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:

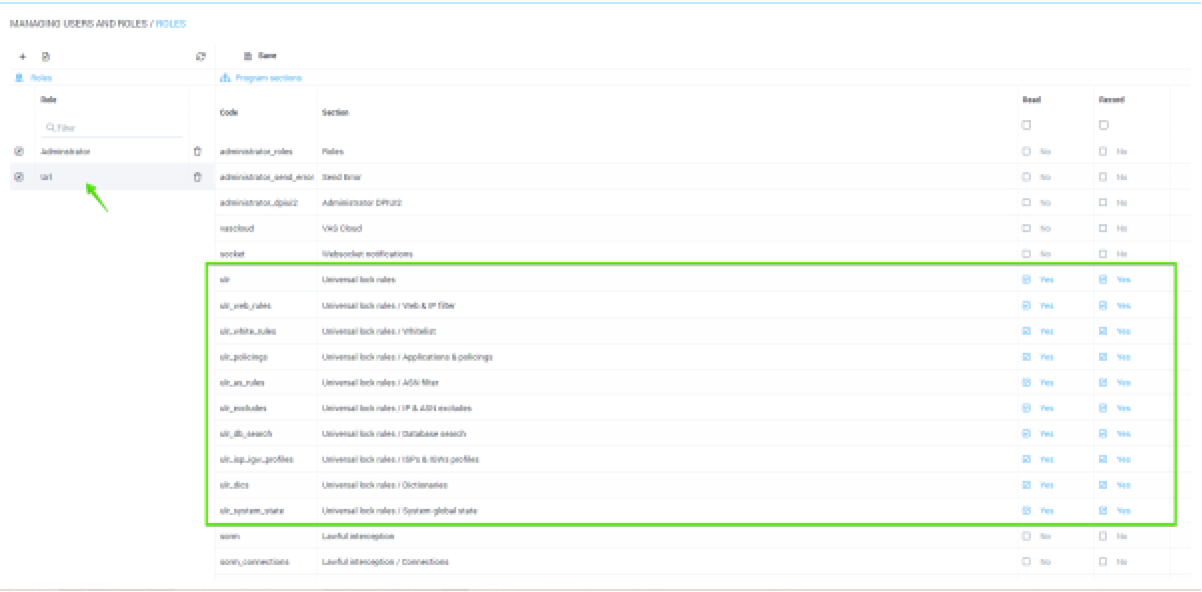
1. Enter license level: standard
2. Enter the license completion date in the Y-m-d format (e.g. 2099-12-31)
3. Enter the license password.

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:

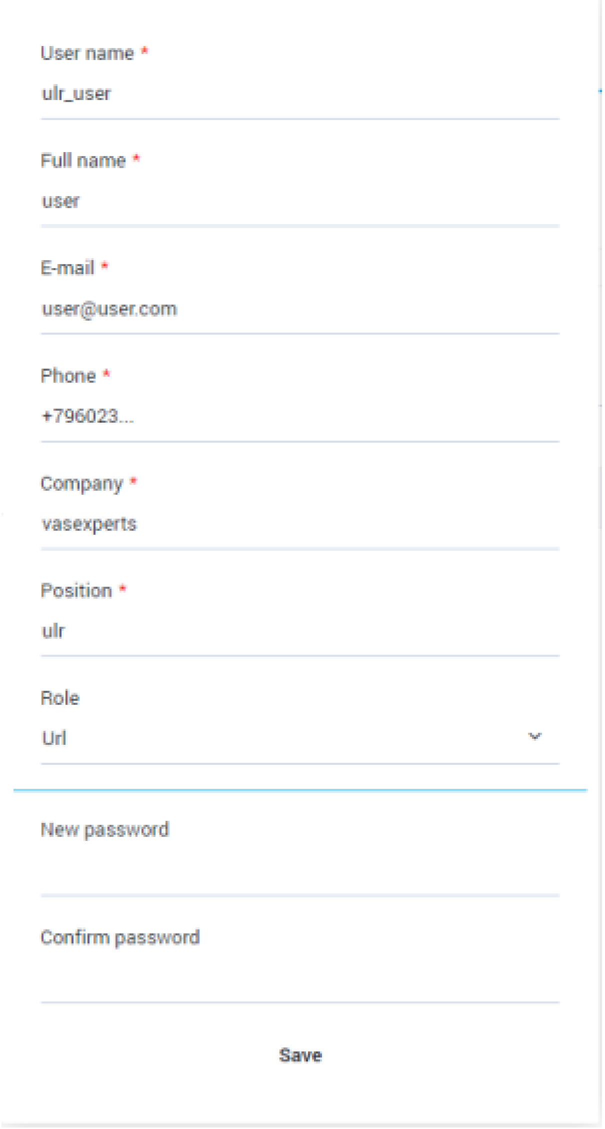


MANAGING USERS AND ROLES / ROLES

Role
Administrator
ulr1

Code	Section	Read	Record
		□	□
administrator_roles	Roles	□ No	□ No
administrator_send_error	Send Error	□ No	□ No
administrator_dpiui2	Administrator DPIUI2	□ No	□ No
vascloud	VAS Cloud	□ No	□ No
socket	Websocket notifications	□ No	□ No
ulr	Universal lock rules	☑ Yes	☑ Yes
ulr_web_rules	Universal lock rules / Web & IP filter	☑ Yes	☑ Yes
ulr_white_rules	Universal lock rules / Whitelist	☑ Yes	☑ Yes
ulr_policings	Universal lock rules / Applications & policings	☑ Yes	☑ Yes
ulr_as_rules	Universal lock rules / ASN filter	☑ Yes	☑ Yes
ulr_excludes	Universal lock rules / IP & ASN excludes	☑ Yes	☑ Yes
ulr_db_search	Universal lock rules / Database search	☑ Yes	☑ Yes
ulr_isp_igw_profiles	Universal lock rules / ISPs & IGWs profiles	☑ Yes	☑ Yes
ulr_dics	Universal lock rules / Dictionaries	☑ Yes	☑ Yes
ulr_system_state	Universal lock rules / System global state	☑ Yes	☑ Yes
sorm	Lawful interception	□ No	□ No
sorm_connections	Lawful interception / Connections	□ No	□ No

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

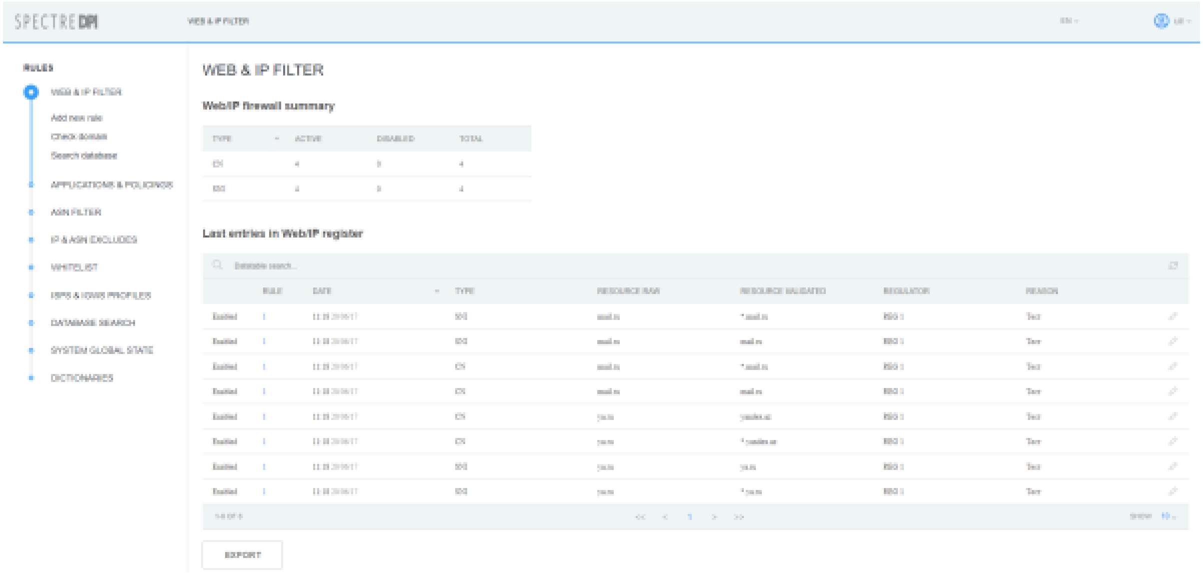
Position *
ulr

Role
Url

New password

Confirm password

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



WEB & IP FILTER

Web/IP firewall summary

TYPE	ACTIVE	DISABLED	TOTAL
CN	4	0	4
DNS	4	0	4

Last entries in Web/IP register

	RULE	DATE	TYPE	RESOURCE RAW	RESOURCE VALIDATED	REGULATOR	REASON
Enabled	1	[illegible]	DNS	mail.ru	*.mail.ru	[illegible]	Test
Enabled	1	[illegible]	DNS	mail.ru	mail.ru	[illegible]	Test
Enabled	1	[illegible]	CN	mail.ru	*.mail.ru	[illegible]	Test
Enabled	1	[illegible]	CN	mail.ru	mail.ru	[illegible]	Test
Enabled	1	[illegible]	CN	ya.ru	yandex.ru	[illegible]	Test
Enabled	1	[illegible]	CN	ya.ru	*.yandex.ru	[illegible]	Test
Enabled	1	[illegible]	DNS	ya.ru	ya.ru	[illegible]	Test
Enabled	1	[illegible]	DNS	ya.ru	*.ya.ru	[illegible]	Test

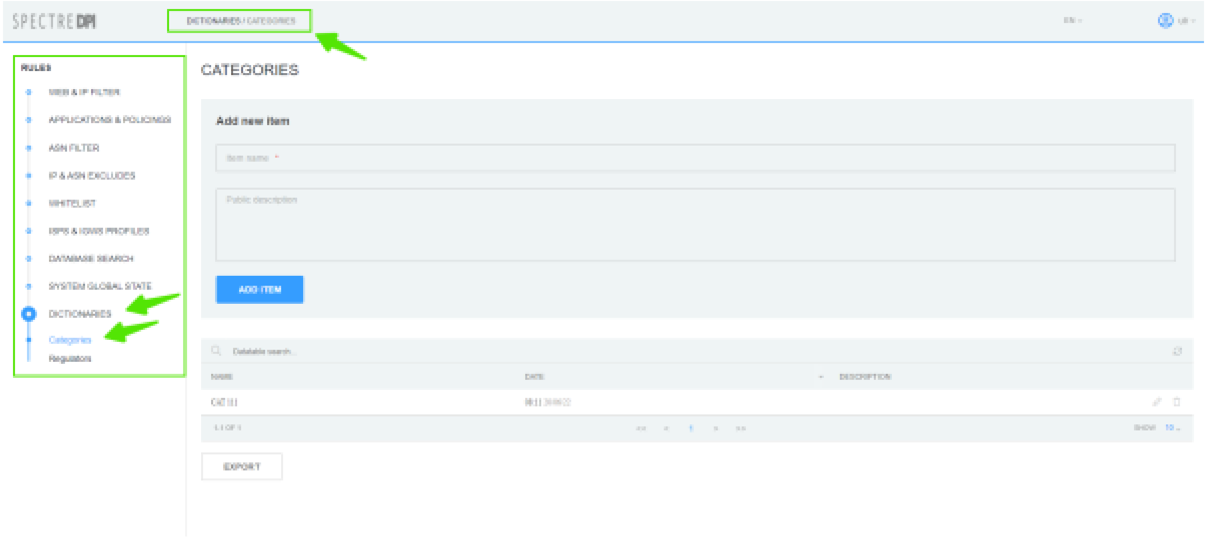
Dictionaries Configuration

- Category Dictionary
- Regulators Dictionary

These dictionaries are used for creating/editing locking rules.

Category Dictionary

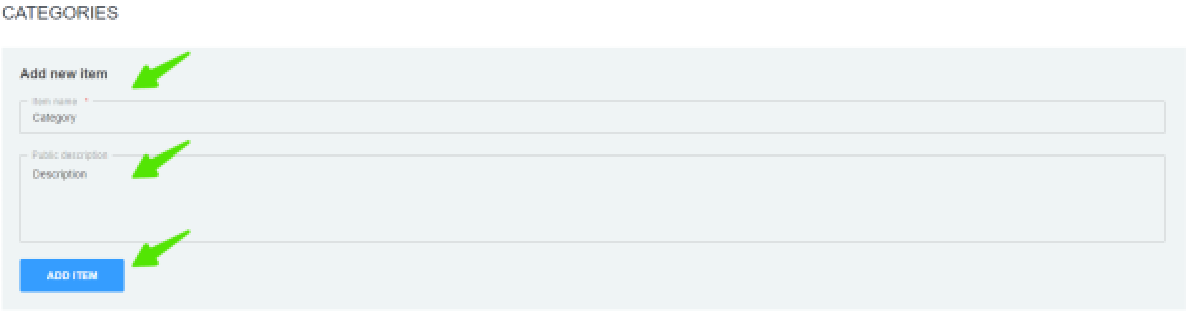
In the Locking Rules management interface go to the Dictionaries → Categories section.



