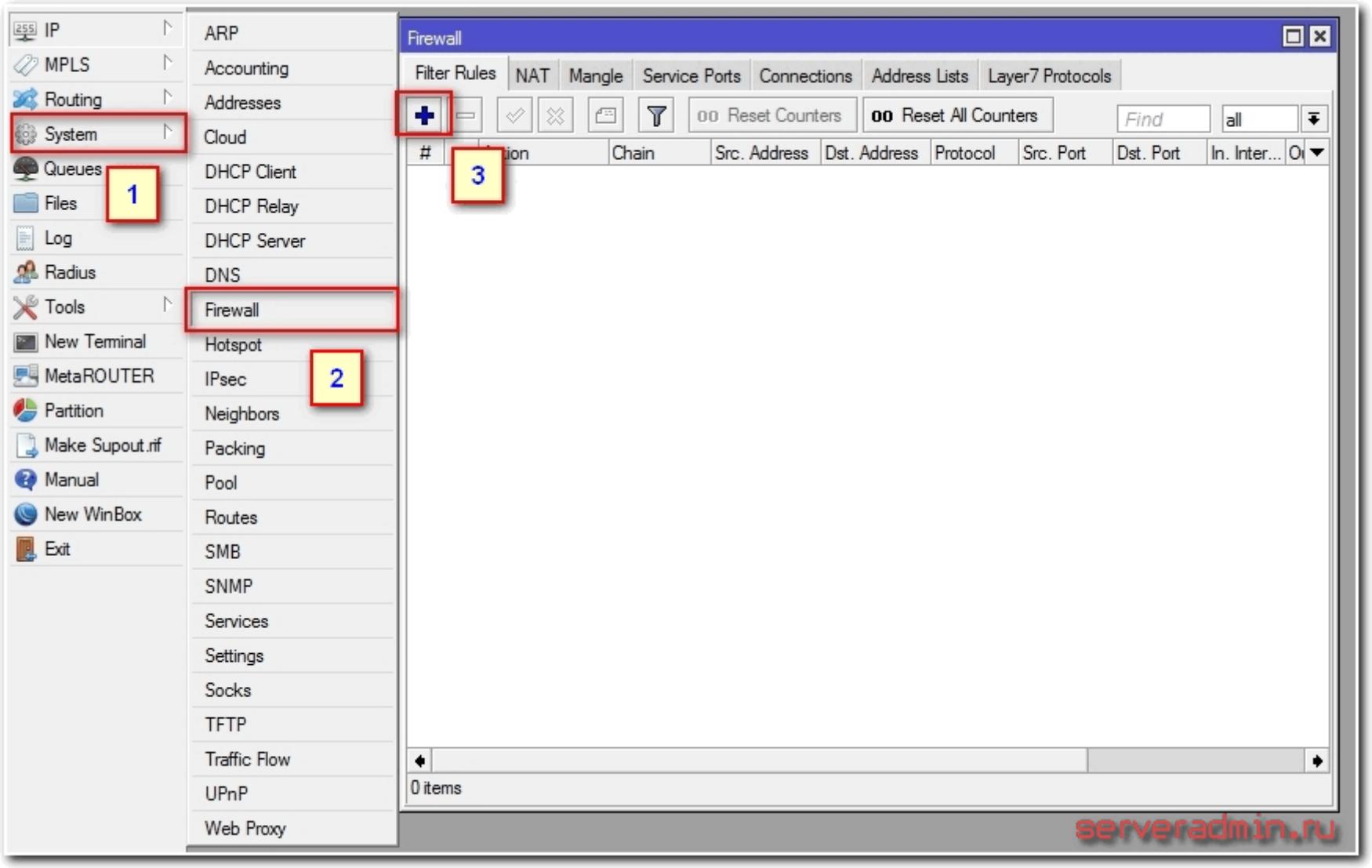
Популярная серия бюджетных маршрутизаторов из Латвии на базе RouterOS предоставляет пользователям широкие возможности по настройке. Сегодня я подробно рассмотрю возможности mikrotik по блокировке сайтов, рекламы, социальных сетей, по созданию списка запретов на доступ. Все эти средства присутствуют в роутерах из коробки и не требуют специальных знаний для настройки, кроме стандартных средств управления.

> Если у вас есть желание научиться работать с роутерами микротик и стать специалистом в этой области, рекомендую пройти курсы по программе, основанной на информации из официального курса MikroTik Certified Network Associate. Все подробности читайте ниже.

