

Содержание

Интерфейс управления правилами фильтрации	3
Введение	3
Установка	3
Настройка	3
Настройки .env	3
Установка ключа	4
Установка роли	5
Настройка справочников	7
Управления профилями IGW	10
Настройка веб-сервера для глобальных списков	12
Собственный веб-сервер	12
Правила DSCP	14
Фильтр номеров AC	15
Исключение IP & AC	17
Исключение IP	18
Исключение номеров AC	20
Настройка ISP	22
Создание ISP профиля	22
Редактирование ISP профиля	23
Удаление ISP профиля	23
Профиль полисинга	24
Фильтр WEB и IP	25
Список правил блокировок	26
Создание/Редактирование правила блокировки	26
Удаление правила блокировки	27
Проверка домена	28
Поиск по базе (среди правил блокировки)	29
Белый список	30
Список правил белого списка	30
Создание/Редактирование белого списка	30
Удаление правила белого списка	32
Управление режимом работы белого списка	32
Поиск по базе (глобальный)	33
Мониторинг задач	34
Логи	34

Интерфейс управления правилами фильтрации

Введение

Интерфейс управления правилами фильтрации предназначен для управления правилами фильтрации на нескольких DPI одновременно с помощью графического интерфейса.

Установка

Для подсистемы можно использовать оборудование или виртуальные машины со сл.характеристиками:

1. Процессор (CPU) 2.5 ГГц, 1 шт
2. Оперативная память (RAM) 512 Мб - 1 Гб
3. Жесткий диск (HDD) 50 Гб - 250 Гб
4. Операционная система Cent OS 7+ (не ставьте `minimal`, иначе большинство зависимостей придется руками ставить)
5. Сетевая плата (NIC) от 10 Мб/сек



Рекомендуемая операционная система Cent OS 7+ (**не ставьте `minimal`, иначе большинство зависимостей придется руками ставить**). Если вам необходимо поставить на Cent OS 6, убедитесь что установлен supervisor 3+. Если у вас нет нужного пакета обращайтесь в тех. поддержку.



Интерфейс управления правилами фильтрации является отдельным разделом [Интерфейса управления SKAT DPI версия 2](#). Процесс установки идентичен скрипту инсталляции [Интерфейса управления SKAT DPI версия 2](#)

Настройка

Настройки .env

Настройка подсистемы выполняется через файл `.env`

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

Содержимое файла следующее:

```
#URL редиректа для услуги "Белый список"
```

```
ULR_WHITE_LIST_REDIRECT_URL=https://google.com
```

```
#Период очистки данных Ulr задач в днях  
ULR_QUEUE_DELETE_TASKS_DAYS_INTERVAL=1
```

```
#ASN для правил IP-исключений.  
ULR_IP_EXCLUDE_ASN=64401
```

```
#Хост для выгрузки списка блокируемых ресурсов. Для подключения к серверу блокируемых  
ресурсов.  
ULR_BLACK_LIST_DEPLOY_HOST=<IP адресс или хост Web сервера глобальных блокировок>
```

```
#Порт для выгрузки списка блокируемых ресурсов. Для подключения к серверу блокируемых  
ресурсов.  
ULR_BLACK_LIST_DEPLOY_PORT=22
```

```
#Имя пользователя для выгрузки списка блокируемых ресурсов. Для подключения к серверу  
блокируемых ресурсов.  
ULR_BLACK_LIST_DEPLOY_USER=default
```

```
#Пароль для выгрузки списка блокируемых ресурсов. Для подключения к серверу  
блокируемых ресурсов  
ULR_BLACK_LIST_DEPLOY_PASS=
```

```
#Использовать sudo при выгрузке списка блокируемых ресурсов. (0 - не использовать, 1 -  
использовать)  
ULR_BLACK_LIST_DEPLOY_SUDO=1
```

```
#Путь для сохранения черных списков.  
ULR_BLACK_LIST_DEPLOY_PATH=/var/www/html/blacklists/
```

```
#Уровень детализации логов.(0 - инфо, 1 - отладка, 2 - трассировка)  
ULR_LOAD_LOG_LEVEL=0
```



Если были внесены изменения в .env, необходимо выполнить команду

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



Данные настройки можно внести в конфигурацию в разделе Администратор→Конфигурация сервера DPIUI2 (GUI) в интерфейсе управления SKAT DPI версия 2

Установка ключа

Для того, чтобы получить возможность пользоваться Интерфейсом управления правилами фильтрации необходимо активировать лицензию Ulr-раздела в DPIUI2.

Для этого необходимо выполнить команду:

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

Далее:

1. Ввести уровень лицензии standard;
2. Ввести дату завершения лицензии в формате Y-m-d (например 2099-12-31);
3. Ввести пароль от лицензии.

В случае, если Вами были введены корректные данные, выведется сообщение об успешной активации лицензии для Ulr-раздела:

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

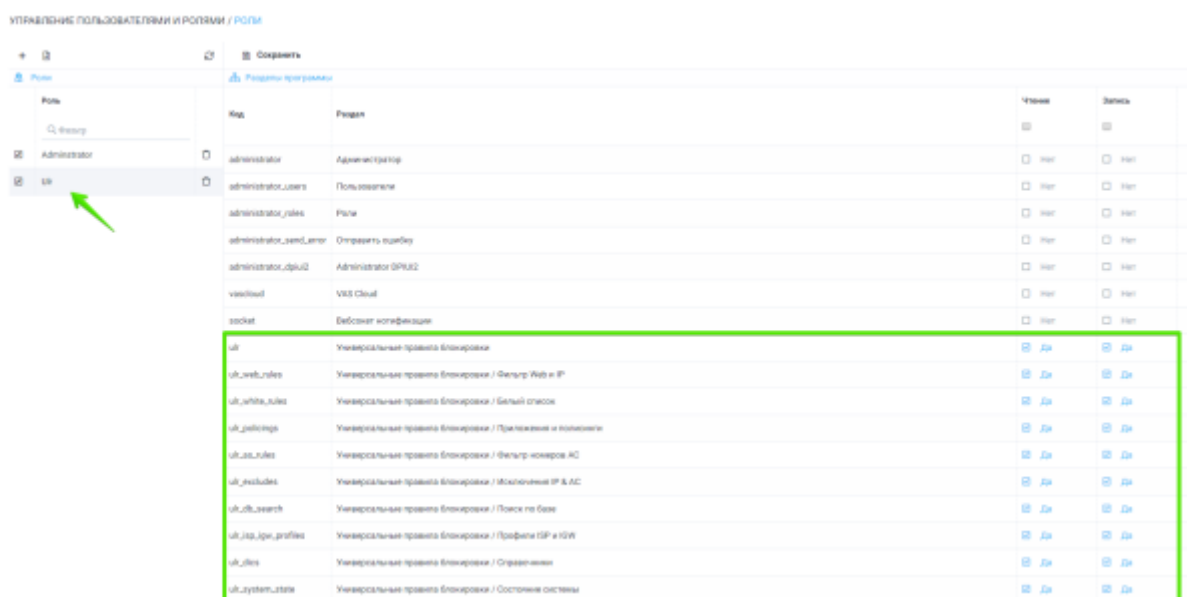
Enter expire date in Y-m-d format:
> 2099-12-31

Enter password:
>

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

Установка роли

В интерфейсе DPIUI2 перейдите в раздел Администратор→Роли. Создайте новую роль и установите в ней права на чтение и запись в разделе ulr_admin как на изображении ниже.



Далее, перейдите в раздел Администратор→Пользователи. Создайте нового пользователя и установите ему роль, которую вы создали ранее.

The screenshot shows a user creation form with the following fields and values:

- Имя пользователя *: ulr_user
- ФИО *: user
- E-mail *: user@user.com
- Телефон *: +70123456789
- Компания *: vasexperts
- Должность *: ulr
- Роль: Ulr (selected from a dropdown menu)
- Новый пароль: *****
- Подтвердить пароль: *****
- Сохранить button

При авторизации от имени этого пользователя, он будет переключен в раздел управления правилами фильтрации.

The screenshot shows the 'Фильтр WEB и IP' (Web/IP Filter) section of the Spectre DPI interface. The left sidebar contains a menu with the following items:

- правила
- фильтр WEB и IP
- Добавить новое правило
- Проверить доступ
- Панель базы
- Приложения и подсети
- Фильтр номеров AS
- Исключения IP & AS
- Свальный список
- Проверка IP и ASN
- Поиск по базе
- Состояние системы
- Справка

The main content area displays the 'Фильтр WEB и IP' section, which includes a table for the statistics of the Web/IP filter rules and a table for the last entries in the Web/IP filter registry.

Фильтр WEB и IP

Статистика правил Web/IP фильтра

тип	активно	выключено	всего
Данные не найдены			

Последние записи в реестре Web/IP фильтра

ID	дата	тип	ресурс	проверенный ресурс	результат	примечание
Данные не найдены						

0 of 0

Экспорт

Настройка справочников

- Справочник категорий
- Справочник регуляторов



Данные справочники используются при создании/редактировании правил.

Справочник категорий

В интерфейсе управления правилами фильтрации перейдите в раздел Справочники→Категории.

СЭКТРЕ DPI

СПРАВОЧНИК КАТЕГОРИЙ

ПРАВИЛА

- ФИЛЬТР WEB И IP
- ПРИЛОЖЕНИЯ И ПОСМОТРЕТЬ
- ФИЛЬТР НОМЕРОВ АС
- ИСКЛЮЧЕНИЯ IP & АС
- БЕЛЫЙ СПИСОК
- ПРОФИЛИ SIP И KAT
- ПОИСК ПО БАЗЕ
- СОСТОЯНИЕ СИСТЕМЫ
- СПРАВОЧНИКИ
 - Категории
 - Регуляторы

КАТЕГОРИИ

Добавить новую запись

Название *

Публичное описание

ДОБАВИТЬ ЗАПИСЬ

Поиск по таблице...

НАЗВАНИЕ	ДАТА	ОПИСАНИЕ
Категория	13.02.2019	Описание

1-1 OF 1

ЭКСПОРТ

Создание

В форме введите название категории, ее описание и нажмите кнопку "Добавить запись".

КАТЕГОРИИ

Добавить новую запись

Название *

Категория

Публичное описание

Описание

ДОБАВИТЬ ЗАПИСЬ

Поиск по таблице...

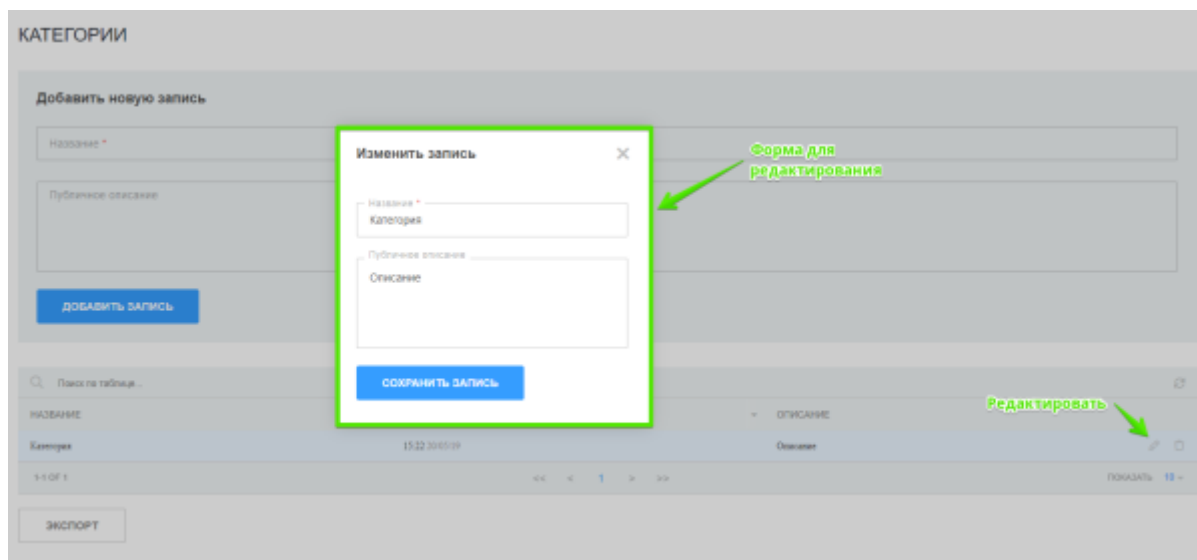
НАЗВАНИЕ	ДАТА	ОПИСАНИЕ
Данные не найдены		