NAME	DATE	DESCRIPTION
CAT 111	[illegible]	

Creating

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

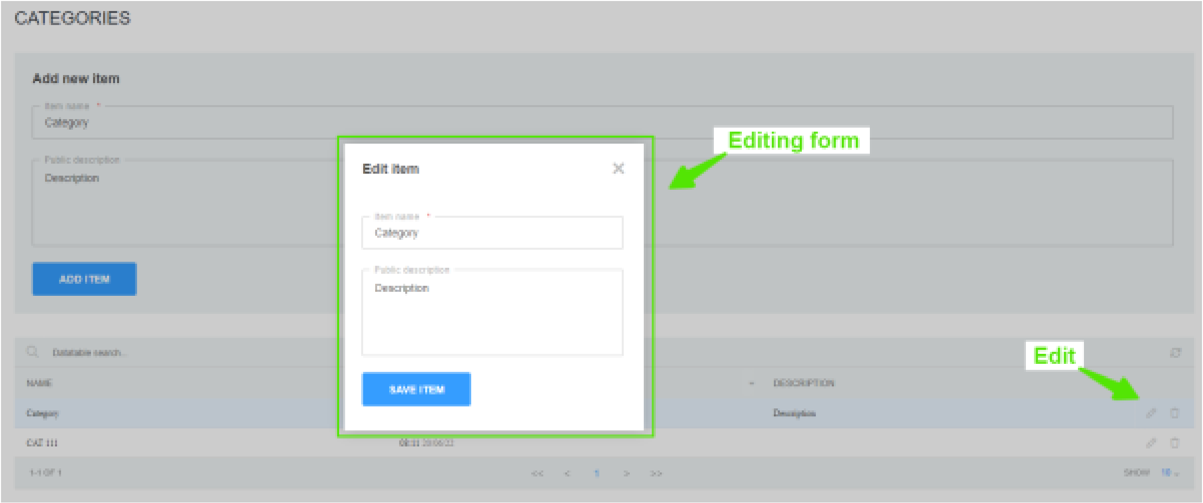


Item name *: Category

Public description: Description

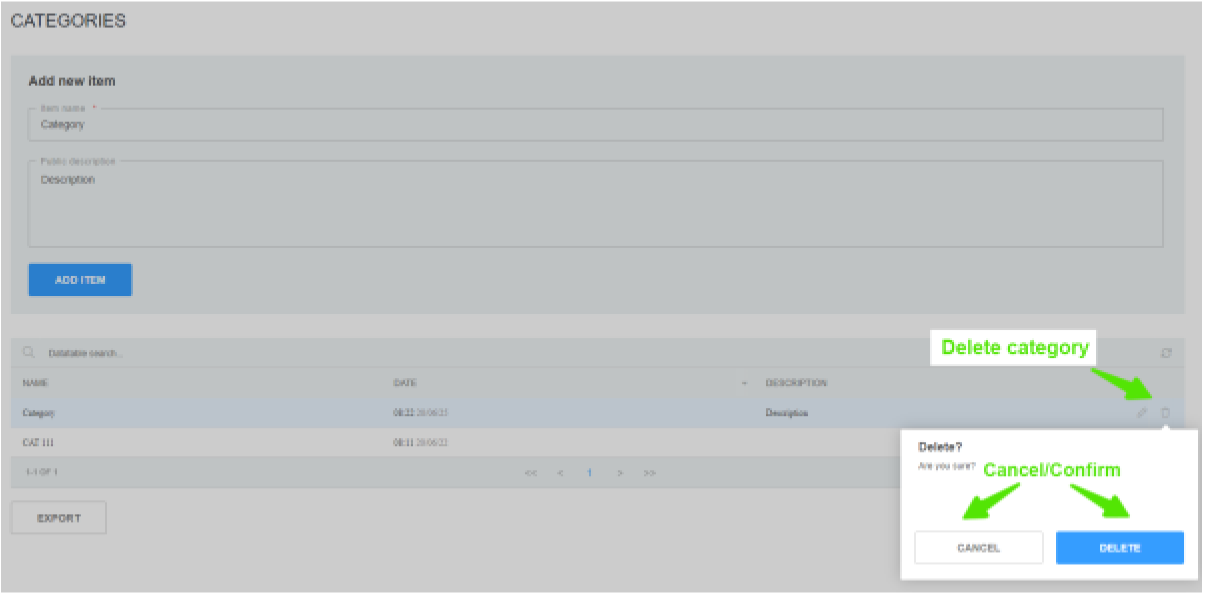
Editing

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.

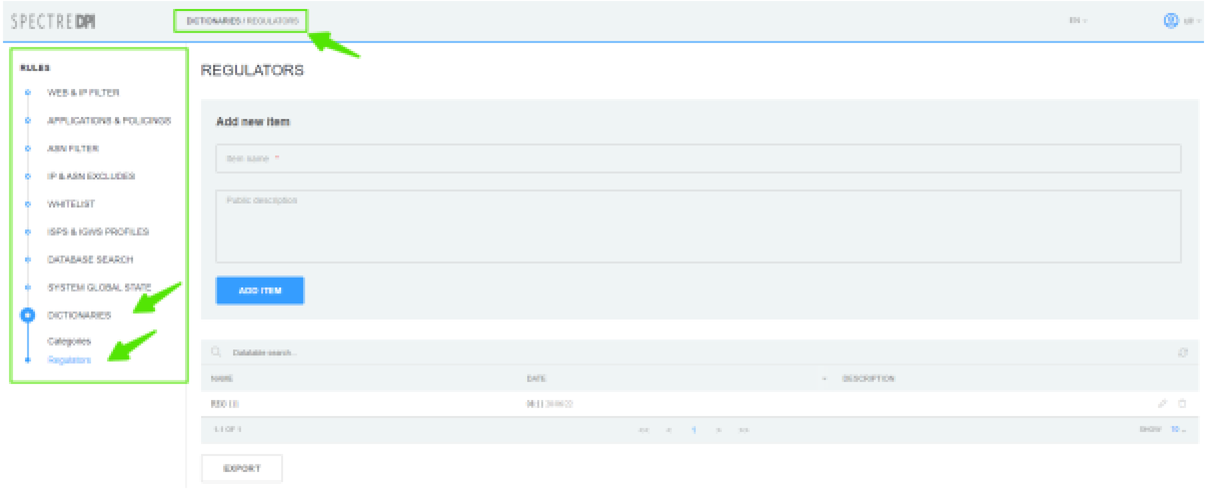


NAME	DATE	DESCRIPTION
Category	08:22 20/06/22	Description
CAT 111	08:11 20/06/22	

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

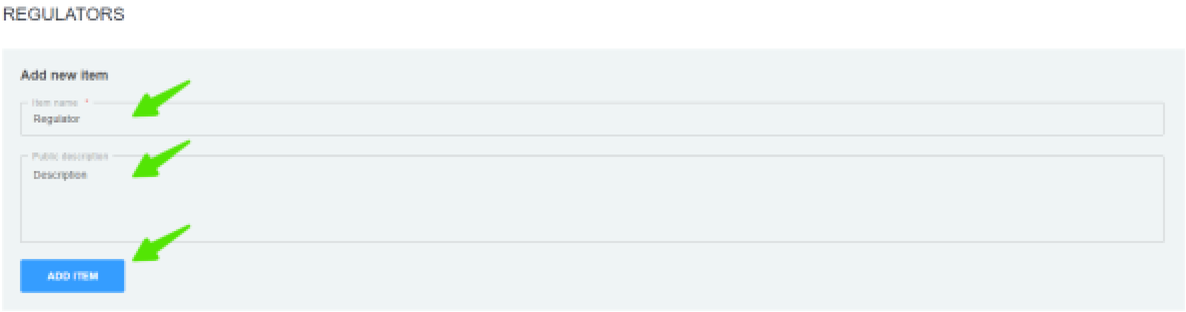
Regulators Dictionary

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.

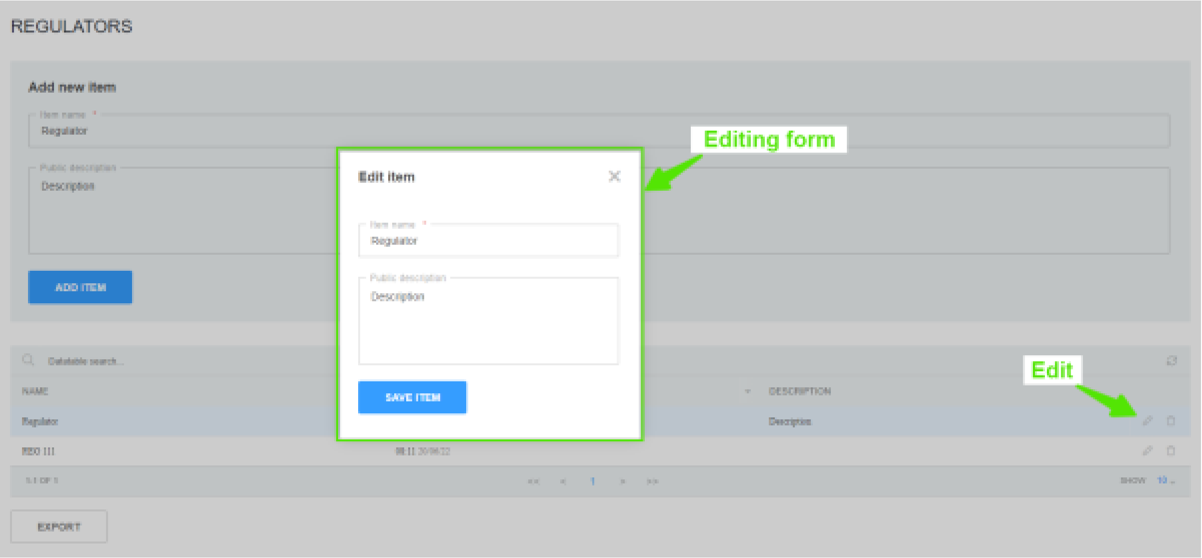


Item name *: Regulator

Public description: Description

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.



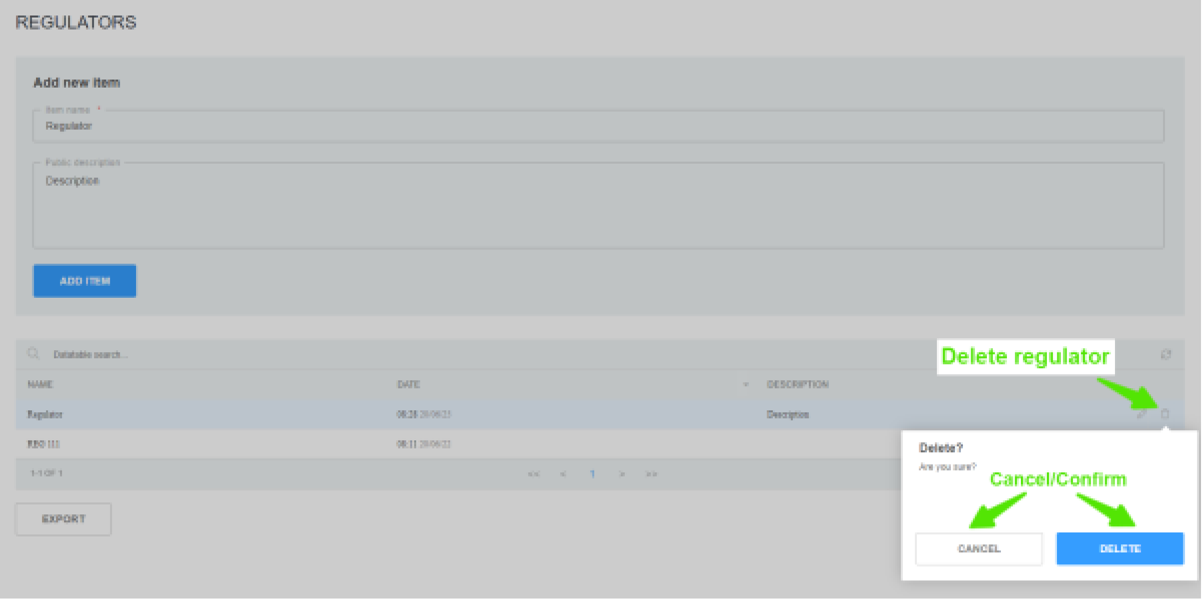
Item name *: Regulator

Public description: Description

NAME	DATE	DESCRIPTION
Regulator		Description
REG III	08.11 20/06/22	

Deleting

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



Item name *: Regulator

Public description: Description

NAME	DATE	DESCRIPTION
Regulator	08:28 20/06/23	Description
REG 111	08:11 20/06/23	

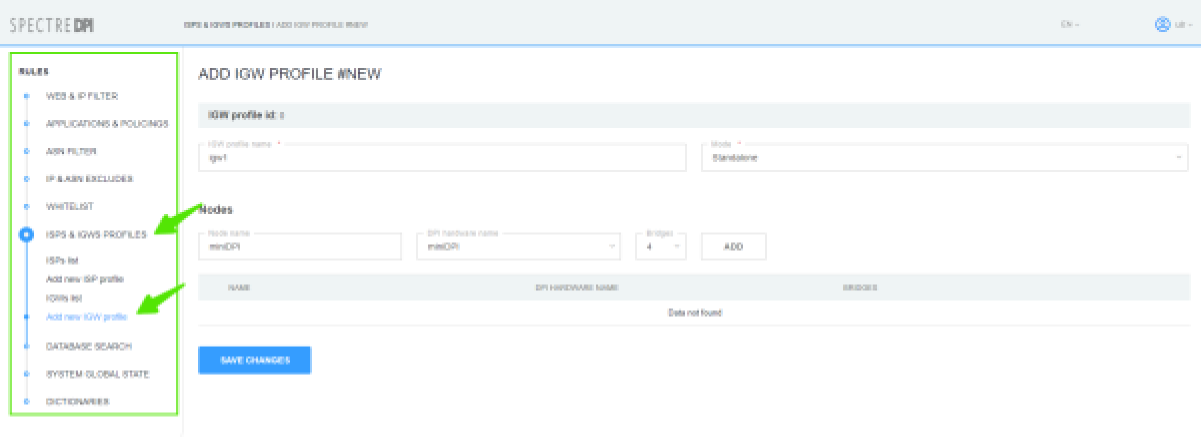
Delete?

Are you sure?

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".



