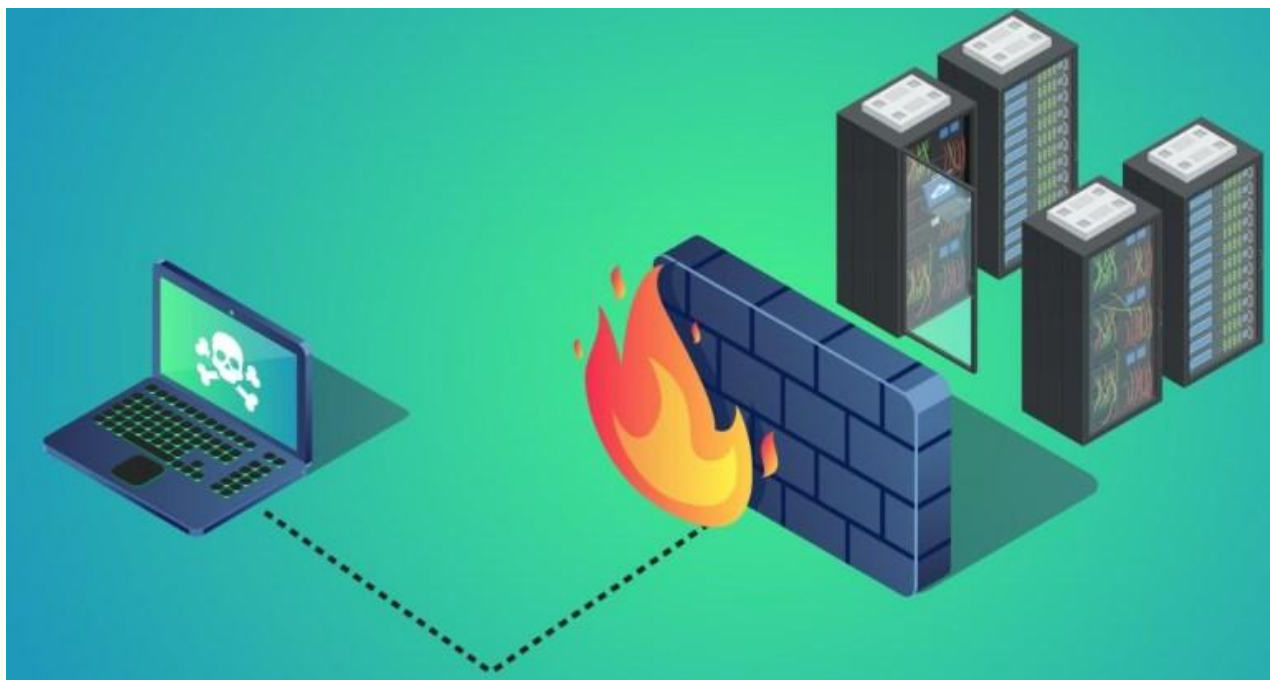


Базовая настройка Firewall на Микротик

 mikrotiklab.ru/nastrojka/artga-firewall.html

April 29, 2020



В сегодняшней статье уделим внимание базовой настройке Firewall на Mikrotik, Address List и блокировке соцсетей. Т.к. RouterOS основан на ядре linux, то нам предоставлен практически весь функционал сетевого ядра, да к тому же еще и в графике. Настройка будет продемонстрирована с помощью Winbox.

Firewall – инструмент, благодаря которому мы можем ограничить нежелательный трафик. Под «нежелательный» я имею ввиду тот, который нам не нужен в первую очередь с точки зрения администрирования, а уже потом от зловредный. Для начала нужно рассказать про 3 стандартные цепочки:

- Input – трафик входящий в роутер, т.е. тот, что адресован непосредственно для него. Пример: роутер имеет несколько адресов, согласно схеме сети ниже. Если мы отправим ping запрос на любой из этих них, то ответит нам именно он.
- Output – трафик исходящий от роутера или же создаваемый им. Отвечая на те самый ping запросы.
- Forward – транзитный трафик, тот, что не предназначен для устройства.

