

Настраиваем родительский контроль на роутерах Mikrotik

 interface31.ru/tech_it/2020/04/nastraivaem-roditelskiy-kontrol-na-routerah-mikrotik.html

Сегодня интернет плотно проник во все сферы нашей жизни и превратился в столь же привычный и необходимый предмет, как электричество или водоснабжение. И это не преувеличение: работа, обучение, онлайн-сервисы - все это требует доступа в сеть, что не только открывает новые возможности, но порождает новые проблемы. Одна из них - защита детей от неподходящей для их возраста информации, а также контроль времени, проводимого ими в сети. При том, что решать данную задачу следует гибко, с учетом возраста и реальных потребностей детей, не ограничивая при этом возможности родителей.



Онлайн-курс по MikroTik

Научиться настраивать MikroTik с нуля или систематизировать уже имеющиеся знания можно на [углубленном курсе по администрированию MikroTik](#). Автор курса, сертифицированный тренер MikroTik Дмитрий Скоромнов, лично проверяет лабораторные работы и контролирует прогресс каждого своего студента. В три раза больше информации, чем в вендорской программе MTCNA, более 20 часов практики и доступ навсегда.

Большинство статей в сети интернет рассматривают отдельные инструменты или методики родительского контроля, в то время как это сложный и многогранный вопрос, особенно если есть несколько детей разного возраста. Действительно, ограничения для ученика начальной школы и подростка могут и должны быть разными. Мы не сторонники жесткого закручивания гаек, стремление оградить ребенка от всего чего только возможно также плохо, как и бесконтрольный его доступ ко всем ресурсам сети. Во всем нужен разумный баланс.

Также не будем забывать об устройствах общего доступа. Это может быть семейный компьютер, доступ к которому имеют все члены семьи, при этом часть времени он остается бесконтрольным, когда родители еще на работе, а дети уже пришли со школы. В эту категорию также можно добавить умные телевизоры, игровые и телевизионные приставки и т.д. и т.п. Для этой категории устройств доступ должен быть выборочным, применяя ограничительные меры на те периоды времени, когда родителей нет дома.

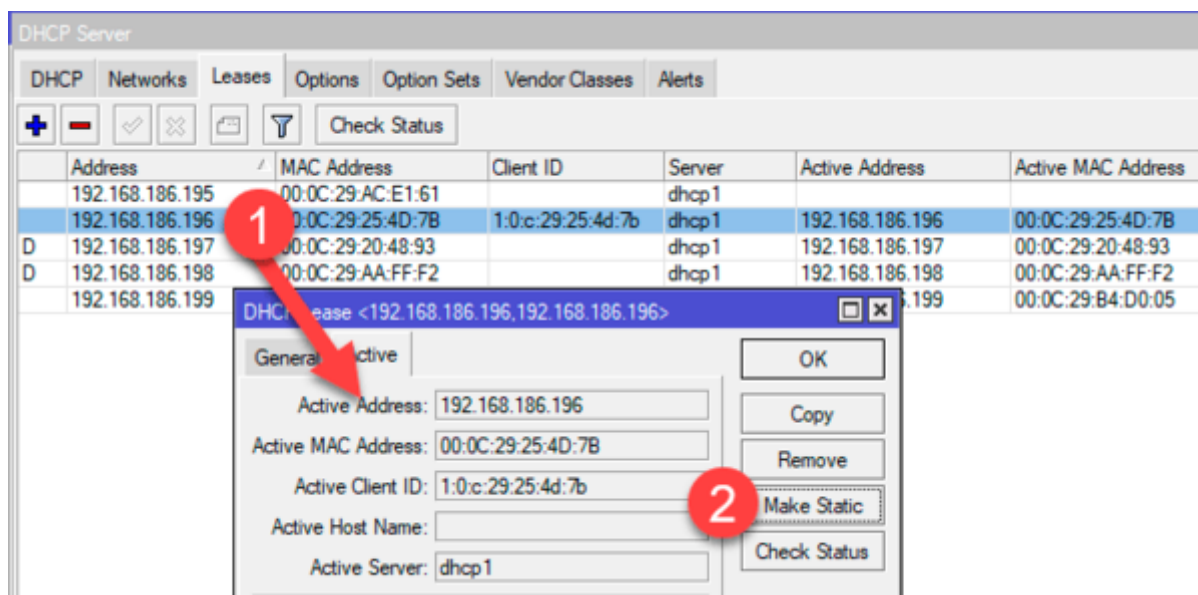
В данной статье мы рассмотрим комплекс мер, который основан на собственном опыте и отражает наше видение политики гибкого родительского контроля, который будет реализован на базе RouterOS.

Распределение устройств по группам

В основе любых ограничительных мер лежат списки объектов, к которым данные меры применяются. И чем более гибкие политики мы хотим создать, тем более точным должно быть разделение на группы. Да, можно создать единственную группу - **Дети**, но вряд ли вы сумеете настроить ограничения таким образом, чтобы они подходили и ребенку 7-8 лет и 14-15 летнему подростку. Поэтому далее будем предполагать, что у нас есть условный младшеклассник Иван, подросток Маша и некоторое количество устройств общего пользования, такие как умный телевизор или компьютер в зале.

Каждый из детей имеет собственные устройства и все эти устройства нам нужно учесть и распределить по группам, здесь нам поможет резервирование DHCP.

Перейдем в раздел **DHCP Server - Leases** и зарезервируем за каждым устройством сетевые настройки. Для этого выбираем нужное устройство в списке, открываем его свойства и нажимаем **Make Static**.



После чего на закладке **General** станут доступны дополнительные настройки, нам нужно указать для каждого устройства свой список адресов. В нашем случае мы создадим свой список для каждого ребенка и еще один для устройств общего пользования. Внизу закладки найдите поле **Address List** и выберите нужный список, если он отсутствует, то просто укажите его название, он будет создан автоматически.