1-1 OF 1

ЭКСПОРТ

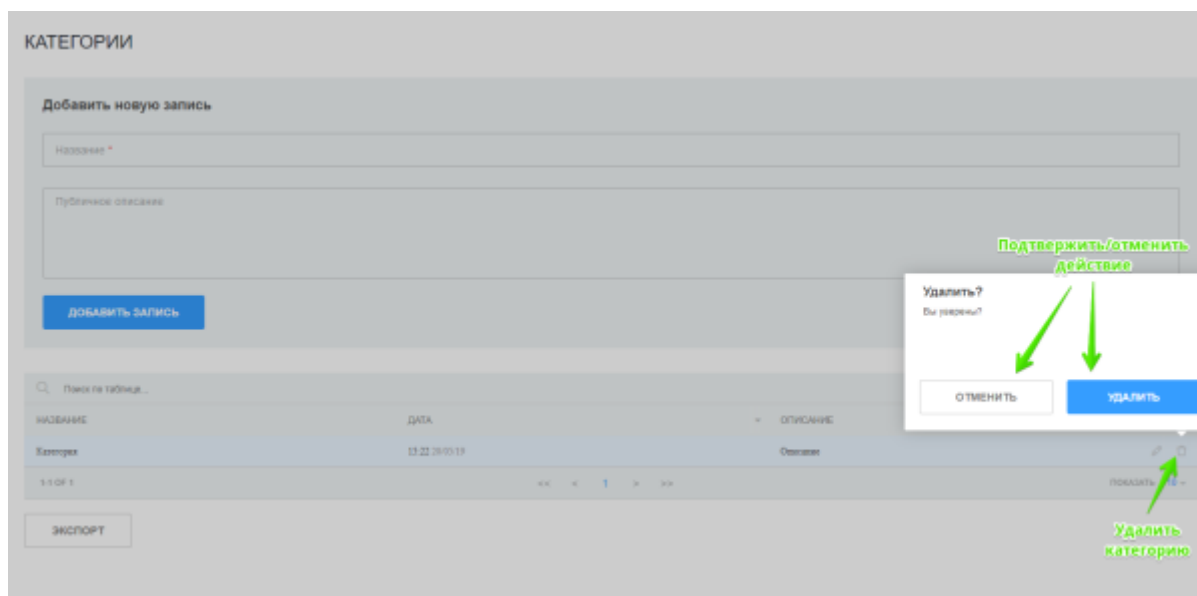
Редактирование

В таблице с категориями нажмите на кнопку редактирования категории, чтобы открылась форма редактирования. В форме измените название и/или описание категории, после чего нажмите кнопку "Сохранить запись".



Удаление

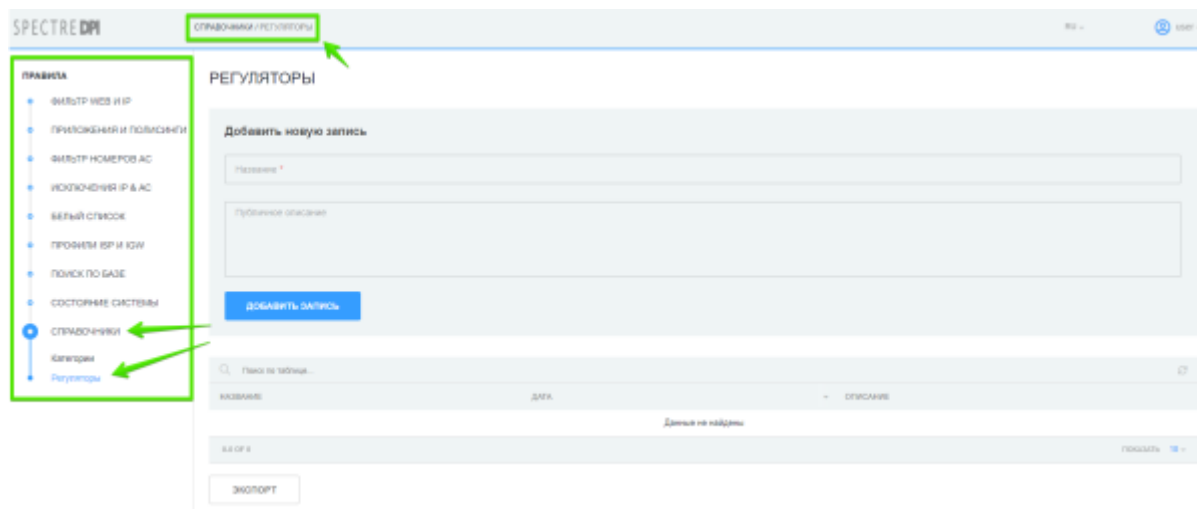
В таблице с категориями нажмите на кнопку удаления категории. В появившемся окне подтвердите или отмените действие.



Внимание: Перед удалением категории проверьте наличие правил, которые ссылаются на эту категорию!

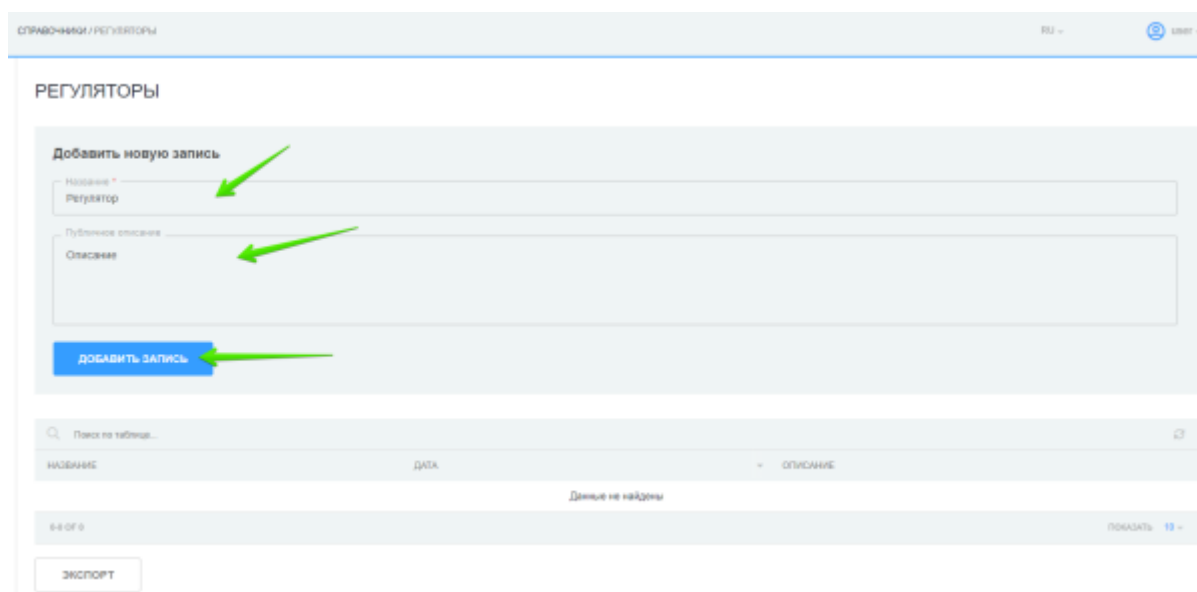
Справочник регуляторов

В интерфейсе управления правилами фильтрации перейдите в раздел Справочники→Регуляторы.



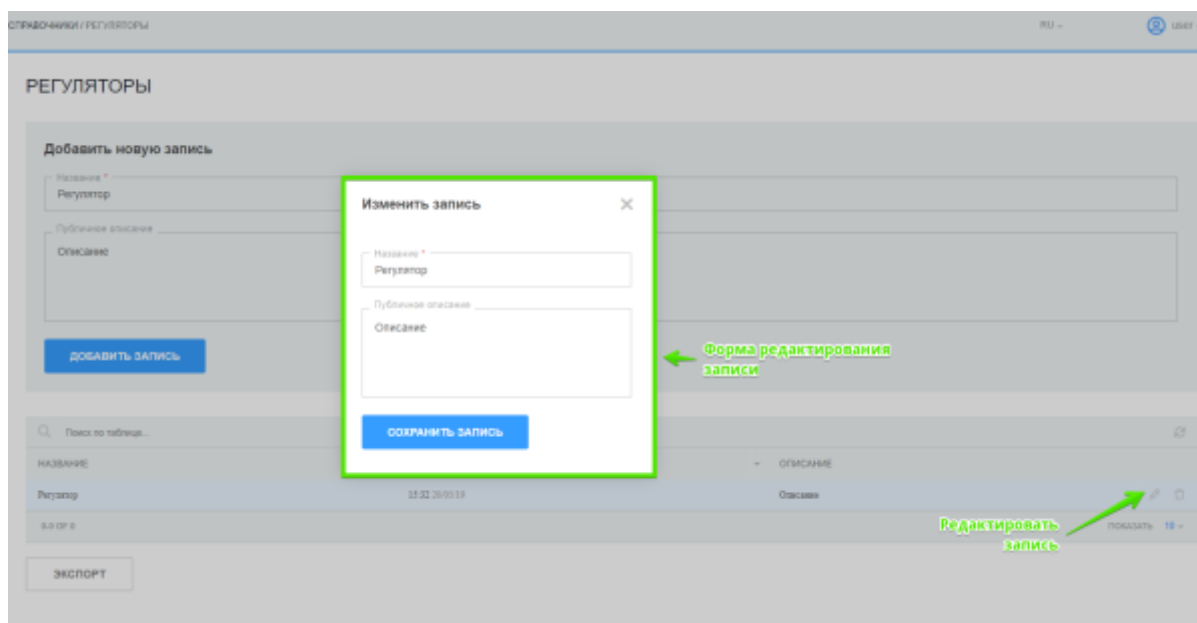
Создание

В форме введите название регулятора, его описание и нажмите кнопку "Добавить запись".



Редактирование

В таблице со списком регуляторов нажмите на кнопку редактирования регулятора, чтобы открылась форма редактирования. В форме измените название и/или описание регулятора, после чего нажмите кнопку "Сохранить запись".



Удаление

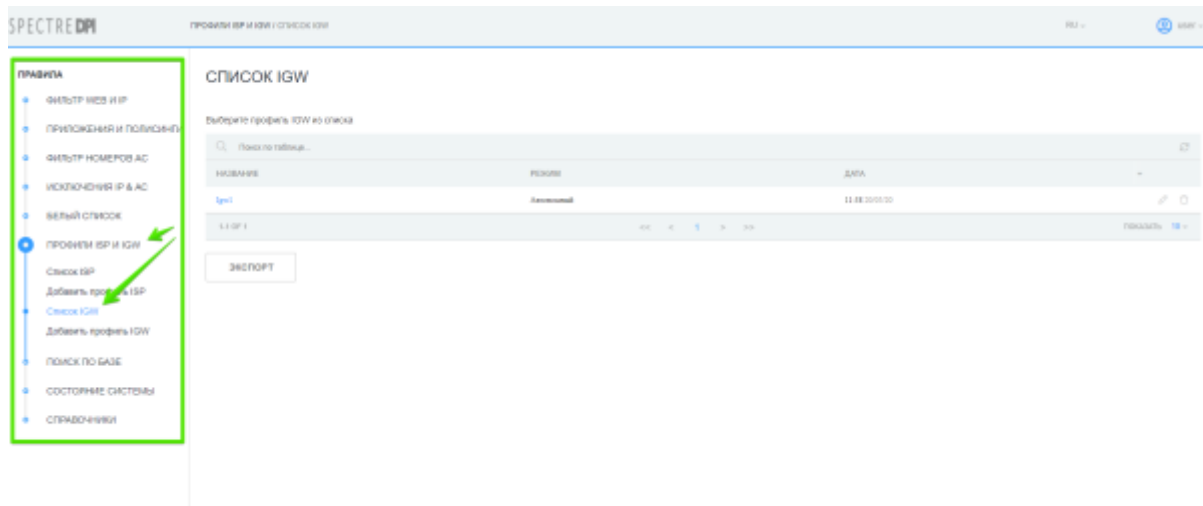
В таблице со списком регуляторов нажмите на кнопку удаления записи. В появившемся окне подтвердите или отмените действие.



