

Содержание

Filtering rules management interface	3
Universal Locking Rules UI	3
<i>Introduction</i>	3
<i>Installation</i>	3
<i>Configuration</i>	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

Filtering rules management interface

Universal Locking Rules UI

Introduction

Universal locking rules (ULR) UI is designed to manage filtering rules on multiple DPs 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

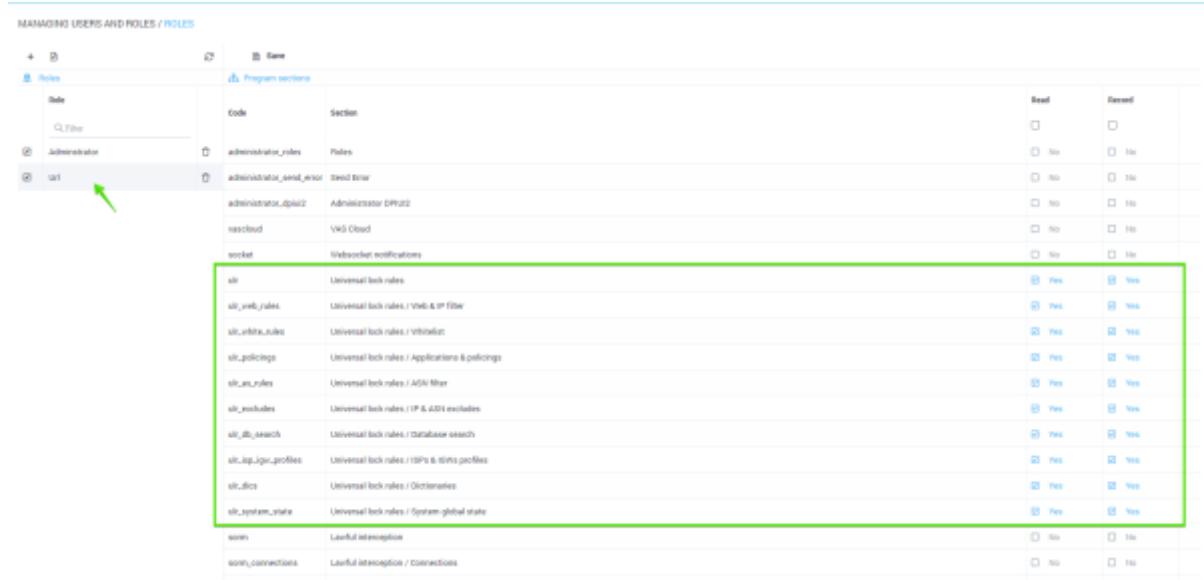
Enter expire date in Y-m-d format:
> 2099-12-31

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
ulr	Universal lock rules	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
ulr_lock_rules	Universal lock rules / Vb6 & IP Filter	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
ulr_write_rules	Universal lock rules / Vb6/ulat	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
ulr_policies	Universal lock rules / Applications & policies	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
ulr_asn_rules	Universal lock rules / ASN Filter	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
ulr_excludes	Universal lock rules / IP & ASN excludes	<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_ip_ipr_profiles	Universal lock rules / IP & IPN profiles	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
ulr_dics	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"/>
ulr_log	Logfile interception	<input type="checkbox"/>	<input type="checkbox"/>
ulr_connections	Logfile interception / 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.

SPECTRE DPI WEB & IP FILTER

WEB & IP FILTER

WebIP firewall summary

TYPE	ACTIVE	DISABLED	TOTAL
OR	4	0	4
AND	2	0	2

Last entries in WebIP register

RULE	DATE	TYPE	RESOURCE IP	RESOURCE VALIDATED	REGULATOR	REASON
Enabled	11.11.2016 11	OR	mail.ru	* mail.ru	REG 1	Test
Enabled	11.11.2016 11	OR	mail.ru	mail.ru	REG 1	Test
Enabled	11.11.2016 11	OR	mail.ru	* mail.ru	REG 1	Test
Enabled	11.11.2016 11	OR	mail.ru	mail.ru	REG 1	Test
Enabled	11.11.2016 11	OR	mail.ru	mail.ru	REG 1	Test
Enabled	11.11.2016 11	OR	mail.ru	* mail.ru	REG 1	Test
Enabled	11.11.2016 11	OR	mail.ru	mail.ru	REG 1	Test
Enabled	11.11.2016 11	OR	mail.ru	* mail.ru	REG 1	Test
Enabled	11.11.2016 11	OR	mail.ru	mail.ru	REG 1	Test

10 of 10

EXPORT

Dictionary 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.