DHCP Lease <192.168.186.196, 192.168.186.196>

General Active

Address: 192.168.186.196

MAC Address: 00:0C:29:25:4D:7B

☐ Use Src. MAC Address

Client ID: 1:0:c:29:25:4d:7b

Server: dhcp1

Lease Time:

☐ Block Access

☒ Allow Dual Stack Queue

☐ Always Broadcast

DHCP Options:

DHCP Option Set:

Rate Limit:

Insert Queue Before: first

Address List: COMMON

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Check Status

В итоге у вас должен получиться набор динамических списков, каждый из которых содержит адреса нужной группы устройств:

DHCP Server							
DHCP		Networks	Leases	Options	Option Sets	Vendor Classes	Alerts
<div><div><div><div>+</div><div>-</div><div>✓</div><div>✗</div><div>📄</div><div>🔍</div></div><div>Check Status</div></div></div>							
	Address	MAC Address	Client ID	Server	Active Address	Active MAC Address	
...	COMMON						
	192.168.186.196	00:0C:29:25:4D:7B	1:0:c:29:25:4d:7b	dhcp1	192.168.186.196	00:0C:29:25:4D:7B	
...	IVAN						
	192.168.186.197	00:0C:29:20:48:93		dhcp1	192.168.186.197	00:0C:29:20:48:93	
...	MASHA						
	192.168.186.198	00:0C:29:AA:FF:F2		dhcp1	192.168.186.198	00:0C:29:AA:FF:F2	
D	192.168.186.199	00:0C:29:B4:D0:05	1:0:c:29:b4:d0:5	dhcp1	192.168.186.199	00:0C:29:B4:D0:05	

Firewall								
Filter Rules		NAT	Mangle	Raw	Service Ports	Connections	Address Lists	Layer7 Protocols
<div><div><div><div>+</div><div>-</div><div>✓</div><div>✗</div><div>📄</div><div>🔍</div></div></div></div>								
	Name	Address	Timeout	Creation Time				
D	COMMON	192.168.186.196		Apr/18/2020 03:28:57				
D	IVAN	192.168.186.197		Apr/18/2020 03:29:17				
D	MASHA	192.168.186.198		Apr/18/2020 03:29:34				
D	US_only	2p.ru		Nov/04/2019 17:03:53				

Не забывайте снабжать комментариями объекты, добавляемые в списки, это поможет сохранять удобочитаемость настроек и облегчит дальнейшее сопровождение.

Блокировка нежелательных ресурсов

Один из самых сложных и ответственных вопросов. Мы уже обсуждали вопрос блокировки на основе списков в наших статьях, но в данном случае это поможет мало. Одно дело - заблокировать наиболее популярные ресурсы-пожиратели

времени в офисе и совсем иное - оградить детей от всего возможного объема нежелательной информации. Здесь нам на помощь придут специализированные DNS.

Первое, что приходит на ум, это **Яндекс.DNS Семейный** и аналогичные сервисы других DNS-провайдеров. Но, на наш взгляд, для детей младшего возраста такой фильтрации недостаточно, так как Яндекс Семейный фильтрует только явные материалы 18+, оставляя очень много неоднозначного контента за бортом.

Поэтому для наиболее полной фильтрации мы используем сервис **SkyDNS**, который представляет гораздо более специализированное коммерческое решение, тариф **SkyDNS.Домашний** обходится всего в 395 руб/год, что по силам любому семейному бюджету. Сервис имеет гибкие настройки и позволяет достаточно тонко управлять блокируемыми тематиками.

Фильтр

Поставьте галочки на категориях сайтов, которые хотите заблокировать, или выберите рекомендованные настройки в левой колонке. Нажмите кнопку "Сохранить" для применения настроек.

Сохранить

☒ **Безопасность**

- ☒ Ботнеты
- ☒ Фишинг
- ☒ Сайты, распространяющие вирусы

☐ **Черные сайты**

- ☒ Агрессия, расизм, терроризм
- ☒ Запаркованные домены
- ☒ Наркотики
- ☒ Прокси и анонимайзеры
- ☐ Грубость, матерщина, непристойность
- ☐ Криптомайнинг
- ☐ Плагиат и рефераты

☐ **Информация для взрослых**

- ☐ Алкоголь и табак
- ☒ Знакомства
- ☒ Порнография и секс
- ☒ Астрология
- ☒ Казино, лотереи, тотализаторы
- ☒ Сайты для взрослых

☐ **Пожиратели трафика**

- ☐ Радио и музыка онлайн
- ☐ Файловые архивы
- ☐ Фотогалереи
- ☐ Торренты и P2P-сети
- ☐ Фильмы и видео онлайн

☐ **Пожиратели времени**

- ☐ Досуг и развлечения
- ☐ Онлайн-реклама и баннеры
- ☐ Форумы
- ☐ Компьютерные игры
- ☐ Социальные сети
- ☐ Чаты и мессенджеры

Мы будем использовать оба DNS-сервиса, Яндекс для более взрослых детей, которых уже не требуется ограждать от всего и вся и SkyDNS для младших, которым пока требуется более безопасная выдача.

Перенаправлять запросы клиентских устройств на нужные нам DNS можно сделать различными способами, мы будем использовать перехват пакетов на роутере, что позволит одновременно организовать защиту от ручного изменения настроек на

клиенте. Для этого перейдем в **IP - Firewall - NAT** и добавим новое правило. Закладка **General** : **Chain** - **dstnat**, **Protocol** - **udp**, **Dst.Port** - **53**.

The screenshot shows the 'New NAT Rule' dialog box with the 'General' tab selected. The 'Chain' dropdown is set to 'dstnat'. The 'Protocol' dropdown is set to 'udp'. The 'Dst. Port' field is set to '53'. The 'Src. Address', 'Dst. Address', 'Src. Port', 'Any. Port', 'In. Interface', and 'Out. Interface' fields are empty. On the right side, there are buttons for 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', 'Remove', 'Reset Counters', and 'Reset All Counters'.

На закладке **Advanced** в поле **Src. Address List** выбираем нужный нам список устройств.

The screenshot shows the 'New NAT Rule' dialog box with the 'Advanced' tab selected. The 'Src. Address List' dropdown is set to 'IVAN'. The 'Dst. Address List' and 'Layer7 Protocol' fields are empty. On the right side, there are buttons for 'OK', 'Cancel', 'Apply', and 'Disable'.

И на закладке **Action** укажем действие: **Action** - **dst-nat**, **To Addresses** - **193.58.251.251**, где в качестве адреса укажем IP-адрес нужного нам сервиса DNS, в данном случае приведен адрес **SkyDNS**.