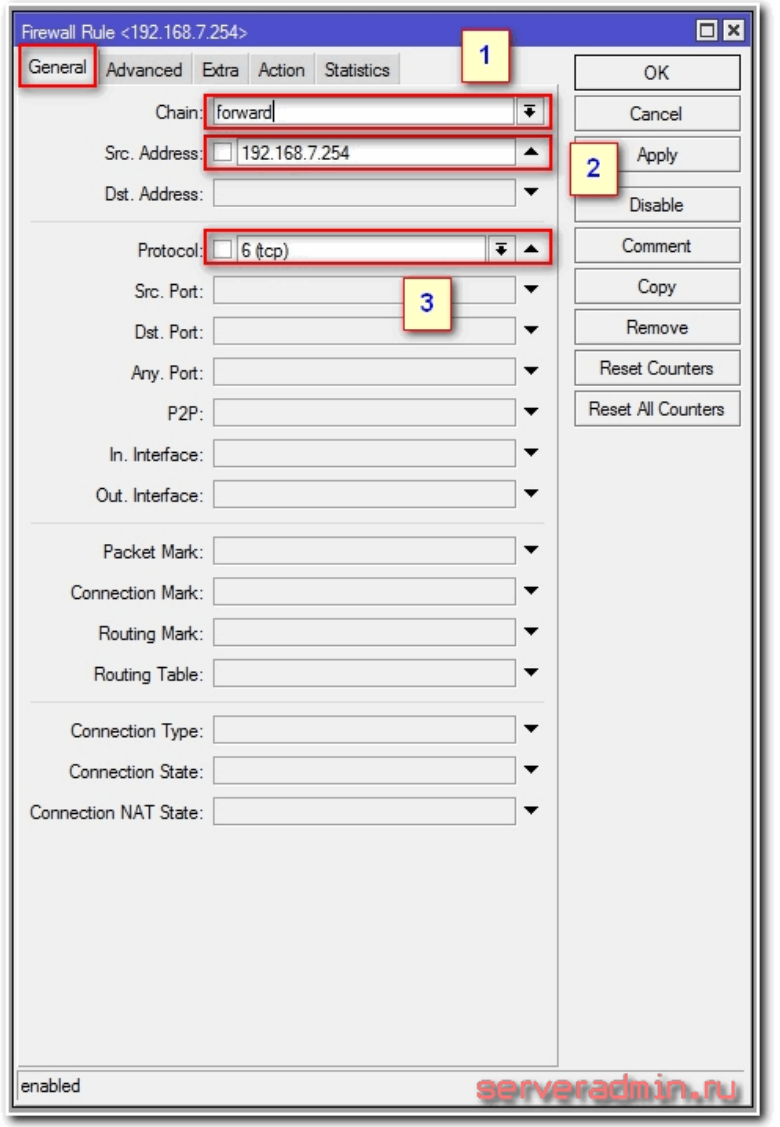
Содержание:

Как быстро закрыть доступ к сайту

Начнем с самого простого. У нас есть роутер Mikrotik, утилита winbox и желание конкретному пользователю установить запрет на посещение определенного сайта. Подключаемся к роутеру и идем в раздел IP -> Firewall, открываем закладку Filter Rules:


IP
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
MetaROUTER
Partition
Make Supout.rif
Manual
New WinBox
Exit
1
ARP
Accounting
Addresses
Cloud
DHCP Client
DHCP Relay
DHCP Server
DNS
Firewall
Hotspot
IPsec
Neighbors
Packing
Pool
Routes
SMB
SNMP
Services
Settings
Socks
TFTP
Traffic Flow
UPnP
Web Proxy
2
Firewall
Filter Rules
NAT
Mangle
Service Ports
Connections
Address Lists
Layer7 Protocols
Reset Counters
Reset All Counters
Find
all
3
#
Chain
Src. Address
Dst. Address
Protocol
Src. Port
Dst. Port
In. Inter...
0 items
serveradmin.ru

Нажимаем на + и добавляем новое правило блокировки сайта:

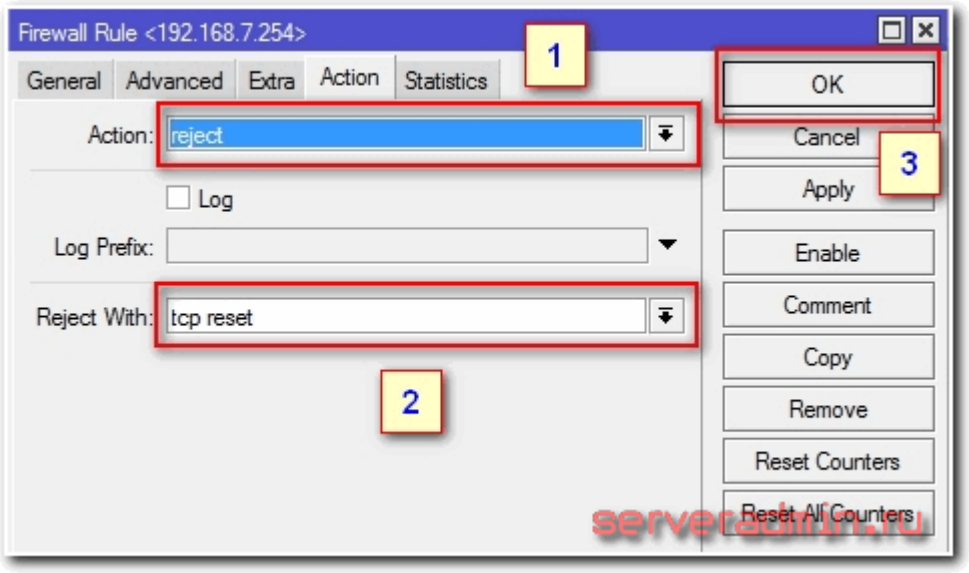

Firewall Rule <192.168.7.254>
General
Advanced
Extra
Action
Statistics
1
2
3
Chain: forward
Src. Address: 192.168.7.254
Dst. Address:
Protocol: 6 (tcp)
Src. Port:
Dst. Port:
Any. Port:
P2P:
In. Interface:
Out. Interface:
Packet Mark:
Connection Mark:
Routing Mark:
Routing Table:
Connection Type:
Connection State:
Connection NAT State:
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters
enabled
serveradmin.ru

На первой вкладке General заполняем:

1. Указываем цепочку Forward.
2. Указываем адрес пользователя, которому будет закрыт доступ к сайту.
3. Выбираем протокол TCP.