Внимание: Перед удалением записи проверьте наличие правил, которые ссылаются на эту запись!

Управления профилями IGW

Перейдите в раздел "Профили ISP и IGW" → "Список IGW".

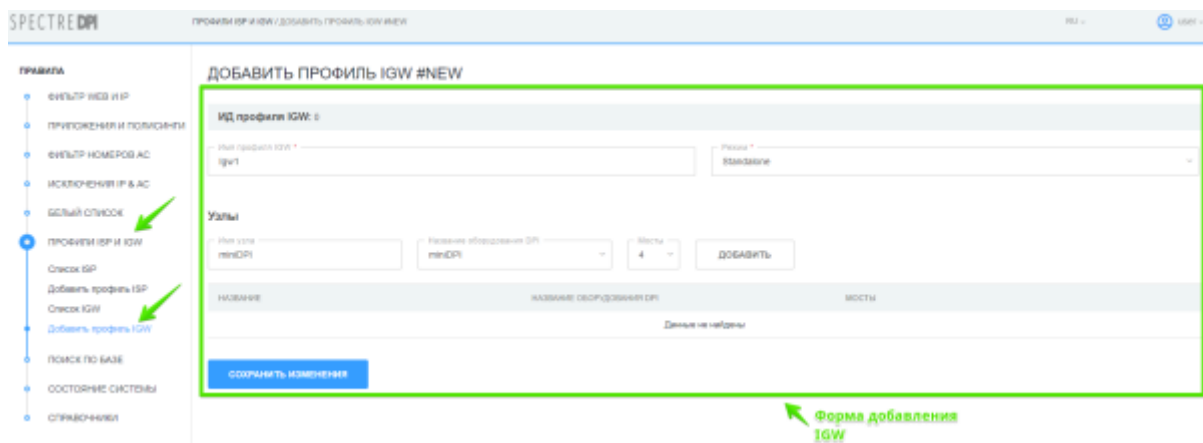


Создание

Для добавления нового профиля IGW перейдите в раздел "Профили ISP и IGW" → "Добавить профиль IGW".

В форме укажите:

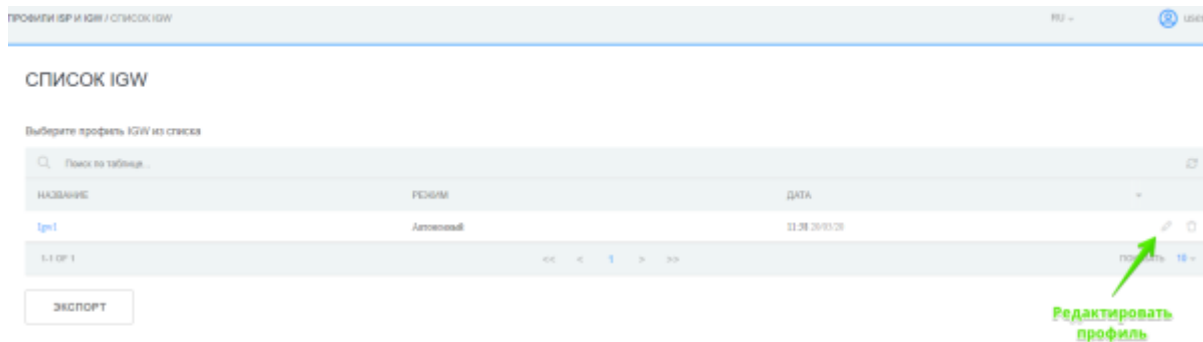
- Имя профиля;
- Режим работы (Snadalone/Cluster)
- Узлы для профиля (Имя узла, DPI оборудование из списка доступных и количество мостов)



Перед тем как создавать профиль IGW добавьте FastDPI сервер в основном интерфейсе DPIUI 2 в разделе "Администратор" → "Оборудование".

Редактирование

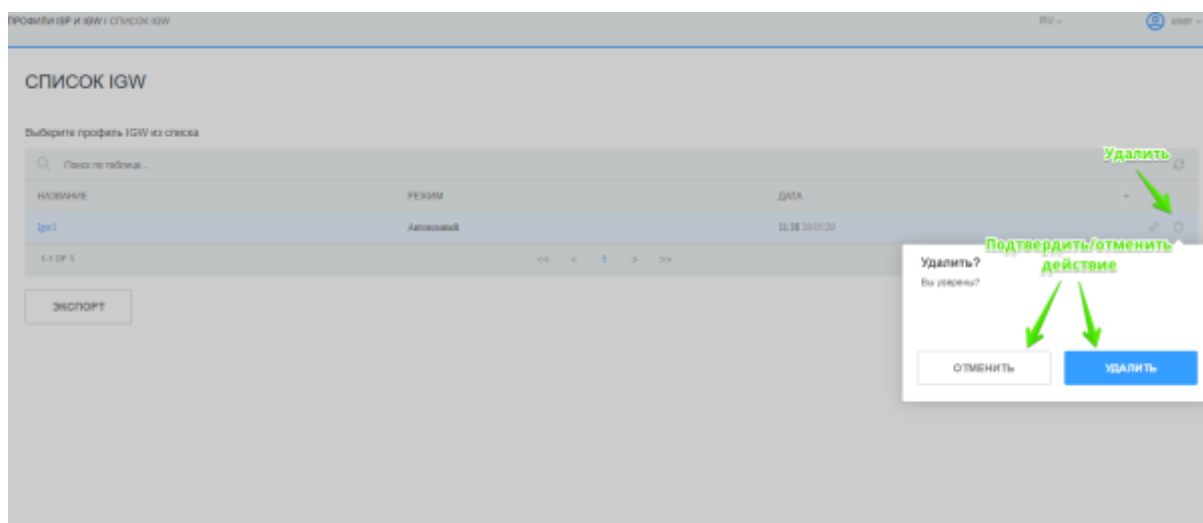
В разделе "Профили ISP и IGW" → "Список IGW" нажмите кнопку "Редактировать профиль".



Откроется форма создания/редактирования профиля IGW, внесите необходимые Вам изменения и нажмите "Сохранить изменения".

Удаление

В разделе "Профили ISP и IGW"→"Список IGW" нажмите кнопку "Удалить" и подтвердите/отмените действие.



Внимание: Перед удалением профиля проверьте наличие ISP профилей, которые ссылаются на этот профиль!

Настройка веб-сервера для глобальных списков

Собственный веб-сервер

1. Подготовить машину с установленной CentOS7+

2. Создать беспарольного sudo пользователя аналогично описанию в разделе [Dpiui2:Настройка подключения к dpi](#)

3. Запустите следующий скрипт:

```
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. В конфигурации dpiui2 в разделе [Ulr настроек](#) указать данные для доступа к Web-серверу

5. В настройках всех подключенных FastDPI-серверов указать путь к Custom спискам блокировок:

```
# Словарь URL для блокирования по протоколу HTTP (custom_url_black_list)
custom_url_black_list=http://<IP адрес Web-сервера>/blacklist.dict

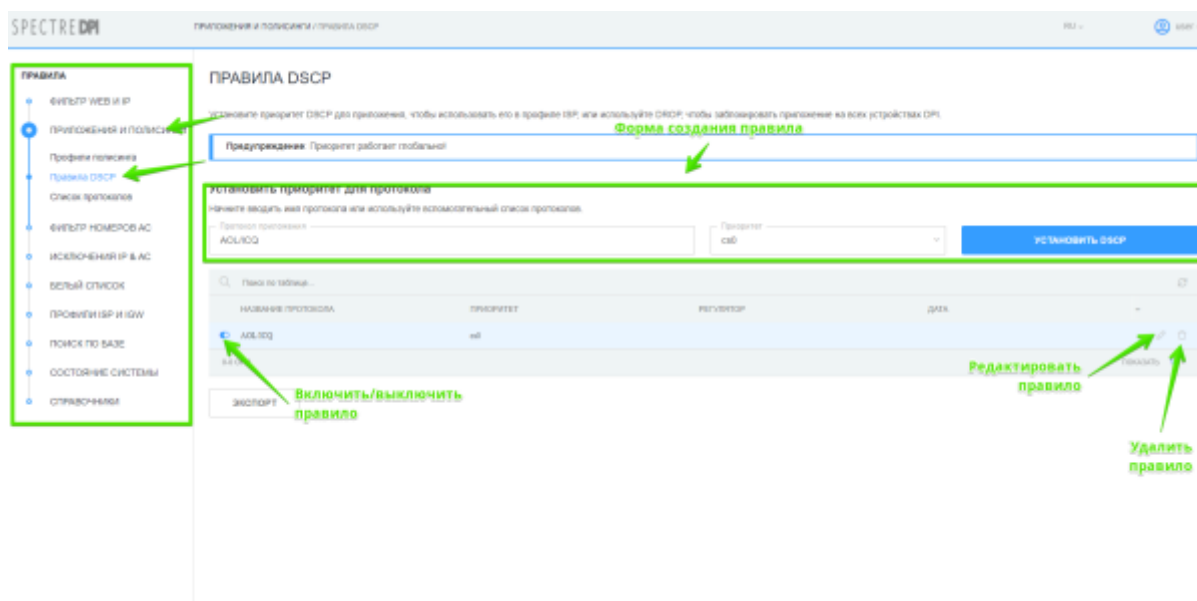
# Словарь имен для блокирования протокола HTTPS по сертификату
(custom_cname_black_list)
custom_cname_black_list=http://<IP адрес Web-сервера>/blacklistcn.dict

# Словарь IP адресов для блокирования протокола HTTPS по IP
(custom_ip_black_list)
custom_ip_black_list=http://<IP адрес Web-сервера>/blacklistip.dict