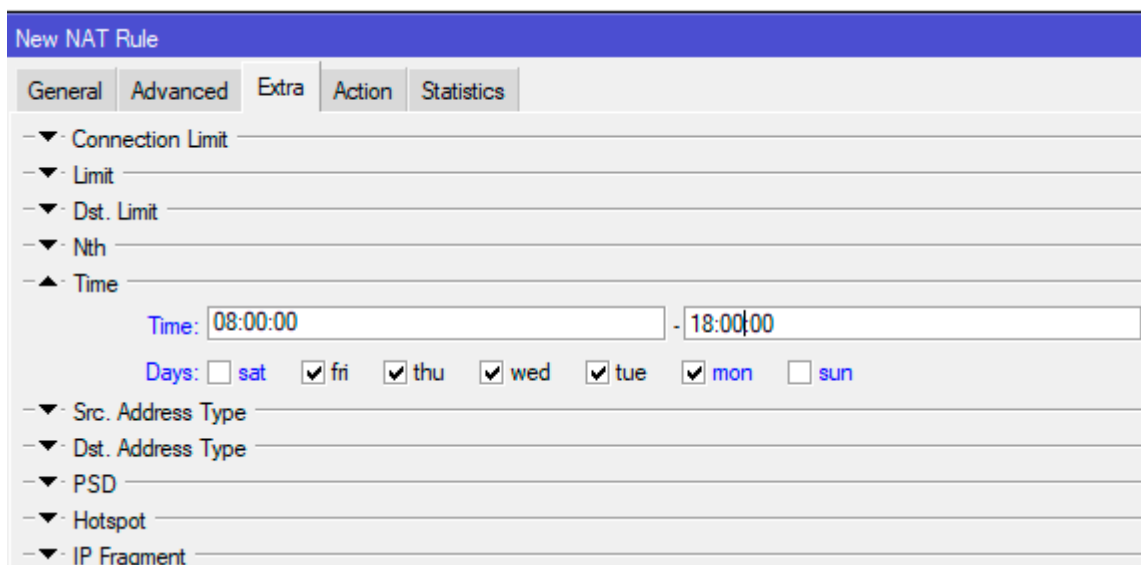
The screenshot shows the 'New NAT Rule' dialog box with the 'Action' tab selected. The 'Action' dropdown is set to 'dst-nat'. The 'Log' checkbox is unchecked. The 'Log Prefix' field is empty. The 'To Addresses' field is set to '193.58.251.251'. The 'To Ports' field is empty. On the right side, there are buttons for 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', and 'Remove'.

Затем сделаем копию этого же правила для протокола **tcp**.

В консоли добавить правила можно командами:

```
/ip firewall nat
add action=dst-nat chain=dstnat dst-port=53 protocol=udp src-address-list=IVAN to-
addresses=193.58.251.251
add action=dst-nat chain=dstnat dst-port=53 protocol=tcp src-address-list=IVAN to-
addresses=193.58.251.251
```

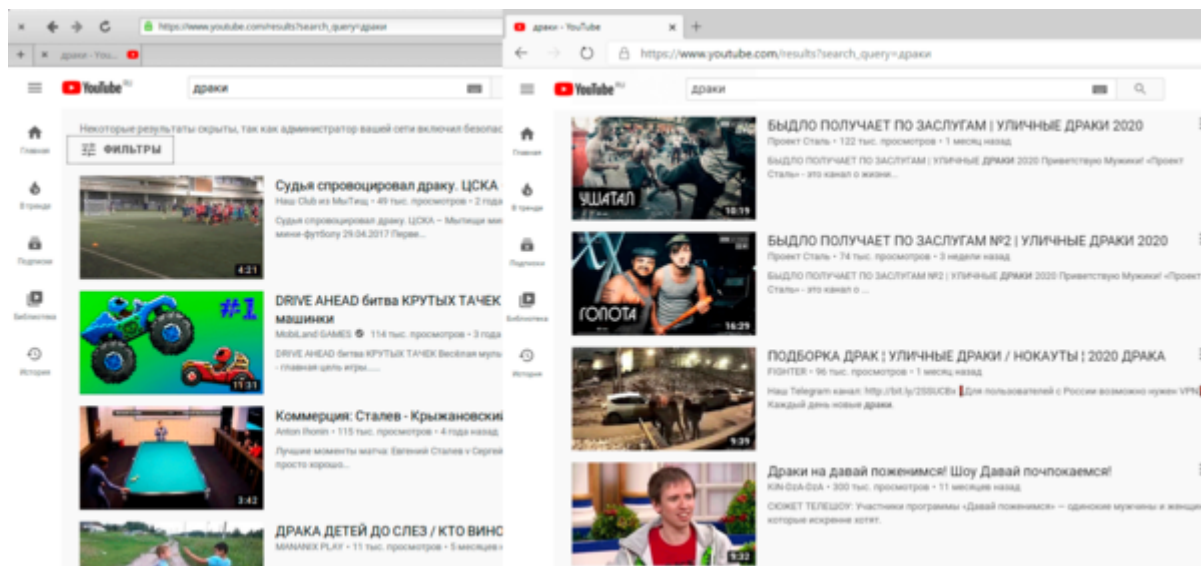
Аналогичным образом добавляем перенаправление для других групп устройств к своим DNS-серверам. Отдельного разговора требует группа общих устройств, для них мы укажем дополнительное условие. Для этого перейдем на закладку **Extra**, развернем блок **Time** и в полях **Time** и **Days** укажем расписание, по которому будем применять ограничения. В указанное время все запросы будут идти к безопасным серверам, а в остальное - к основному DNS-серверу и фильтрация производиться не будет.