ADD IGW PROFILE #NEW

IGW profile id: 0

IGW profile name *: igw1

Mode *: Standalone

Nodes

Node name: miniDPI

DPI hardware name: miniDPI

Bridges: 4

NAME	DPI HARDWARE NAME	BRIDGES
Data not found		

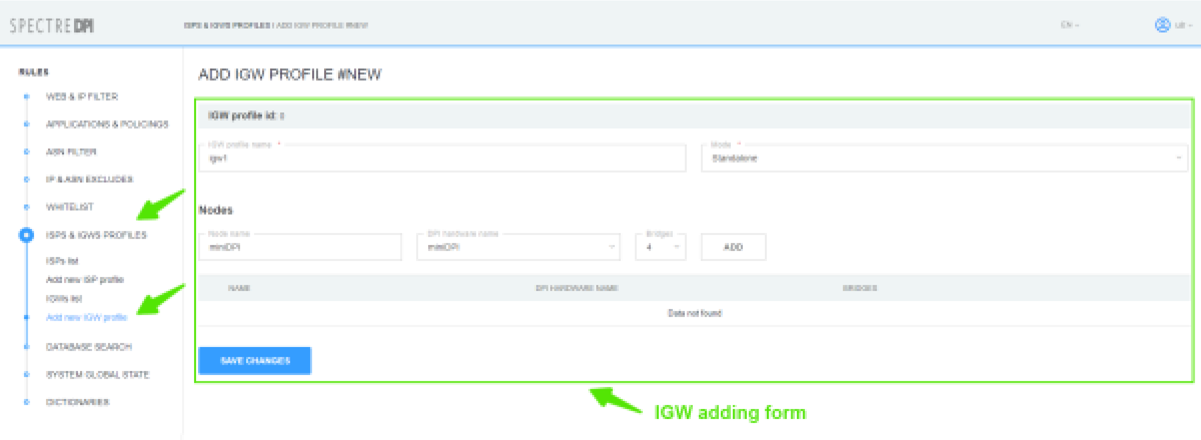
Creating

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:

IGW profile name *: igw1

Mode *: Standalone

Nodes

Node name: miniDPI

DPI hardware name: miniDPI

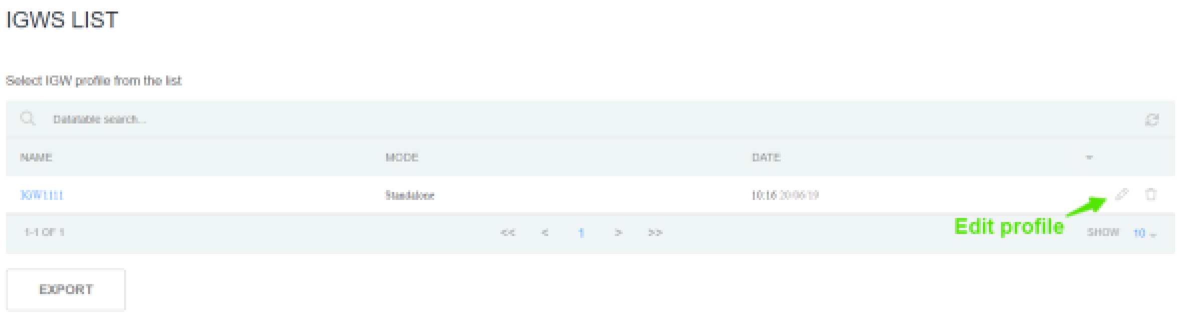
Bridges: 4

NAME	DPI HARDWARE NAME	BRIDGES
Data not found		

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

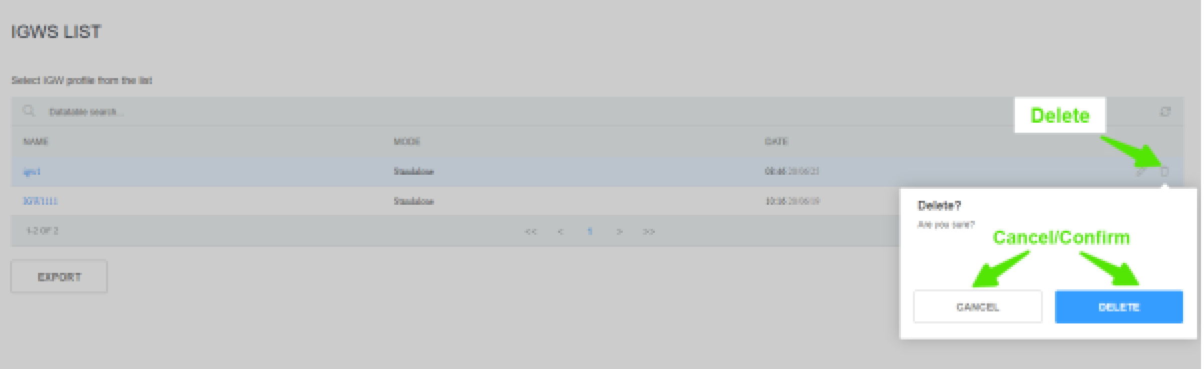
NAME	MODE	DATE
IGW1111	Standalone	10:16 20/06/19

1-1 OF 1

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.



IGWS LIST

Select IGW profile from the list

Datatable search...

NAME	MODE	DATE
igw1	Standalone	08:46 20.06.21
IGW1111	Standalone	10:16 20.06.19

1-2 OF 2

Delete?

Are you sure?