Дальше переходим на вкладку Advanced:

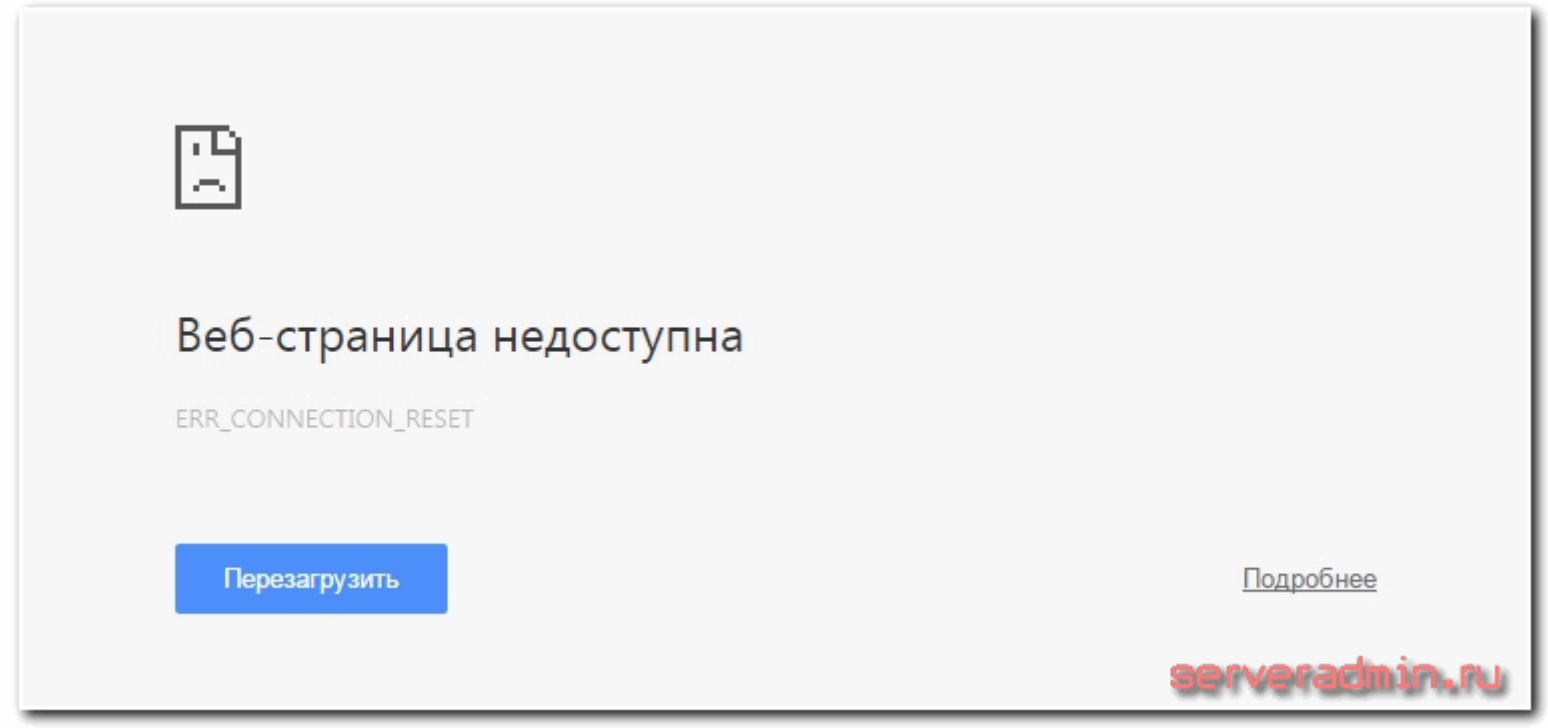
В поле **Content** указываем адрес сайта, который нужно заблокировать, например vk.com. Переходим на вкладку Action:



Здесь выполняем следующие действия:

1. В поле Action выбираем reject.
2. В пункте Reject With указываем tcp reset.
3. Нажимаем OK.