Самое главное, есть трафик, который направляется устройству и который устройство пересылает. Существует возможность создавать собственные цепочки правил с отличными именами.

Порядок правил. Следите за ним. В списке у каждого есть свой номер. Соответственно, то правило, что имеет число меньше т.е. стоит выше и будет приоритетным, если, конечно, оно подпадает под условия самого правила.

Наша команда рекомендует изучить Наша команда рекомендует изучить углубленный курс по администрированию сетевых устройств MikroTik В курсе много лабораторных работ по итогам которых вы получите обратную связь. После обучения вы получите диплом гос. образца РФ. Подробности и доступ к началу курса бесплатно [тут](#).

Содержание

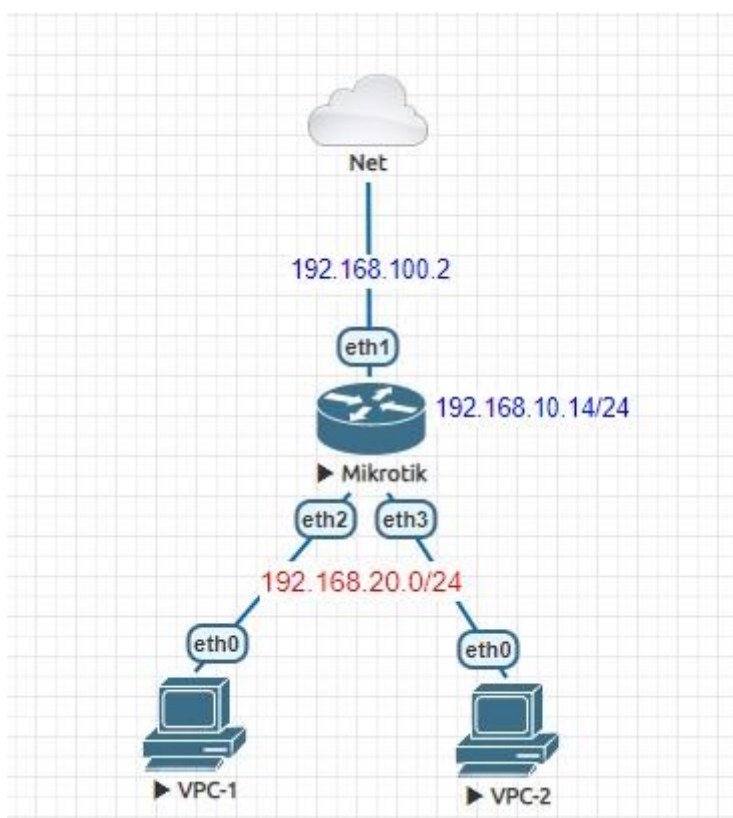
1. Схема сети
2. Базовая настройка Firewall
3. Защита локальной сети от атак из сети провайдера
4. Блокировка соц сетей на Mikrotik с помощью Address List и Firewall

Схема сети

Наша схема, будет до безобразия проста, но на основе нее будет продемонстрирована защита от атаки внутри сети провайдера и запрета соцсетей.

Итого имеем следующую конфигурацию:

- 168.10.14/24 – адрес роутера в сети провайдера;
- 168.100.2 – провайдер предоставляет доступ в интернет через L2TP, это адрес в туннеле;
- 168.20.1/24 – адрес в локальной сети с DHCP сервером для VPC-1 и VPC-2;
- RouterOS 6.46.



Базовая настройка Firewall

Смотря на схему, следует понять, какой тип трафика нужен в данной сети. Т.к. она простая, то достаточно разрешить входящий трафика управления (Winbox, SSH, WWW) и DNS с локальной сети, т.к. нам не нужно чтобы роутер резолвил имена для товарищей из интернет и не только.