The screenshot shows the SPECTRE DPI interface with the 'Dictionaries | Categories' tab selected. The left sidebar has a 'RULES' section with various items like 'ASPB & IP FILTER', 'APPLICATIONS & POLICIES', 'ASN FILTER', etc., and a 'DICTIONARIES' section with 'Categories' and 'Regulators'. The main area shows a 'CATEGORIES' section with an 'Add new Item' form and a table of categories. The 'CATEGORIES' tab is highlighted with a green box and an arrow. Another green arrow points from the 'Categories' link in the sidebar to the 'CATEGORIES' tab.

Creating

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

The screenshot shows the 'Add new Item' form for creating a category. It has fields for 'Item name' (labeled 'Category') and 'Public description' (labeled 'Description'). A green arrow points to each of these fields. Below the fields is a 'ADD ITEM' button, which is also highlighted with a green arrow.

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.

The screenshot shows the 'Categories' management interface. At the top, there is a form for 'Add new Item' with fields for 'Item name' (set to 'Category') and 'Public description' (set to 'Description'). Below this is a blue 'ADD ITEM' button. In the center, a modal dialog titled 'Edit Item' is open, also containing fields for 'Item name' (set to 'Category') and 'Public description' (set to 'Description'), with a 'SAVE ITEM' button at the bottom. In the bottom right corner of the main interface, there is a table with columns 'NAME', 'DATE', and 'DESCRIPTION'. The table has two rows: 'Category' (date 08/22/20/06/22) and 'CAT III' (date 08/11/20/06/22). To the right of the 'CAT III' row is an 'Edit' button, which is highlighted with a green arrow and the label 'Edit'.

Deleting

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

The screenshot shows the 'Categories' management interface. At the top, there is a form for 'Add new Item' with fields for 'Item name' (set to 'Category') and 'Public description' (set to 'Description'). Below this is a blue 'ADD ITEM' button. In the center, a modal dialog titled 'Edit Item' is open, also containing fields for 'Item name' (set to 'Category') and 'Public description' (set to 'Description'), with a 'SAVE ITEM' button at the bottom. In the bottom right corner of the main interface, there is a table with columns 'NAME', 'DATE', and 'DESCRIPTION'. The table has two rows: 'Category' (date 08/22/20/06/22) and 'CAT III' (date 08/11/20/06/22). To the right of the 'CAT III' row is a 'Delete category' button, which is highlighted with a green arrow and the label 'Delete category'. A modal dialog titled 'Delete?' is open in the bottom right, with the text 'Are you sure? Cancel/Confirm' and two buttons: 'CANCEL' and 'DELETE', both highlighted with green arrows and the label 'DELETE'.



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.

SPECTRE DPI

DICTIONARIES/REGULATORS

REGULATORS

Add new Item

Item name: Regulator

Public description: Description

ADD ITEM

NAME DESCRIPTION

Regulator Regulator

EXPORT

Creating

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

REGULATORS

Add new item

Item name: Regulator

Public description: Description

ADD ITEM

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.

REGULATORS

Add new item

Item name: Regulator

Public description: Description

ADD ITEM

NAME DESCRIPTION

Regulator Regulator

EXPORT

Edit

Edit item

Item name: Regulator

Public description: Description

SAVE ITEM

Deleting

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

The screenshot shows the 'REGULATORS' page. At the top, there is a form to 'Add new item' with fields for 'Item name' (Regulator) and 'Public description' (Description). Below this is a table with a single row: 'Regulator' (NAME), '08.10.2016' (DATE), and 'Description' (DESCRIPTION). The table has a header row with columns for NAME, DATE, and DESCRIPTION. At the bottom of the table are 'EXPORT' and 'ADD ITEM' buttons. A green arrow points to the 'Delete regulator' button in the top right corner of the table. A second green arrow points to the 'Delete?' confirmation dialog box that appears when the button is clicked.



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".

The screenshot shows the 'SPECTRE DPI' interface with the title 'ISPS & IGWS PROFILES | ADD IGW PROFILE #NEW'. The left sidebar has a green box around it, and a green arrow points to the 'Add new IGW profile' option under the 'ISPS & IGWS PROFILES' section. The main form is titled 'ADD IGW PROFILE #NEW' and contains fields for 'IGW profile id' (set to 'igw1'), 'IGW profile name' (set to 'igw1'), 'Mode' (set to 'Standalone'), 'Nodes' (with 'node name' 'mmeDPI' and 'DPI hardware name' 'mmeDPI'), and a 'Bridge' dropdown set to '4'. Below the form is a table with columns 'NAME', 'DPI HARDWARE NAME', and 'BRIDGE'. A green arrow points to the 'SAVE CHANGES' button at the bottom of the form.