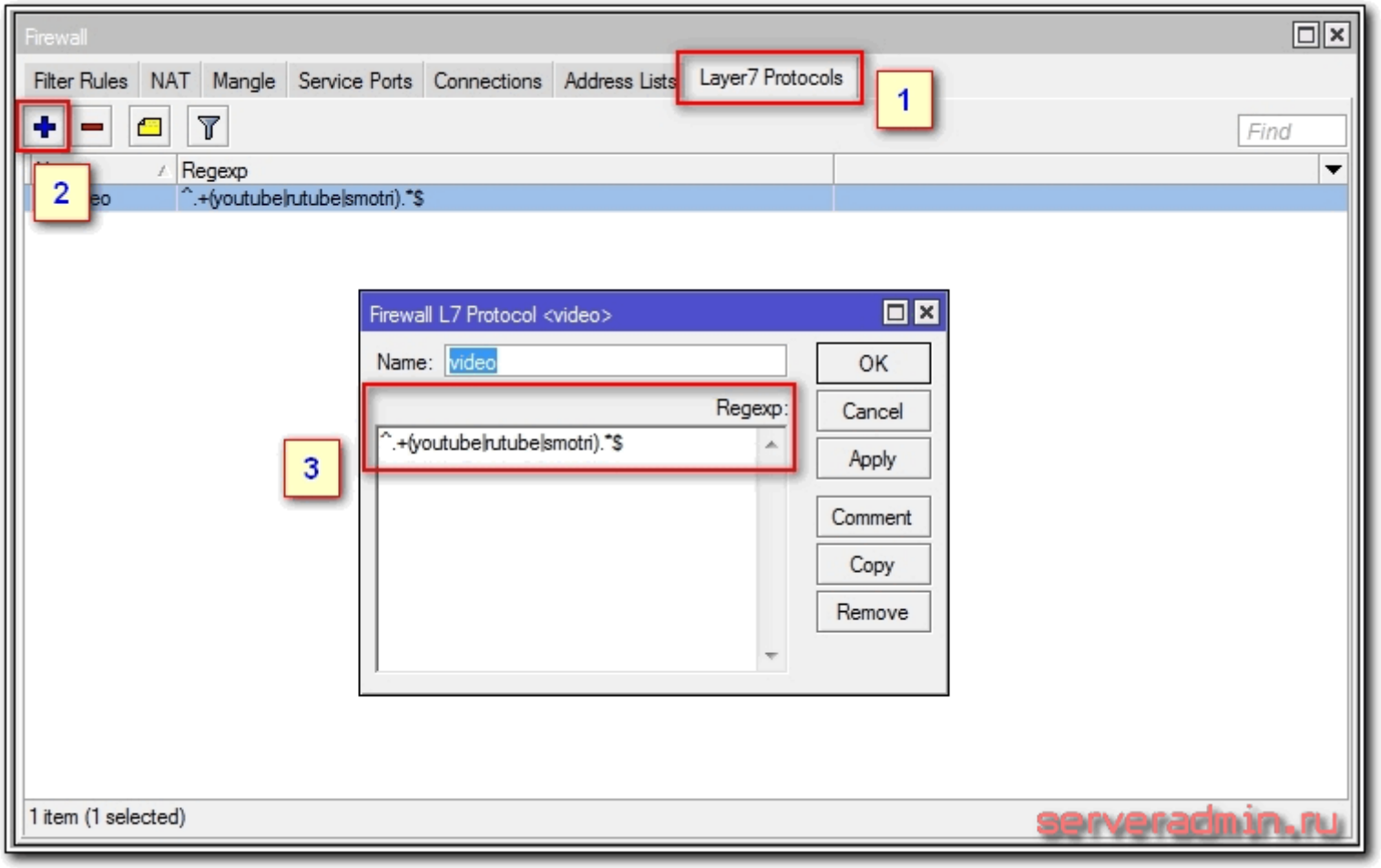
На этом основная настройка закончена. В данный момент правило по фильтрации сайта уже работает. Мы с помощью стандартных средств mikrotik смогли заблокировать vk.com. Это нетрудно проверить на клиенте. При попытке открыть адрес сайта популярной соц. сети он получит следующее сообщение в браузере chrome:



В данном случае мы в ручном режиме сделали блокировку сайта конкретному пользователю. Если у вас таких сайтов и пользователей много, процесс надо по-возможности автоматизировать.

Черный список сайтов для фильтрации

Давайте создадим отдельно список сайтов и укажем его в правиле, чтобы не создавать запрет для каждого имени отдельно. Сделать это не сложно. Для этого опять идем в раздел IP -> Firewall, открываем вкладку Layer7 Protocols и нажимаем «+» для добавления списка:

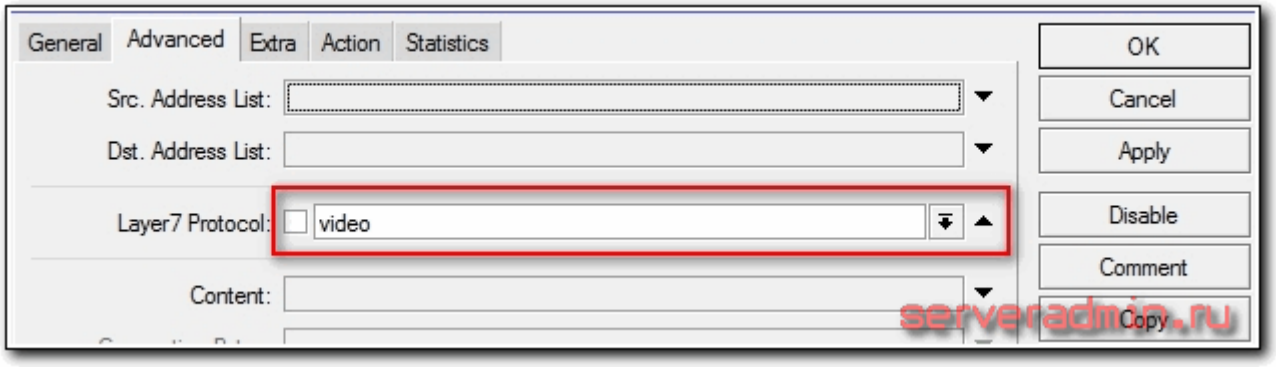


В поле **regexp** необходимо ввести регулярное выражение для организации списка сайтов. Я сам лично не умею составлять правильно регулярные выражения, поэтому приходится их искать в интернете. Подавляющее большинство регулярок, которые я нашел, у меня не заработали. Привожу вам список видеохостинга для блокировки в виде регулярного выражения, которое заработало лично у меня:

```
^.+(youtube|rutube|smotri).*$
```

Список можно расширить, добавляя значения в скобках через знак вертикальной палки, что означает логическое «или».