Рекомендую менять стандартные порты управления и отключать не используемые службы, есть большая вероятность, что начнут брутфорсить ваш девайс. Это можно сделать в IP – Services.

	Name	Port	Available From	Certificate
X	api	8728		
X	api-ssl	8729		none
X	ftp	21		
	ssh	2222		
X	telnet	23		
	winbox	58291		
	www	80	192.168.20.0/24	
X	www-ssl	443		none

8 items (1 selected)

Настройка цепочки input. Не стреляем себе в ногу и жмем на Safe Mode прежде, чем что-либо делать!



Из примера выше мы изменили стандартные порты для SSH, Winbox и WWW. Все они работают по TCP. Создадим соответствующие правила в фильтре. IP – Firewall – Filter.

New Firewall Rule

General Advanced Extra Action Statistics

Chain: input

Src. Address:

Dst. Address:

Protocol: ☐ 6 (tcp)

Src. Port:

Dst. Port: ☐ 2222,58291

Any. Port:

In. Interface:

Out. Interface:

In. Interface List:

Out. Interface List:

Packet Mark:

Connection Mark:

Routing Mark:

Routing Table:

Connection Type:

Connection State: ☐ invalid ☐ established ☐ related ☒ new ☐ untracked

Connection NAT State:

OK Cancel Apply Disable Comment Copy Remove Reset Counters Reset All Counters

Интерпретируем правило: если есть новое соединение с любого адреса на роутер по протоколу TCP на порт 2222 или 58291 — разрешить. Обязательно комментируем правило в списке правил. Почему именно новое соединение? Ответ узнаем дальше.

Далее разрешим input на 80 порт с ЛВС.

New Firewall Rule

General Advanced Extra Action Statistics

Action: accept

☐ Log

Log Prefix:

Firewall

Filter Rules NAT Mangle Raw Service P

+ - ✓ ✗ 📁 🔍 ⏏ Reset Cou

#	Action	Chain	Src. Add
...	input-SSH_Winbox-Allow		
0	✓ accept	input	

New Firewall Rule

General Advanced Extra Action Statistics

Chain: input

Src. Address: 192.168.20.0/24

Dst. Address:

Protocol: 6 (tcp)

Src. Port:

Dst. Port: 80

Any. Port:

In. Interface:

Out. Interface:

In. Interface List:

Out. Interface List:

Packet Mark:

Connection Mark:

Routing Mark:

Routing Table:

Connection Type:

Connection State: ☐ invalid ☐ established ☐ related ☒ new ☐ untracked

Connection NAT State:

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Reset Counters

Reset All Counters

Если новое соединение с 192.168.20.0/24 по TCP на 80 порт – разрешить. Далее нужно разрешить DNS. Он может работать как по TCP, так и по UDP, наш случай это UDP, т.к. запросы на разрешение имен идут именно по UDP.

New Firewall Rule

General Advanced Extra Action Statistics

Chain:

Src. Address: ☐ 192.168.20.0/24

Dst. Address:

Protocol: ☐ udp

Src. Port:

Dst. Port: ☐ 53

Any. Port:

In. Interface:

Out. Interface:

In. Interface List:

Out. Interface List:

Packet Mark:

Connection Mark:

Routing Mark:

Routing Table:

Connection Type:

Connection State:

Connection NAT State:

enabled

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters

Обратите внимание, что мы разрешаем весь трафик по UDP:53 с 192.168.20.0/24, это связано с тем, что данный протокол не поддерживает установку соединения и подтверждение получения каждого пакета, поэтому ставить Connection State – New бессмысленно. Создаем следующее правило.