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

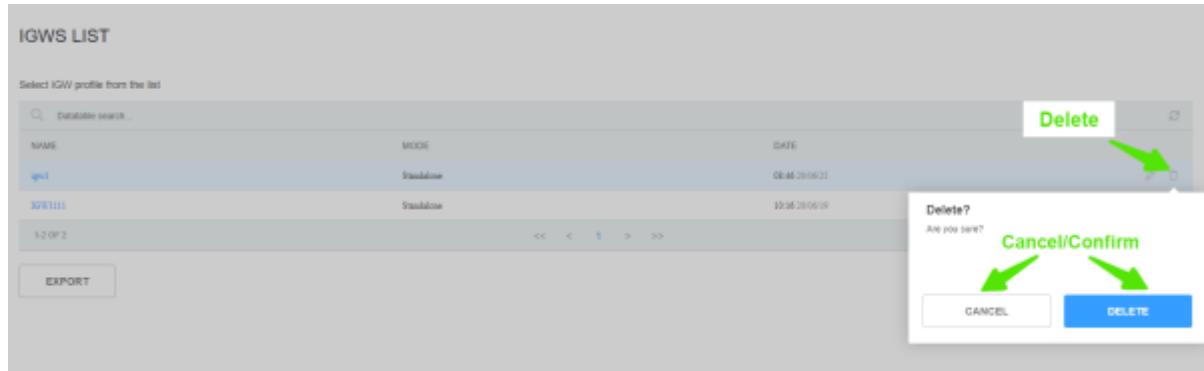
In the "ISPS & IGWS Profiles" → "IGWs List" section click the button "Edit profile".

IGWS LIST		
Select IGW profile from the list.		
NAME	MODE	DATE
IGW1111	Standalone	10/16/20/06/19
1-1 OF 1	<< < > >>	SHOW 10
<input type="button" value="EXPORT"/> <input type="button" value="Edit profile"/> <input type="button" value="Delete"/>		

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

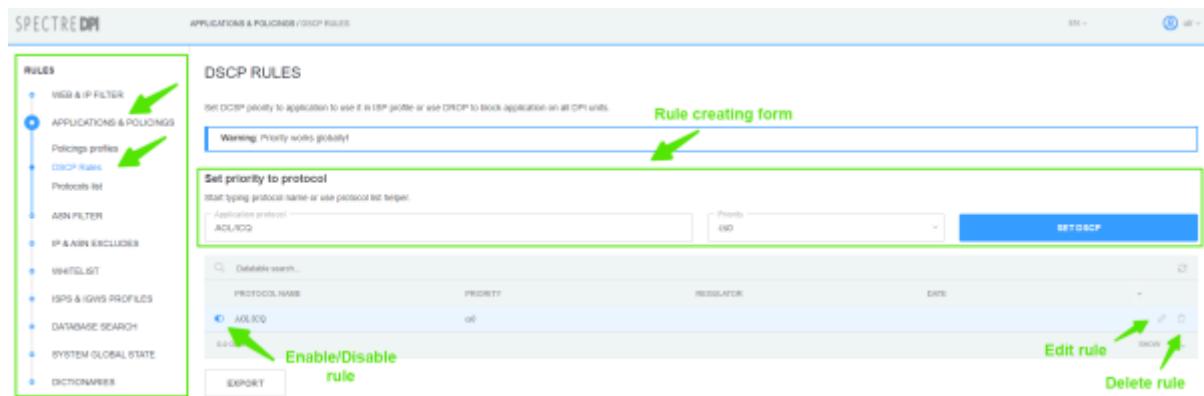
# Names dictionary for blocking HTTPS protocol by certificate
(custom_cname_black_list)
custom_cname_black_list=http://<IP address of Web-server>/blacklistcn.dict

