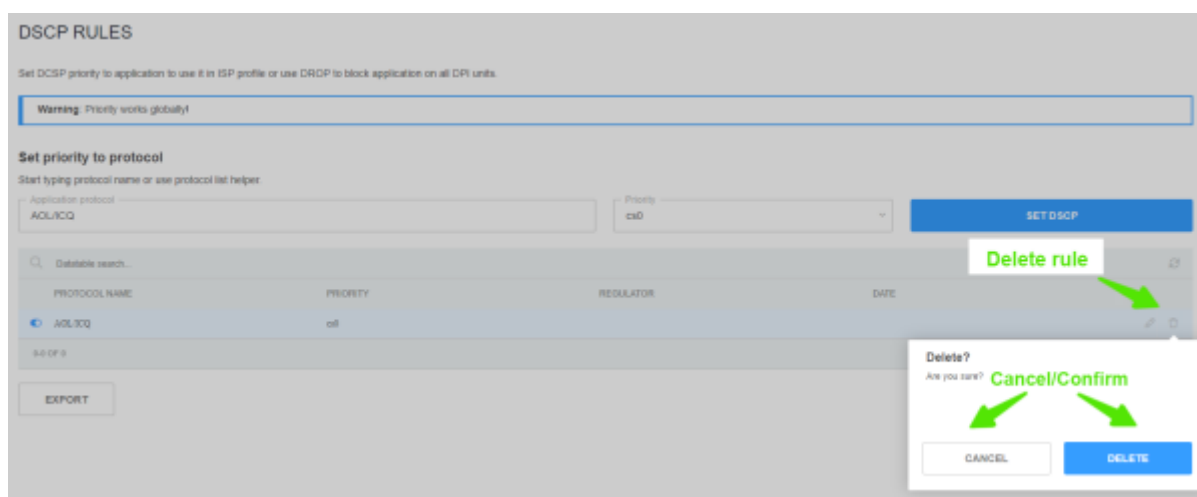
Editing

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.

SPECTRE DPM ADMINISTER DSCP RULES

RULES

- WEB & IP FILTER
- APPLICATIONS & POLICIES
- ASN FILTER**
- IP & ASN EXCLUDES
- WHITELIST
- QoS & QoS PROFILES
- DATABASE SEARCH
- SYSTEM GLOBAL STATE
- DICTIONARIES

DSCP RULES

Set DSCP priority to ASN direction to use it in ISP profile or use DSCP to block ASN traffic on all DPM units

Warning: Priority works globally!

Rule creating form

Add new rule

AS number: 12345

Priority: 100

Rule name: Rule1

Rule Description: Rule1 Description

SET DSCP

AS NUMBER	RULE NAME	PRIORITY	REGULATIONS	DESCRIPTION	DATE
12345	Rule1	100	up	Rule1 Description	27-01-2019 12:00

1 of 1

EXPORT

Edit rule

Delete rule

Enable/Disable rule

Creating

In the form of rule creating:

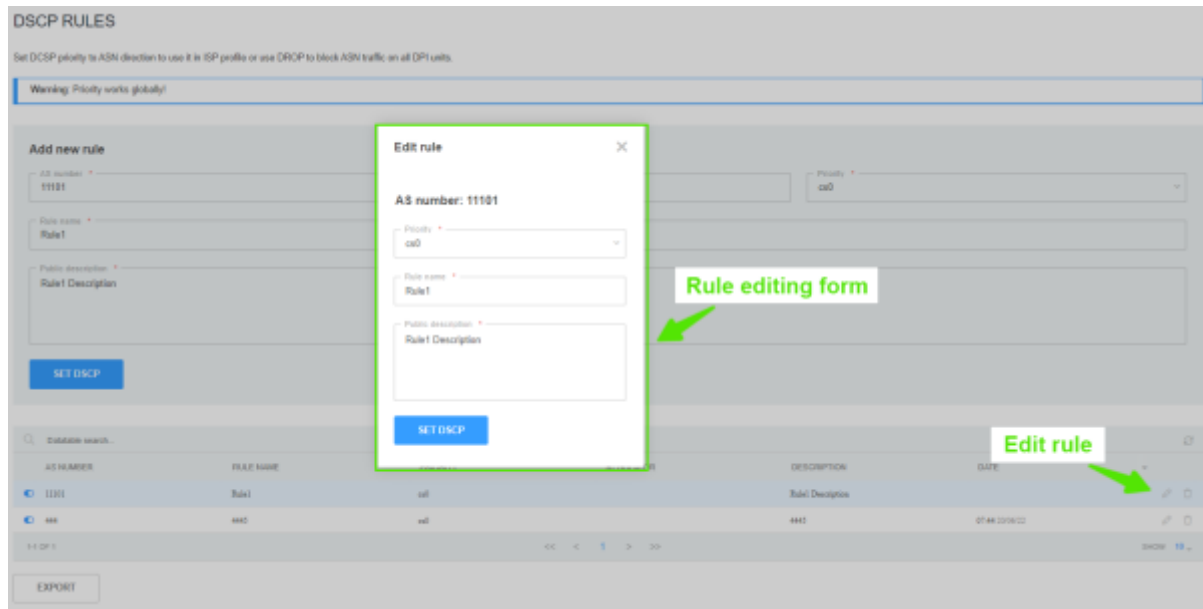
- Specify the number of AS;
- Choose the priority from the list;
- Enter the rule name;
- Enter the rule description.