# Словарь имен хостов для блокирования HTTPS по SNI (custom_sni_black_list)
custom_sni_black_list=http://<IP адрес Web-сервера>/blacklistsni.dict
```

Правила DSCP

Перейдите в раздел "Приложения и полисинги"→"Правила DSCP".



Создание

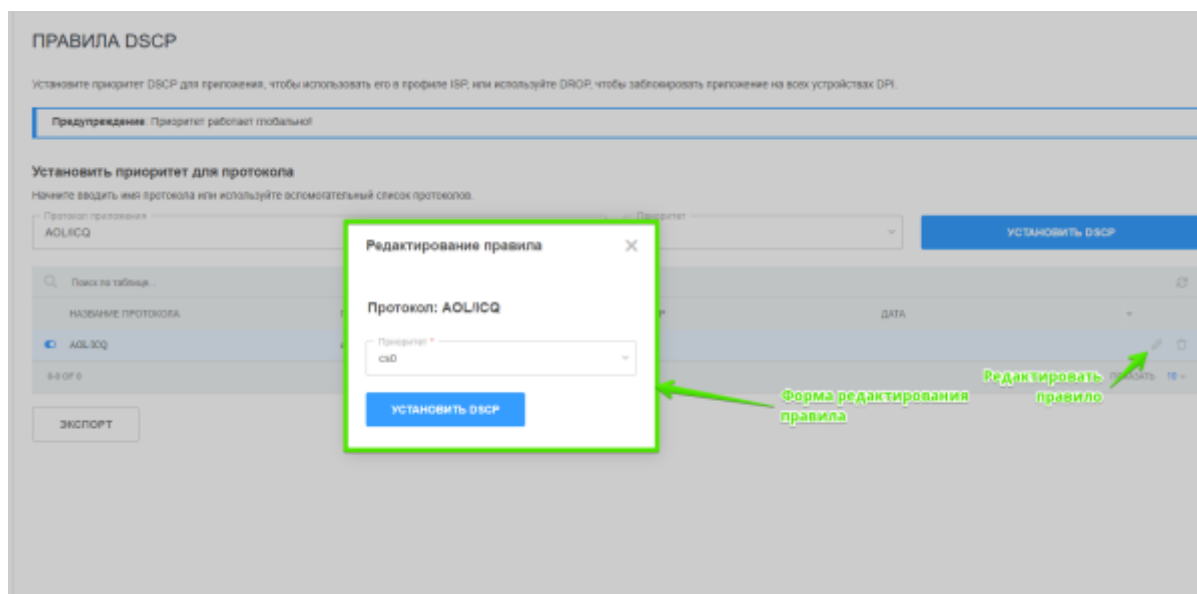
В форме создания правила:

- Введите имя протокола приложения и выберите нужный из представленного списка;
- Выберите приоритет из представленного списка.

Сохраните правило путем нажатия кнопки "Установить DSCP".

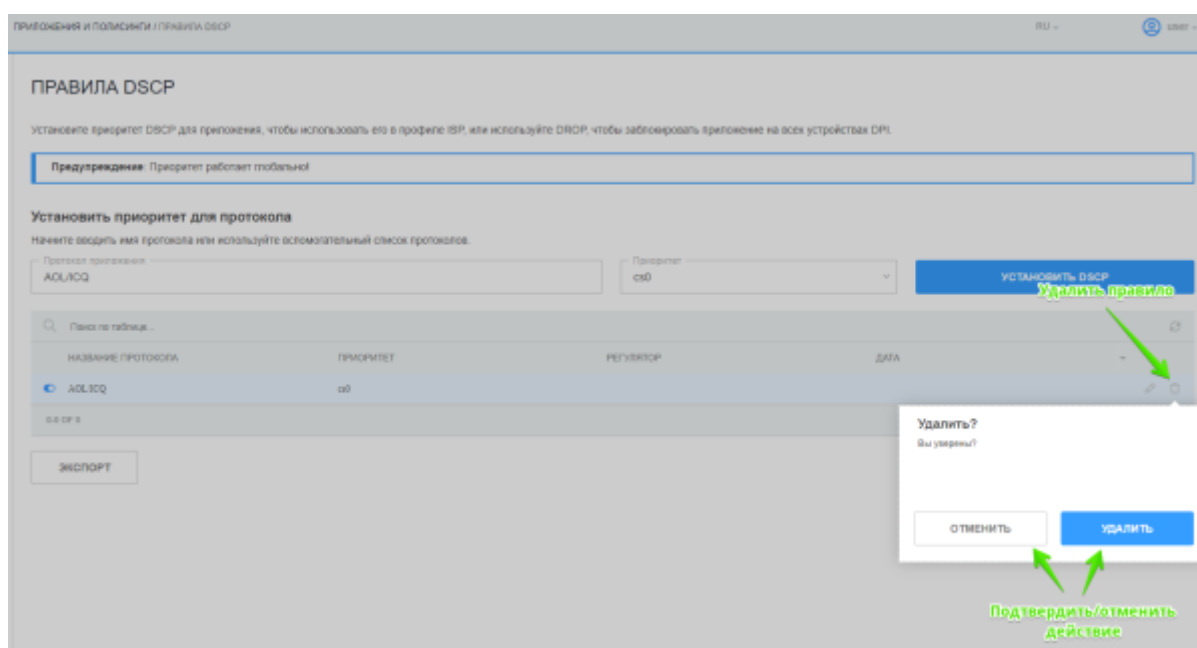
Редактирование

В списке правил DSCP нажмите на кнопку "Редактировать правило". В открывшейся форме редактирования правила DSCP задайте необходимый приоритет и сохраните изменения нажатием кнопки "Установить DSCP".



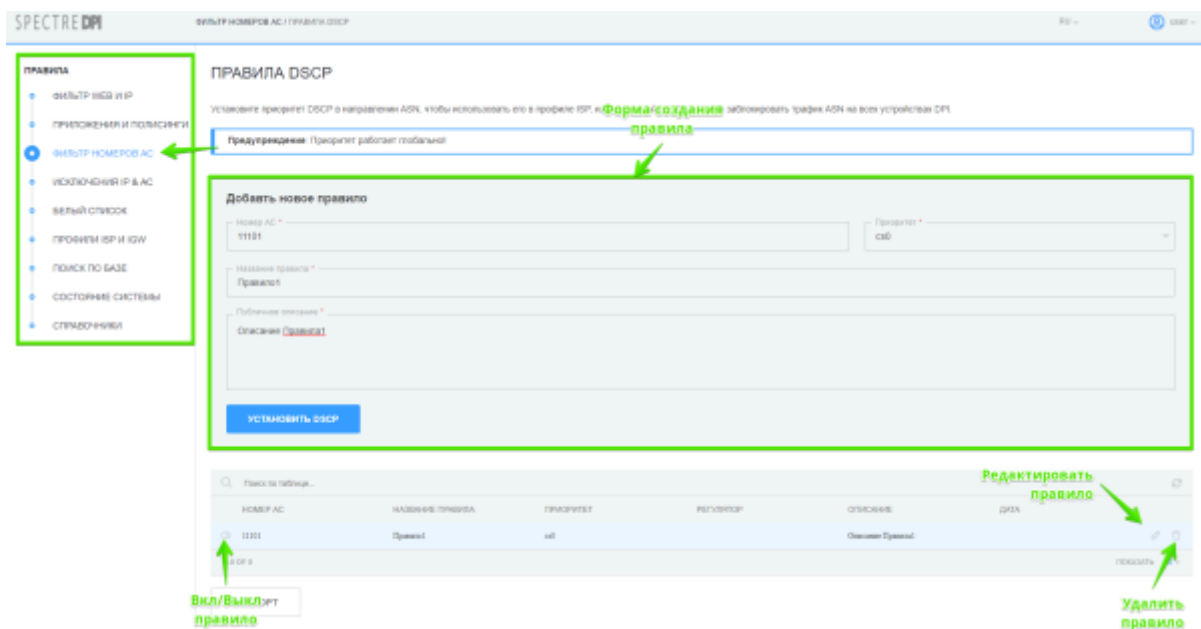
Удаление

В списке правил DSCP нажмите на кнопку "Удалить правило" и, в появившемся окне, подтвердите либо отмените действие.



Фильтр номеров AC

Перейдите в раздел "Фильтр номеров AC".



Создание

В форме создания правила:

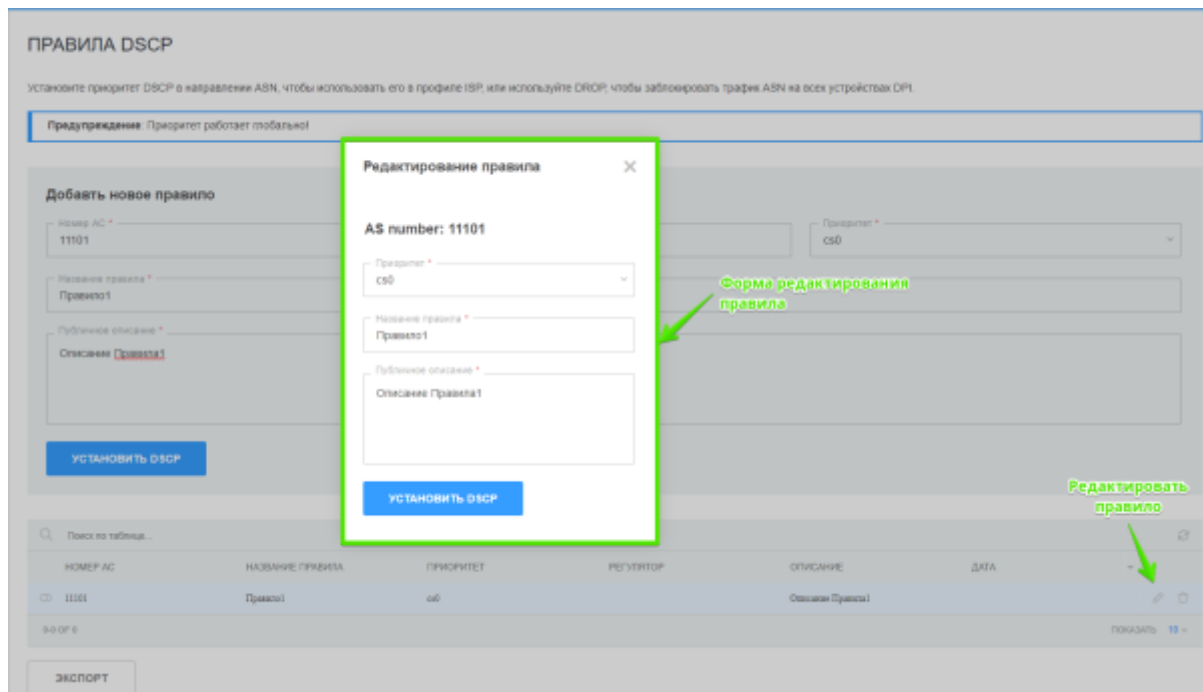
- Укажите номер АС;
- Выберите приоритет из представленного списка;
- Укажите название правила;
- Укажите описание правила;

Сохраните правило путем нажатия кнопки "Установить DSCP".

Редактирование

В списке правил DSCP в направлении ASN нажмите на кнопку "Редактировать правило". В открывшейся форме редактирования правила DSCP в направлении ASN при необходимости:

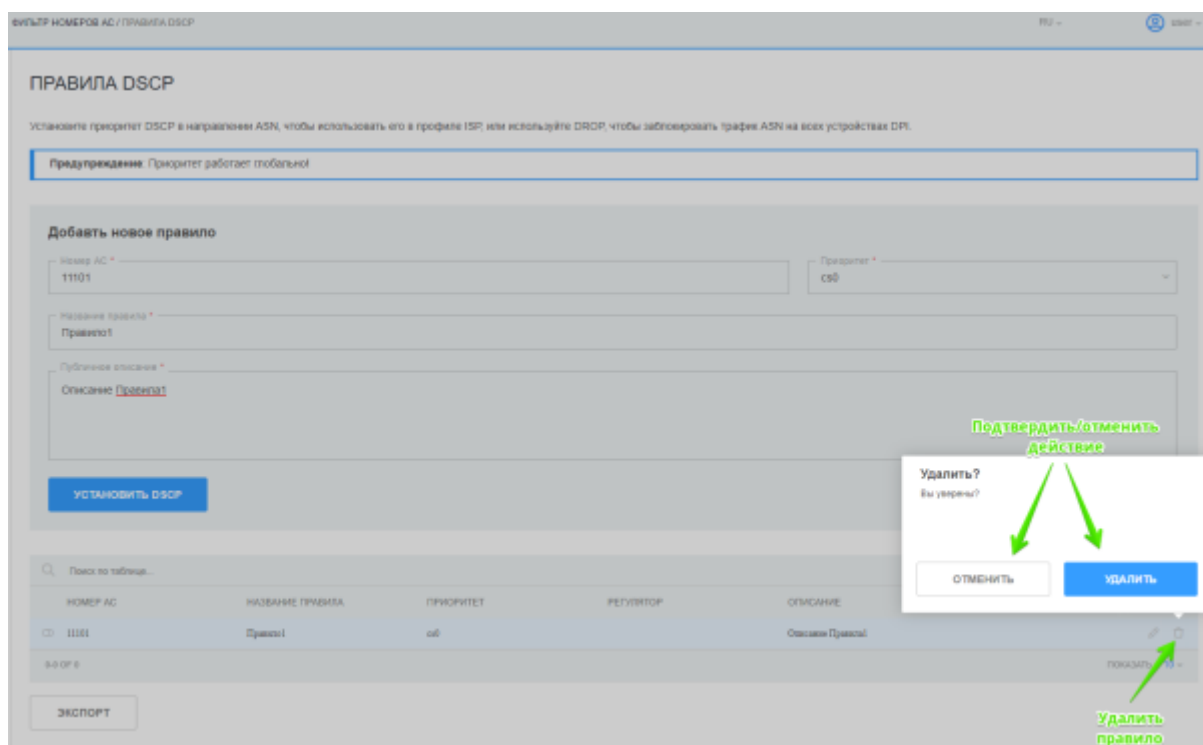
- Выберите приоритет из представленного списка;
- Укажите название правила;
- Укажите описание правила;



Сохраните изменения путем нажатия кнопки "Установить DSCP".

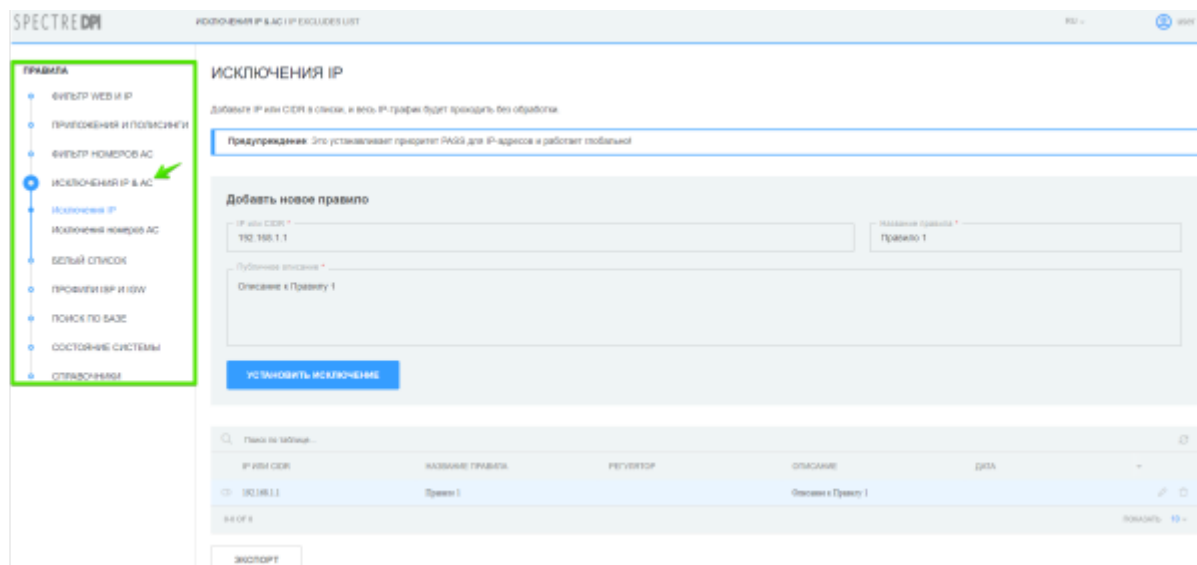
Удаление

В списке правил DSCP в направлении ASN нажмите на кнопку "Удалить правило" и, в появившемся окне, подтвердите либо отмените действие.



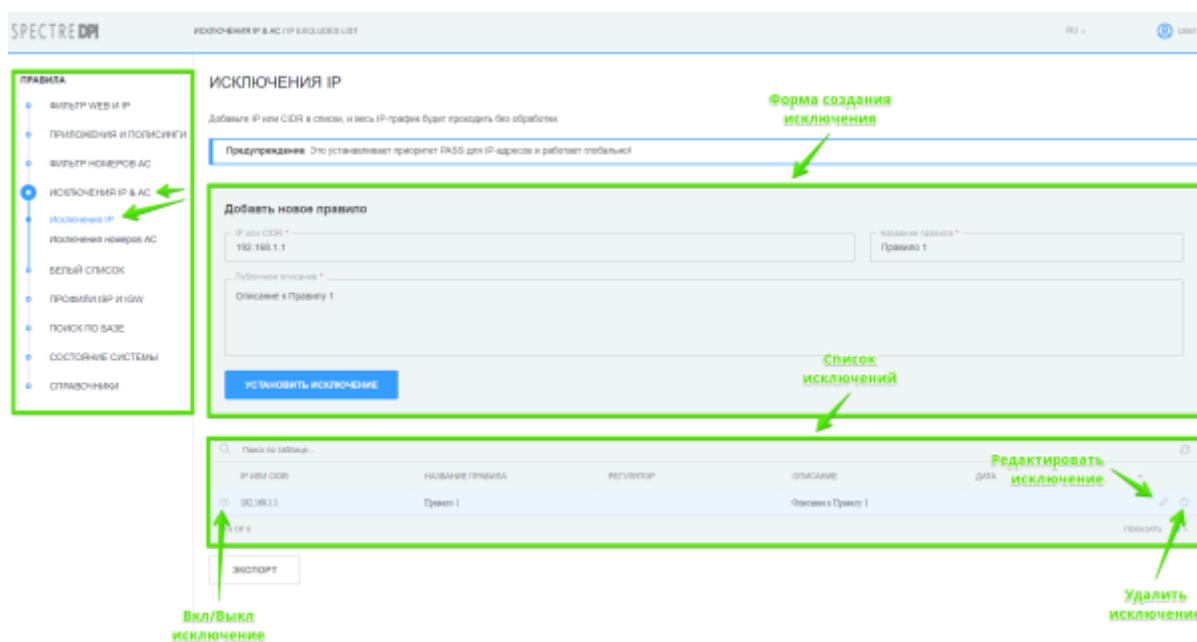
Исключение IP & AC

Перейдите в раздел "Исключение IP & AC".



Исключение IP

Перейдите в раздел "Исключение IP & AC"→"Исключение IP".



Создание

В форме создания правила:

- Укажите IP/CIDR;
- Укажите название правила;
- Укажите описание правила;

Сохраните правило путем нажатия кнопки "Установить исключение".

Редактирование

Нажмите на кнопку "Редактировать исключение". В форме редактирования правила есть возможность изменить:

- название правила;
- описание правила.

Редактирование правила

×

IP or CIDR: 192.168.1.1

Название правила *

Правило 1

Публичное описание *

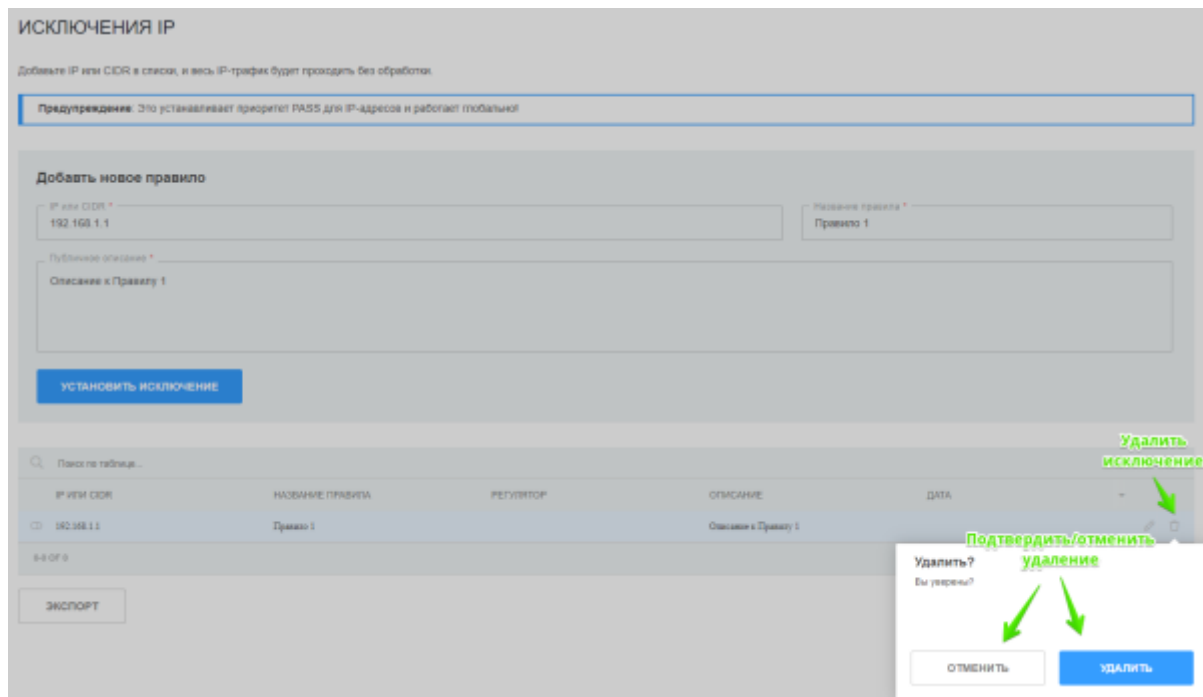
Описание к Правилу 1

УСТАНОВИТЬ DSCP

Сохраните изменения путем нажатия кнопки "Установить DSCP".

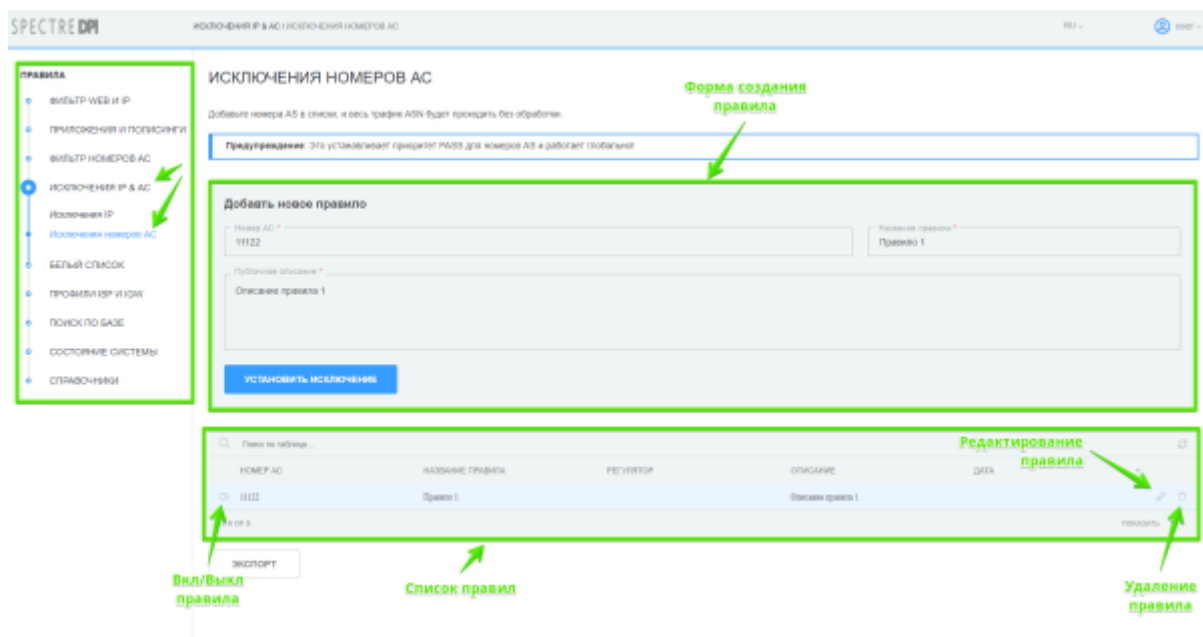
Удаление

В списке исключений нажмите на кнопку "Удалить исключение" и, в появившемся окне, подтвердите либо отмените удаление.



Исключение номеров АС

Перейдите в раздел "Исключение IP & АС"→"Исключение номеров АС".



Создание

В форме создания правила:

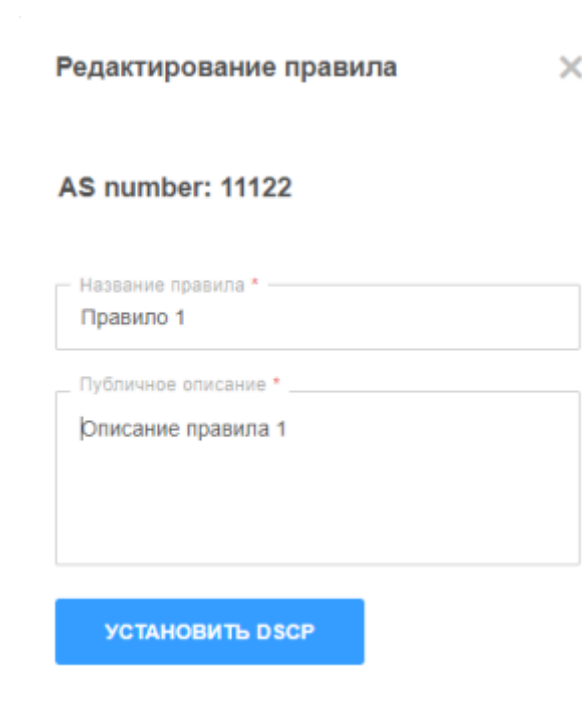
- Укажите номер АС;
- Укажите название правила;
- Укажите описание правила;

Сохраните правило путем нажатия кнопки "Установить исключение".

Редактирование

Нажмите на кнопку "Редактировать правило". В форме редактирования правила есть возможность изменить:

- название правила;
- описание правила.



Редактирование правила

AS number: 11122

Название правила *
Правило 1

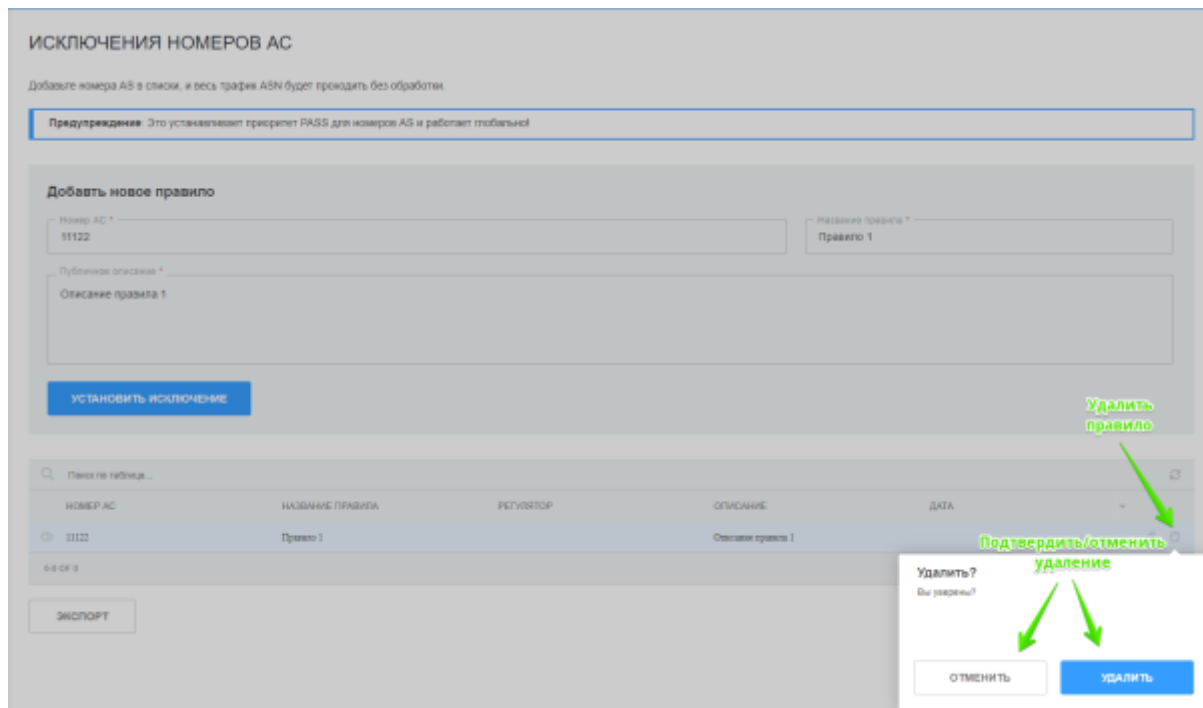
Публичное описание *
Описание правила 1

УСТАНОВИТЬ DSCP

Сохраните изменения путем нажатия кнопки "Установить DSCP".

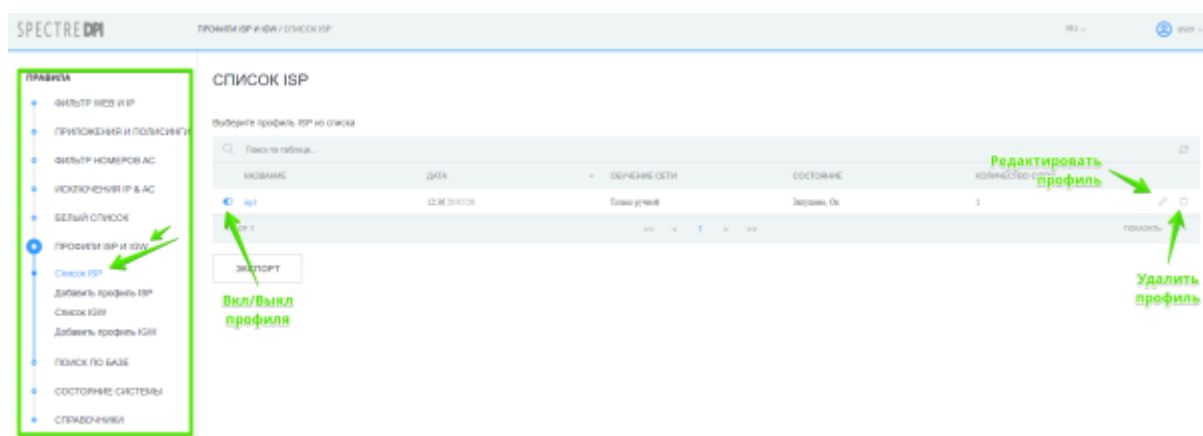
Удаление

В списке исключений нажмите на кнопку "Удалить правило" и, в появившемся окне, подтвердите либо отмените удаление.



Настройка ISP

Перейдите в раздел "Профили ISP и IGW"→"Список ISP".



Создание ISP профиля

Для добавления нового профиля IGW перейдите в раздел "Профили ISP и IGW"→"Добавить профиль ISP".

В форме укажите:

- Имя профиля ISP;
- Выберите бордер из представленного списка;
- Логин, который будет использоваться на узле DPI;