The image shows the 'New Firewall Rule' window with the following configuration:

- Chain:** input
- Src. Address:** (empty)
- Dst. Address:** (empty)
- Protocol:** (empty)
- Src. Port:** (empty)
- Dst. Port:** (empty)
- Any. Port:** (empty)
- In. Interface:** (empty)
- Out. Interface:** (empty)
- In. Interface List:** (empty)
- Out. Interface List:** (empty)
- Packet Mark:** (empty)
- Connection Mark:** (empty)
- Routing Mark:** (empty)
- Routing Table:** (empty)
- Connection Type:** (empty)
- Connection State:**
 - ☐ invalid
 - ☒ established
 - ☒ related
 - ☐ new
 - ☐ untracked
- Connection NAT State:** (empty)

Buttons on the right: OK, Cancel, Apply, Disable, Comment, Copy, Remove, Reset Counters, Reset All Counters.

Любое связанное и установившееся входящее соединение разрешить. Дело все в том, что Mikrotik понимает все входящие, исходящие и транзитные соединения. Т.к. мы хотим оптимизировать нагрузку на устройство, то создаем данное правило, иначе ранее созданные правила будут работать только на новые соединения, но не на устоявшиеся или связанные. В итоге первый пакет прилетит, а остальные нет. Это справедливо только для TCP. Собственно, это и ответ на предыдущий вопрос. Следующим правилом мы запретим абсолютно весь input, будьте осторожны и следите за Safe Mode.

New Firewall Rule

General Advanced Extra Action Statistics

Chain: **input**

Src. Address:

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

In. Interface:

Out. Interface:

In. Interface List:

Out. Interface List:

Packet Mark:

Connection Mark:

Routing Mark:

Routing Table:

Connection Type:

Connection State:

Connection NAT State:

enabled

OK Cancel Apply Disable Comment Copy Remove Reset Counters Reset All Counters

New Firewall Rule

General Advanced Extra Action Statistics

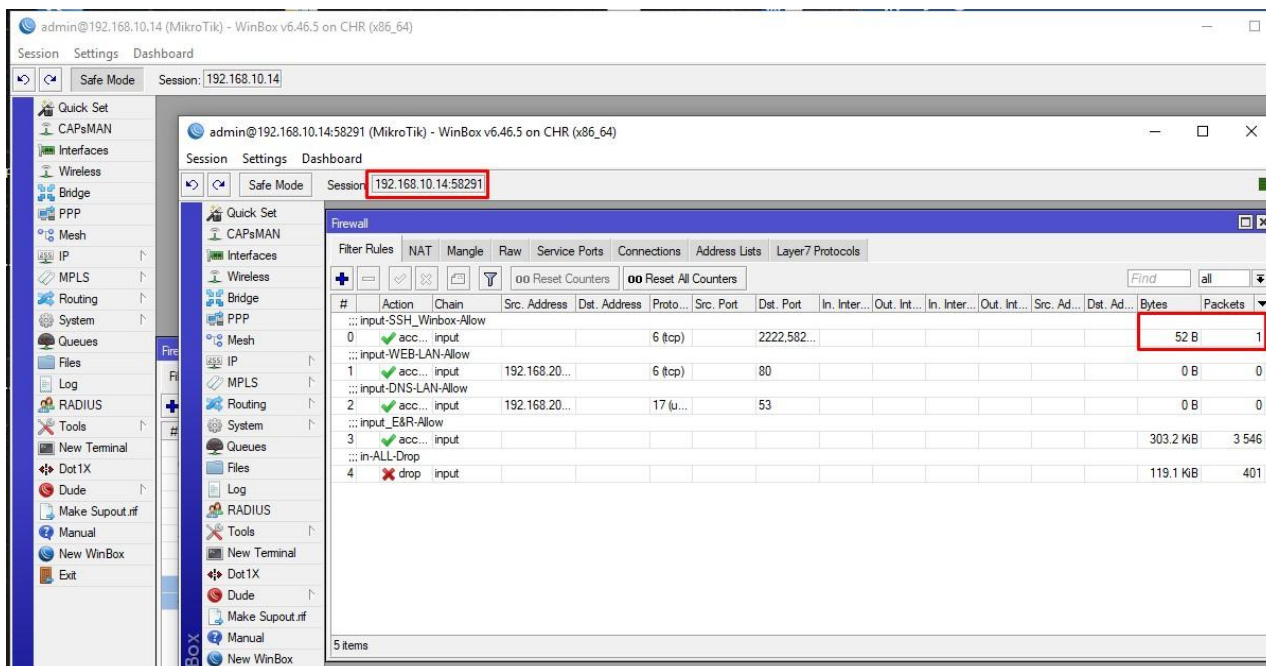
Action: **drop**

☐ Log

Log Prefix:

OK Cancel Apply Disable Comment Copy Remove Reset Counters Reset All Counters

Попробуем подключиться к устройству по нестандартным портам Winbox не отпуская Safe Mode.



На скриншоте видно, что сработал счетчик самого верхнего правила. Далее можно отпускать безопасный режим и закрывать старую сессию Winbox. Почему сработало правило только на 1 пакет? При подключении по TCP:58291 роутер понял, что это новое соединение, т.к. ничего не мешало подключению (подошел логин пароль, нет запрещающих правил и др.) соединение превратилось в устоявшееся.

Firewall									
Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols									
Tracking									
	Src. Address	/	Dst. Address	Protocol	Connecti...	Timeout	TCP State	Orig./Repl. Rate	Orig./Repl. Bytes
C	0.0.0.0:68		255.255.255.255:67	17 (udp)		00:00:09		5.2 kbps/0 bps	3213.4 KiB/0 B
SAC	192.168.10.1:1701		192.168.10.14:1701	17 (udp)		00:02:59		3.9 kbps/3.9 kbps	1240.8 KiB/1248...
SAC	192.168.10.51:50476		192.168.10.14:58291	6 (tcp)		23:59:59	established	320 bps/15.6 kbps	54.9 KiB/1113.4 ...
SACs	192.168.100.1:5678		8.8.4.4:53	17 (udp)		00:02:59		0 bps/1280 bps	2816 B/392.0 KiB
SACs	192.168.100.1:5678		8.8.8.8:53	17 (udp)		00:02:59		0 bps/1280 bps	2816 B/393.0 KiB

Настроим правила пересылки. Если у вас нет особенных требования для этого, то будет достаточно двух правил. Разрешим новые, устоявшиеся и зависимые соединения.

New Firewall Rule

General Advanced Extra Action Statistics

Chain: forward

Src. Address:

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

In. Interface:

Out. Interface:

In. Interface List:

Out. Interface List:

Packet Mark:

Connection Mark:

Routing Mark:

Routing Table:

Connection Type:

Connection State: ☐ invalid ☒ established ☒ related ☒ new ☐ untracked

Connection NAT State:

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Reset Counters

Reset All Counter

Запретим invalid.

Внимание. Будьте осторожны с ним, т.к. на практике могут возникнуть нюансы, если у вас не стандартный setup.

New Firewall Rule

General Advanced Extra Action Statistics

Chain: **forward**

Src. Address:

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

In. Interface:

Out. Interface:

In. Interface List:

Out. Interface List:

Packet Mark:

Connection Mark:

Routing Mark:

Routing Table:

Connection Type:

Connection State: ☒ invalid ☐ established ☐ related ☐ new ☐ untracked

Connection NAT State:

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Reset Counters

Reset All Counters

New Firewall Rule

General Advanced Extra Action Statistics

Action: **drop**

☐ Log

Log Prefix:

Давайте взглянем на список созданных правил.