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:

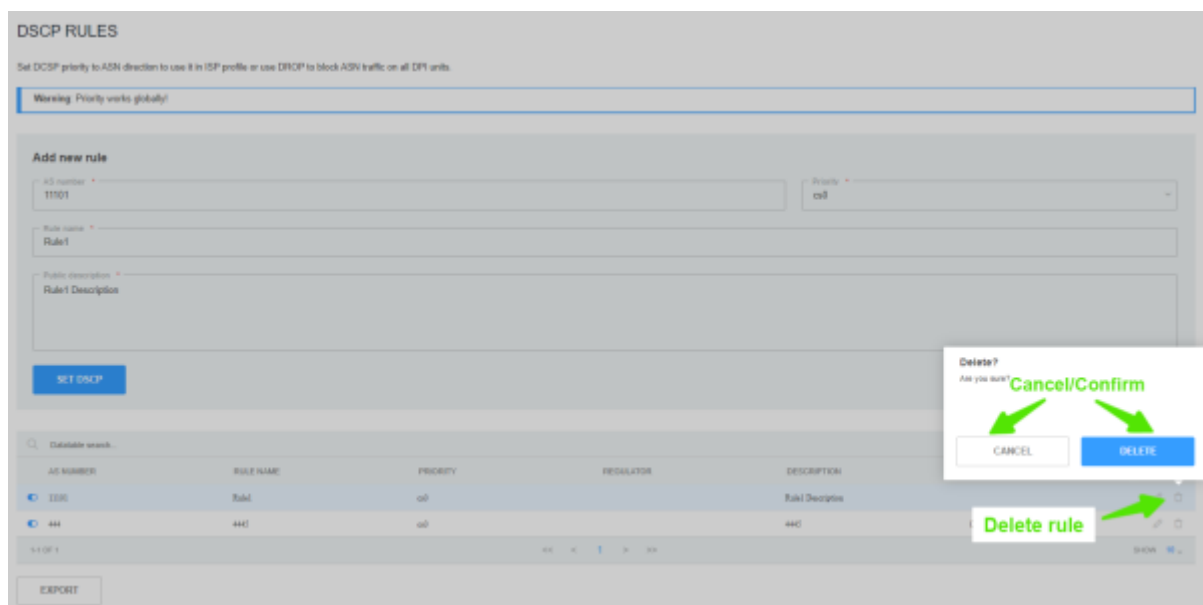
- choose the priority from the list;
- Enter the rule name;
- Enter the rule description.