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
```

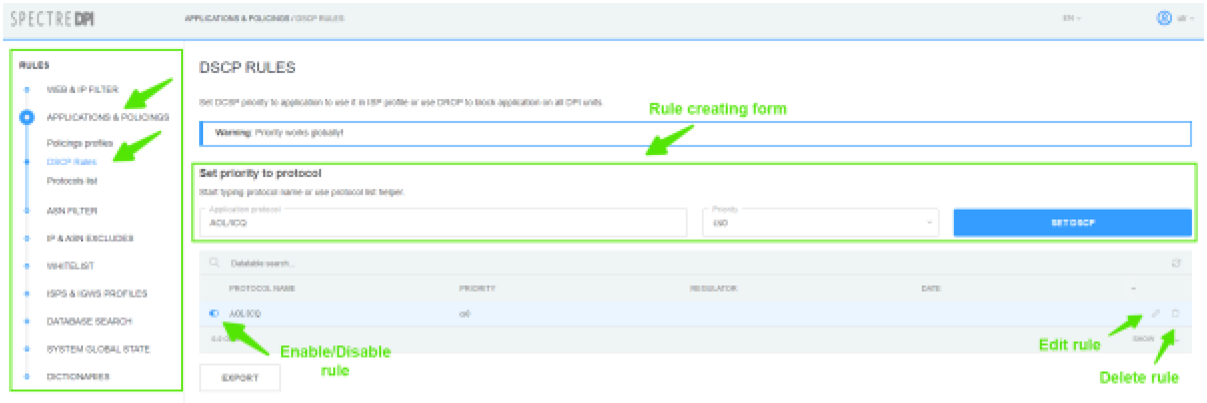
4. In dpiui2 configuration specify the web-server access parameters in ULR settings section

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".



Set DCSP priority to application to use it in ISP profile or use DROP to block application on all DPI units.

Warning: Priority works globally!

Set priority to protocol

Start typing protocol name or use protocol list helper.

Application protocol: AOL/ICQ

Priority: cs0

AOL/ICQ cs0

Rule creating form

Enable/Disable rule

Edit rule

Delete rule

Creating

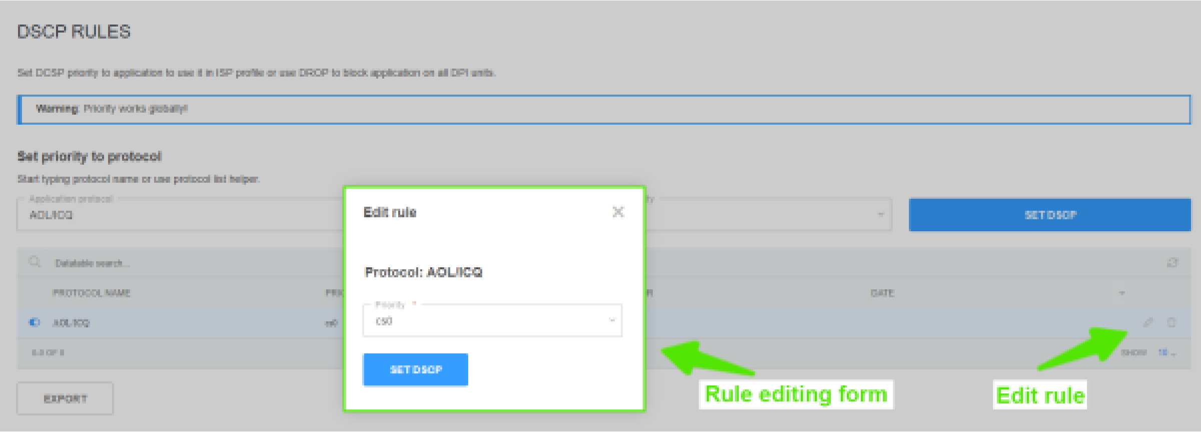
In the form of rule creating:

- 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.



DSCP RULES

Set DCSP priority to application to use it in ISP profile or use DROP to block application on all DPI units.

Warning: Priority works globally!

Set priority to protocol

Start typing protocol name or use protocol list helper.

Application protocol: AOL/ICQ

PROTOCOL NAME	PRI...	...R	DATE
AOL/ICQ	cs0		

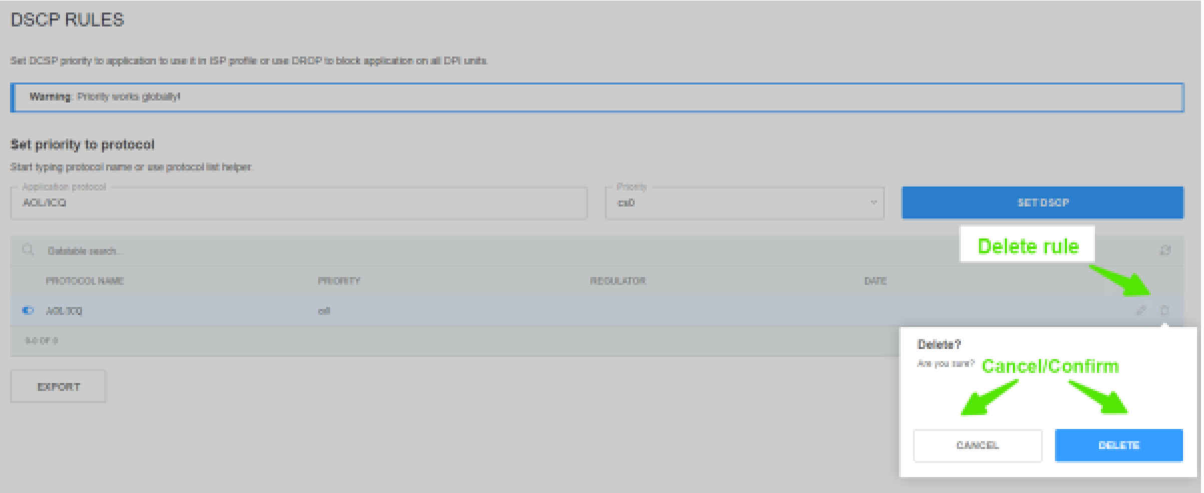
Edit rule

Protocol: AOL/ICQ

Priority *: cs0

Deleting

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



DSCP RULES

Set DCSP priority to application to use it in ISP profile or use DROP to block application on all DPI units.

Warning: Priority works globally!

Set priority to protocol

Start typing protocol name or use protocol list helper

Application protocol: AOL/ICQ

Priority: cs0

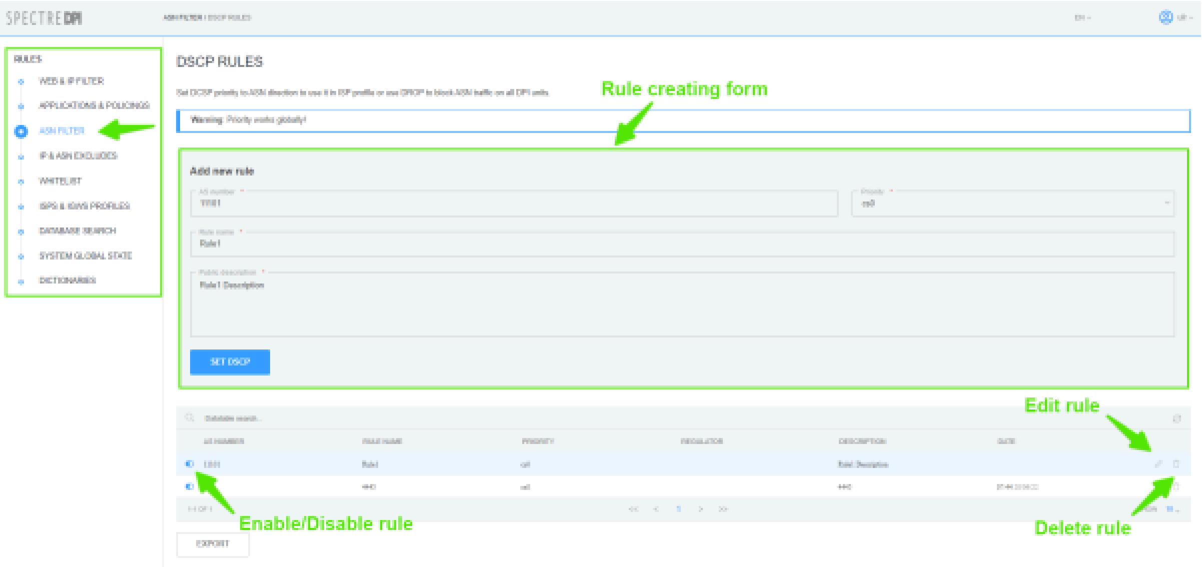
PROTOCOL NAME	PRIORITY	REGULATOR	DATE
AOL/ICQ	cs0		

Delete?

Are you sure?

ASN Filter

Change to the "ASN Filter" section.



Creating

In the form of rule creating:

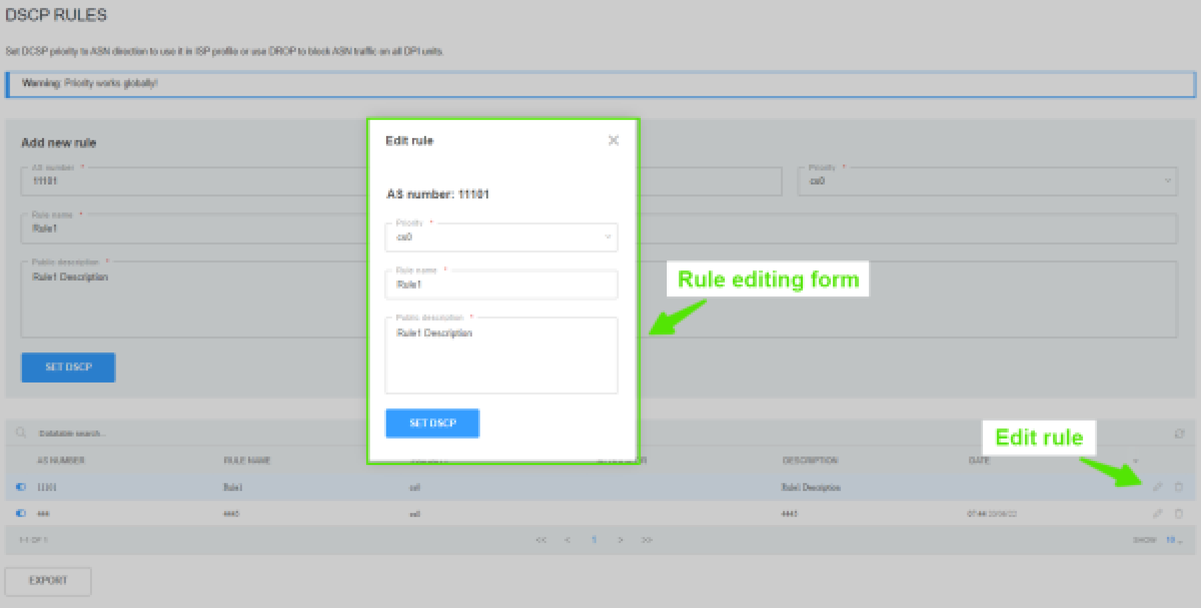
- Specify the number of AS;
- Choose the priority from the list;
- Enter the rule name;
- Enter the rule description.

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.



DSCP RULES

Set DCSP priority to ASN direction to use it in ISP profile or use DROP to block ASN traffic on all DPI units.

Warning: Priority works globally!

Add new rule

AS number *: 11101

Priority *: cs0

Rule name *: Rule1

Public description *: Rule1 Description

Edit rule

AS number: 11101

Priority *: cs0

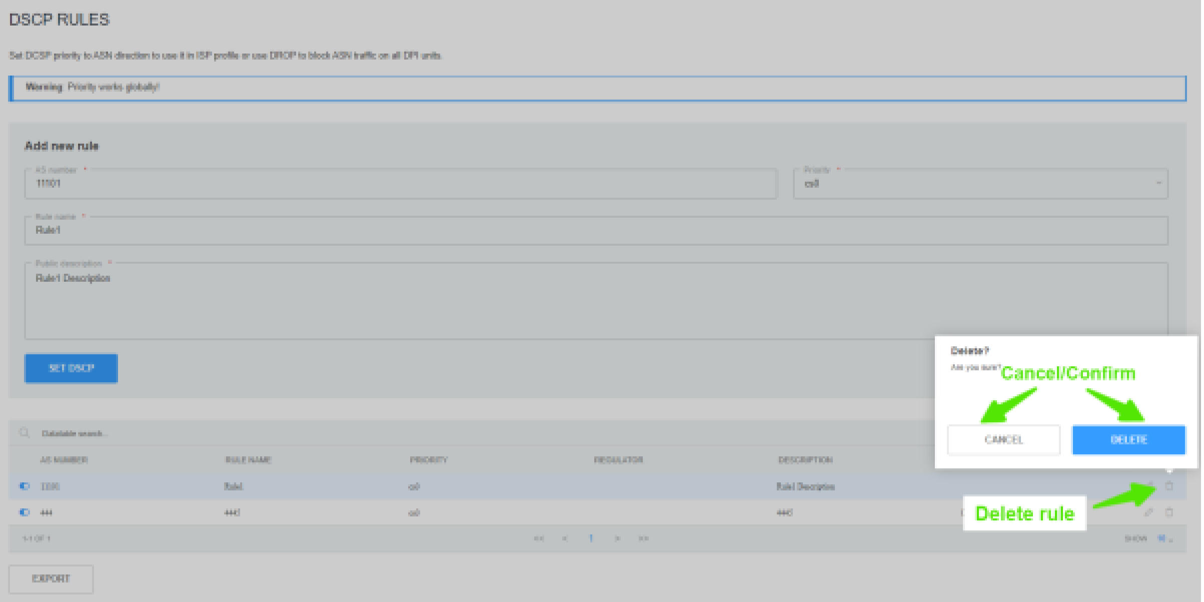
Rule name *: Rule1

Public description *: Rule1 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.



DSCP RULES

Set DCSP priority to ASN direction to use it in ISP profile or use DROP to block ASN traffic on all DPI units.

Warning: Priority works globally!

Add new rule

AS number *: 11101

Priority *: cs0

Rule name *: Rule1

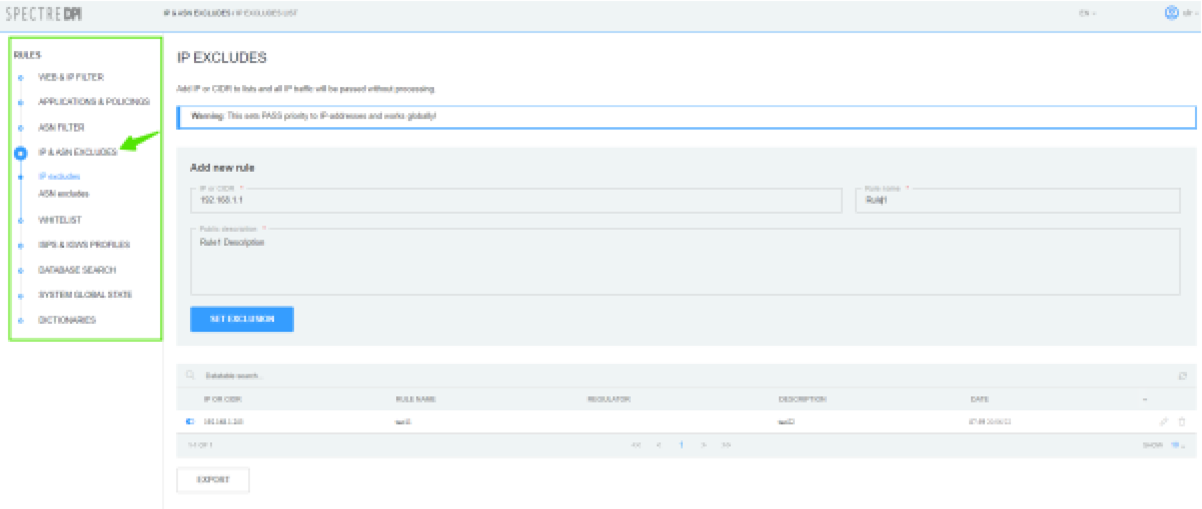
Public description *: Rule1 Description

Delete?

Are you sure?

IP & ASN Excludes

Change to the "IP & ASN Excludes" section.



IP EXCLUDES

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

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

Add new rule

IP or CIDR * 192.168.1.1

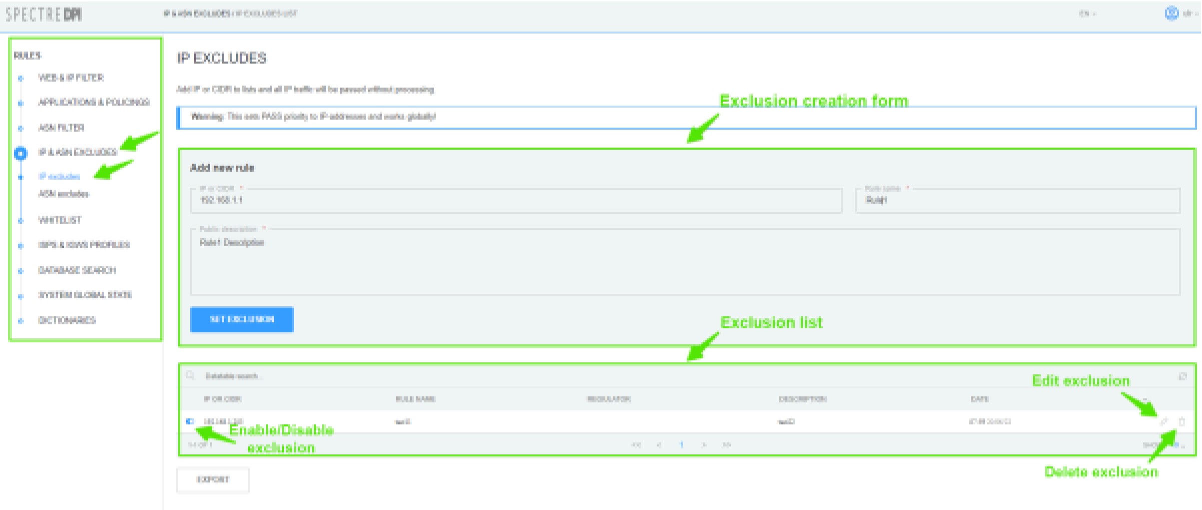
Rule name * Rule1

Public description * Rule1 Description

IP OR CIDR	RULE NAME	REGULATOR	DESCRIPTION	DATE

IP Excludes

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



IP EXCLUDES