# 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

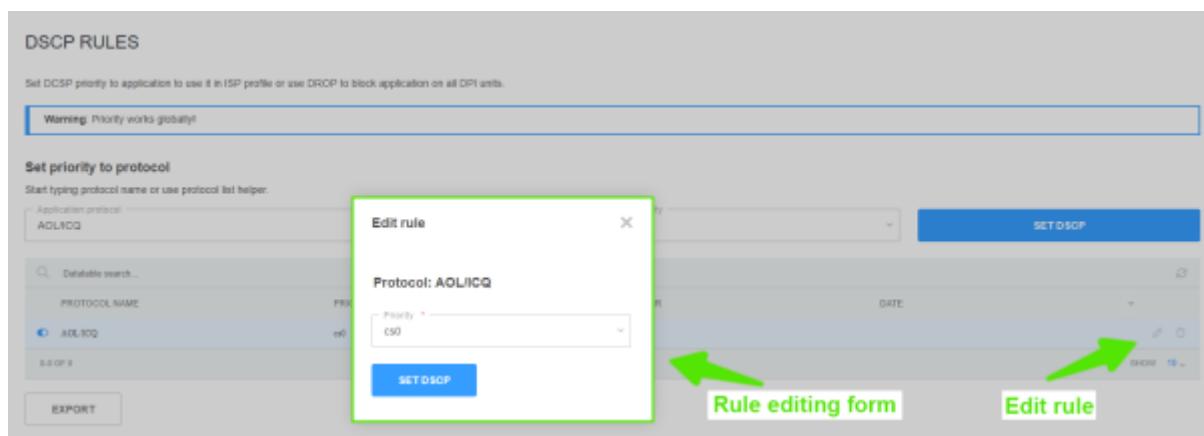
In the form of rule creating:

- 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.

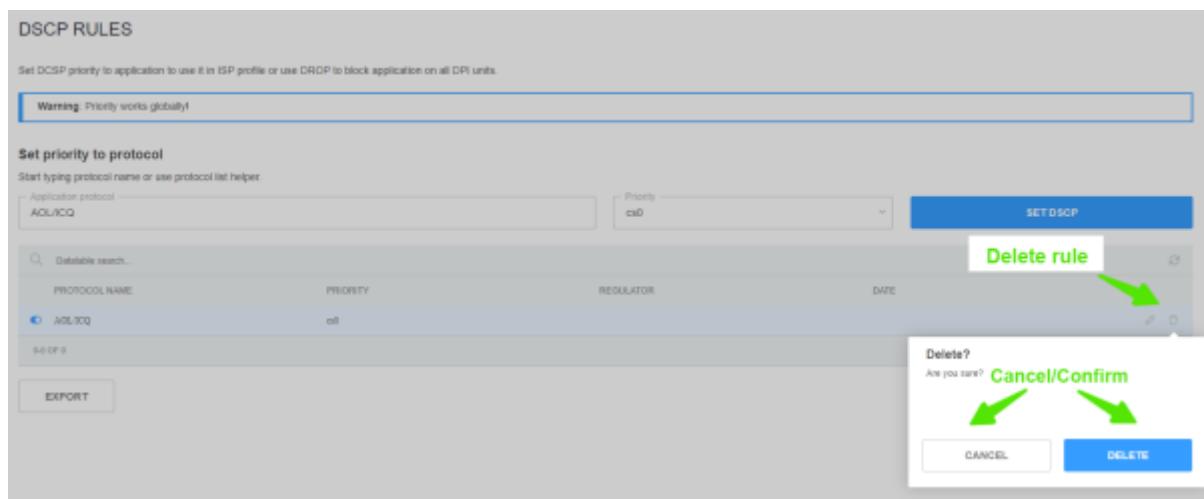
Editing

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.

Rule creating form

Edit rule

Delete rule

Enable/Disable rule

AS NUMBER	RULE NAME	PRIORITY	DESCRIPTION	DATE
1981	Rule1	0	Rule1 Description	27.04.2016 00:00
440	440	0	440	27.04.2016 00:00

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.

The screenshot shows the 'DSCP RULES' interface. On the left, there is a form titled 'Add new rule' with fields for AS number (11101), Rule name (Rule1), and Public description (Rule1 Description). A 'SET DSCP' button is at the bottom. On the right, there is an 'Edit rule' form for AS number 11101, showing Priority (as0), Rule name (Rule1), and Public description (Rule1 Description). A 'SET DSCP' button is also here. Below these forms is a table listing rules. The first rule has 'Edit' and 'Delete' buttons. A green box labeled 'Rule editing form' points to the 'Edit rule' form, and a green arrow points to the 'Edit' button in the table.