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

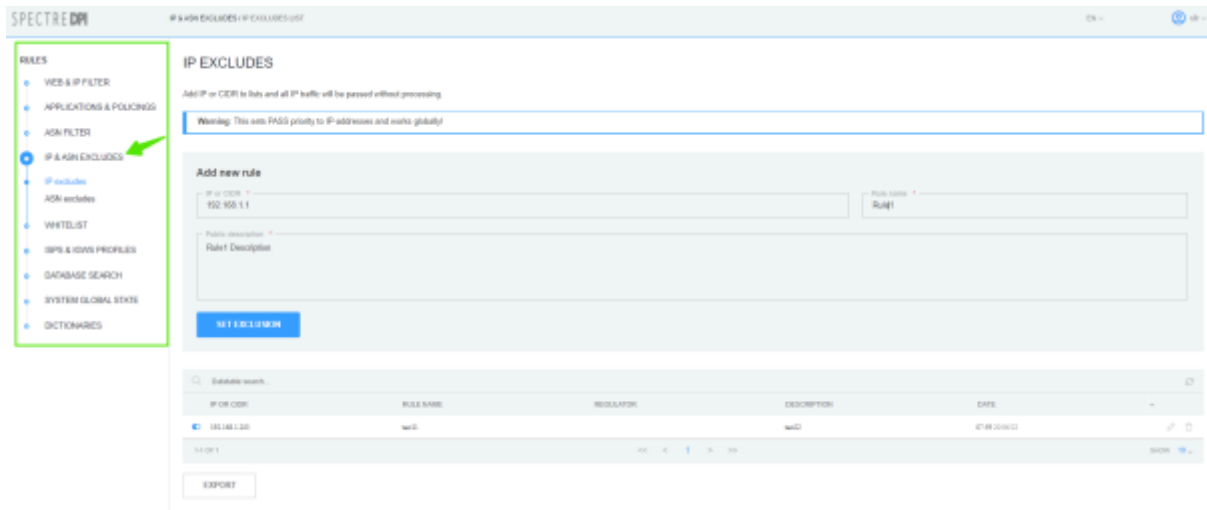
Deleting

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



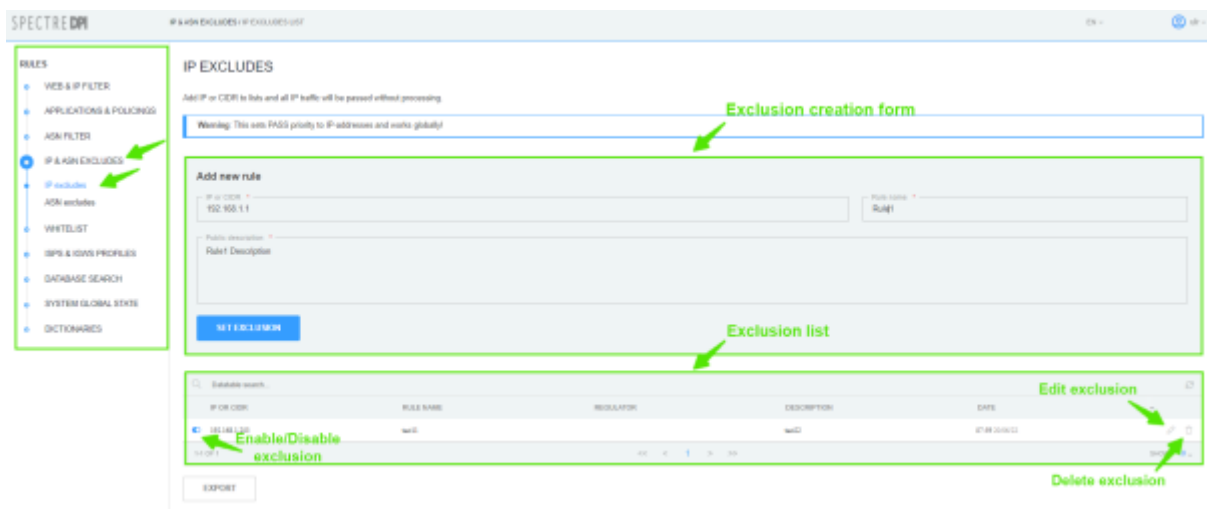
IP & ASN Excludes

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 description;

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.

Edit rule

IP or CIDR: 192.168.1.203

Rule name * Rule1

Public description * Rule1 Description

SET DSCP

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.

IP EXCLUDES

Add IP or CIDR to lists and all IP traffic will be passed without processing.

Warning: This sets PRIORITY to IP-addresses and works globally!

Add new rule

IP or CIDR: 192.168.1.1 Rule name: Rule1

Public description: Rule1 Description

SET EXCLUSION

IP OR CIDR	RULE NAME	REGULATOR	DESCRIPTION
192.168.1.1	net1		net2

Delete exclusion

Delete?
Are you sure?

Cancel/Confirm

CANCEL **DELETE**

ASN Excludes

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

The screenshot shows the SPECTRE DPM interface for IP & ASN Excludes. The left sidebar has a menu with 'IP & ASN EXCLUDES' selected. The main content area is titled 'IP EXCLUDES' and includes a warning message: 'Warning: This sets PASS priority to IP addresses and marks globally!'. Below this is a form to 'Add new rule' with fields for 'IP or CIDR' (containing '192.168.1.1'), 'Rule Name' (containing 'Rule1'), and 'Rule Description'. A 'SET EXCLUSION' button is at the bottom of the form. Below the form is a table with columns: 'IP OR CIDR', 'RULE NAME', 'REGULATION', 'DESCRIPTION', and 'DATE'. The table contains one row with the value '192.168.1.1' in the 'IP OR CIDR' column. An 'EXPORT' button is at the bottom of the table.

Creating

In the form of rule creating:

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

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.

Edit rule

AS number: 1234

Rule name *

Rule1

Public description *

Rule1 Description

SET DSCP

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

Add new rule

AS number *

Rule name *

Public description *

SET EXCLUSION

Delete?

Cancel/Confirm

CANCEL

DELETE

Delete exclusion

Database search...

AS NUMBER	RULE NUMBER	REGULATOR	DESCRIPTION	DATE
1234	12345		12345	2020-10-10-10

EXPORT

VIP Subscriber Management

VIP Subscribers and their privileges

VIP Subscriber is a special subscriber whose traffic is passed with a dedicated priority (cs0 by default) regardless of the priority settings for application protocols. The allocated priority is set by the special_dscp configuration parameter. See section [Configuration](#). The subscriber is connected through the installation of service 15 on DPI.