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>00</div> <div>Reset Counters</div> <div>00</div> <div>Reset All Counters</div> </div> <div>Find</div> <div>all</div> <div>▼</div> </div>															
#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	In. Inter...	Out. Int...	Src. Ad...	Dst. Ad...	Bytes	Packets
::: input-SSH_Winbox-Allow															
0	✓ acc...	input			6 (tcp)		2222,582...							52 B	1
::: input-WEB-LAN-Allow															
1	✓ acc...	input	192.168.20...		6 (tcp)		80							0 B	0
::: input-DNS-LAN-Allow															
2	✓ acc...	input	192.168.20...		17 (u...		53							0 B	0
::: input_E&R-Allow															
3	✓ acc...	input												622.6 KB	7 293
::: in-ALL-Drop															
4	✗ drop	input												624.6 KB	2 091
::: frw_N&E&R-Allow															
5	✓ acc...	forward												16.8 KB	216
::: frw_invalid-Drop															
6	✗ drop	forward												0 B	0

Читая комментарии, можно примерно понять, что настроено. Используйте их, если конечно не хотите усложнять жизнь себе и другим.

Защита локальной сети от атак из сети провайдера

Все бы хорошо, есть одно, но. Прописав маршрут в нашу сеть из серой сети провайдера, наш девайс начнет пересылку трафика. Конечно, устройства не смогут отправить обратно ответы, но принимать данные будут. Создадим соответствующее правило.

Firewall Rule <>

General Advanced Extra Action Statistics

Chain:

Src. Address:

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

In. Interface: ☐

Out. Interface: ☐

In. Interface List:

Out. Interface List:

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

Firewall Rule <>

General Advanced Extra Action Statistics

Action:

☐ Log

Log Prefix:

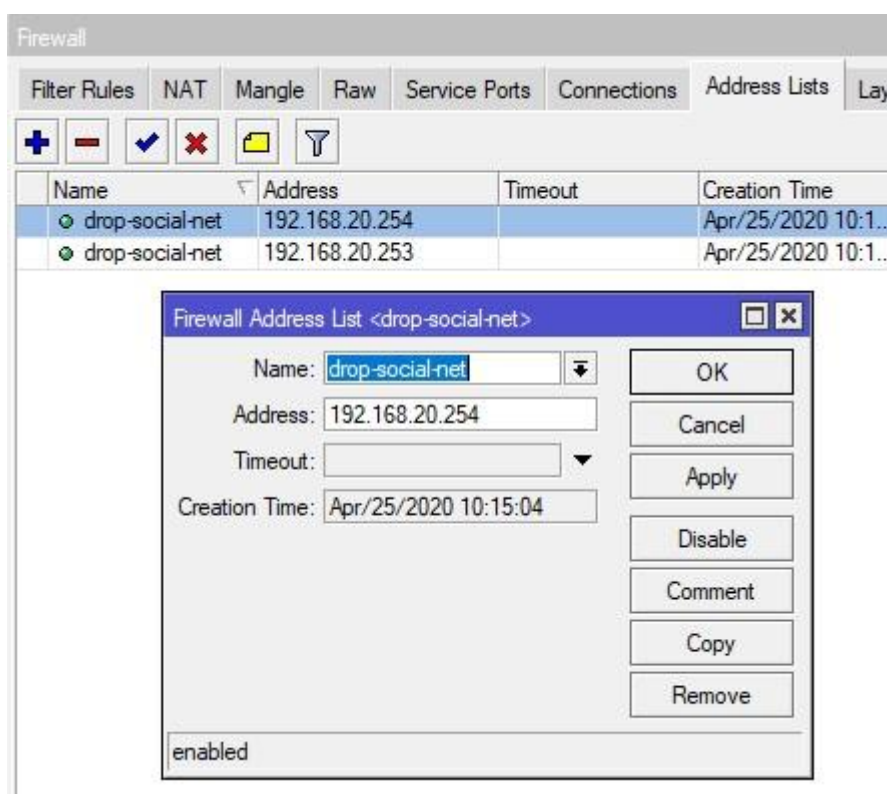
Поместим его выше разрешающего правила пересылки.