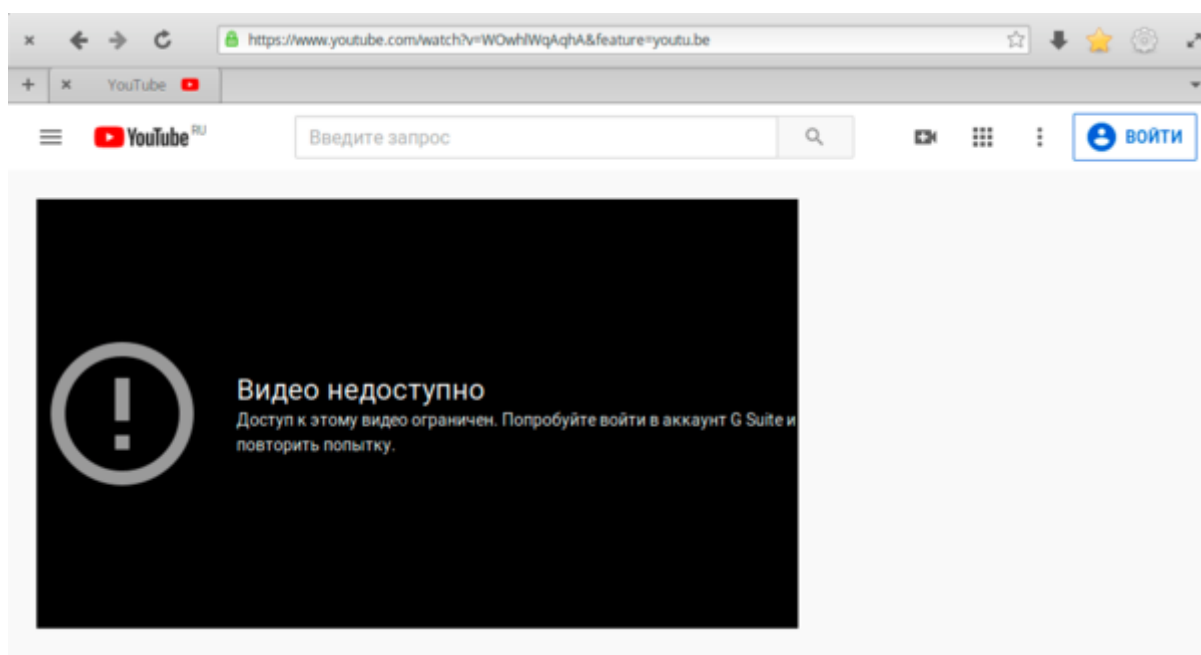
Это же действие в терминале:

```
/ip firewall nat
add action=dst-nat chain=dstnat dst-port=53 protocol=udp src-address-list=COMMON
time=8h-18h,mon,tue,wed,thu,fri to-addresses=77.88.8.7
add action=dst-nat chain=dstnat dst-port=53 protocol=tcp src-address-list=COMMON
time=8h-18h,mon,tue,wed,thu,fri to-addresses=77.88.8.7
```

В результате у вас должен получиться набор правил для каждой группы устройств, обратите внимание, что правило для группы общих устройств выделено красным и снабжено комментарием **# inactive time**, в данный момент указанные нами условия не выполняются и такое правило применено не будет.



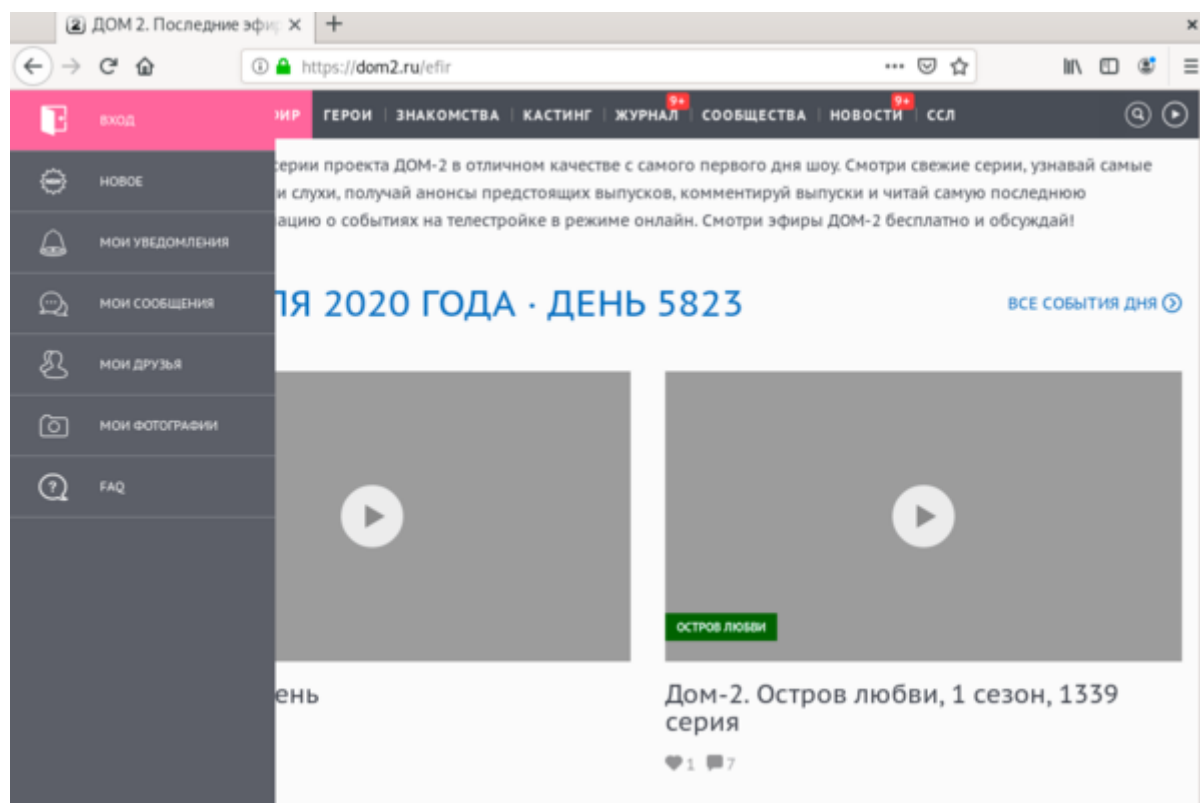
Как видим, фильтр работает весьма эффективно, отсекая практически весь нежелательный контент, при этом возможность изменить параметры фильтров в браузере будут заблокированы, даже при наличии прав локального администратора. А что будет, если на нежелательный ролик кто-то пришлет ссылку? Ничего страшного:



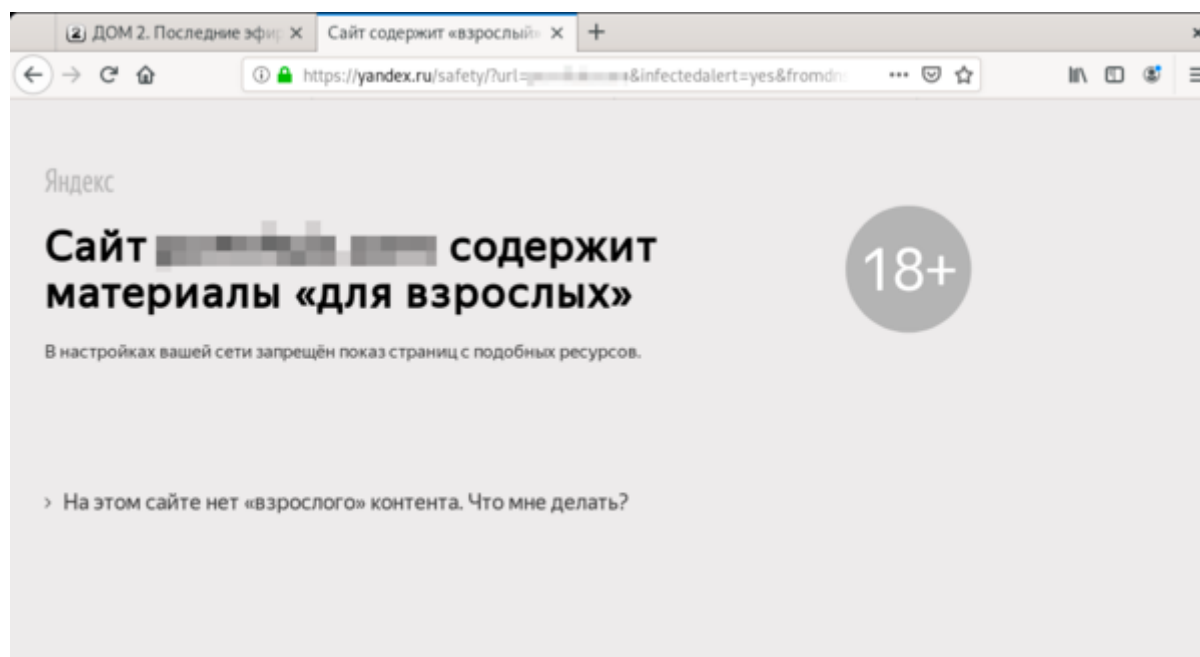
Разблокировать такие ролики локально также невозможно. Дополнительно можно включить безопасный поиск, когда все поисковые запросы будут перенаправляться на Безопасный поиск SkyDNS.

В общем, за два года использования данный сервис подтвердил свою эффективность и гибкость в использовании, по мере взросления ребенка часть фильтров можно отключать, предоставляя ему больше свободы в сети, не отказываясь при этом от контроля по тематикам ресурсов.

Яндекс.DNS Семейный подобной гибкостью похвастаться не может, он фильтрует преимущественно ресурсы, явно относящиеся к категории 18+. Неоднозначное шоу имея более низкий возрастной рейтинг (16+) будет спокойно доступно к просмотру.



Тем не менее явные сайты категории "для взрослых" будут однозначно заблокированы.



На наш взгляд, сервисы Яндекса хорошо подходят для более старших детей и использования на устройствах общего пользования, возможно даже на постоянной основе. Вместе с категорией 18+ блокируются явно нежелательные сайты: фишинг,

мошенничество, вarez и т.д., что неплохо подходит и для остальных членов семьи, особенно технически малограмотных.

Кроме **Семейного** у Яндекса есть безопасный **Безопасный** режим, который блокирует большинство небезопасных сайтов, но пропускает сайты 18+, его можно использовать, например, для старших членов семьи, которые не обладают достаточными навыками безопасного поведения в интернете.

Ограничение времени доступа в интернет при помощи функции Kid Control

Ограничение времени пребывания в сети - вторая по актуальности задача родительского контроля. В актуальных версиях RouterOS для этой цели есть специальный инструмент. Для его настройки перейдем в **IP - Kid Control** и на вкладке **Kids** добавим записи для каждого ребенка и группы устройств общего пользования, если доступ нужно ограничивать и к ним. В открывшемся окне добавляем промежутки времени для каждого дня недели в которые будет разрешена работа, таких промежутков может быть несколько.

Kid <Ivan>

Name: Ivan

Unlimited Rate Sun: [dropdown]

Unlimited Rate Mon: [dropdown]

Unlimited Rate Tue: [dropdown]

Unlimited Rate Wed: [dropdown]

Unlimited Rate Thu: [dropdown]

Unlimited Rate Fri: [dropdown]

Unlimited Rate Sat: [dropdown]

Sun: 10:00:00-23:00:00 [dropdown]

Mon: 17:00:00-23:00:00 [dropdown]

Tue: 17:00:00-23:00:00 [dropdown]

Wed: 17:00:00-23:00:00 [dropdown]