Privilege:

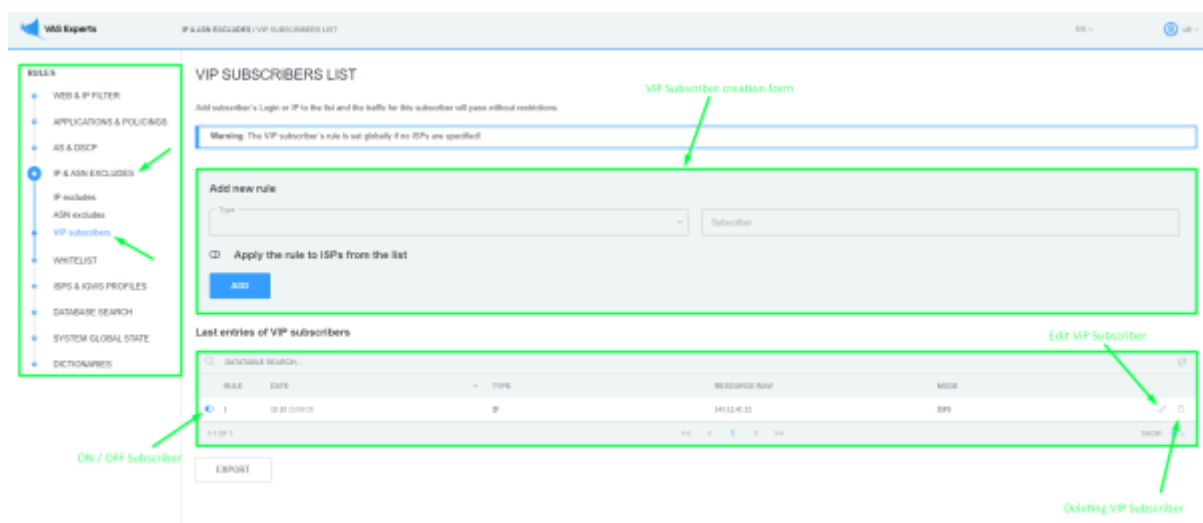
- Free access to applications and resources that are subject to restrictions on use.

Purpose of section

This section is designed to manage VIP Subscribers.

Getting started with section

Go to "IP & AC Exclusion"→"VIP Subscribers".



Creation

In the form of creating a VIP Subscriber:

- BSelect the type of IP or Login from the drop-down list;
- Specify IP or Login in the Subscriber field, depending on what you have chosen in the drop-down list;
- You can apply the rule to an ISP from the list and select multiple ISPs or click on the "Select All" button. If you accidentally clicked the "Select All" button, then click on the "Uncheck All" button;
- If your slider is disabled on apply to specific ISPs, then the new rule will be set globally to all ISPs.

Add new rule Enable or disable application to a specific ISP

Type: Subscriber:

☒ Apply the rule to ISPs from the list

Select ISP which the rule will be applied

☐ ISP Select all / Unselect all ISP
☒ Ростелеком
 ☐ SkyNet

☒ ДомРy
 ☐ MNS

Add VIP Subscriber

Save the VIP Subscriber by clicking the "Add" button.

Editing

Click on the "Edit VIP Subscriber" button. In the rule editing form, you can change:

- Application to certain ISPs from the list;
- Remove or add ISP.

Edit rule ×

VIP subscriber IP is 143.12.41.32.

☒ Apply the rule to ISPs from the list

Select ISP which the rule will be applied

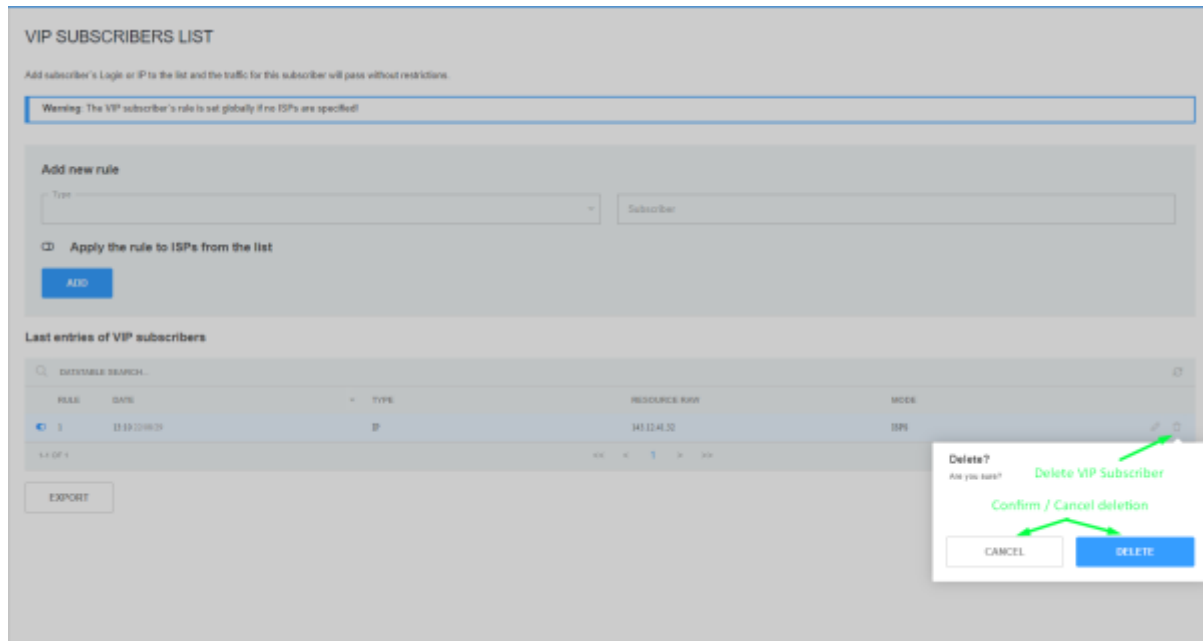
☒ ISP
 ☐ Ростелеком
 ☐ SkyNet

☐ ДомРy
 ☐ MNS

Save your changes by clicking the "Save" button.