- Префикс для списков на узле DPI(будет использоваться как имя профиля услуг на узле);
- Выберите используемые мосты выбранного бордера;
- Выберите Обучение сети для получения адресов данного профиля;
- Укажите адрес/сети данного ISP (при необходимости).

Нажмите кнопку "Сохранить изменения" или "Сохранить и Отключить/Включить".



По умолчанию профиль ISP при создании включен. На узлы DPI выгружаются только включенные профили.

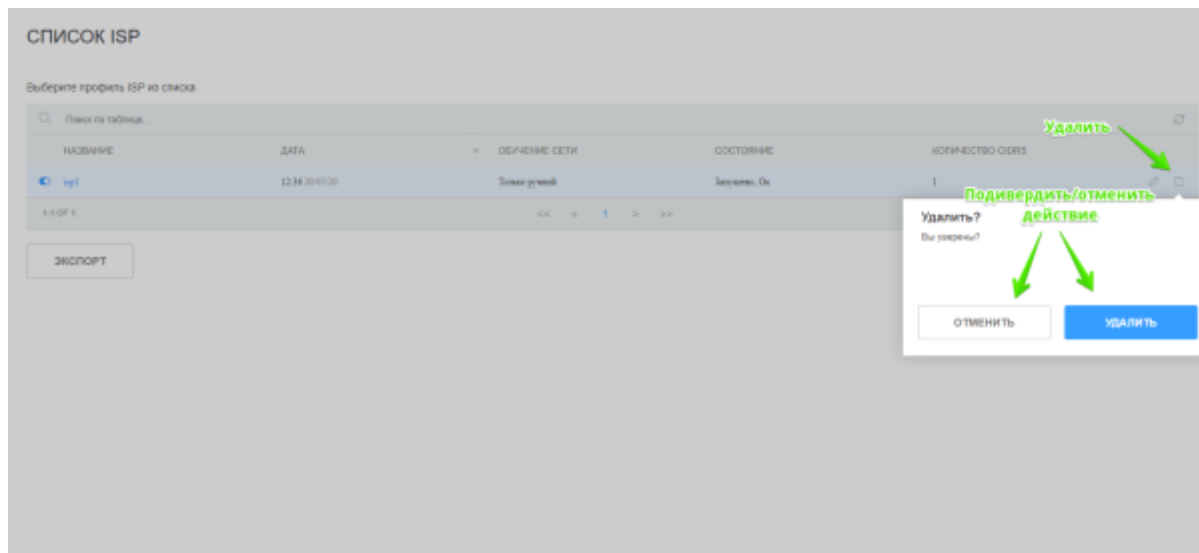
Редактирование ISP профиля

В разделе "Профили ISP и IGW"→"Список ISP" нажмите кнопку "Редактировать профиль".

Откроется форма создания/редактирования профиля ISP, внесите ,необходимые Вам, изменения и нажмите кнопку "Сохранить изменения" или "Сохранить и Отключить/Включить".

Удаление ISP профиля

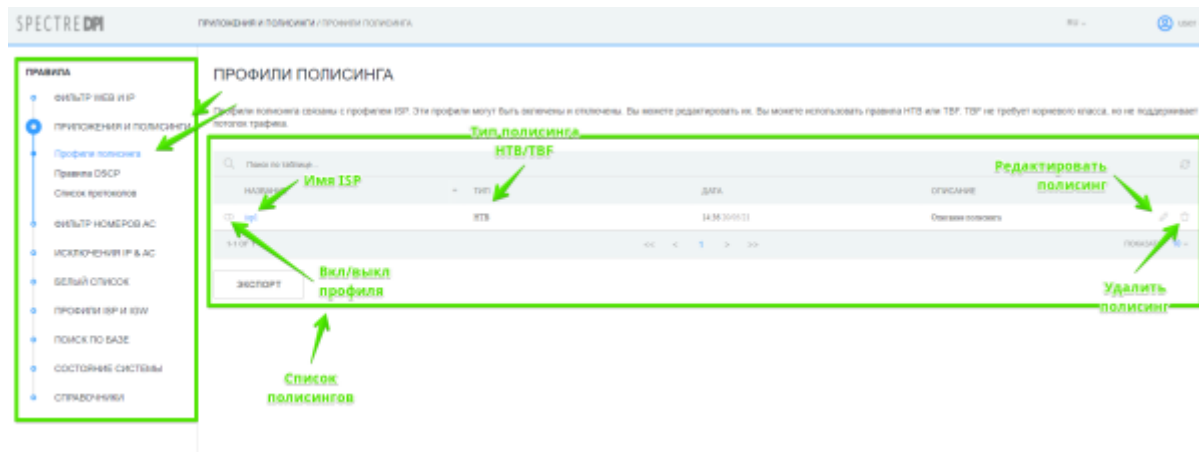
В разделе "Профили ISP и IGW"→"Список ISP" нажмите кнопку "Удалить" и подтвердите/отмените действие.



Внимание: Перед удалением профиля проверьте наличие правил, которые ссылаются на этот профиль!

Профиль полисинга

Перейдите в раздел "Приложения и полисинги" → "Профили полисинга".



Редактирование профиля полисинга

Нажмите на кнопку "Редактировать полисинг".

Профили полисинга связаны с профилем ISP. Эти профили могут быть включены и отключены. Вы можете редактировать их. Вы можете использовать права TBW или TBF. TBW не требует корневого класса, но не поддерживает поток трафика.

Имя профиля: **isp1** (Включено)

[Настройка профиля ISP](#)

Описание *

Описание полисинга

Тип полисинга *

TBF

АВТОЗАПОЛНЕНИЕ

Входящий профиль:

CS0	8	Ед. изм.	Бит/с
CS1	8	Ед. изм.	Бит/с
CS2	8	Ед. изм.	Бит/с
CS3	8	Ед. изм.	Бит/с
CS4	8	Ед. изм.	Бит/с
CS5	8	Ед. изм.	Бит/с
CS6	8	Ед. изм.	Бит/с

Исходящий профиль:

CS0	8	Ед. изм.	Бит/с	Список приложений для CS0
CS1	8	Ед. изм.	Бит/с	Список приложений для CS1
CS2	8	Ед. изм.	Бит/с	Список приложений для CS2
CS3	8	Ед. изм.	Бит/с	Список приложений для CS3
CS4	8	Ед. изм.	Бит/с	Список приложений для CS4
CS5	8	Ед. изм.	Бит/с	Список приложений для CS5
CS6	8	Ед. изм.	Бит/с	Список приложений для CS6

В открываемой форме редактирования полисинга:

- Введите описание профиля;
- Выберите тип полисинга TBF/HTB (в зависимости от выбранного типа форма со значениями по классам будет выглядеть по-разному)

Вы можете воспользоваться автозаполнением конфигурации:



- Для HTB типа: rate=8Бит/с, ceil=значение, которое было указано в форме автозаполнения;
- Для TBF типа: rate=значение, которое было указано в форме автозаполнения.

Для того, чтобы сохранить изменения профиля, нажмите кнопку "Сохранить профиль" либо "Сохранить и отключить/включить".



По умолчанию профиль полисинга отключен.

Удаление профиля полисинга

Удалить профиль можно либо путем нажатия кнопки "Удалить профиль" в списке профилей полисингов либо на странице редактирования профиля нажатием кнопки "Удалить профиль".

Фильтр WEB и IP

Список правил блокировок

Перейдите в раздел "Фильтр WEB и IP".

ПРАВИЛА

- Фильтр WEB и IP
- Добавить новое правило
- Проверить данные
- Поиск по базе
- ПРИЛОЖЕНИЯ И ПОЛИСИТИ
- ФИЛЬТР НОМЕРОВ АС
- ИСКЛЮЧЕНИЯ IP & АС
- БЕЛЫЙ СПИСОК
- ПРОФИЛИ И КОИ
- ПОИСК ПО БАЗЕ
- СОСТОЯНИЕ СИСТЕМЫ
- СПРАВКА

ФИЛЬТР WEB и IP

Статистика правил Web/IP фильтра

Тип	активно	выключено	всего
OK	2	0	2
SSL	2	0	2

Последние записи в реестре Web/IP фильтра

ID	DATA	ТИП	РЕСУРС	проверенный ресурс	регулятор	примеч.
Включено	11.04.2019 02	SSL	facebook.com	*facebook.com	Регулятор	facebook
Включено	11.04.2019 02	SSL	facebook.com	facebook.com	Регулятор	facebook
Включено	11.04.2019 02	OK	facebook.com	*facebook.com	Регулятор	facebook
Включено	11.04.2019 02	OK	facebook.com	facebook.com	Регулятор	facebook

1-4 OF 4

Экспорт

Редактировать правило

Создание/Редактирование правила блокировки

- Для создания нового правила блокировка ресурса перейдите в раздел "Фильтр WEB и IP" → "Добавить новое правило";
- Для внесения изменений в существующее правило перейдите в раздел "Фильтр WEB и IP" и нажмите на кнопку "Редактировать правило".

В открывшейся форме:

- Выберите регулятор;