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

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

Add new rule

IP or CIDR * 192.168.1.1

Rule name * Rule1

Public description * Rule1 Description

IP OR CIDR	RULE NAME	REGULATOR	DESCRIPTION	DATE

Creating

In the form of rule creating:

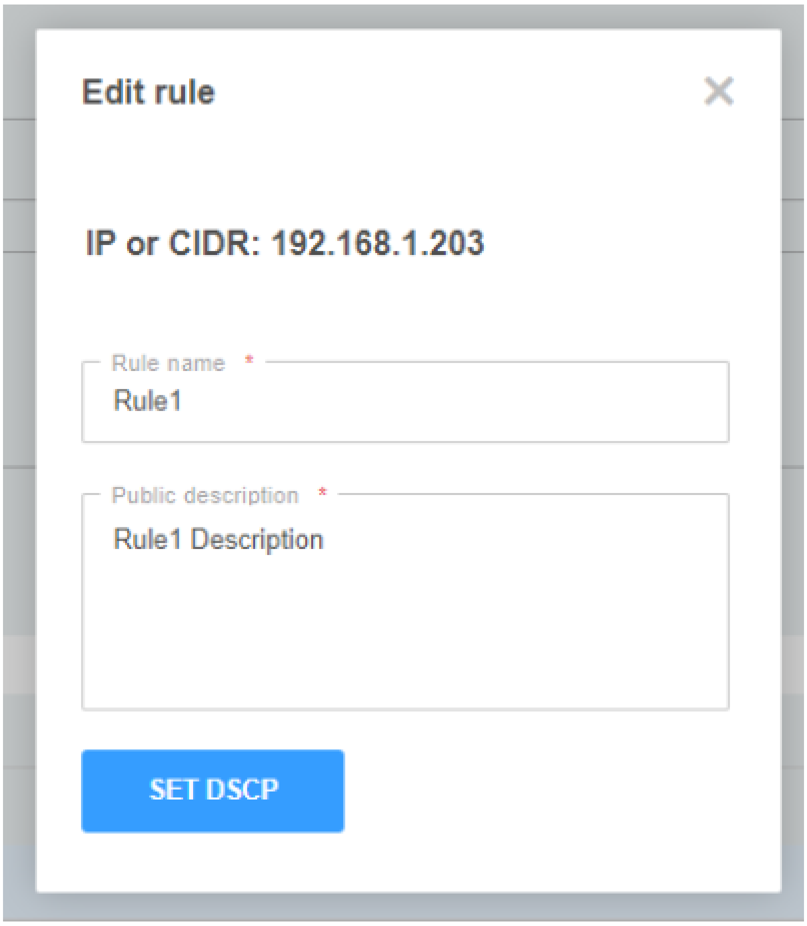
- Specify IP/CIDR;
- Enter the rule name;
- Enter the rule descriptuin;

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.



Edit rule

IP or CIDR: 192.168.1.203

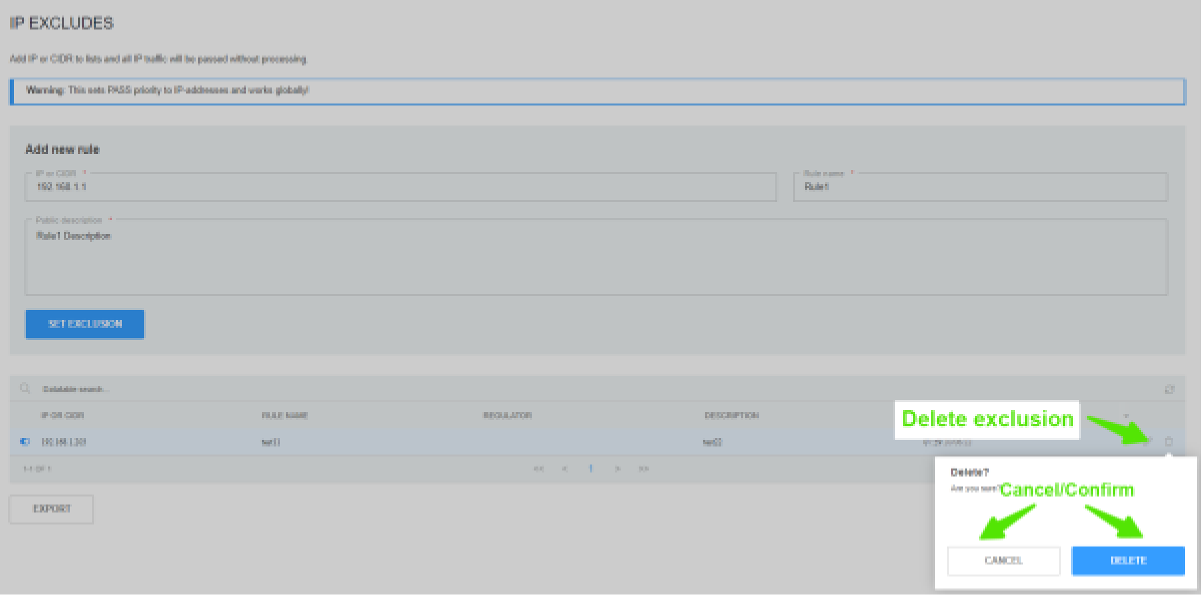
Rule name *: Rule1

Public description *: Rule1 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.



IP EXCLUDES

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

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

Add new rule

IP or CIDR *: 192.168.1.1

Rule name *: Rule1

Public description *: Rule1 Description

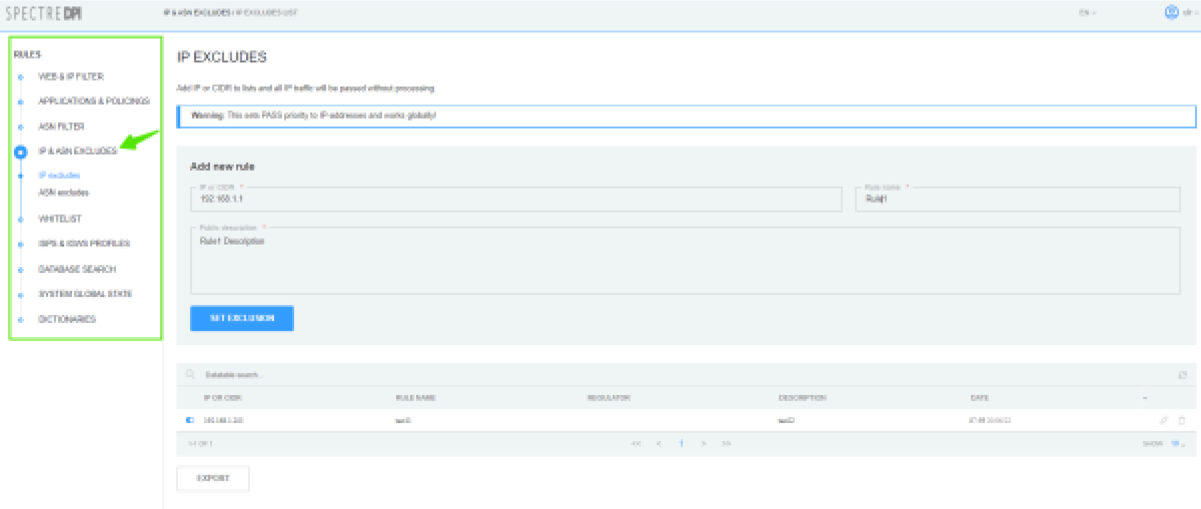
IP OR CIDR	RULE NAME	REGULATOR	DESCRIPTION
192.168.1.201	test1		test2

Delete?

Are you sure?

ASN Excludes

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



IP EXCLUDES

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

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

Add new rule

IP or CIDR *: 192.168.1.1

Rule name *: Rule1

Public description *: Rule1 Description

IP OR CIDR	RULE NAME	REGULATOR	DESCRIPTION	DATE
[illegible]	[illegible]		[illegible]	[illegible]

Creating

In the form of rule creating:

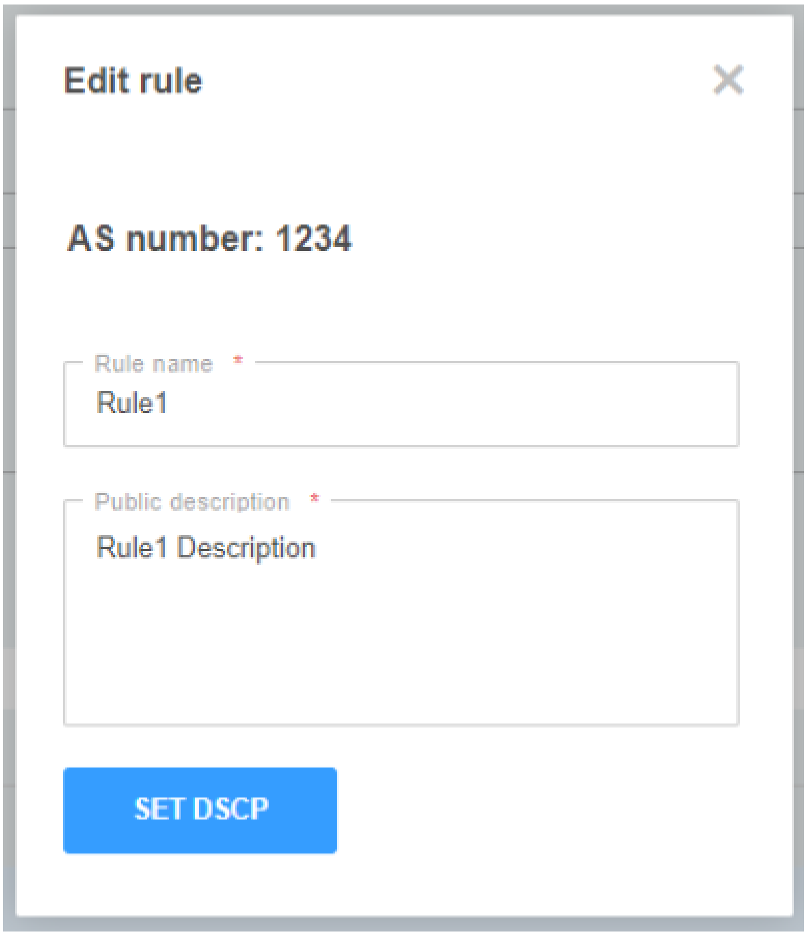
- Specify AS number;
- Enter the rule name;
- Enter the rule descriptuin;

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.



Edit rule

AS number: 1234

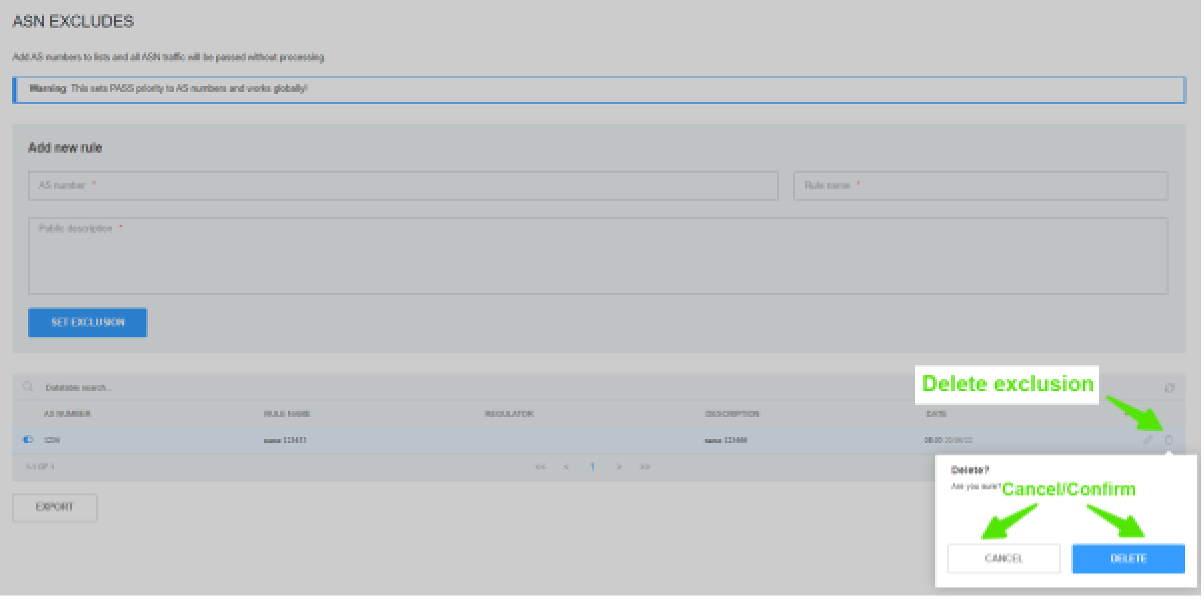
Rule name *: Rule1

Public description *: Rule1 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

Add AS numbers to lists and all ASN traffic will be passed without processing.

Warning: This sets PASS priority to AS numbers and works globally!

Add new rule

AS number *

Rule name *

Public description *

AS NUMBER	RULE NAME	REGULATOR	DESCRIPTION	DATE
1234	[illegible]		[illegible]	[illegible]

Delete?

Are you sure?

VIP Subscriber Management

VIP Subscribers and their privileges

VIP Subscriber is a special subscriber whose traffic is passed with a dedicated priority (default is cs0) 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:

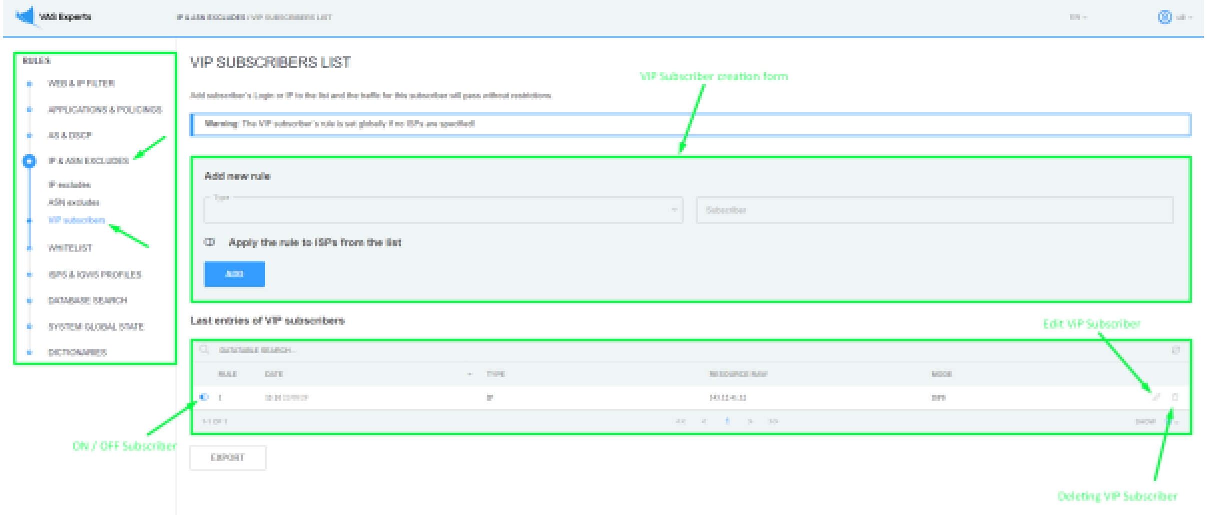
- Unlimited access to applications and resources that are subject to restrictions on use.

Purpose of section

This section is purpose to manage VIP Subscribers.

Getting started with section

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



VIP SUBSCRIBERS LIST

Add subscriber's Login or IP to the list and the traffic for this subscriber will pass without restrictions.

Warning: The VIP subscriber's rule is set globally if no ISPs are specified!

Add new rule

Apply the rule to ISPs from the list

Last entries of VIP subscribers

VIP Subscriber creation form

Edit VIP Subscriber

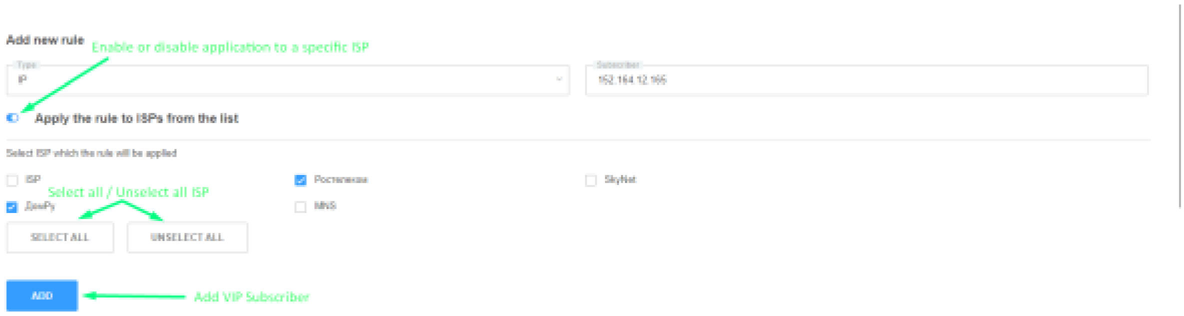
ON / OFF Subscriber

Deleting VIP Subscriber

Creation

In the VIP Subscriber`s creating form:

- Select the type from the drop-down list (IP/Login);
- Enter 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