1	✓ acc...	input	192.168.20...	6 (tcp)	80			
;;; input-DNS-LAN-Allow								
2	✓ acc...	input	192.168.20...	17 (u...	53			
;;; input_E&R-Allow								
3	✓ acc...	input						
;;; in-ALL-Drop								
4	✗ drop	input						
;;; fw_Drop-From-ISP-LAN								
5	✗ drop	forward					ether1	bridge 1
;;; fw_N&E&R-Allow								
6	✓ acc...	forward						
;;; fw_invalid-Drop								
7	✗ drop	forward						

8 items (1 selected)

Блокировка соц сетей на Mikrotik с помощью Address List и Firewall

RouterOS есть функционал Address List. Он может содержать подсеть, конкретный адрес или доменное имя. Ниже я покажу как заблокировать vk.com. Есть условие, заблокировать доступ с 192.168.20.254 и 192.168.20.253. Открываем IP – Firewall – Address List. Создадим новые листы. Первый лист, будет содержать ip, с которых запрещено ходить на vk.com.



Вторым, vk.com. Задаем доменные имена.

Firewall

Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols

Find

Name	Address	Timeout	Creation Time
vk.com	vk.com		Apr/25/2020 10:1...
vk.com	87.240.190.78		Apr/25/2020 10:1...
vk.com	87.240.139.194		Apr/25/2020 10:1...
vk.com	93.186.225.208		Apr/25/2020 10:1...
vk.com	87.240.137.158		Apr/25/2020 10:1...
vk.com	87.240.190.72		Apr/25/2020 10:1...
vk.com	87.240.190.67		Apr/25/2020 10:1...
vkontakte.com	vkontakte.com		Apr/25/2020 10:1...
vk.com	95.142.192.88		Apr/25/2020 10:1...
drop-social-net	192.168.20.254		Apr/25/2020 10:1...
drop-social-net	192.168.20.253		Apr/25/2020 10:1...

11 items (1 selected)

Firewall Address List <vk.com>

Name: vk.com

Address: vk.com

Timeout:

Creation Time: Apr/25/2020 10:16:17

enabled

OK Cancel Apply Disable Comment Copy Remove

После создания, роутер отрезолвит имя на тех серверах, что указаны в DNS и добавит в адрес лист. Далее простым правилом цепочки forward запрещаем пересылку из одного листа в другой. Чтобы пользователь не ждал долго, а получал отбойник что соединение разорвано укажем некоторые уточнения. Если новый транзитный TCP.

New Firewall Rule

General Advanced Extra Action Statistics

Chain: forward

Src. Address:

Dst. Address:

Protocol: ☐ 6 (tcp)

Src. Port:

Dst. Port:

Any. Port:

In. Interface:

Out. Interface:

In. Interface List:

Out. Interface List:

Packet Mark:

Connection Mark:

Routing Mark:

Routing Table:

Connection Type:

Connection State: ☐ invalid ☐ established ☐ related ☒ new ☐ untracked

Connection NAT State:

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Reset Counters

Reset All Counters

И пересылка происходит из одного листа в другой.

New Firewall Rule

General Advanced Extra Action Statistics

Src. Address List: ☐ drop-social-net

Dst. Address List: ☐ vk.com

Layer7 Protocol:

Content:

Connection Bytes:

Connection Rate:

Per Connection Classifier:

OK

Cancel

Apply

Disable

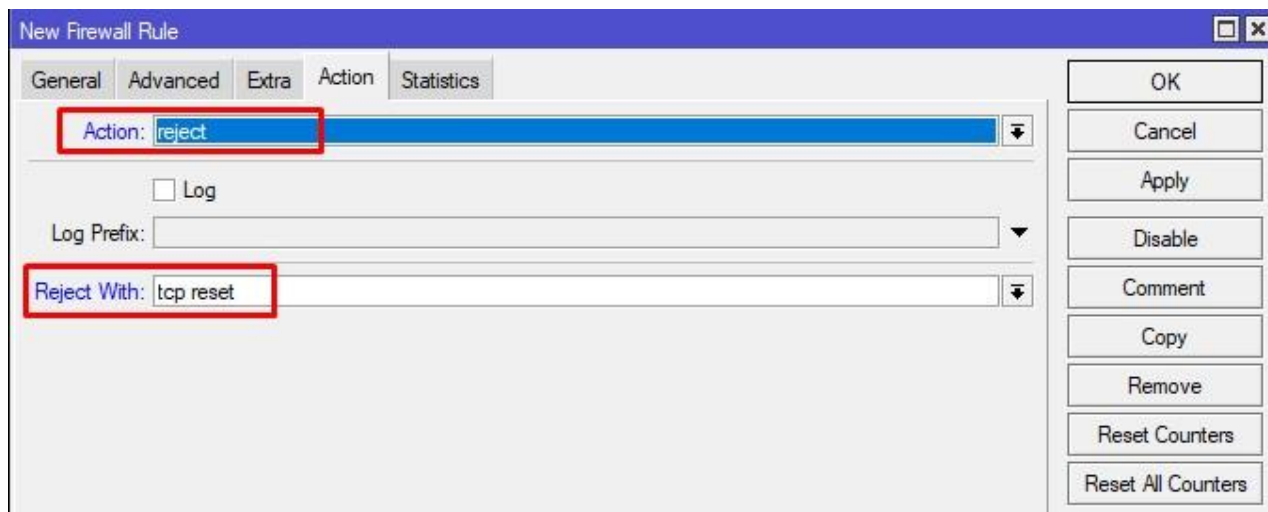
Comment

Copy

Remove

Reset Counters

То говорим, что соединение было сброшено.



Не забываем поместить его выше разрешающего правила пересылки.

Firewall														
Filter Rules														
NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols														
+ - ✓ ✗ 📁 🔍 00 Reset Counters 00 Reset All Counters Find all														
#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	In. Inter...	Out. Int...	Src. Ad...	Dst. Ad...	Bytes
0	✓ acc...	input			6 (tcp)		2222,582...							0 B
1	✓ acc...	input	192.168.20...		6 (tcp)		80							0 B
2	✓ acc...	input	192.168.20...		17 (u...		53							0 B
3	✓ acc...	input												905.8 KiB
4	✗ drop	input												815.8 KiB
5	✗ drop	forward						ether1	bridge1					1424 B
6	✗ reject	forward			6 (tcp)							drop-so...	vk.com	0 B
7	✓ acc...	forward												127.0 KiB
8	✗ drop	forward												0 B

Теперь вы можете добавлять адреса и имена в листы, правило фаервола автоматически будет применять к ним действия. Самое главное в блокировке по доменному имени, чтобы DNS сервером для клиентов в вашей сети был Mikrotik. Если вы зададите DNS вручную на машине, допустим 8.8.8.8, то vk.com может изменить один из адресов и правило не сработает. Так же смотрите на TTL в кэше, его следует изменить на меньшее.

DNS Settings

Servers: 1.0.0.1

Dynamic Servers:

☒ Allow Remote Requests

Max UDP Packet Size: 4096

Query Server Timeout: 2.000 s

Query Total Timeout: 10.000 s

Max. Concurrent Queries: 100

Max. Concurrent TCP Sessions: 20

Cache Size: 2048 KiB

Cache Max TTL: 04:00:00

Cache Used: 20 KiB

OK

Cancel

Apply

Static

Cache

Может возникнуть вопрос, а не грузят ли ЦП эти ваши Address List? Ответ – Нет! Они работают аппаратно на специальных чипах (асиках), и тысячи листов с тысячами IP не будут грузить ЦП и устройство в целом. На этом все, желаю удачи!

Вы хорошо разбираетесь в Микротиках? Или впервые недавно столкнулись с этим оборудованием и не знаете, с какой стороны к нему подступиться? В обоих случаях вы найдете для себя полезную информацию в углубленном курсе «Администрирование сетевых устройств MikroTik». В курсе много практических лабораторных работ по результату выполнения которых вы получите обратную связь. После окончания обучения вы получите диплом гос. образца РФ. Подробности и доступ к началу курса бесплатно [тут](#).