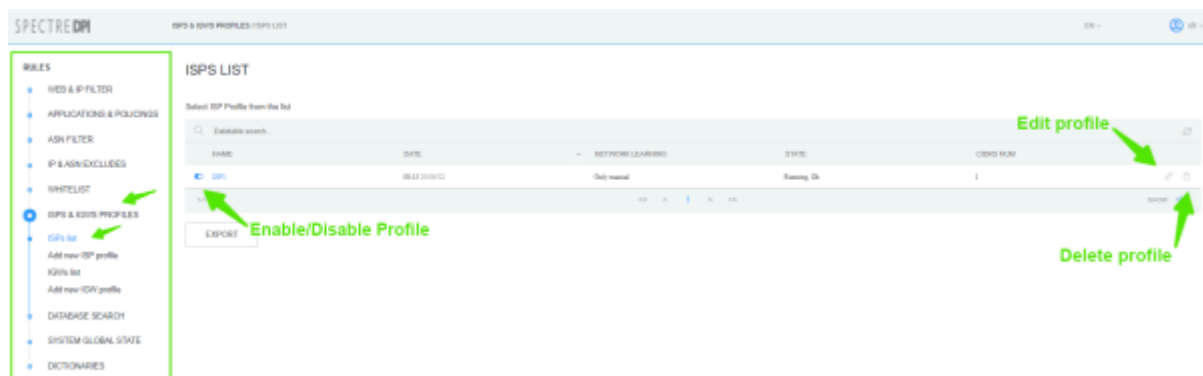
Deleting

In the list of VIP Subscribers, click on the "Delete VIP Subscriber" button and, in the window that appears, confirm or cancel the deletion.



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 changes you need and click on the "Save changes" or "Save and Disable/Enable" button.

Deleting ISP Profile

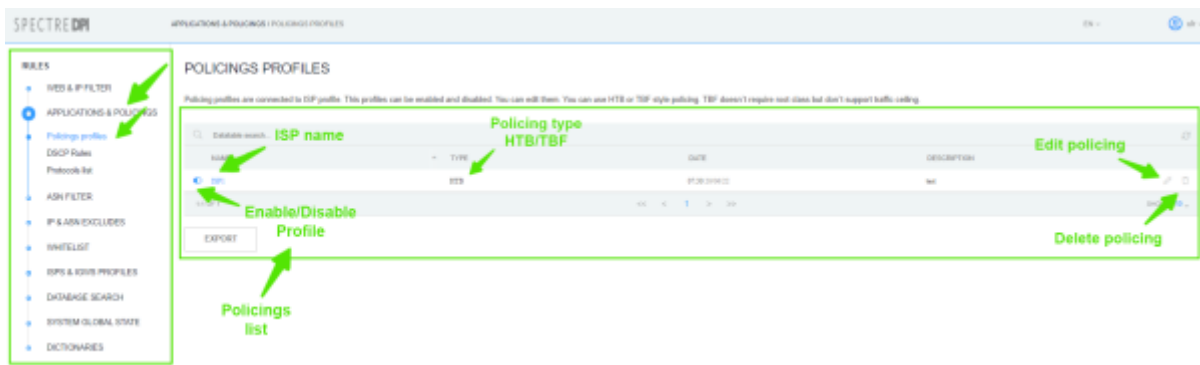
In the "ISPS & IGWS Profiles" section → "ISPs List" click on the "Delete" button and confirm/cancel the action.



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

Policing Profile

Change to the "Applications and Policing" profile → "Policing Profiles".



Editing Policing Profile

Click on the "Edit policing" button.

EDIT APPLICATION POLICING PROFILE #1

Policing profiles are connected to ISP profile. This profiles can be enabled and disabled. You can edit them. You can use HTB or TBF style policing. TBF doesn't require root class but don't support traffic ceiling.