Type: IP

Subscriber: 152.164.12.165

● Apply the rule to ISPs from the list

Select ISP which the rule will be applied

□ ISP ☑ Ростелеком □ SkyNet

☑ ДомРу □ MNS

Enable or disable application to a specific ISP

Select all / Unselect all ISP

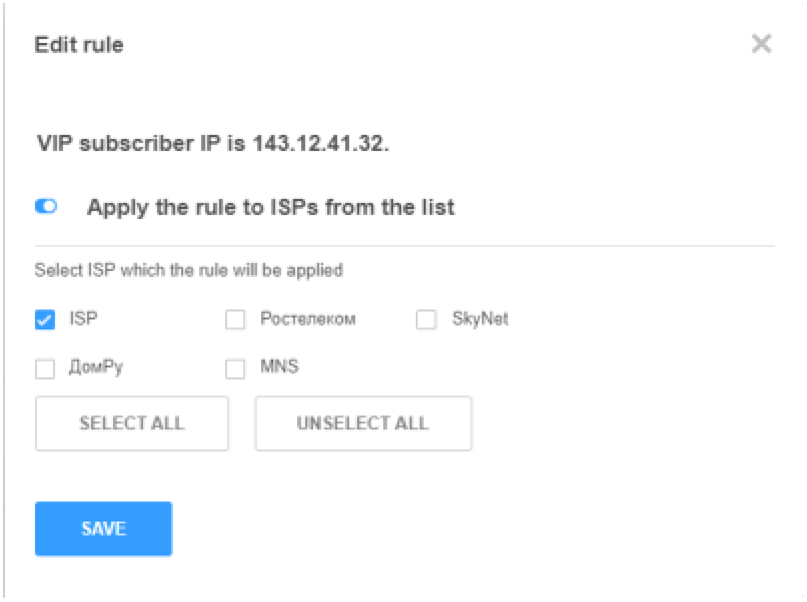
Add VIP Subscriber

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

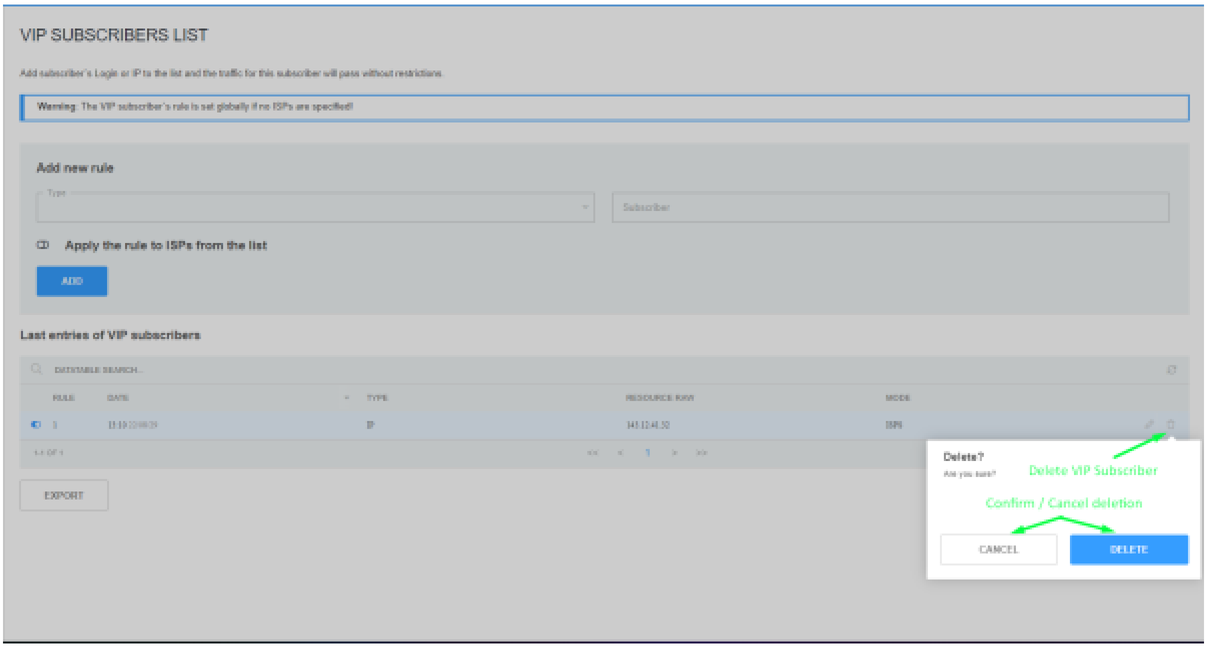
☑ ISP □ Ростелеком □ SkyNet

□ ДомРу □ MNS

Save your changes by clicking the "Save" button.

Deleting

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



VIP SUBSCRIBERS LIST

Add subscriber's Login or IP to the list and the traffic for this subscriber will pass without restrictions.

Warning: The VIP subscriber's rule is set globally if no ISPs are specified!

Add new rule

□ Apply the rule to ISPs from the list

Last entries of VIP subscribers

	RULE	DATE	TYPE	RESOURCE RAW	MODE
●	1	13:10 22/08/19	IP	141.12.41.32	ISP8

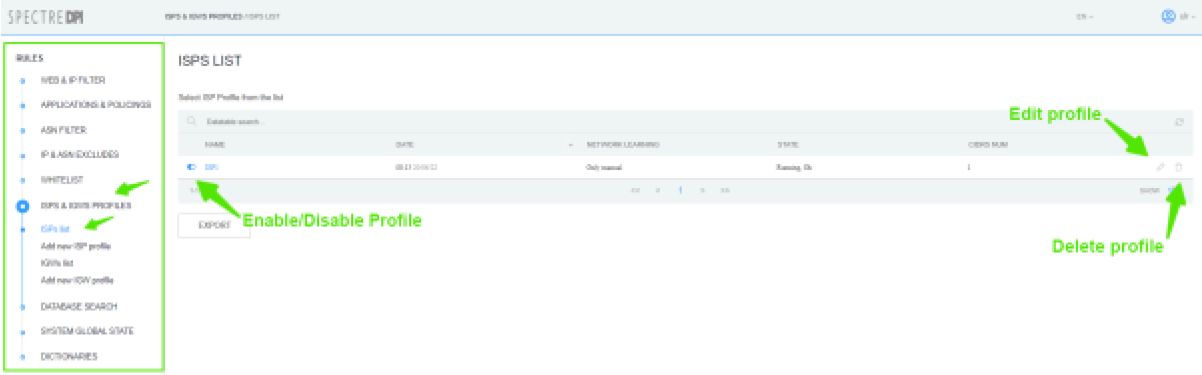
Delete?
Are you sure?

Delete VIP Subscriber

Confirm / Cancel deletion

ISP Configuration

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



ISPS LIST

Select ISP Profile from the list

	NAME	DATE	NETWORK LEARNING	STATE	CIDRS NUM
●	ISP1	08:43 20/08/23	Only manual	Running, Ok	1

Edit profile

Enable/Disable Profile

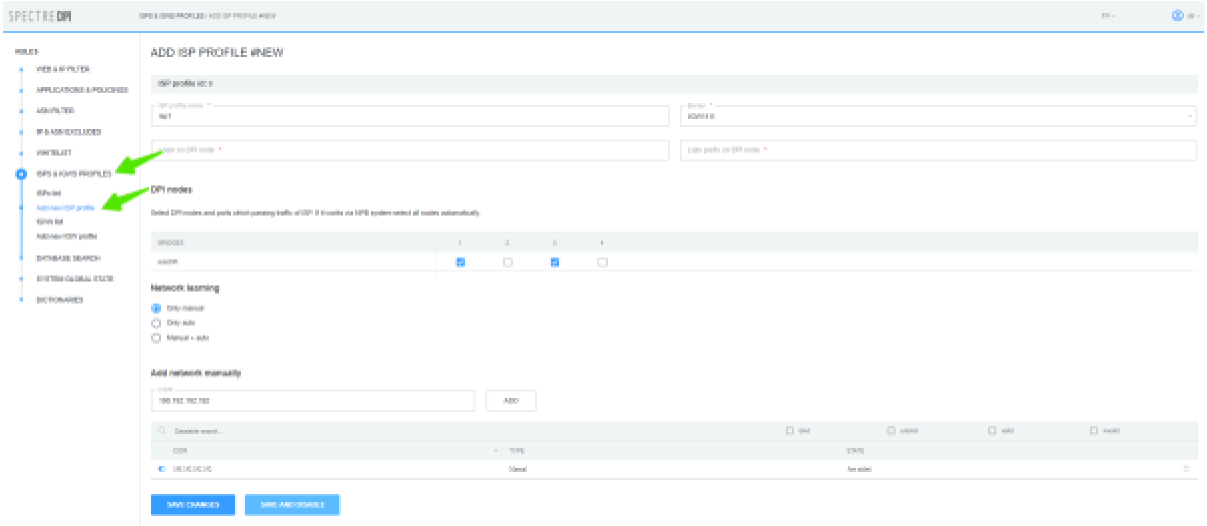
Delete profile

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.

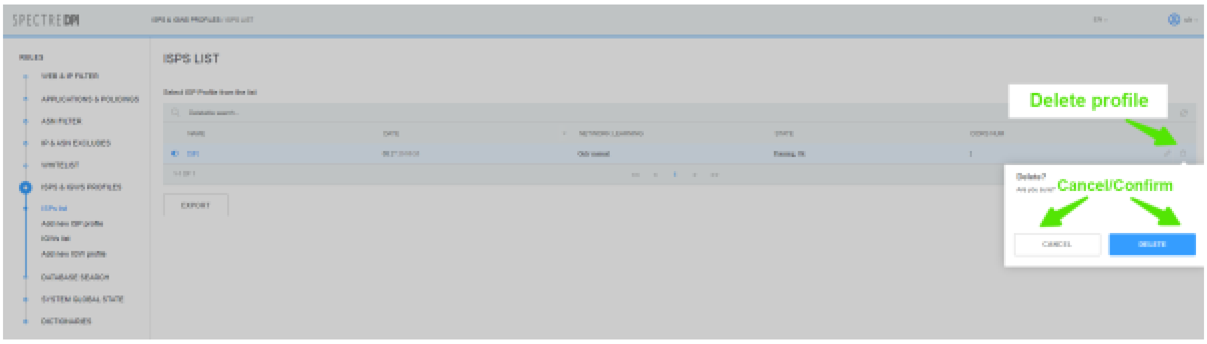
Editing ISP Profile

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

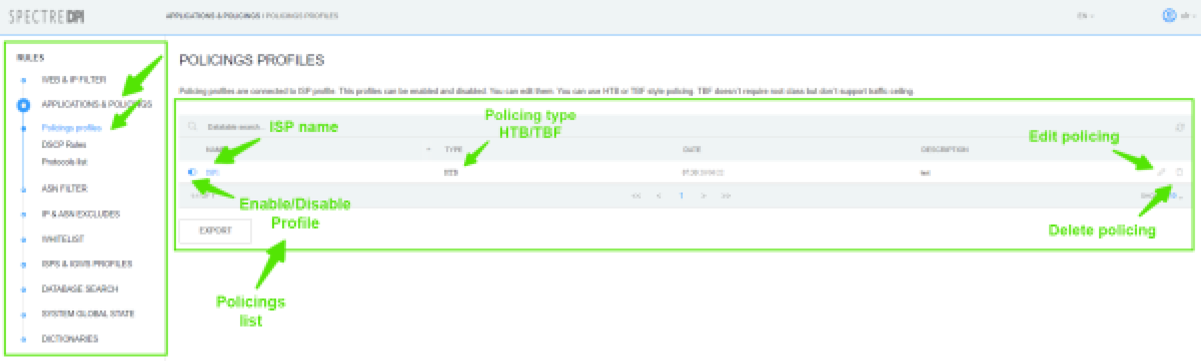
In the "ISPS & IGWS Profiles" section → "ISPs List" click on the "Delete" button and confirm/cancel the action.



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".



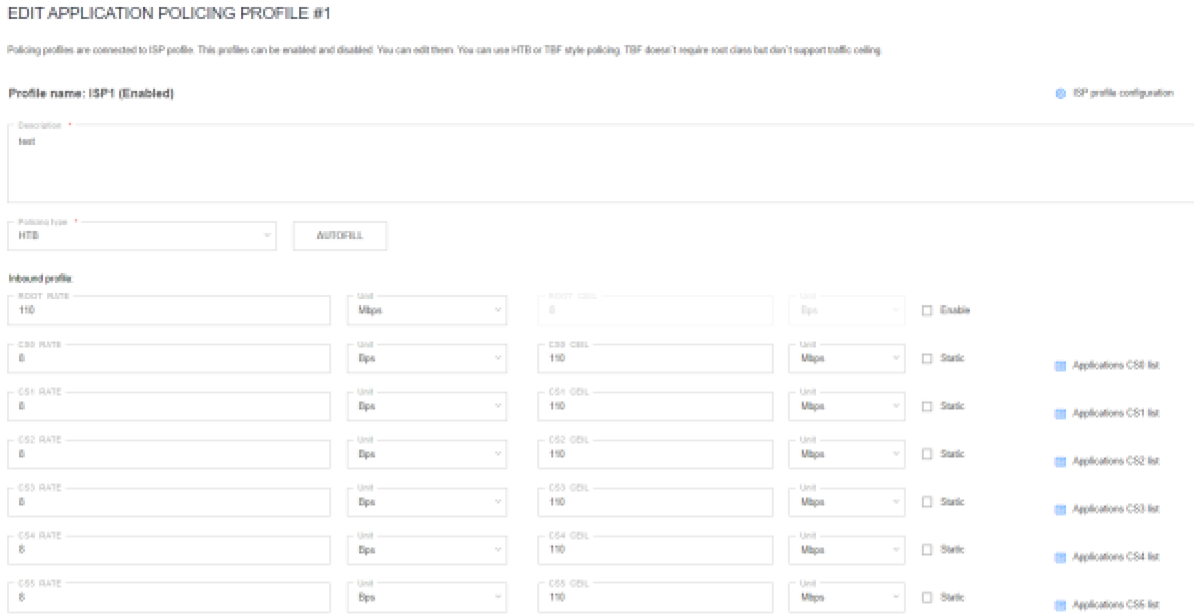
POLICINGS PROFILES

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.

NAME	TYPE	DATE	DESCRIPTION
ISP1	HTB	[illegible]	test

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 *: test

Policing type *: HTB

AUTOFILL

Inbound profile

ROOT RATE: 110	Unit: Mbps	ROOT CEIL: 0	Unit: Bps	□ Enable	
CS0 RATE: 8	Unit: Bps	CS0 CEIL: 110	Unit: Mbps	□ Static	Applications CS0 list
CS1 RATE: 8	Unit: Bps	CS1 CEIL: 110	Unit: Mbps	□ Static	Applications CS1 list
CS2 RATE: 8	Unit: Bps	CS2 CEIL: 110	Unit: Mbps	□ Static	Applications CS2 list
CS3 RATE: 8	Unit: Bps	CS3 CEIL: 110	Unit: Mbps	□ Static	Applications CS3 list
CS4 RATE: 8	Unit: Bps	CS4 CEIL: 110	Unit: Mbps	□ Static	Applications CS4 list
CS5 RATE: 8	Unit: Bps	CS5 CEIL: 110	Unit: Mbps	□ Static	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)

note

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.

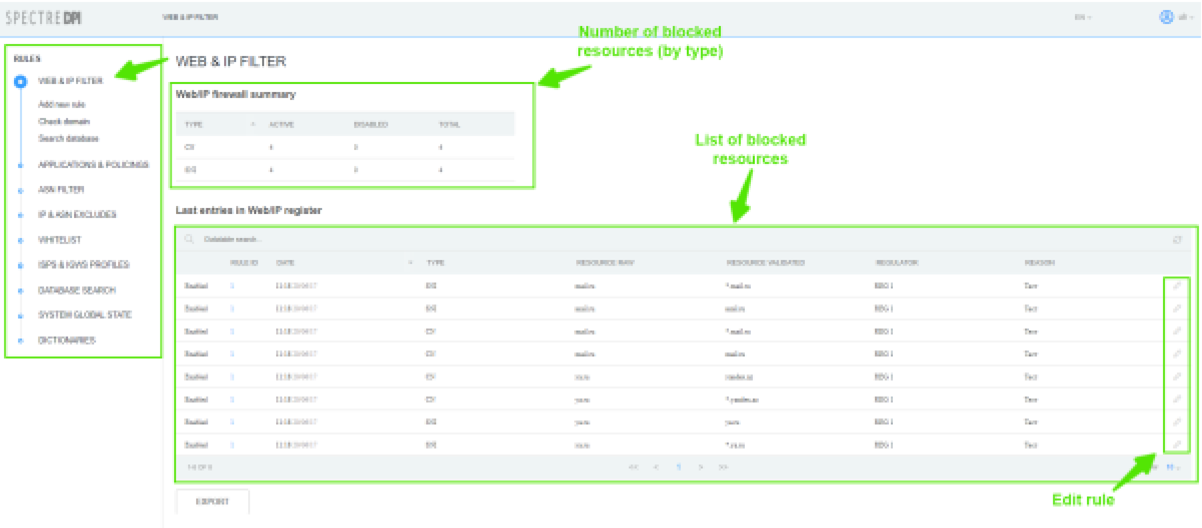
Deletenig Policing Profile

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.



WEB & IP FILTER

Web/IP firewall summary

TYPE	ACTIVE	DISABLED	TOTAL
CF	4	0	4
DS	4	0	4

Last entries in Web/IP register

	RULE ID	DATE	TYPE	RESOURCE RAW	RESOURCE VALIDATED	REGULATOR	REASON
Enabled	1	[illegible]	DS	mail.ru	*.mail.ru	REG 1	Test
Enabled	1	[illegible]	DS	mail.ru	mail.ru	REG 1	Test
Enabled	1	[illegible]	CF	mail.ru	*.mail.ru	REG 1	Test
Enabled	1	[illegible]	CF	mail.ru	mail.ru	REG 1	Test