AS NUMBER	RULE NAME	PRIORITY	REGULATOR	DESCRIPTION	DATE
11101	Rule1	as0		Rule1 Description	4440 07.04.2016 00:00
444	4440	as0		4440	07.04.2016 00:00

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.

The screenshot shows the 'DSCP RULES' interface. On the right, there is a table with a 'Delete rule' button next to the first row. A green box labeled 'Delete rule' points to this button. A 'Delete?' dialog box with 'Cancel/Confirm' buttons is overlaid on the interface. A green arrow points to the 'DELETE' button in the dialog, and another green arrow points to the 'Cancel/Confirm' buttons.

AS NUMBER	RULE NAME	PRIORITY	REGULATOR	DESCRIPTION	DATE
11101	Rule1	as0		Rule1 Description	4440 07.04.2016 00:00
444	4440	as0		4440	07.04.2016 00:00

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 *

Public 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 PASS priority to IP-addresses and works globally!

Add new rule

IP or CIDR: Rule name:

Public description:

SET EXCLUSION

IP or CIDR	Rule name	Regulator	Description	Ref ID
192.168.1.5	Rule1			refID12345678

Delete exclusion 

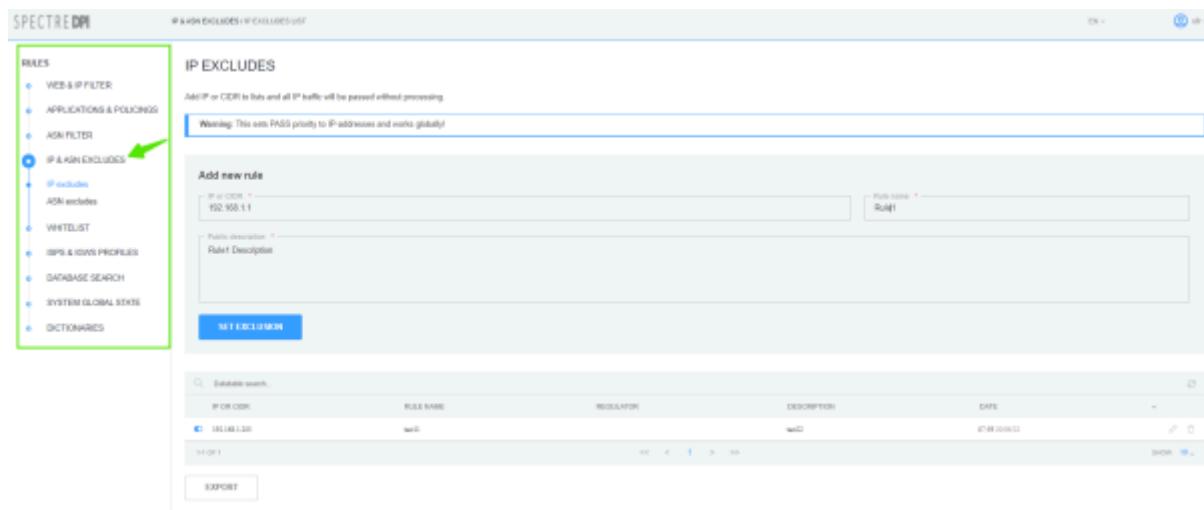
Delete?

Are you sure? **Cancel/Confirm**

CANCEL **DELETE**

ASN Excludes

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



IP or CIDR	RULE NAME	REGULATOR	DESCRIPTION	DATE
192.168.1.100	Rule1		Rule1 Description	07.09.2018 00:00:00

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 *

Public 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 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 *

SET EXCLUSION

AS NUMBER	Rule name	REGULATOR	DESCRIPTION	DATE
123455	name 123455		name 123455	26.02.2016 00:00

Delete exclusion

Delete? Are you sure? **Cancel/Confirm**

CANCEL **DELETE**

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

Open section "IP & AC Exclusion"→"VIP Subscribers".

The screenshot shows the 'VIP SUBSCRIBERS LIST' page. The sidebar on the left is titled 'RULES' and contains the following items: WEB & IP FILTER, APPLICATIONS & POLICIES, AS & DSCP, IP & ASN EXCLUDES, WHITELIST, ISPs & IGRIS PROFILES, DATABASE SEARCH, SYSTEM GLOBAL STATE, and ELECTRONICS. The 'IP & ASN EXCLUDES' item is highlighted with a green box and has an 'On / Off Subscriber' button. The main area has a 'VIP Subscriber creation form' with fields for 'Type' (IP/Login) and 'Subscriber'. Below it is a table 'Last entries of VIP subscribers' with one entry: '1 10-01-2019 09:30:00 192.168.1.100 192.168.1.100'. There are buttons for 'Edit VIP Subscriber' and 'Delete VIP Subscriber'. A 'REPORT' button is also visible.