После составления списка, включаем его в правило. Как создать правило я уже рассказал в первой части статьи. В данном случае отличие будет только в одном пункте:



Вместо поля **Content** выбираем название нашего списка для блокировки *video* в поле **Layer7 Protocol**.

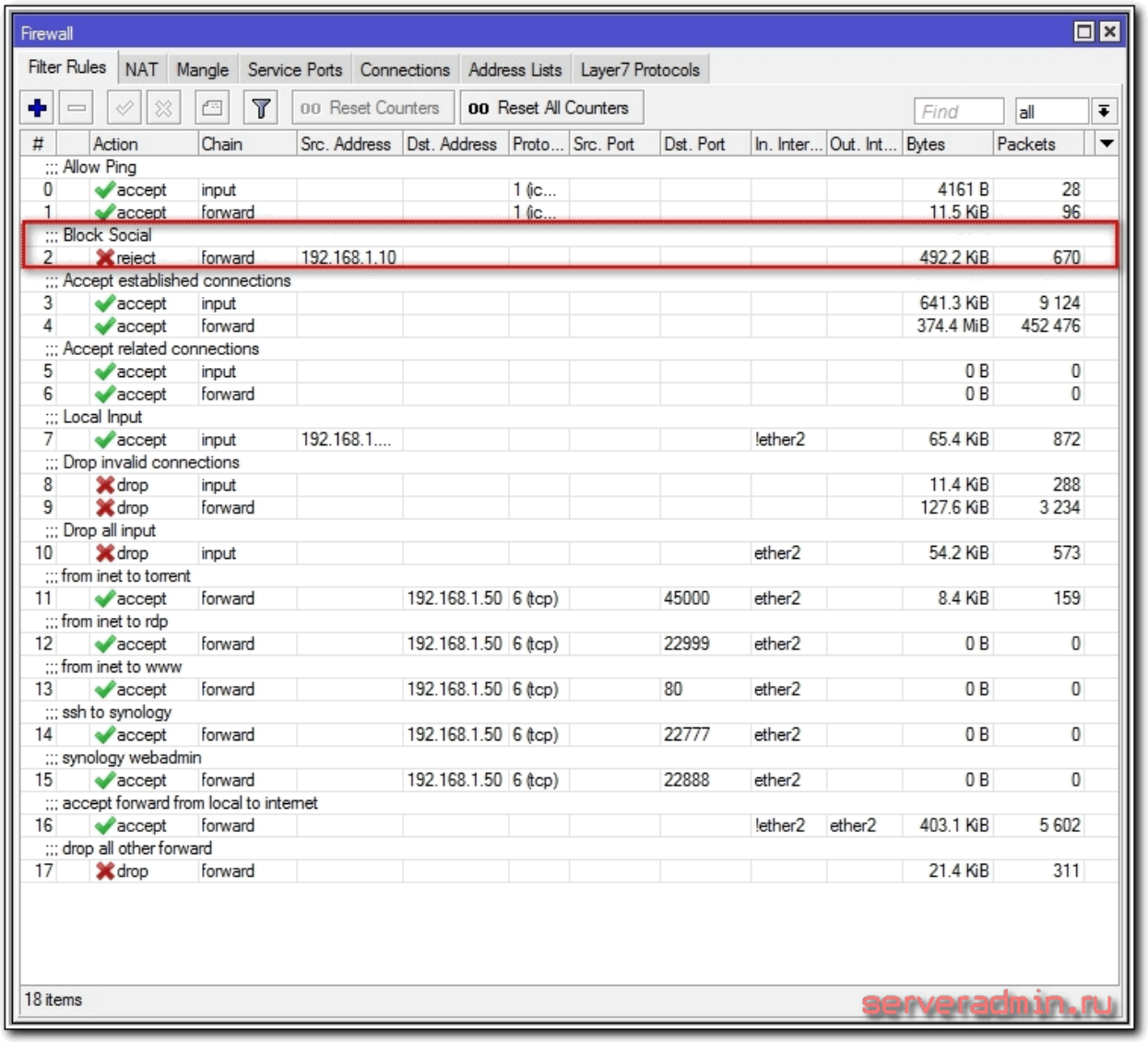
Если у вас настроен firewall на микротике и в нем присутствуют какие-то правила, то текущее правило блокировки нужно правильно разместить в списке, чтобы оно работало. Например, у меня есть материал на тему настройки firewall. Там есть правила:

```
Разрешаем установленные подключения
add chain=input action=accept connection-state=established
add chain=forward action=accept connection-state=established
```

Текущее правило блокировки списка сайта на основе Layer7 Protocol должно стоять выше этого правила, иначе оно не будет работать. Я не до конца понял, почему, но я провел достаточно много тестов, чтобы убедиться, что его реально надо ставить выше. Ну и, разумеется, оно должно стоять выше правила, разрешающего соединения forward из локальной сети.

В этом правиле блокировки в поле **Src.Address** вы можете указать конкретный ip пользователя, можете указать всю подсеть, либо вообще оставить поле пустым для запрета выхода на закрытые сайты всему транзитному трафику маршрутизатора, в независимости от его источника.