Profile name: ISP1 (Enabled)

ISP profile configuration

Description:

Policing type:

Inbound profile:

INBOUND RATE	<input type="text" value="110"/>	UNIT	<input type="text" value="Mbps"/>	ROOT CEIL	<input type="text" value="0"/>	UNIT	<input type="text" value="Bps"/>	<input type="checkbox"/> Enable
CSS RATE	<input type="text" value="0"/>	UNIT	<input type="text" value="Bps"/>	CSS CEIL	<input type="text" value="110"/>	UNIT	<input type="text" value="Mbps"/>	<input type="checkbox"/> Static
CS1 RATE	<input type="text" value="0"/>	UNIT	<input type="text" value="Bps"/>	CS1 CEIL	<input type="text" value="110"/>	UNIT	<input type="text" value="Mbps"/>	<input type="checkbox"/> Static
CS2 RATE	<input type="text" value="0"/>	UNIT	<input type="text" value="Bps"/>	CS2 CEIL	<input type="text" value="110"/>	UNIT	<input type="text" value="Mbps"/>	<input type="checkbox"/> Static
CS3 RATE	<input type="text" value="0"/>	UNIT	<input type="text" value="Bps"/>	CS3 CEIL	<input type="text" value="110"/>	UNIT	<input type="text" value="Mbps"/>	<input type="checkbox"/> Static
CS4 RATE	<input type="text" value="0"/>	UNIT	<input type="text" value="Bps"/>	CS4 CEIL	<input type="text" value="110"/>	UNIT	<input type="text" value="Mbps"/>	<input type="checkbox"/> Static
CS5 RATE	<input type="text" value="0"/>	UNIT	<input type="text" value="Bps"/>	CS5 CEIL	<input type="text" value="110"/>	UNIT	<input type="text" value="Mbps"/>	<input type="checkbox"/> Static

☐ Applications CS8 list
☐ Applications CS1 list
☐ Applications CS2 list
☐ Applications CS3 list
☐ Applications CS4 list
☐ Applications CS5 list

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.

To save the changes click on the button "Save profile" or "Save and disable/enable".



Thy policing profile is disabled by default.

Deleting 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.

WEB & IP FILTER

WebIP firewall summary

TYPE	ACTIVE	DISABLED	TOTAL
OS	4	0	4
OS	4	0	4

Last entries in WebIP register

PROJID	DATE	TYPE	RESOURCE NAME	RESOURCE VALIDATED	REGULATOR	REASON
Default	11.08.2019 17	OS	malware	*malware	RSG 1	Tam
Default	11.08.2019 17	OS	malware	*malware	RSG 1	Tam
Default	11.08.2019 17	OS	malware	*malware	RSG 1	Tam
Default	11.08.2019 17	OS	malware	*malware	RSG 1	Tam
Default	11.08.2019 17	OS	malware	*malware	RSG 1	Tam
Default	11.08.2019 17	OS	malware	*malware	RSG 1	Tam
Default	11.08.2019 17	OS	malware	*malware	RSG 1	Tam
Default	11.08.2019 17	OS	malware	*malware	RSG 1	Tam

Edit rule

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;

ADD RULE #NEW

Rule ID: 0

Resource: REG 111

Category: CAT 111

Public description: Public Description

Internal description: Internal Description

Resource

Select type of resource and put the URL, SNI, CN, IP, IP-PORT or CDR in this field.

Resource: facebook.com

Type: URL

VALIDATE

Validation result: This is SSL/TLS resource. We can block FULL DOMAIN! Next SNI and CN will be added to the list: SNI: facebook.com, CN: facebook.com, CN: facebook.com

ADD TO LIST

IMPORT FROM FILE

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

- If it is not necessary to validate the resource, 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.

List of resources

TYPE	RESOURCE ANY	RESOURCE VALIDATED	STATUS	Delete resource
SSL	facebook.com	*facebook.com	VALID	
SSL	facebook.com	facebook.com	VALID	
CN	facebook.com	*facebook.com	VALID	
CN	facebook.com	facebook.com	VALID	

CLEAR ALL

Apply the rule to ISPs from the list

Select ISP which the rule will be applied

☐ ISP1

SELECT ALL

UNSELECT ALL

Applying the rule to ISP profile

Actions log

DATE	USER	ACTION	NEW VALUE	OLD VALUE
Data not found				

SAVE CHANGES

SAVE AND DISABLE

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.

Select type of resource and put the URL, SNL, CN, IP, IP:PORT or CIDR to this field.

Resource: Type:

List of resources

TYPE	RESOURCE NAME	RESOURCE VALUATED	STATUS
❏ CI	facebook.com	facebook.com	Valid
❏ CI	facebook.com	*facebook.com	Valid
❏ IDC	facebook.com	facebook.com	Valid
❏ IDC	facebook.com	*facebook.com	Valid

☐ Apply the rule to ISPs from the list The rule will be applied for all ISPs by default.

Actions log

DATE	USER	ACTION	NEW VALUE	OLD VALUE
11.23.2019.01.21	ad	The rule created		

Delete rule (green arrow pointing to the DELETE 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".

SPECTRE DM WEB & IP FILTER | CHECK DOMAIN

RALES

- WEB & IP FILTER (selected)
- Add new rule
- Check domain
- Search database
- APPLICATIONS & POLICIES
- ASN FILTER
- IP & ASN EXCLUSIONS
- WHITELIST
- ISPs & ISPs PROFILES
- DATABASE SEARCH
- SYSTEM GLOBAL STATE
- DICTIONARIES

CHECK DOMAIN

Enter IP or URL with http/https prefix to check resource create correct rule

Resource Check:

Domain check form (green arrow pointing to the form)

In the "Resource Check" field type in the URL of resource 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.