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 Enable or disable application to a specific ISP

Type: ISP Port Application

Subscriber:

Apply the rule to ISPs from the list

Select ISP which the rule will be applied

ISP ДомРу Ростелеком MNS SkyNet

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

Type: Subscriber:

Apply the rule to ISPs from the list

ADD

Last entries of VIP subscribers

Rule	Date	Type	Resource IP	Mode
1	11/19/2016 09:39	IP	143.124.1.30	ISPs

1 of 1

EXPORT

Delete?
Are you sure?
Delete VIP Subscriber
Cancel
Delete

ISP Configuration

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

SPECTRE DPI

ISPS & IGWS PROFILES - ISPs LIST

ISPs LIST

Select ISP Profile from the list

NAME	DATE	NETWORK LEARNING	STATE	CROSSING ID	CROSSING NAME
ISP	08/23/2016 02	Only manual	Active	1	ISP

EXPORT

Enable/Disable Profile

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

Deleting ISP Profile

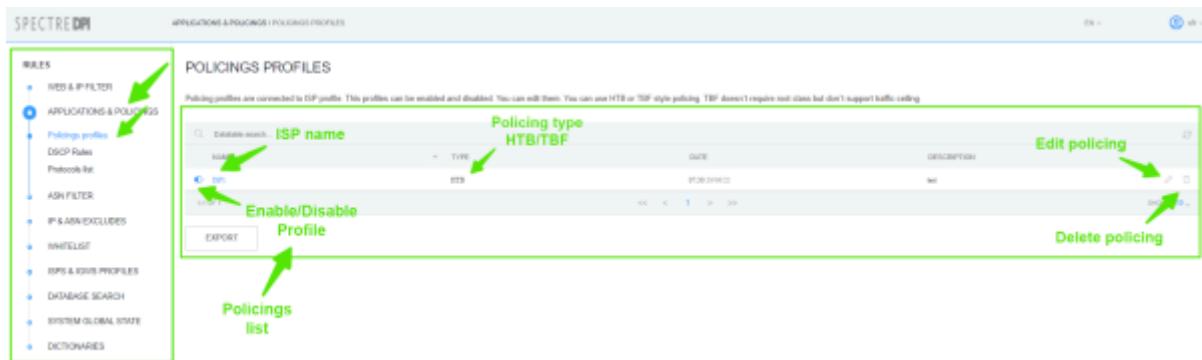
In the "ISPS & IGWS Profiles" section → "ISPs List" click on the "Delete" button and confirm/cancel the action.