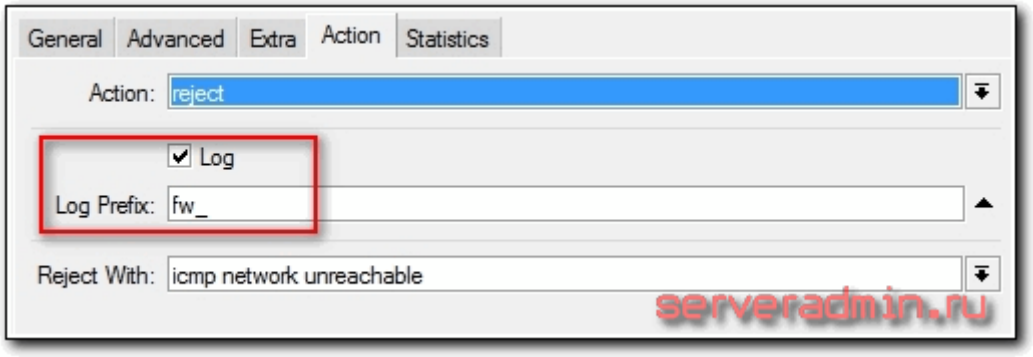
Вот как у меня выглядит список моих правил на фаерволе с учетом добавленного правила блокировки:



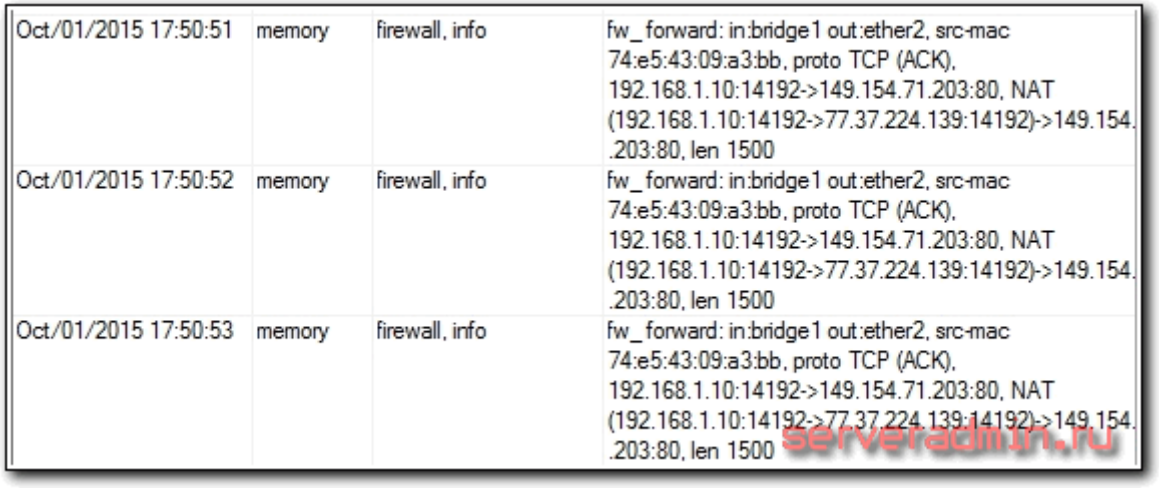
#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
;;; Allow Ping											
0	accept	input			1 (ic...					4161 B	28
1	accept	forward			1 (ic...					11.5 KiB	96
;;; Block Social											
2	reject	forward	192.168.1.10							492.2 KiB	670
;;; Accept established connections											
3	accept	input								641.3 KiB	9 124
4	accept	forward								374.4 MiB	452 476
;;; Accept related connections											
5	accept	input								0 B	0
6	accept	forward								0 B	0
;;; Local Input											
7	accept	input	192.168.1....					!ether2		65.4 KiB	872
;;; Drop invalid connections											
8	drop	input								11.4 KiB	288
9	drop	forward								127.6 KiB	3 234
;;; Drop all input											
10	drop	input						ether2		54.2 KiB	573
;;; from inet to torrent											
11	accept	forward		192.168.1.50	6 (tcp)		45000	ether2		8.4 KiB	159
;;; from inet to rdp											
12	accept	forward		192.168.1.50	6 (tcp)		22999	ether2		0 B	0
;;; from inet to www											
13	accept	forward		192.168.1.50	6 (tcp)		80	ether2		0 B	0
;;; ssh to synology											
14	accept	forward		192.168.1.50	6 (tcp)		22777	ether2		0 B	0
;;; synology webadmin											
15	accept	forward		192.168.1.50	6 (tcp)		22888	ether2		0 B	0
;;; accept forward from local to internet											
16	accept	forward						!ether2	ether2	403.1 KiB	5 602
;;; drop all other forward											
17	drop	forward								21.4 KiB	311

Тут я блокирую доступ с тестового ip адреса. Все остальные правила похожи на те, что я описывал в своей статье по настройке простого фаервола на микротике, ссылку на которую я приводил выше.