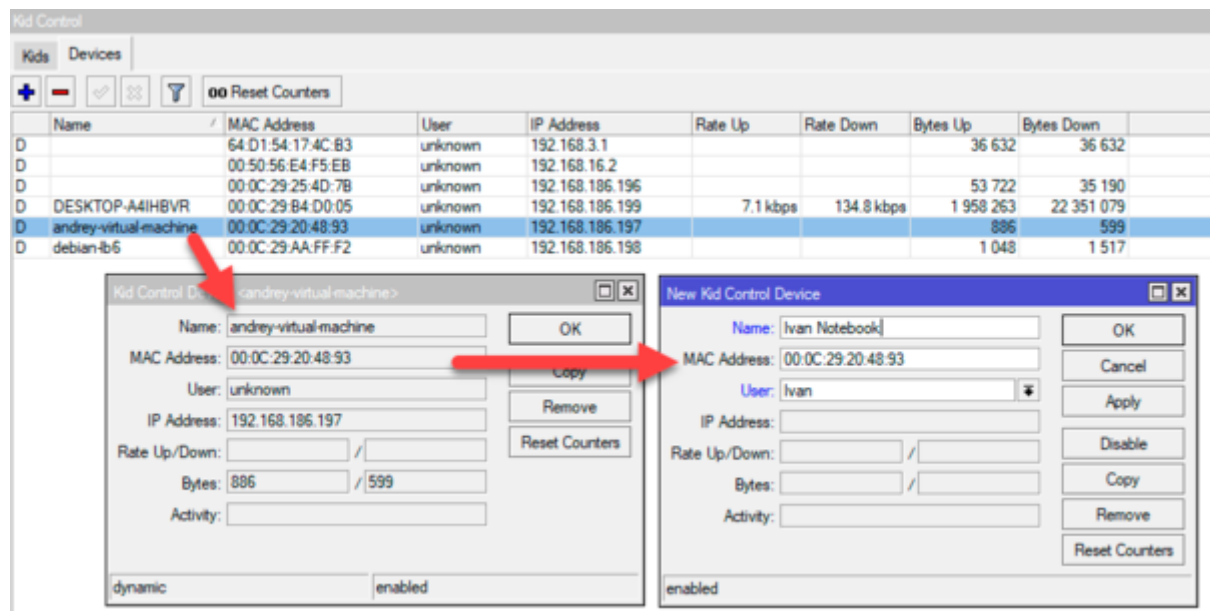
Thu: 17:00:00-23:00:00 [dropdown]

Fri: 17:00:00-23:00:00 [dropdown]

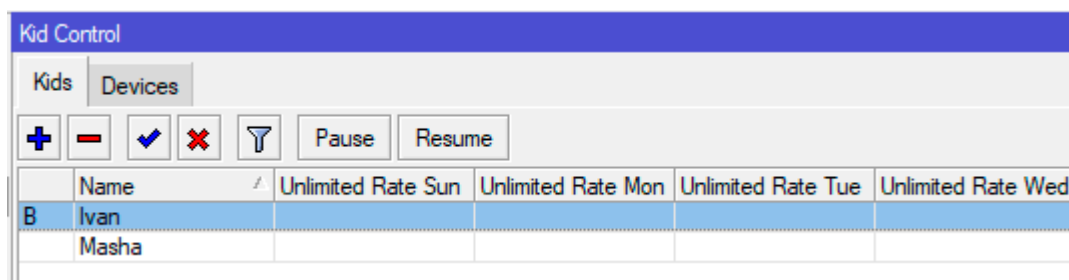
Sat: 10:00:00-23:00:00 [dropdown]

Buttons: OK, Cancel, Apply, Disable, Copy, Remove, Pause, Resume

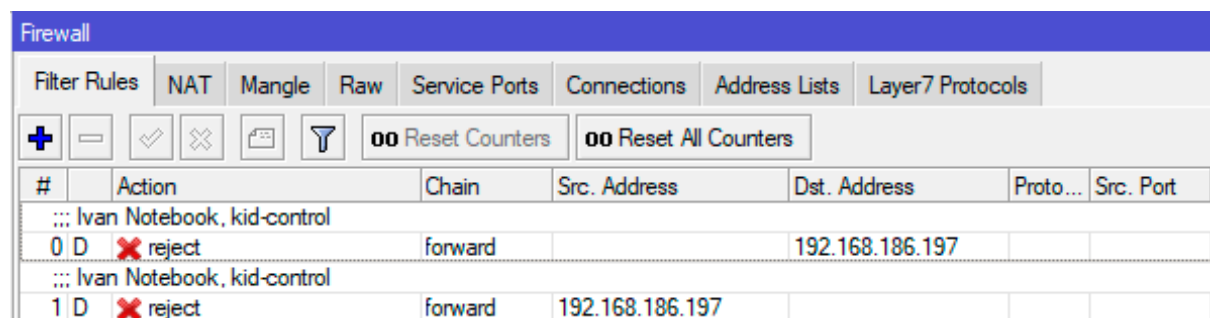
Затем к каждой записи ребенка нужно привязать устройства, принцип здесь аналогичен резервированию DHCP - точно также привязываем MAC-адрес. Для этого на закладке **Devices** создаем новую запись и указываем там нужный MAC, его можно скопировать из динамической записи, которая исчезнет после привязки устройства.



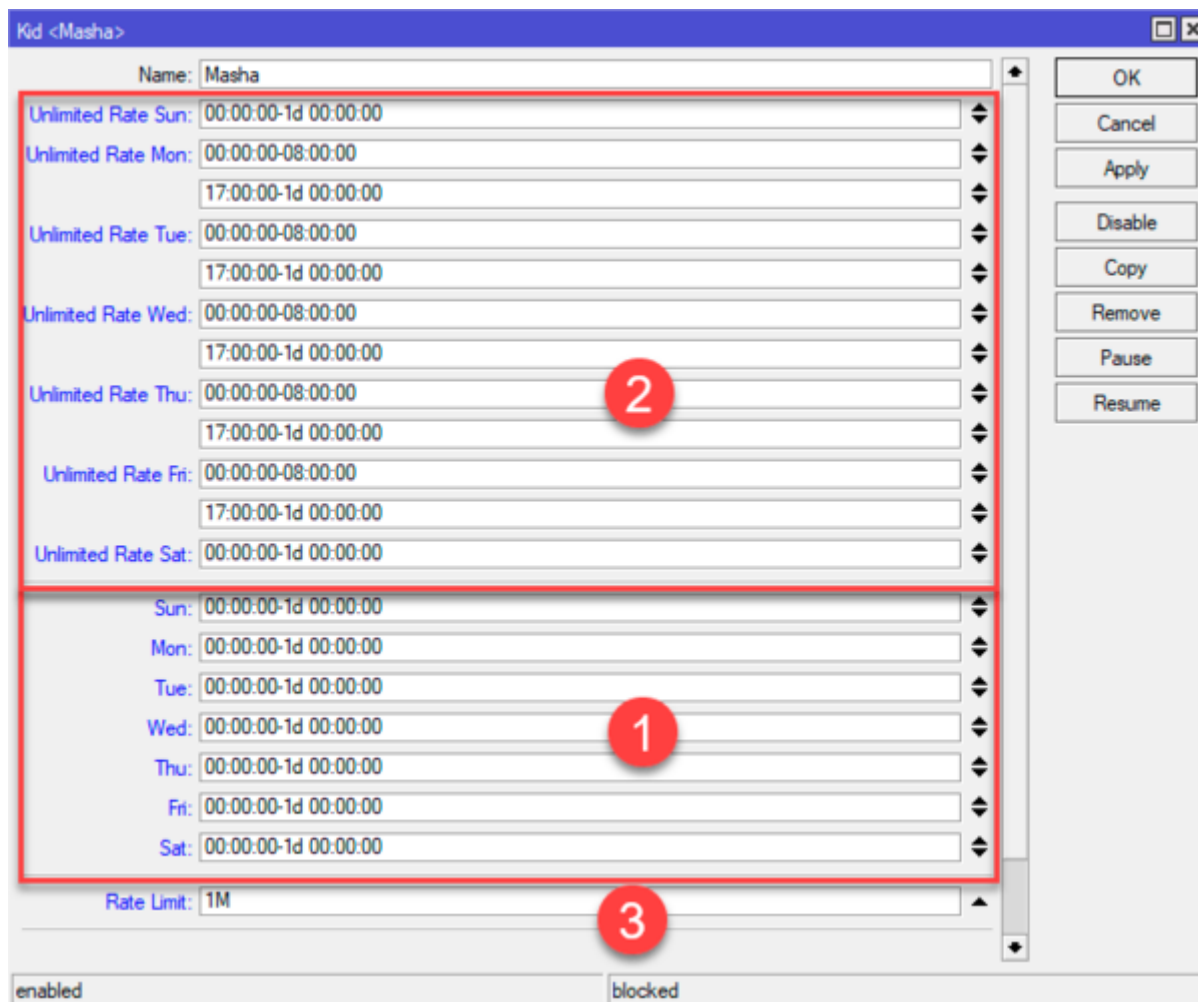
Таким образом получим еще один список, содержащие записи детей и расписание доступа в сеть для них, заблокированная запись обозначается в списке флагом **B**.