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

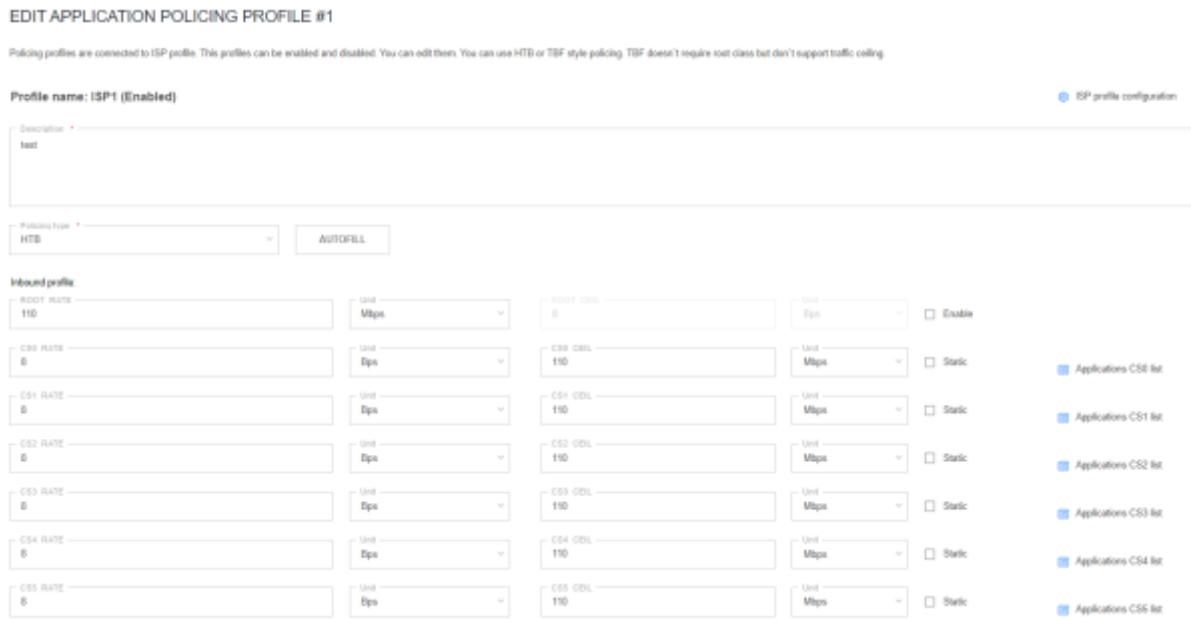
Policing Profile

Change to the "Applications and Policings" profile → "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.

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



Thy policing profile is disabled by default.

Deleteing 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.

Number of blocked resources (by type)

TYPE	ACTIVE	ENABLED	TOTAL
URL	1	0	1
IP	1	0	1
			4

List of blocked resources

INDEX	CREATE	TYPE	RESOURCE NAME	RESOURCE VALIDATED	REGULATOR	REASON
1	11.11.2019.07	URL	malicious	*.malicious	BBG I	Test
2	11.11.2019.07	URL	malicious	malicious	BBG I	Test
3	11.11.2019.07	URL	malicious	*.malicious	BBG I	Test
4	11.11.2019.07	URL	malicious	malicious	BBG I	Test
5	11.11.2019.07	URL	malicious	malicious	BBG I	Test
6	11.11.2019.07	URL	malicious	*.malicious	BBG I	Test
7	11.11.2019.07	URL	malicious	malicious	BBG I	Test
8	11.11.2019.07	URL	malicious	*.malicious	BBG I	Test

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

Resource: REG 111

Category: CAT 111

Public Description: Public Description

Internal Description: Internal Description

This description will be shown if you have public blocked resources.

This internal description helps you to find this rule in edit or change state.

Resource

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

Resource:

Type:

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.ca
CN: *.facebook.ca

Buttons: ADD TO LIST, IMPORT FROM FILE, VALIDATE

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 NAME	RESOURCE VALIDATED	STATUS	Delete resource
URL	facebook.com	*facebook.com	Valid	<input type="button" value="Delete"/>
URL	facebook.com	*facebook.com	Valid	<input type="button" value="Delete"/>
URL	facebook.com	*facebook.com	Valid	<input type="button" value="Delete"/>
URL	facebook.com	*facebook.com	Valid	<input type="button" value="Delete"/>

Buttons: CLEAR ALL

Section: Apply the rule to ISPs from the list

Select ISP which the rule will be applied

ISP1

Section: Actions log

DATE	USER	ACTION	NEW VALUE	OLD VALUE
Data not found				

Buttons:

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:

List of resources

TYPE	RESOURCE RAW	RESOURCE VALIDATED	STATUS	OPTIONS
OS	facebook.com	facebook.com	Valid	<input type="checkbox"/>
OS	facebook.com	*facebook.com	Valid	<input type="checkbox"/>
IE	facebook.com	facebook.com	Valid	<input type="checkbox"/>
IE	facebook.com	*facebook.com	Valid	<input type="checkbox"/>

Apply the rule to ISPs from the list This rule will be applied for all ISP by default.

Actions log

DATE	USER	ACTION	NEW VALUE	OPTIONS
11.11.2016 01	ak	The rule created.		<input type="checkbox"/> 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".

SPECTRE WEB & IP FILTER / CHECK DOMAIN

RULES

- WEB & IP FILTER
- Add new rule
- Check domain
- Search database

APPLICATIONS & POLICIES

- ASH FILTER
- IP & ARI EXCLUSIONS
- WHITELIST
- ISPs & IOPS PROFILES
- DATABASE SEARCH
- SYSTEM GLOBAL SITE
- DICTIONARIES

CHECK DOMAIN

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

Resource check:

Domain check 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.