Вы можете включить логирование заблокированных соединений с сайтами из списка на вкладке **Action** самого правила:



Mikrotik будет генерировать подобные логи:

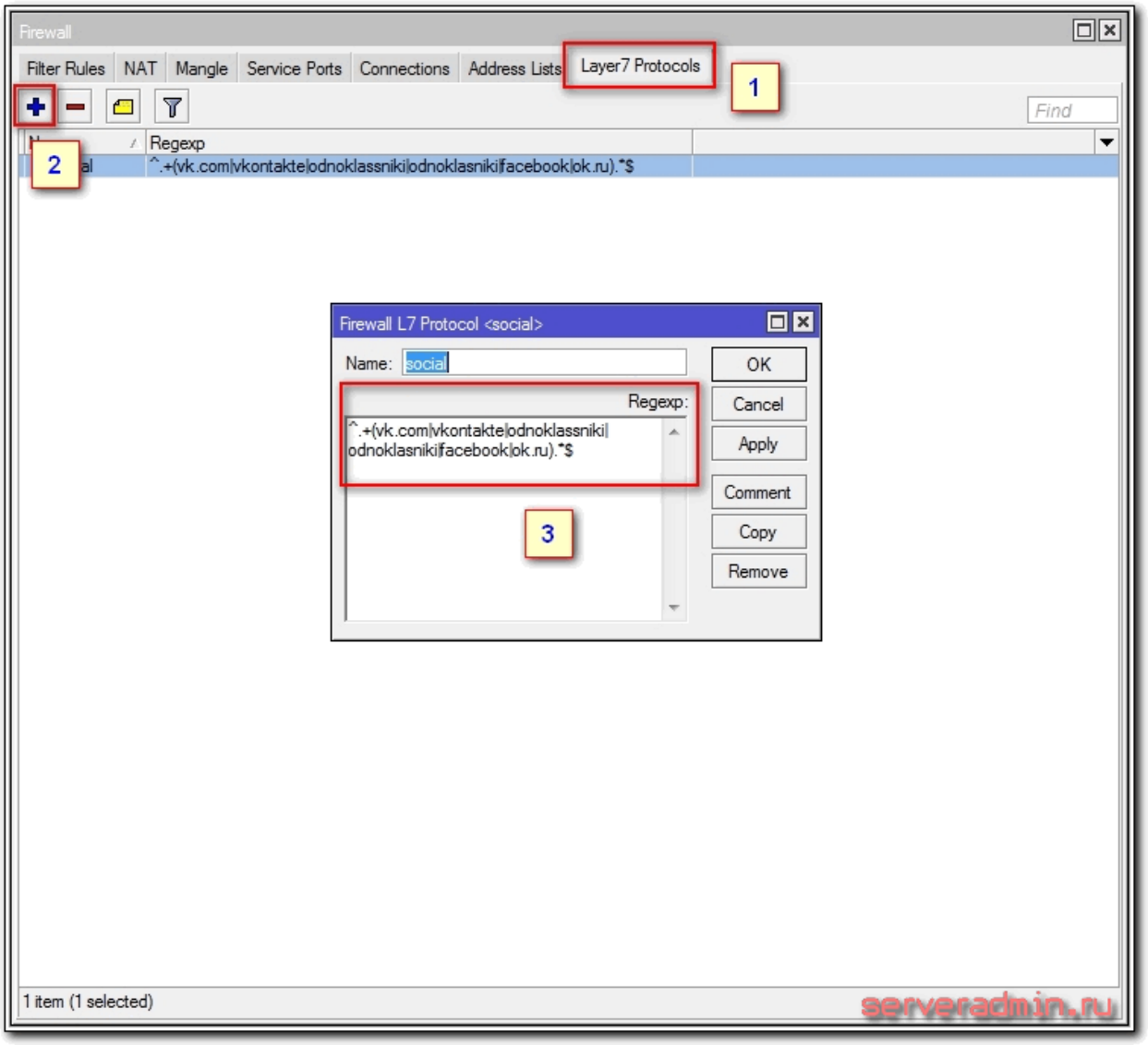


Oct/01/2015 17:50:51	memory	firewall, info	fw_forward: in:bridge1 out:ether2, src-mac 74:e5:43:09:a3:bb, proto TCP (ACK), 192.168.1.10:14192->149.154.71.203:80, NAT (192.168.1.10:14192->77.37.224.139:14192)->149.154. .203:80, len 1500
Oct/01/2015 17:50:52	memory	firewall, info	fw_forward: in:bridge1 out:ether2, src-mac 74:e5:43:09:a3:bb, proto TCP (ACK), 192.168.1.10:14192->149.154.71.203:80, NAT (192.168.1.10:14192->77.37.224.139:14192)->149.154. .203:80, len 1500
Oct/01/2015 17:50:53	memory	firewall, info	fw_forward: in:bridge1 out:ether2, src-mac 74:e5:43:09:a3:bb, proto TCP (ACK), 192.168.1.10:14192->149.154.71.203:80, NAT (192.168.1.10:14192->77.37.224.139:14192)->149.154. .203:80, len 1500

Эти записи вы можете перенаправить на удаленный сервер для логов, чтобы потом анализировать статистику срабатывания правила. Для удобства, эти правила можно разделить по сайтам, по пользователям и т.д. В общем, поле для контроля работы правила обширное.