- Выберите категорию;
- Введите публичное описание правила;
- Введите скрытое описание правила;

ДОБАВИТЬ ПРАВИЛО #NEW

Ид правила: 0

Регулятор *

Категория *

Публичное описание

vk.com

Скрытое *

vk.com

Это описание будет показано, если у вас есть публичная база данных черного списка

Ресурс

Выберите тип ресурса и укажите в этом поле URL, SNI, CN, IP, IP:PORT или CIDR.

Ресурс

vk.com

Тип

URL

ПРОВЕРИТЬ

✗ **Результат проверки:** Это ресурс SSL / TLS. Мы можем заблокировать ДОМЕН (ЦЕЛЫЙ ДОМЕН).
Следующие SNI и CN будут добавлены в список:
SNI: vk.com
SNI: *vk.com
CN: vk.com
CN: *vk.com

ДОБАВИТЬ В СПИСОК

ИМПОРТ ИЗ ФАЙЛА

В форме проверки/валидации ресурса введите ресурс и выберите его тип:

- В случае, если нет необходимости в проверке/валидации ресурса нажмите "Добавить в список";
- Нажмите кнопку "Проверить". Будет произведен вывод информации по ресурсу, которую можно будет добавить в список блокировок по этому правилу нажатием кнопки "Добавить в список".

Список ресурсов

ТИП	РЕСУРС	ПРОВЕРЕННЫЙ РЕСУРС	СТАТУС
ISP	vk.com	*vk.com	Применен
ISP	vk.com	vk.com	Применен
SN	vk.com	*vk.com	Применен
SN	vk.com	vk.com	Применен

ОЧИСТИТЬ ВСЕ

☒ Применить правило к ISP из списка

Выберите ISP, к которому будет применено правило

☐ isp1

ВЫБРАТЬ ВСЕ СНЯТЬ ВСЕ

Журнал действий

ДАТА	ПОЛЬЗОВАТЕЛЬ	ДЕЙСТВИЕ	НОВОЕ ЗНАЧЕНИЕ	СТАРОЕ ЗНАЧЕНИЕ
Данные не найдены				

0-0 OF 0 ПОКАЗАТЬ 10

СОХРАНИТЬ ИЗМЕНЕНИЯ СОХРАНИТЬ И ОТКЛЮЧИТЬ

В подразделе привязки правила к профилям ISP:

- В случае, если опция "Применит правило к ISP из списка" отключена, данное правило считается глобальным и ресурсы из данного правила включаются в глобальные списки заблокированных ресурсов.
- В случае, если опция "Применит правило к ISP из списка" включена, данное правило применяется только к ISP профилям, которые отмечены в данном правиле и ресурсы из данного правила включаются в списки блокировок по этим ISP профилям.

Удаление правила блокировки

Перейдите в раздел «Фильтр WEB и IP» и нажмите на кнопку «Редактировать правило».

Выберите тип ресурса и укажите в этом поле URL, SNI, CN, IP, PORT или CIDR.

Ресурс: Тип: URL

Список ресурсов

ТИП	РЕСУРС	ПРОВЕРЕННЫЙ РЕСУРС	СТАТУС
СН	facebook.com	facebook.com	Правильный ☐
СН	facebook.com	*facebook.com	Правильный ☐
SNI	facebook.com	facebook.com	Правильный ☐
SNI	facebook.com	*facebook.com	Правильный ☐

Правило будет применяться ко всем ISP по умолчанию.

Журнал действий

ДАТА	ПОЛЬЗОВАТЕЛЬ	ДЕЙСТВИЕ	НОВОЕ ЗНАЧЕНИЕ	
11.08.2015 22	anon	Удалить правило		УДАЛИТЬ ПРАВИЛО

1 of 1



Внимание: Перед удалением убедитесь, что данное правило не ссылается на ISP профили.

Проверка домена

Перейдите в раздел "Фильтр WEB и IP" → "Проверить домен".

SPECTREDPI **ФИЛЬТР WEB И IP / ПРОВЕРИТЬ ДОМЕН**

ПРАВИЛА

- ☒ **ФИЛЬТР WEB И IP**
 - Добавить новое правило
 - Проверить домен
 - Поиск по базе
- ☐ ПРИЛОЖЕНИЯ И ПОДКОМПОНЕНТЫ
- ☐ ФИЛЬТР НОМЕРОВ АС
- ☐ ИСКЛЮЧЕНИЯ IP & АС
- ☐ БЕЛЫЙ СПИСОК
- ☐ ПРОФИЛИ ISP И CN
- ☐ ПОИСК ПО БАЗЕ
- ☐ СОСТОЯНИЕ СИСТЕМЫ
- ☐ СПРАВОЧНИК

ПРОВЕРИТЬ ДОМЕН

Введите IP или URL, с префиксом **http://** или **https://**, чтобы проверить, что ресурс создает правильное правило

Проверка ресурса:

Форма проверки домена

В поле ввода "Проверка ресурса" введите URL ресурса, информацию о котором Вы хотите проверить, и нажмите кнопку "Проверить". Под формой выведется информация о введенном Вами ресурсе:

- SSL/TLS, тип блокировки;
- Информация о сертификате;
- Список DNS;
- Рекомендации о значениях, которые нужно использовать для блокировки данного

ресурса.

ПРОВЕРИТЬ ДОМЕН

Введите IP или URL с префиксом **http/https**, чтобы проверить, что ресурс создаст правильное правило

Проверить ресурс

lesta.ru

ПРОВЕРИТЬ

Этот ресурс **SSL/TLS**. Тип блокировки **FULL DOMAIN**

Информация о сертификате

Общая информация по сертификату

Общая информация	*lesta.ru
SAZa	
DNS	*lesta.ru
DNS	lesta.ru
Общее количество SAZa	2
SSL	
Автоматическая подпись	sha256RSA2048signature
Тип ключа	RSA
Размер ключа	2048 bits
Серийный номер	3779084738084788349626457172971484008