CHECK DOMAIN

Enter IP or URL, with http/https prefix to check resource create control rule

Resource search
http://www

Certificate info

CHECK

This is SSL/TLS resource. Type of block is FULL DOMAIN

SSL/TLS, locking type

Certificate general information

Common name	http://www
Issued To	www.http://www
Issued To CN	http://www
Issued To OU	http://www
Issued To O	http://www
Issued To ST	http://www
Total number of SSL/TLS	1
SSL	
Signature algorithm	sha256WithRSAEncryption
Key type	RSA
Key size	2048 bits
Serial Number	2176233871346247098714701
Issued Before	11.08.2018 12:00:00
Issued After	08.08.2018 12:00:00
Number of valid	1

DNS info

TYPE	DOMAIN/VALUE	ADDRESS	TTL
A	http://www	171.255.24.81	300
A	http://www	171.255.24.81	300
A	http://www	171.255.24.81	300
A	http://www	171.255.24.81	300
NS	http://www	ns1.http://www	600
NS	http://www	ns2.http://www	600
NS	http://www	ns3.http://www	600
NS	http://www	ns4.http://www	600
SOA	http://www	ns1.http://www	3600
MX	http://www	mail.http://www	300

Result information

To block this resource only with certificate use	
QID	http://www
QID	*http://www
QID	http://www
QID	*http://www

DNS list

Recommendations
for resource locking

Download file to report to rule

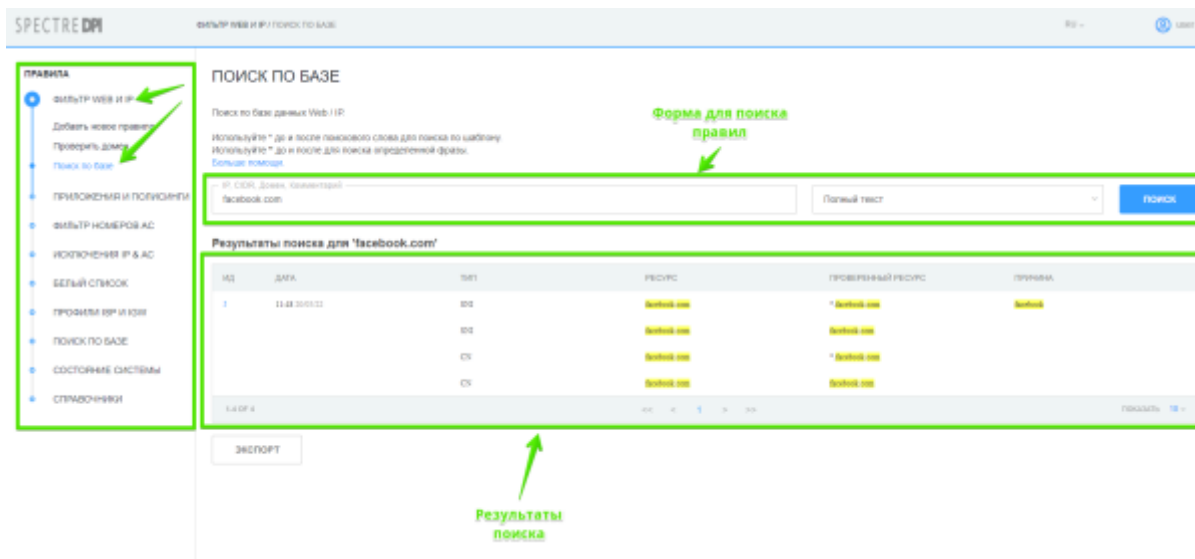
DOWNLOAD FILE 1

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.

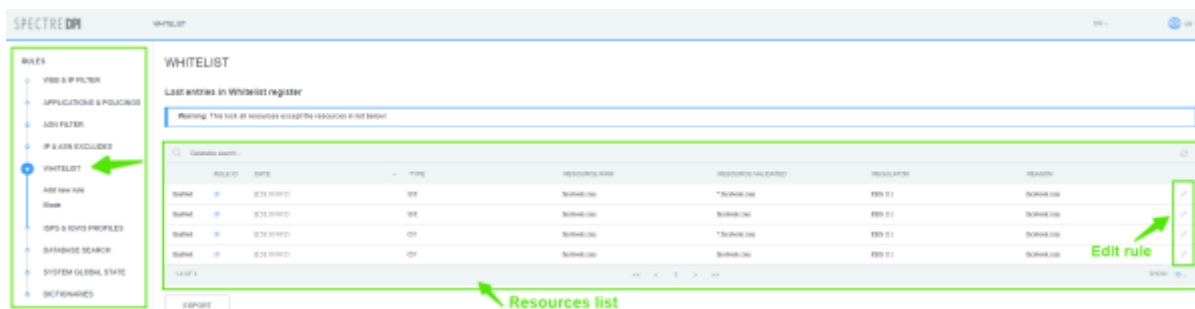
As a result, all blocking rules that match the selected search parameters will be displayed.