Запретить социальные сети в mikrotik

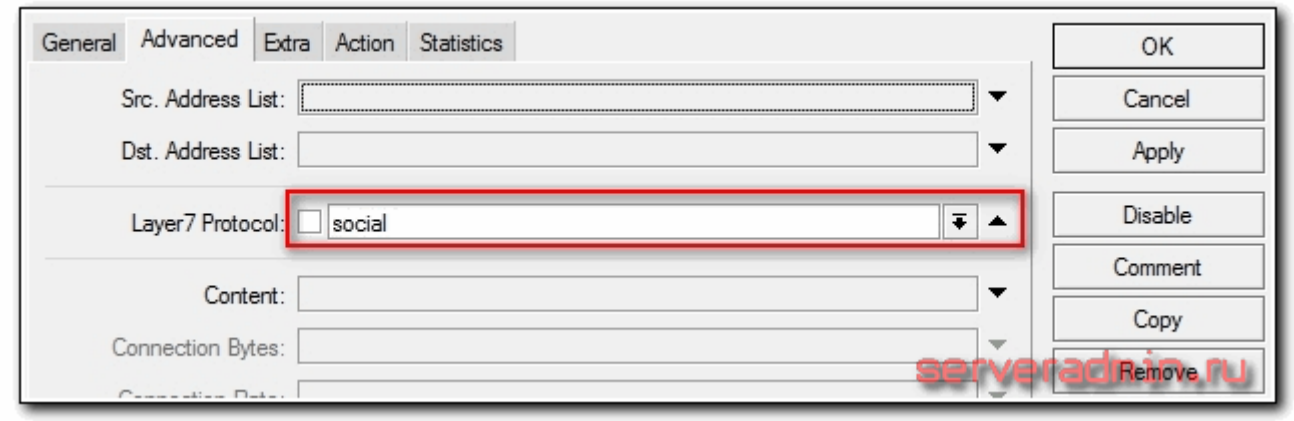
Так как мы научились составлять списки для блокировки сайтов, на основе этой информации легко закрыть доступ в социальные сети одним правилом. Для этого как и ранее добавляем регулярное выражение со списком соц сетей:


Firewall
Filter Rules
NAT
Mangle
Service Ports
Connections
Address Lists
Layer7 Protocols
1
Find
Regexp
2
^.+(vk.com|vkontakte|odnoklassniki|odnoklasniki|facebook|ok.ru).*$
Firewall L7 Protocol <social>
Name:
social
OK
Cancel
Apply
Comment
Copy
Remove
Regexp:
^.+(vk.com|vkontakte|odnoklassniki|
odnoklasniki|facebook|ok.ru).*$
3
1 item (1 selected)
serveradmin.ru

Текст регулярки:

```
^.+(vk.com|vkontakte|odnoklassniki|odnoklasniki|facebook|ok.ru).*$
```

Дальше создаем правило, как мы это делали выше и выбираем список, который только что добавили:



Выбираем как и ранее адреса источников для блокировки и добавляем правило. Все, этого достаточно для того, чтобы заблокировать социальные сети у пользователей. А включив логи, сможете еще и следить за тем, кто время от времени пытается в них зайти.

Блокировка рекламы средствами mikrotik

С помощью изученного средства по ограничению доступа к сайтам достаточно просто блокировать рекламу. Для примера рассмотрим вариант по блокировке рекламы в Skype. Так как я знаю адреса серверов, куда скайп лезет за рекламой, я могу его заблокировать в mikrotik. У меня есть список:

```
rad.msn.com
apps.skype.com
vortex-win.data.microsoft.com
settings-win.data.microsoft.com
```

Это адреса, откуда загружается реклама. Списки эти могут меняться время от времени, нужно периодически проверять и обновлять. Самому подготовить список рекламных адресов для конкретного сервиса можно, к примеру, с помощью настройки собственного dns сервера и включения логирования запросов.

Дальше как обычно создаем regexp выражение для списка адресов:

```
^.+(rad.msn.com|apps.skype.com|vortex-win.data.microsoft.com|settings-win.data.microsoft.com).*$
```

Добавляем новое правило, подключаем к нему список, созданный ранее и наслаждаемся работой скайпа без рекламы.

Заключение

Материала в интернете по Микротику много. Я сам пока разбирался в данном вопросе перечитал кучу статей. И все они какие-то недоделанные. Либо вопрос слабо раскрыт, либо что-то вообще не работает. Не знаю, в чем причина такой ситуации. Возможно что-то меняется в настройках и информация становится неактуальной. Сходу у меня не заработала фильтрация на основе Layer7 Protocols, пришлось повозиться, покопаться в regexp, в правилах, в их расположениях. Надеюсь мой материал немного исправит данную ситуацию.

Буду рад любым замечаниям к статье, так как сам учусь в процессе написания. В своей работе лично я не использую какие либо ограничения доступа к сайтам, так как считаю это бесполезным занятием. Но многие пользуются, поэтому разбираться в этом вопросе считаю полезным делом.

Онлайн курсы по Mikrotik

Если у вас есть желание научиться работать с роутерами микротик и стать специалистом в этой области, рекомендую пройти курсы по программе, основанной на информации из официального курса MikroTik Certified Network Associate. Помимо официальной программы, в курсах будут лабораторные работы, в которых вы на практике сможете проверить и закрепить полученные знания. Все подробности на сайте Курсы по ИТ. Стоимость обучения весьма демократична, хорошая возможность получить новые знания в актуальной на сегодняшний день предметной области.

Рекомендую полезные материалы по схожей тематике:

- Базовая настройка роутера mikrotik на примере RB951G-2HnD.
- Настройка Capsman в Mikrotik для организации бесшовного Wifi.
- Организация резервирования канала в интернет на базе роутера Микротик.
- Быстрая и простая настройка firewall на микротике.