На до	00:00:18:18:18:18
На после	12.00:20:12:07
Количество сертификатов	3

Информация о DNS

Тип	НАЗВАНИЕ ДОМЕНА	АДРЕС	TTL
A	lesta.ru	81.18.72.38	336
A	lesta.ru	81.18.72.33	336
A	lesta.ru	81.18.72.17	336
A	lesta.ru	81.18.72.32	336
A	lesta.ru	81.18.72.39	336
A	lesta.ru	81.18.72.56	336
NS	lesta.ru	ns4.cambridge.ru	600
NS	lesta.ru	ns7.cambridge.ru	600
NS	lesta.ru	ns2.cambridge.ru	600
NS	lesta.ru	ns3.cambridge.ru	600
NSD	lesta.ru	lesta.cambridge.ru	3600
NSD	lesta.ru	lesta.cambridge.ru	3600

DNS ресурс: Нет

Информация о результате

1

Чтобы заблокировать этот ресурс с помощью сертификата используйте

CN	lesta.ru
CN	*lesta.ru
SSL	lesta.ru
SSL	*lesta.ru

Скачать файл для загрузки в браузер

Рекомендации для блокировки ресурса

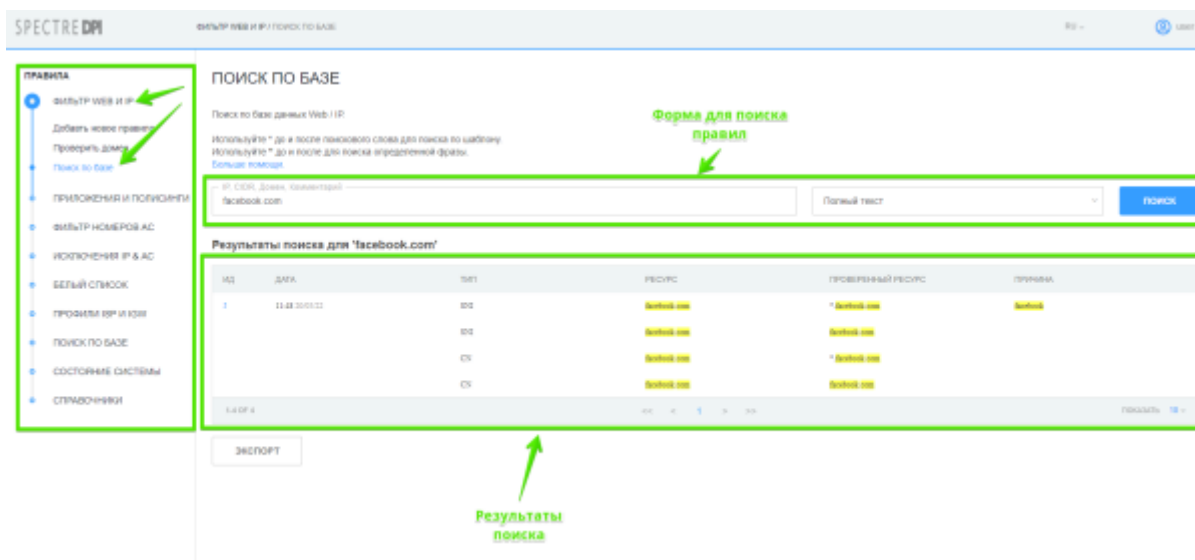
Поиск по базе (среди правил блокировки)

Перейдите в раздел "Фильтр WEB и IP"→"Поиск по базе".

В поле "IP,CIDR,Домен, Комментарий" введите значение в соответствии с подсказками вверху страницы, выберите тип поиска: Полный текст, По ресурсами или По описанию. Нажмите на кнопку "Поиск".

В результате поиска отобразятся все правила блокировок, которые соответствуют выбранным

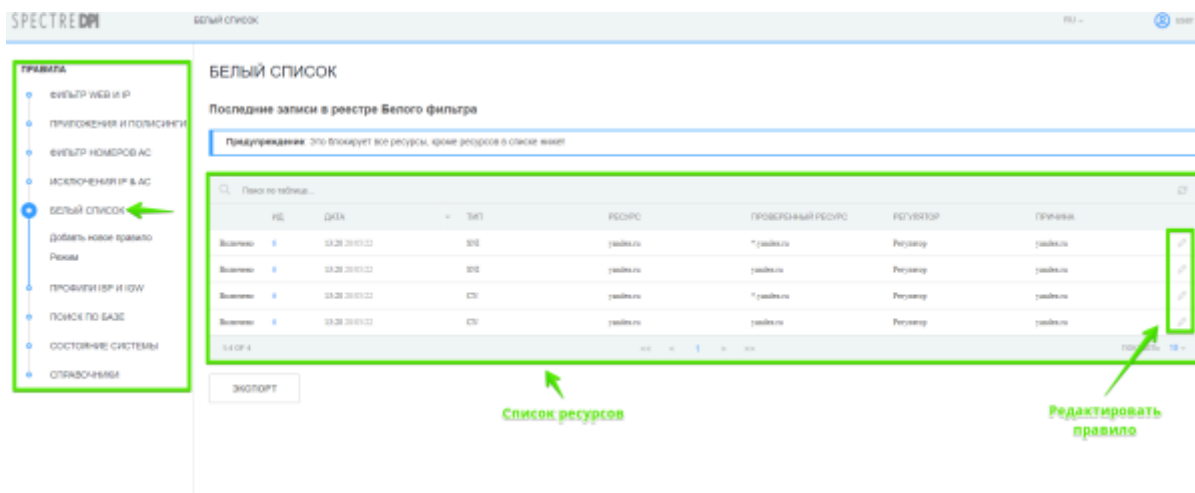
параметрам поиска.



Белый список

Список правил белого списка

Перейдите в раздел "Белый список".



Создание/Редактирование белого списка

- Для создания нового правила белого списка перейдите в раздел "Белый список" → "Добавить новое правило";
- Для внесения изменений в существующее правило перейдите в раздел "Белый список" и нажмите на кнопку "Редактировать правило".

В открывшейся форме:

- Выберите регулятор;
- Выберите категорию;

- Введите публичное описание правила;
- Введите скрытое описание правила;

ДОБАВИТЬ ПРАВИЛО #NEW

Предупреждение: Это блокирует все ресурсы, кроме ресурсов в списке ниже

Ид. правила: 0

Ресурс: Категория:

Публичное описание:

Скрытое описание:

Проверка/валидация ресурса

Ресурс

Выберите тип ресурса и укажите в поле поле URL, DNS, CN, IP, IP: PORT или CIDR.

Ресурс: Тип:

Результат проверки: Это ресурс SSL / TLS. Мы можем заблокировать ДОМЕН ЦЕЛЮЮ! Сторонний DNS и CN будут добавлены в список.

В форме проверки/валидации ресурса введите ресурс и выберите его тип:

- В случае, если нет необходимости в проверке/валидации ресурса нажмите "Добавить в список";
- Нажмите кнопку "Проверить". Будет произведен вывод информации по ресурсу, которую можно будет добавить в список блокировок по этому правилу нажатием кнопки "Добавить в список".

Список ресурсов

ТИП	РЕСУРС	ПРОВЕРЕННЫЙ РЕСУРС	СТАТУС
DNS	yandex.ru	* yandex.ru	Принятый
DNS	yandex.ru	yandex.ru	Принятый
CN	yandex.ru	* yandex.ru	Принятый
CN	yandex.ru	yandex.ru	Принятый

ОЧИСТИТЬ ВСЕ

Применить правило к ISP из списка

Выберите ISP, к которому будет применено правило

☒ isp1

Привязка ISP к правилу

Список добавленных ресурсов

Журнал действий

ДАТА	ПОЛЬЗОВАТЕЛЬ	ДЕЙСТВИЕ	НОВОЕ ЗНАЧЕНИЕ	СТАРОЕ ЗНАЧЕНИЕ
Данные не найдены				

6-8 OF 0

В подразделе привязки правила к профилям ISP:

- В случае, если опция "Применит правило к ISP из списка" отключена, данное правило считается глобальным и ресурсы из данного правила применяются ко всем ISP, у которых

включен белый список.

- В случае, если опция "Применит правило к ISP из списка" включена, данное правило применяется только к ISP профилям, которые отмечены в данном правиле.

Удаление правила белого списка

Перейдите в раздел «Белый список» и нажмите на кнопку «Редактировать правило».

Список ресурсов

ТИП	РЕСУРС	ПРОВЕРЕННЫЙ РЕСУРС	СТАТУС
DN	yandex.ru	yandex.ru	Применен
DN	yandex.ru	*yandex.ru	Применен
URL	yandex.ru	yandex.ru	Применен
URL	yandex.ru	*yandex.ru	Применен

ОЧИСТИТЬ ВСЕ

☒ Применить правило к ISP из списка

Выберите ISP, к которому будет применено правило

☒ isp

ВЫБРАТЬ ВСЕ СНЯТЬ ВСЕ

Журнал действий

ДАТА	ПОЛЬЗОВАТЕЛЬ	ДЕЙСТВИЕ	НОВОЕ ЗНАЧЕНИЕ	СТАРОЕ ЗНАЧЕНИЕ
19.09.2016 12:22	user	The rule created.		Удалить правило

1 of 1

СОХРАНИТЬ ИЗМЕНЕНИЯ СОХРАНИТЬ И ОТКАЗАТЬСЯ ЭКСПОРТИРОВАТЬ ПРАВИЛО