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 category;
- Enter rule public description;
- Enter rule hidden description;

Resource

Select type of resource and put the URL, DNS, CIDR, IP, IP-PORT or CIDR to this field.

Resource: Type:

List of resources

TYPE	RESOURCE NAME	RESOURCE ALIASES	STATUS
IP	Resource.com	Resource.com	1000
IP	Resource.com	*Resource.com	1000
IP	Resource.com	Resource.com	1000
IP	Resource.com	*Resource.com	1000

☐ Apply the rule to ISPs from the list. The rule will be applied for all ISPs by default.

Actions log

DATE	USER	ACTION	NEW VALUE	STATUS
12.12.2017	id	Disable internet		

1 / 1 OF 1

Delete rule



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".

SPECTRE DPI

WHITELIST / MODE

Global Whitelist

Set mode for Global Whitelist. If activated all Whitelist rules marked as global. The Global Whitelist rules applied for all ISPs.

State: ☒ **Enable/Disable whitelist**

Whitelist for ISPs

Set Whitelist mode for ISPs. If enabled for some ISP the Whitelist rules which connected to ISP will be applied.

ISP	WHITELIST
DPI	<input checked="" type="checkbox"/>

Enable/Disable whitelist for ISP

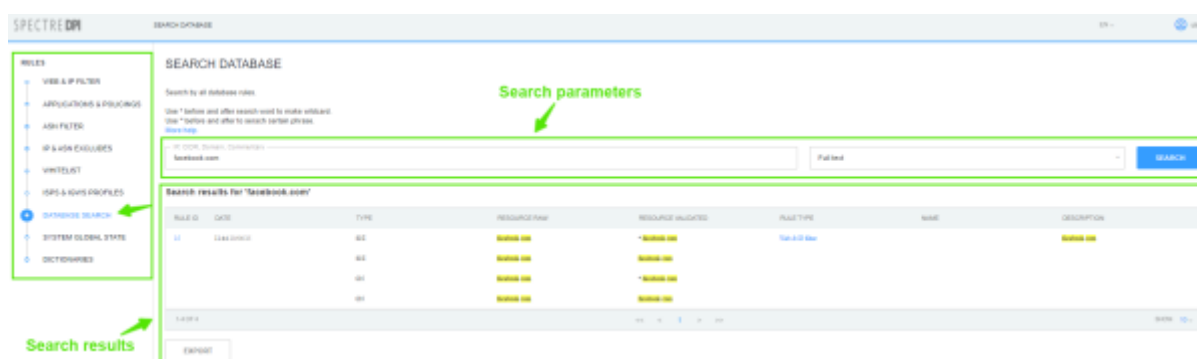
- With the global whitelist mode enabled, the whitelist service is applied to all ISP profiles and resource lists are formed only from global whitelist rules;
- When the whitelist mode is enabled for a separate ISP profile, the service is applied only to ISP which has it enabled. The lists are formed 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.

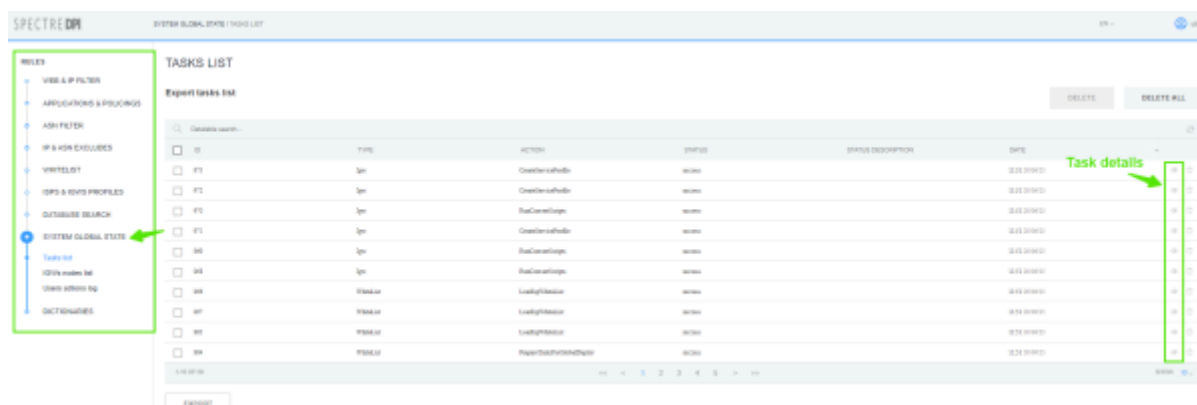
In the "IP, CIDR, Domain, Comment" field enter the value in accordance with the prompts at the top of the page, choose search type: Full Text, By Resources or By Description. Click on "Search" button.

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.