Enabled	1	[illegible]	CF	ya.ru	yandex.ru	REG 1	Test
Enabled	1	[illegible]	CF	ya.ru	*.yandex.ru	REG 1	Test
Enabled	1	[illegible]	DS	ya.ru	ya.ru	REG 1	Test
Enabled	1	[illegible]	DS	ya.ru	*.ya.ru	REG 1	Test

1-8 OF 8

Number of blocked resources (by type)

List of blocked resources

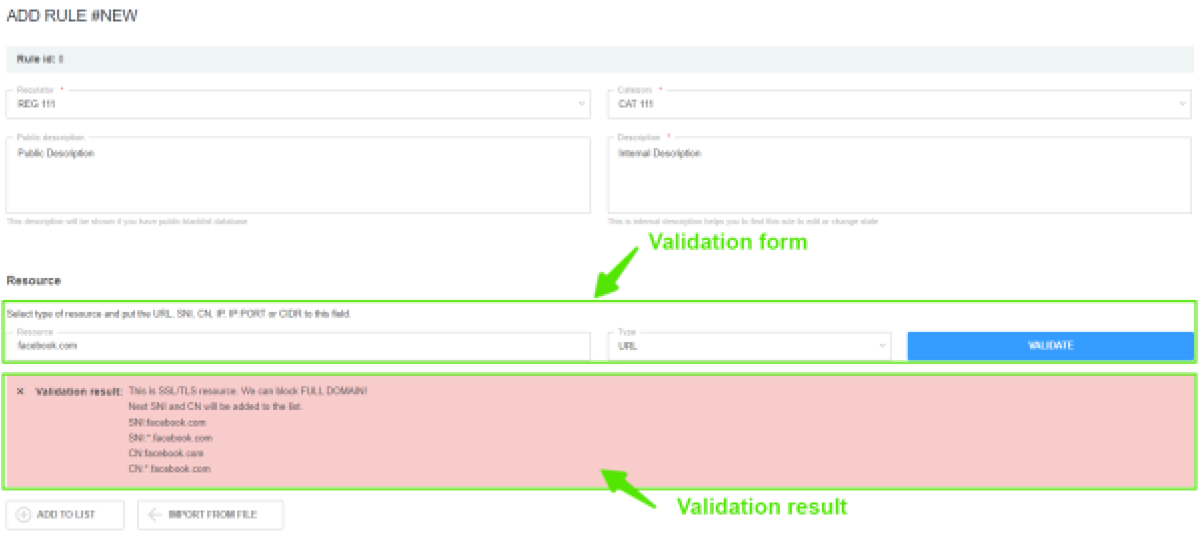
Edit rule

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: 1

Regulator *: REG 111	Category *: CAT 111
Public description: Public Description	Description *: Internal Description
This description will be shown if you have public blacklist database	This is internal description helps you to find this rule to edit or change state

Validation form

Resource

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

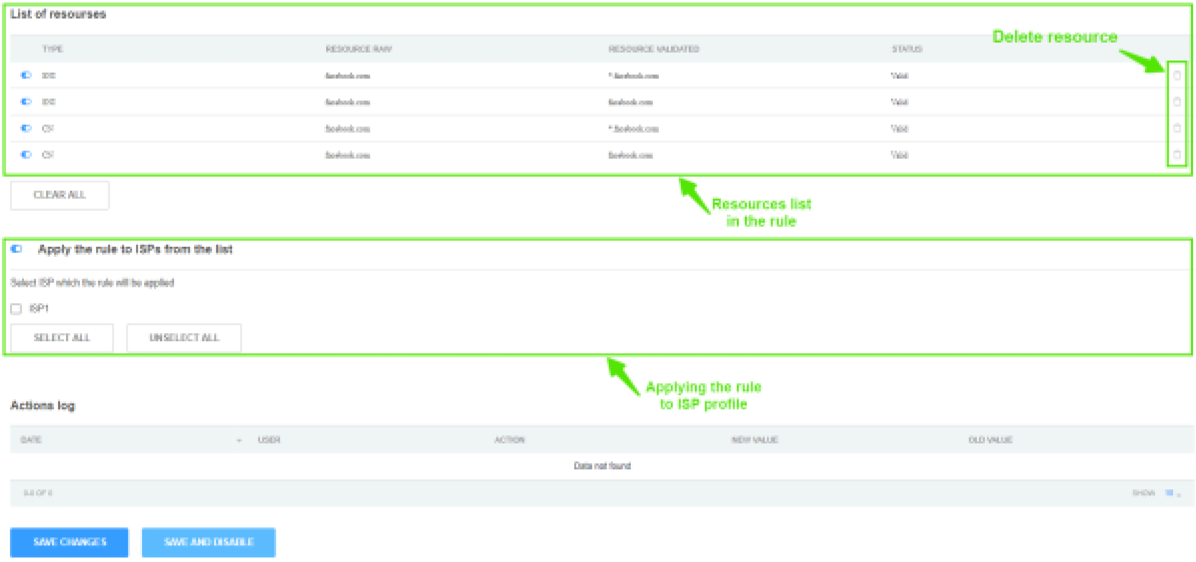
Resource: facebook.com
Type: URL

× 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
SNI:*.facebook.com
CN:facebook.com
CN:*.facebook.com

Validation result

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.



List of resourses

TYPE	RESOURCE RAW	RESOURCE VALIDATED	STATUS
SNI	facebook.com	*.facebook.com	Valid
SNI	facebook.com	facebook.com	Valid
CN	facebook.com	*.facebook.com	Valid
CN	facebook.com	facebook.com	Valid

Delete resource

Resources list
in the rule

Apply the rule to ISPs from the list

Select ISP which the rule will be applied

□ ISP1

Applying the rule
to ISP profile

Actions log

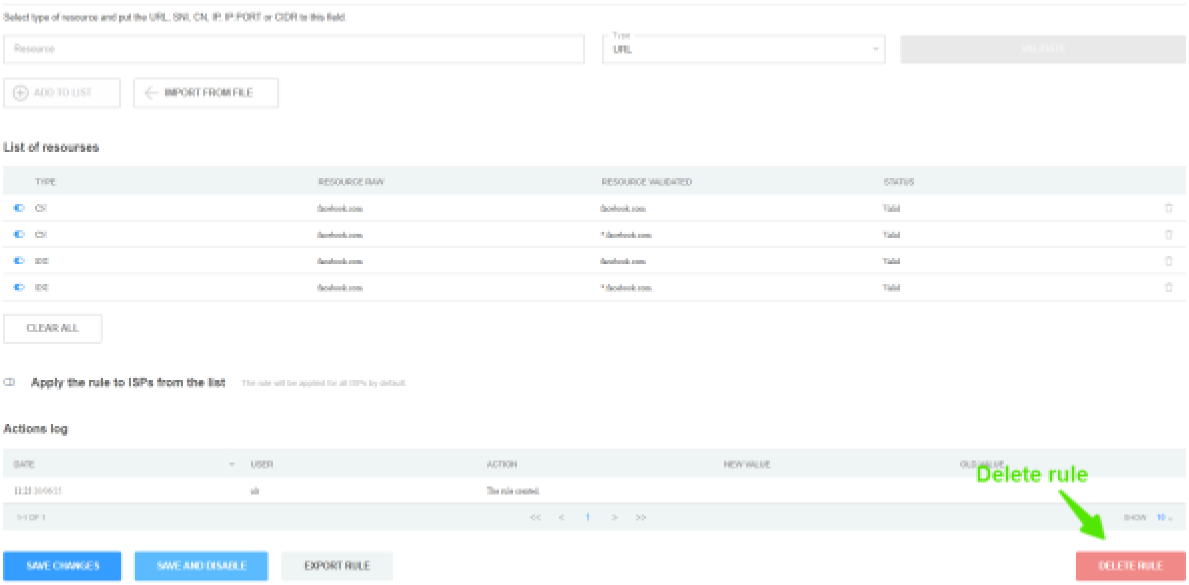
DATE	USER	ACTION	NEW VALUE	OLD VALUE
Data not found				

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, SNI, CN, IP, IP:PORT or CIDR to this field.

Resource

Type: URL

VALIDATE

List of resourses

TYPE	RESOURCE RAW	RESOURCE VALIDATED	STATUS
CN	facebook.com	facebook.com	Valid
CN	facebook.com	*.facebook.com	Valid
SNI	facebook.com	facebook.com	Valid
SNI	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 30/06/21	sk	The rule created.		

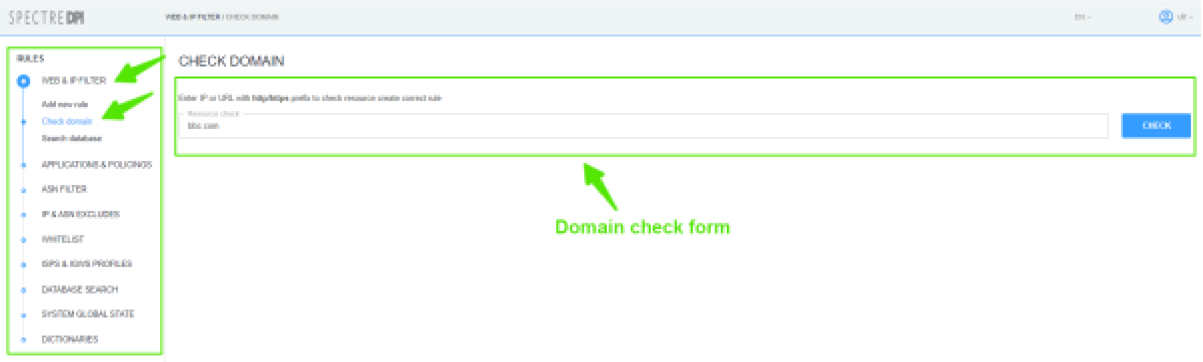
1-1 OF 1

Delete rule

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".



CHECK DOMAIN

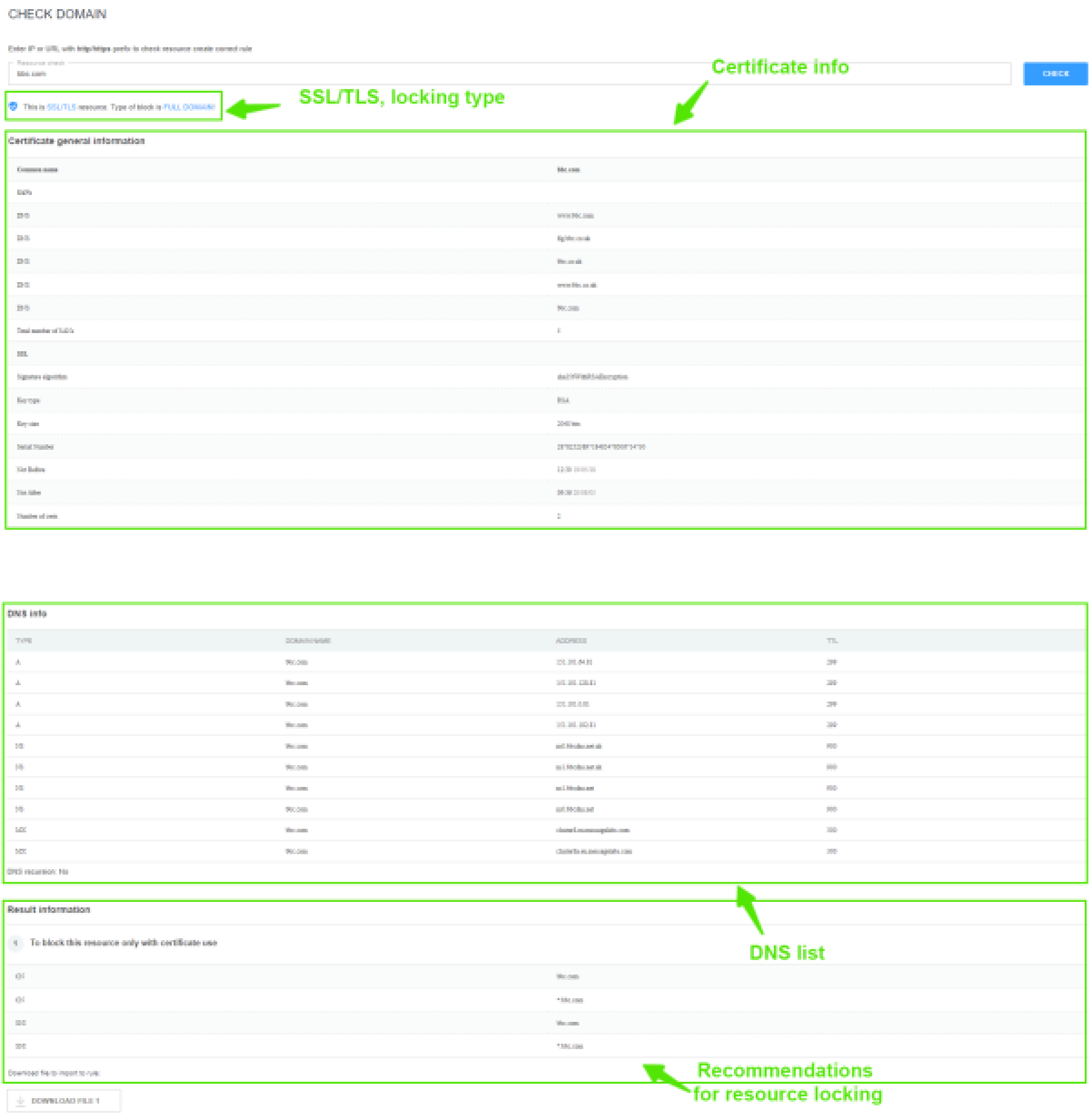
Enter IP or URL with http/https prefix to check resource create correct rule

Resource check: bbc.com

Domain check form

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.



CHECK DOMAIN

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

Resource check: bbc.com

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

Certificate general information

Common name	bbc.com
SANs	
DNS	www.bbc.com
DNS	fig.bbc.co.uk
DNS	bbc.co.uk
DNS	www.bbc.co.uk
DNS	bbc.com
Total number of SANs	[illegible]
SSL	
Signature algorithm	sha256WithRSAEncryption
Key type	RSA
Key size	2048 bits
Serial Number	[illegible]
Not Before	[illegible]
Not After	[illegible]
Number of [illegible]	2

DNS info

TYPE	DOMAIN NAME	ADDRESS	TTL
A	bbc.com	[illegible]	[illegible]
A	bbc.com	[illegible]	[illegible]
A	bbc.com	[illegible]	[illegible]
A	bbc.com	[illegible]	[illegible]
NS	bbc.com	[illegible]	[illegible]
NS	bbc.com	[illegible]	[illegible]
NS	bbc.com	[illegible]	[illegible]
NS	bbc.com	[illegible]	[illegible]
MX	bbc.com	[illegible]	[illegible]
MX	bbc.com	[illegible]	[illegible]

DNS recursion: No

Result information

1 To block this resource only with certificate use