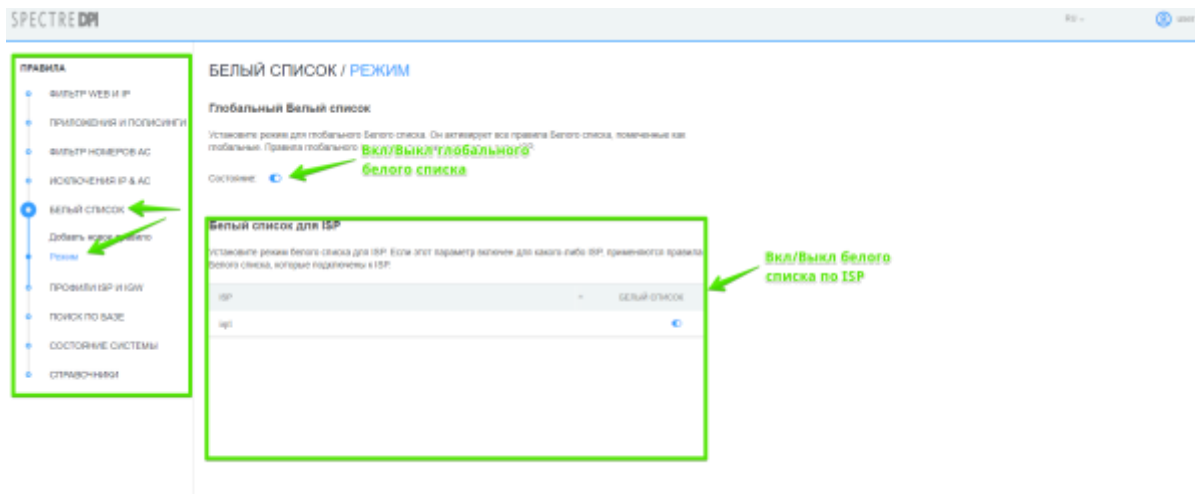
УДАЛИТЬ ПРАВИЛО



Внимание: Перед удалением убедитесь, что данное правило не ссылается на ISP профили.

Управление режимом работы белого списка

Перейдите в раздел "Белый список"→"Режим".



- При включенном глобальном режиме белого списка услуга белого списка применяется на все ISP профили и списки ресурсов формируются только из глобальных правил белого списка;
- При включенном режиме белого списка по отдельному профилю ISP услуга белого списка применяется только к ISP, у которого она включена и списки ресурсов формируются только из правил белого списка, в которых отмечен этот ISP профиль;
- В случае комбинации включенных режимов глобального белого списка и белого списка по отдельному профилю ISP происходит конкатенация списков ресурсов для глобальных правил и правил, в которых отмечен ISP профиль. Для остальных ISP применяется услуга белого списка с использованием только глобальных правил белого списка.

Поиск по базе (глобальный)

Перейдите в раздел "Поиск по базе".

В поле "IP,CIDR,Домен, Комментарий" введите значение в соответствии с подсказками вверху страницы, выберите тип поиска: Полный текст, По ресурсами или По описанию. Нажмите на кнопку "Поиск".

В результате поиска отобразятся все правила (с указанием типа правила), которые соответствуют выбранным параметрам поиска.

ПРЕЖДЕ

- ФИЛЬТР WEB И IP
- ПРИЛОЖЕНИЯ И ПОДКАСЫ
- ФИЛЬТР НОМЕРОВ АС
- ИСКЛЮЧЕНИЯ IP & АС
- БЕЛЫЙ СПИСОК
- ПРОВЕРКА ISP И IDN
- ПОИСК ПО БАЗЕ**
- СОСТОЯНИЕ СИСТЕМЫ
- ОПРАВЧЕНАЯ

ПОИСК ПО БАЗЕ

Поиск по всем правилам базы данных.
Используйте "*" до и после ключевого слова для поиска по шаблону.
Используйте "+" до и после для поиска определенной фразы.
[Справка по поиску](#)

IP: 192.168.1.1, domain: facebook.com
facebook.com

Полный текст

Параметры поиска

Результаты поиска для 'facebook.com'

ID	Дата	Тип	Ресурс	Проверенный ресурс	Тип правила	Норматив	Описание
3	10.08.2015	SPK	facebook.com	* facebook.com	Фильтр Web и IP	Принят	Описание: Принят
4	10.08.2015	SPK	facebook.com	* facebook.com	Фильтр Web и IP	Принят	Описание: Принят
5	10.08.2015	SPK	facebook.com	* facebook.com	Фильтр Web и IP	Принят	Описание: Принят
6	10.08.2015	SPK	facebook.com	* facebook.com	Фильтр Web и IP	Принят	Описание: Принят

1-4 OF 6

Экспорт

Результаты поиска для '192.168.1.1'

ID	Дата	Тип	Ресурс	Проверенный ресурс	Тип правила	Норматив	Описание
3	10.08.2015	IPSP	192.168.1.1	192.168.1.1	Исключение IP	Принят	Описание: Принят

1-1 OF 1

Экспорт

Результаты поиска

Мониторинг задач

Перейдите в раздел "Состояние системы".

СРЕДНЕ

- ФИЛЬТР WEB И IP
- ПРИЛОЖЕНИЯ И ПОДКАСЫ
- ФИЛЬТР НОМЕРОВ АС
- ИСКЛЮЧЕНИЯ IP & АС
- БЕЛЫЙ СПИСОК
- ПРОВЕРКА ISP И IDN
- ПОИСК ПО БАЗЕ
- СОСТОЯНИЕ СИСТЕМЫ**
- ОПРАВЧЕНАЯ

СОСТОЯНИЕ СИСТЕМЫ

Список задач экспорта

Поиск по задачам...

ID	Тип	Действие	Статус	Описание статуса	Дата	Детали задачи
1	TaskType	LoadInitialTaskList	error	Task not completed	14.03.2015.20	Детали задачи
11	Ip	InitialTaskList	error	Task not completed	14.03.2015.20	Детали задачи
22	Ip	LoadInitialTaskList	error	Task not completed	12.08.2015.20	Детали задачи
21	Ip	LoadInitialTaskList	error	Task not completed	12.08.2015.20	Детали задачи
30	Ip	LoadInitialTaskList	error	Task not completed	12.07.2015.20	Детали задачи
19	Ip	UpdateTaskList	error	Task not completed	12.07.2015.20	Детали задачи
18	Ip	UpdateTaskList	error	Task not completed	12.07.2015.20	Детали задачи
17	Ip	UpdateTaskList	error	Task not completed	12.07.2015.20	Детали задачи
16	Ip	UpdateTaskList	error	Task not completed	12.07.2015.20	Детали задачи
15	Ip	UpdateTaskList	error	Task not completed	12.07.2015.20	Детали задачи

1-18 OF 20

Экспорт

В данном разделе отображается очередь выполнения задач, статус и время. Для того, чтобы увидеть детали выполнения задачи нажмите на "Детали задачи".

Логи

Логи по данному разделу хранятся в файлах:

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



Уровень детализации логов задается опцией `ULR_LOAD_LOG_LEVEL` в `.env` файле



конфигурации.