Блокировка устройств, связанных с записью, осуществляется при помощи динамически формируемых правил брандмауэра, которые запрещают прохождение транзитных пакетов от устройства и к нему.



Кроме блокировок мы можем задавать ограничение скорости интернета, для этого придется в первую очередь заполнить время доступа, если этого не сделать, то будет считаться, что работа пользователя запрещена, затем выше, в полях **Unlimited Rate** для каждого дня недели указываем промежутки, когда возможен доступ без ограничения скорости, таких промежутков может быть несколько. И наконец в самом низу, в поле **Rate Limit** указываем ограничение скорости, в нашем случае 1 Мбит/с.



При указании даты есть свои особенности, формат записи не поддерживает значение секунд отличное от нуля, поэтому для **окончания суток** вместо **23:59:59** используйте запись вида **1d 00:00:00**.

Следующий момент - ограничение скорости не работает при включенном **Fasttrack**, отключение которого может привести к высокой нагрузке на процессор, поэтому для слабых роутеров такой вариант скорее всего будет неприменим. Да и скажем честно, ограничение скорости - нетипичный сценарий для домашнего использования.

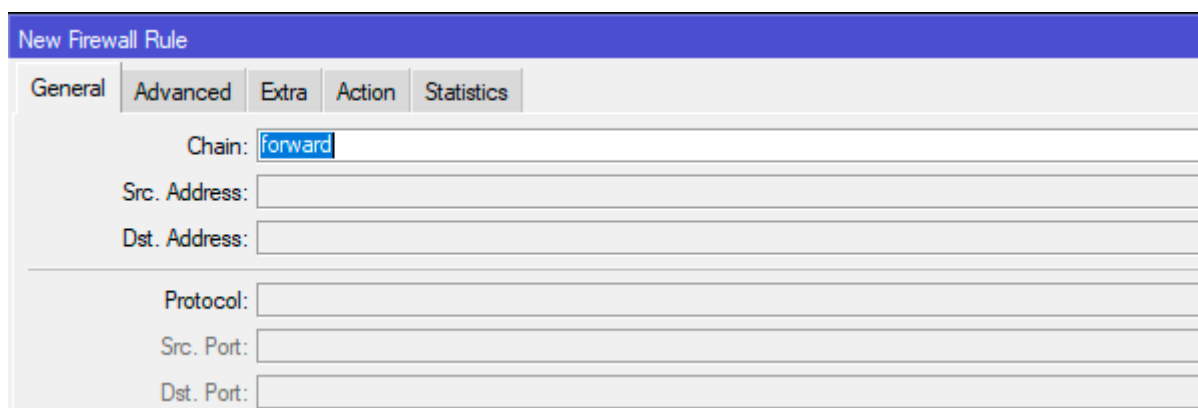
Также мы неоднократно наблюдали высокую нагрузку на CPU просто при включении ограничения времени доступа, что может сделать применение **Kid Control** на слабых устройствах невозможным. Но это не является серьезной проблемой, ограничение по времени можно без особых проблем реализовать обычными правилами брандмауэра.

Ограничение времени доступа в интернет при помощи брандмауэра

По сути, **Kid Control** не делает ничего нового или уникального, он является всего лишь высокоуровневым интерфейсом для управления правилами брандмауэра и очередями. А значит все это можно сделать руками и в некоторых случаях это будет еще гораздо проще.

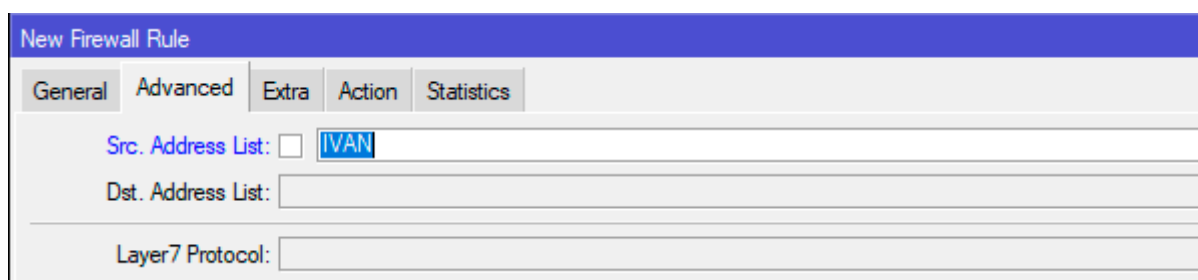
Есть два сценария реализации поставленной задачи: либо мы указываем диапазоны времени когда доступ клиента разрешен и запрещаем его в остальное время, либо запрещаем определенный временной промежуток и разрешаем вне его пределов.