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

Resource check
dns.com

 **SSL/TLS, locking type** 

Certificate info 

Certificate general information	
Common name	dns.com
Subject	
Subject Alternative Name	www.dns.com
Organization	digitecgroup
Organizational Unit	
State/Province	Wien, Austria
City/Local	
Country	AT
Total number of blocks	1
SSL	
Signature algorithm	sha256WithRSAEncryption
Key type	RSA
Key size	2048 bits
Not Before	12/30/2015 00:00:00
Not After	28/02/2018 00:00:00
Number of cert	1

DNS info 

TYPE	DOMAIN NAME	ADDRESS	TTL
A	dns.com	12.211.14.81	300
A	dns.com	10.10.10.41	300
A	dns.com	121.251.0.00	300
A	dns.com	10.10.10.41	300
NS	dns.com	ns1.digitecgroup.com	300
NS	dns.com	ns2.digitecgroup.com	300
NS	dns.com	ns3.digitecgroup.com	300
MX	dns.com	cluster1.digitecgroup.com	300
MX	dns.com	cluster2.digitecgroup.com	300

DNS recursion No

Result information 

Q1	dns.com
Q1	dns.com
Q2	dns.com
Q3	dns.com
Q4	dns.com

Download file to import to rule: 

 **Recommendations for resource locking** 

To block this resource only with certificate use

01
01
02
03

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.

ПРАВИЛА

- фильтр WEB и IP (highlighted with a green arrow)
- Добавить новое правило
- Преобразовать домен
- Поиск по базе

ПРИЛОЖЕНИЯ И ПОДСЧЕТЫ

- фильтр Номеров АС
- Использование IP & АС
- БЕЛЫЙ СПИСОК
- ПРОФИЛИ ВМ и ОС
- Поиск по базе
- СОСТОЯНИЕ СИСТЕМЫ
- СПРАВОЧНИК

ПОИСК ПО БАЗЕ

Поиск по базе данных Web + IP

Используйте "д" и после первоначального слова для поиска по шаблону. Используйте "д" и после слова для поиска предшествующей фразы.

Больше помощи.

Форма для поиска правил

М. СДН, домен, клиентский

facebook.com

Полный текст

ПОИСК

Результаты поиска для 'facebook.com'

ID	ДАТА	WEB	РЕСУРС	ПРОВЕРЕННЫЙ РЕСУРС	ПРИЧИНА
1	11.11.2013 11:11	00	facebook.com	* facebook.com	facebook
		00	facebook.com	* facebook.com	facebook
		05	facebook.com	* facebook.com	facebook
		05	facebook.com	* facebook.com	facebook

1 из 4

Показать 10

ЭКСПОРТ

Результаты поиска

Whitelist

Whitelist rule list

Change to the "Whitelist" section.

WHITELIST

Last entries in Whitelist register

Warning: This tool list resources except the resources in list below

ID	NAME	DESCRIPTION	ACTION
1	Resource 1	* Resource 1	Block (B)
2	Resource 2	* Resource 2	Block (B)
3	Resource 3	* Resource 3	Block (B)
4	Resource 4	* Resource 4	Block (B)

Resources list

Edit rule

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;

Warning: This list of resources exceed the resources in list below

Rule Id: 0

Resource: Censors:

Resource description: Description:

Resource validation

Resource: Type:

Validation result

X Validation result: This is SSL/TLS resource. We can't find FULL DGA(LB) level URL and CNAME will be added to the list.
URL:facebook.com
URL:facebook.com
CNAME:facebook.com
CNAME:facebook.com

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.



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, SSL, CNAME, IP, IP-PORT or CDSR in this field.

Resource: Type:

List of resources

TYPE	RESOURCE NAME	RESOURCE VALIDATED	STATUS
URL	facebook.com	facebook.com	1000
URL	facebook.com	*facebook.com	1000
URL	facebook.com	facebook.com	1000
URL	facebook.com	*facebook.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	OLD VALUE
2023-01-01 10:00:00	admin	Rule created.		
2023-01-01 10:00:00	admin	Rule edited.		



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

ISP: VANTAGE

ISP: 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.

SEARCH DATABASE

Search by all database rules.

Use 1 space and after search word to make wildcard search "book" and after it to search certain phrase "book help".

Search parameters:

IP, CIDR, Domain, Comment: **laptopbook.com**

Search results for 'laptopbook.com':

Rule ID	Code	Type	Resource Name	Resource Validated	Rule Type	Name	Description
12	22222222	RE	Resource 1	Resource 1	Random Rule	Resource 1	Resource 1
13	33333333	RE	Resource 2	Resource 2	Random Rule	Resource 2	Resource 2
14	44444444	RE	Resource 3	Resource 3	Random Rule	Resource 3	Resource 3
15	55555555	RE	Resource 4	Resource 4	Random Rule	Resource 4	Resource 4

Search results:

Export:

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.