CN	bbc.com
CN	*.bbc.com
SNI	bbc.com
SNI	*.bbc.com

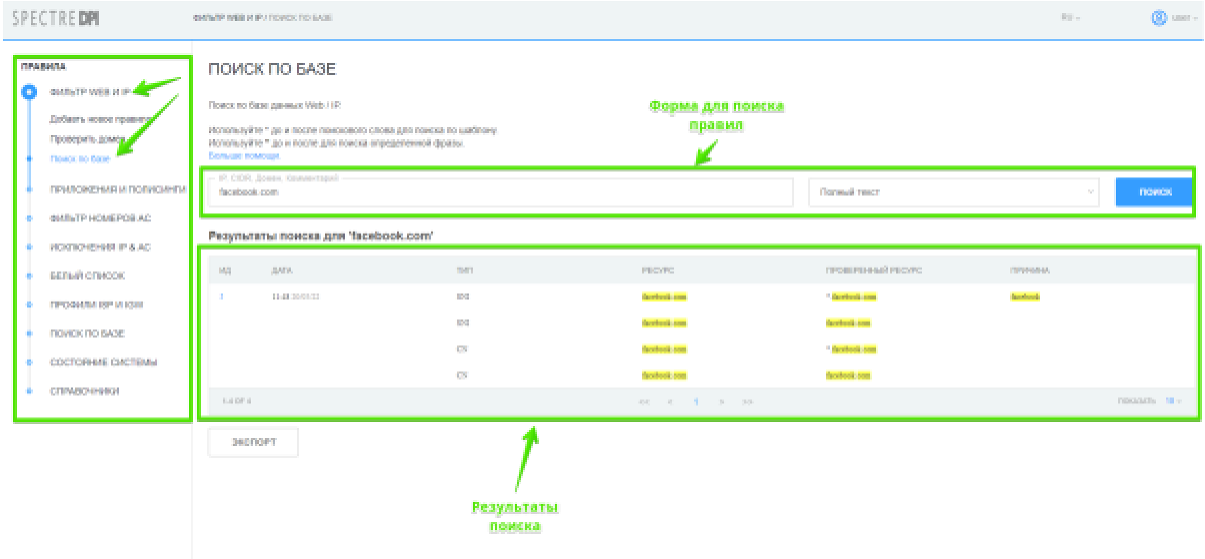
Download file to import to rule:

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.



Поиск по базе данных Web / IP

Используйте * до и после поискового слова для поиска по шаблону
Используйте * до и после для поиска определенной фразы
Больше помощи

facebook.com

Результаты поиска для 'facebook.com'

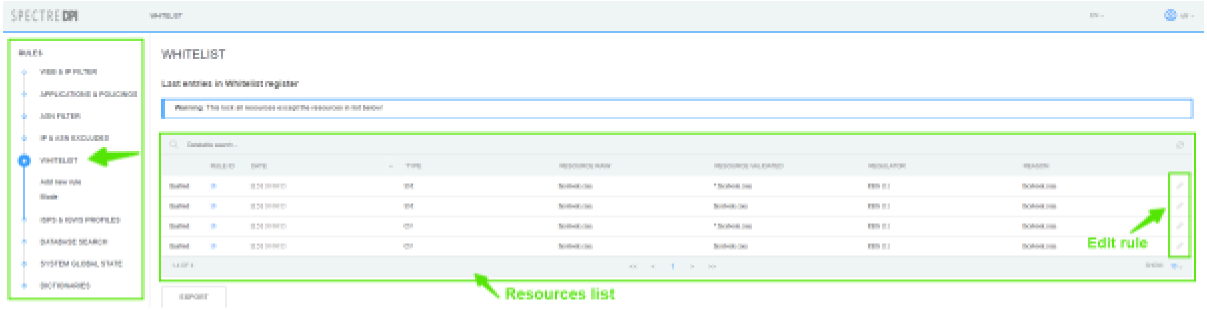
ИД	ДАТА	ТИП	РЕСУРС	ПРОВЕРЕННЫЙ РЕСУРС	ПРИЧИНА
1	[illegible]	[illegible]	facebook.com	*.facebook.com	facebook
		[illegible]	facebook.com	facebook.com	
		CN	facebook.com	*.facebook.com	
		CN	facebook.com	facebook.com	

1-4 OF 4

Whitelist

Whitelist rule list

Change to the "Whitelist" section.



Last entries in Whitelist register

Warning: This lock all resources except the resources in list below!

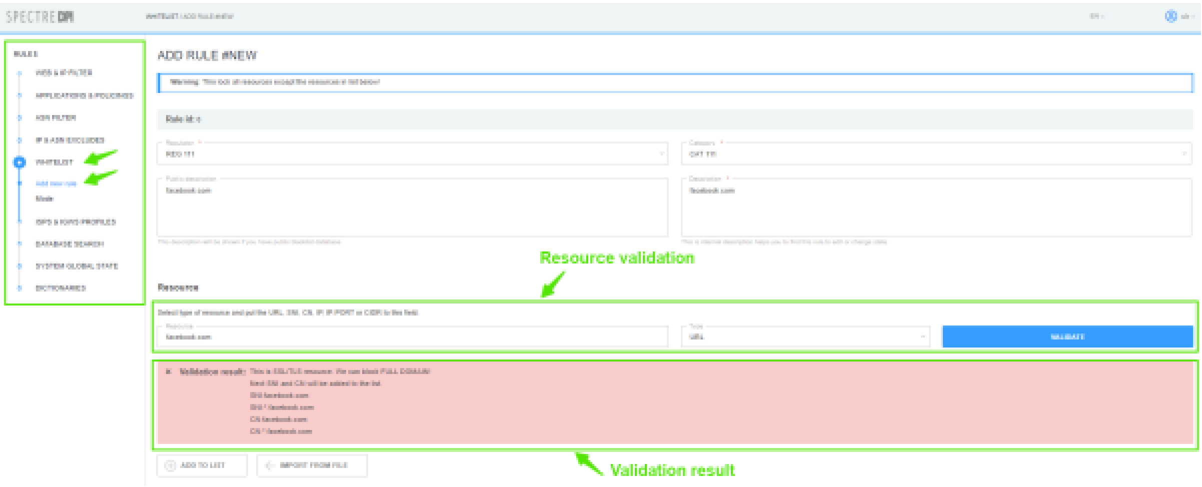
	RULE ID	DATE	TYPE	RESOURCE RAW	RESOURCE VALIDATED	REGULATOR	REASON
[illegible]	[illegible]	[illegible]	[illegible]	facebook.com	*.facebook.com	[illegible]	facebook.com
[illegible]	[illegible]	[illegible]	[illegible]	facebook.com	facebook.com	[illegible]	facebook.com
[illegible]	[illegible]	[illegible]	CN	facebook.com	*.facebook.com	[illegible]	facebook.com
[illegible]	[illegible]	[illegible]	CN	facebook.com	facebook.com	[illegible]	facebook.com

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;



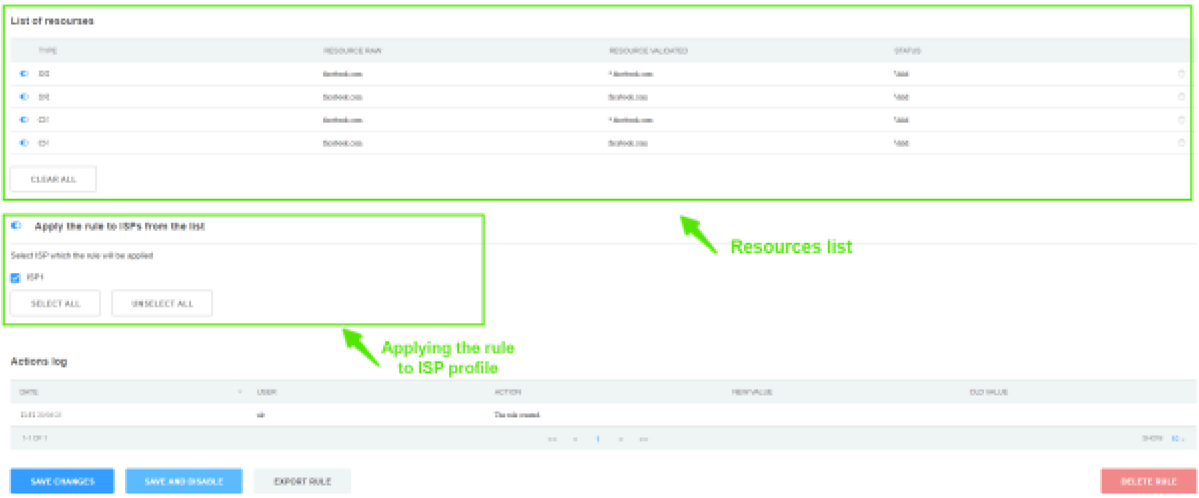
ADD RULE #NEW

Resource

Validation result:

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.



List of resourses

TYPE	RESOURCE RAW	RESOURCE VALIDATED	STATUS

☑ Apply the rule to ISPs from the list

Select ISP which the rule will be applied

☑ ISP1

Actions log

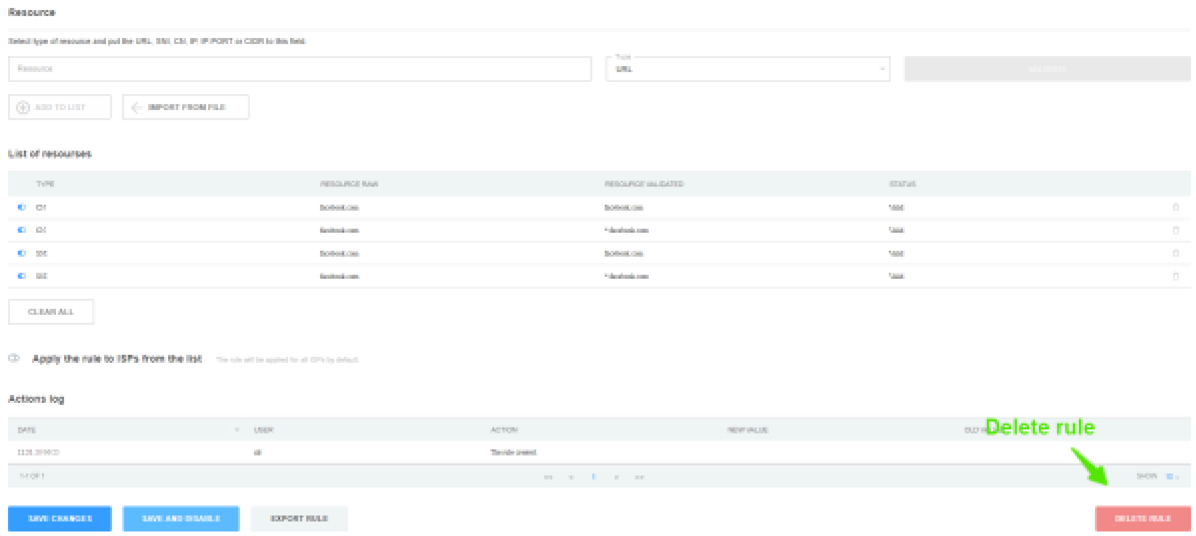
DATE	USER	ACTION	NEW VALUE	OLD VALUE

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.



Resource

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

List of resources

TYPE	RESOURCE RAW	RESOURCE VALIDATED	STATUS
CN	facebook.com	facebook.com	Valid
CN	facebook.com	*.facebook.com	Valid
SNI	facebook.com	facebook.com	Valid
SNI	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

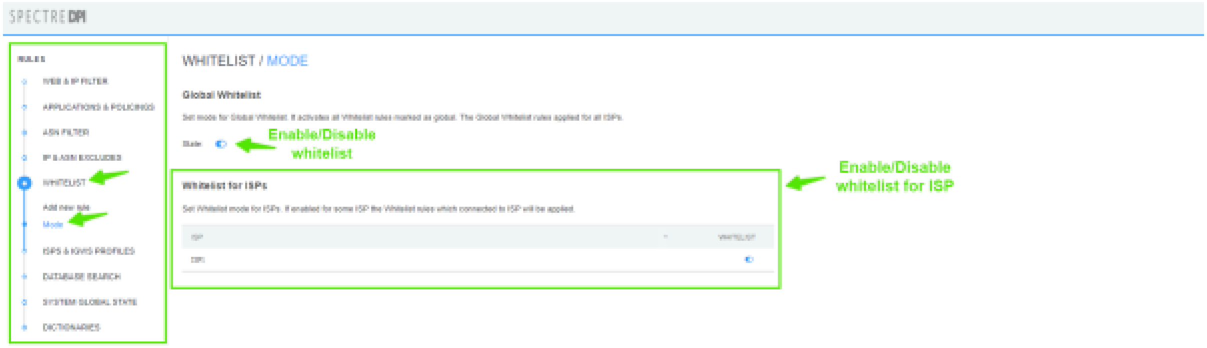
DATE	USER	ACTION	NEW VALUE	OLD VALUE
[illegible]	[illegible]	The rule created.		

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".



WHITELIST / MODE

Global Whitelist

Set mode for Global Whitelist. It activates 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	●

Enable/Disable whitelist for ISP

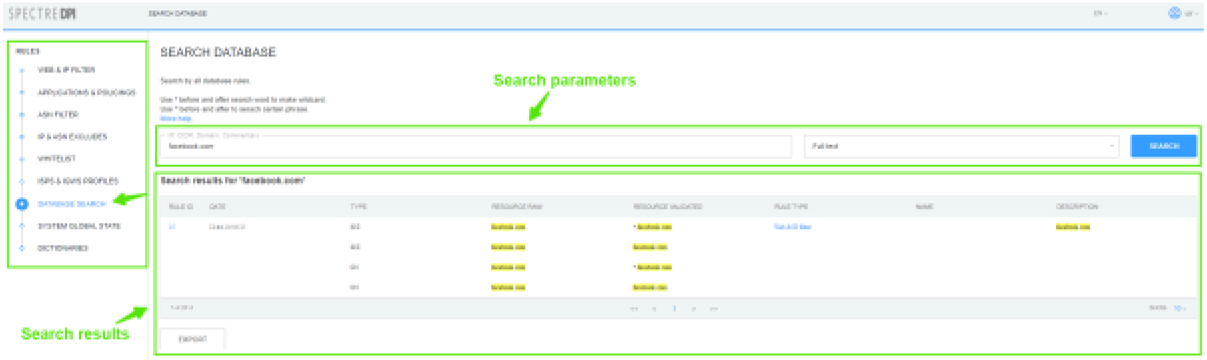
- With the global whitelist mode enabled, the whitelist service is applied to all ISP profiles and resource lists are formed only from global whitelist rules;
- When the whitelist mode is enabled for a separate ISP profile, the service is applied only to ISP which has it enabled. The lists are formed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

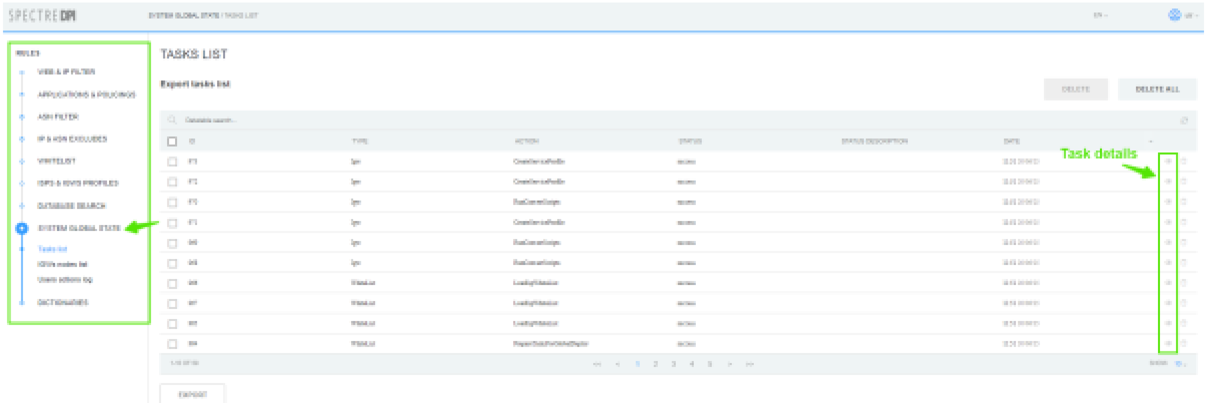
In the "IP, CIDR, Domain, Comment" field enter the value in accordance with the prompts at the top of the page, choose search type: Full Text, By Resources or By Description. Click on “Search” button.

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.