Для начала рассмотрим первый вариант. Допустим мы хотим разрешить доступ с 10:00 до 23:00 вы выходные и с 17:00 до 23:00 в рабочие дни. Переходим в **IP - Firewall - Filter** и создаем новое правило. На закладке **General** указываем цепочку для транзитного трафика: **Chain - forward**.



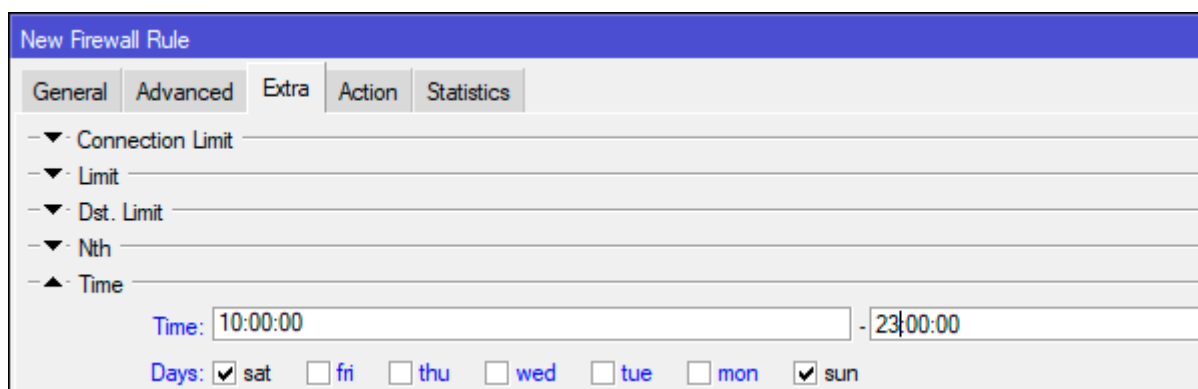
The screenshot shows the 'New Firewall Rule' window with the 'General' tab selected. The 'Chain' dropdown is set to 'forward'. The 'Src. Address' and 'Dst. Address' fields are empty. The 'Protocol' dropdown is set to 'all'. The 'Src. Port' and 'Dst. Port' fields are empty.

На закладке **Advanced** в опции **Src. Address List** указываем список адресов устройств ребенка.



The screenshot shows the 'New Firewall Rule' window with the 'Advanced' tab selected. The 'Src. Address List' dropdown is set to 'IVAN'. The 'Dst. Address List' dropdown is empty. The 'Layer7 Protocol' dropdown is empty.

На закладке **Extra** в разделе Time выбираем нужные дни и указываем требуемый временной диапазон (ниже указано расписание для выходных дней).



The screenshot shows the 'New Firewall Rule' window with the 'Extra' tab selected. The 'Time' section is expanded, showing a time range from '10:00:00' to '23:00:00'. The 'Days' section shows checkboxes for 'sat' and 'sun' selected, and 'fri', 'thu', 'wed', 'tue', and 'mon' unselected.

После чего сохраняем правило. Затем делаем его копию и настраиваем расписание для рабочей недели. Если требуется задать несколько диапазонов, то создаем необходимое количество правил копированием, в каждом из которых меняем время действия правила на закладке **Extra**.

И завершаем наш набор правил запрещающим, для него мы заполняем закладки: **General** - указывая цепочку **Chain - forward**, **Advanced** - задав список адресов в **Src. Address List** и **Action - reject**.

В терминале это можно сделать командами:

```
/ip firewall filter
add action=accept chain=forward src-address-list=IVAN time=10h-23h,sun,sat
add action=accept chain=forward src-address-list=IVAN time=17h-
23h,mon,tue,wed,thu,fri
add action=reject chain=forward reject-with=icmp-network-unreachable src-address-
list=IVAN
```

Другой вариант предусматривает запрет только в определенный период времени, для этого мы создаем новое правило, как и в предыдущем примере заполняя закладки **General**, **Advanced** и **Extra**, после чего на закладке **Action** добавляем действие **reject**. Разрешающего правила в комплект с ним не нужно, так как политика по умолчанию разрешает все исходящие транзитные соединения.

В терминале выполните (для примера мы запретили доступ с 08:00 до 17:00):

```
/ip firewall filter
add action=reject chain=forward reject-with=icmp-network-unreachable src-address-
list=MASHA time=8h-17h,mon,tue,wed,thu,fri
```

Данные правила следует разместить в самом начале цепочки FORWARD (т.е. выше всех остальных правил), также не забывайте снабжать правила понятными комментариями. Неактивные правила также будут выделены красным цветом и комментарием **# inactive time**.

#	Action	Chain	Src. Address	Dest. Address	Proto.	Src. Port	Dest. Port	In. Inter.	Out. Int.	In. Inter.	Out. Int.	Src. Ad...	Dest...
0	D passthrough	forward											
1	✓ accept	input	192.168.186.0/24						bridge1				
2	✓ accept	input									wan		
3	✓ accept	input			1 (ic...						wan		
4	✗ drop	input									wan		
5	FASTTRACK	forward											
6	✓ accept	forward										IVAN	
7	✗ accept	forward										IVAN	
8	✗ reject	forward										IVAN	
9	✗ reject	forward										MASHA	
10	✓ accept	forward											

Подобные наборы правил фактически делают все тоже самое, что и **Kid Control**, но не создают при этом лишней нагрузки на устройство.

Как видим, роутеры Mikrotik предоставляют достаточно широкие возможности по родительскому контролю, которые, к тому же, можно настроить несколькими разными способами.

Онлайн-курс по MikroTik

Научиться настраивать MikroTik с нуля или систематизировать уже имеющиеся знания можно на углубленном курсе по администрированию MikroTik. Автор курса, сертифицированный тренер MikroTik Дмитрий Скоромнов, лично проверяет лабораторные работы и контролирует прогресс каждого своего студента. В три раза больше информации, чем в вендорской программе MTCNA, более 20 часов практики и доступ навсегда.