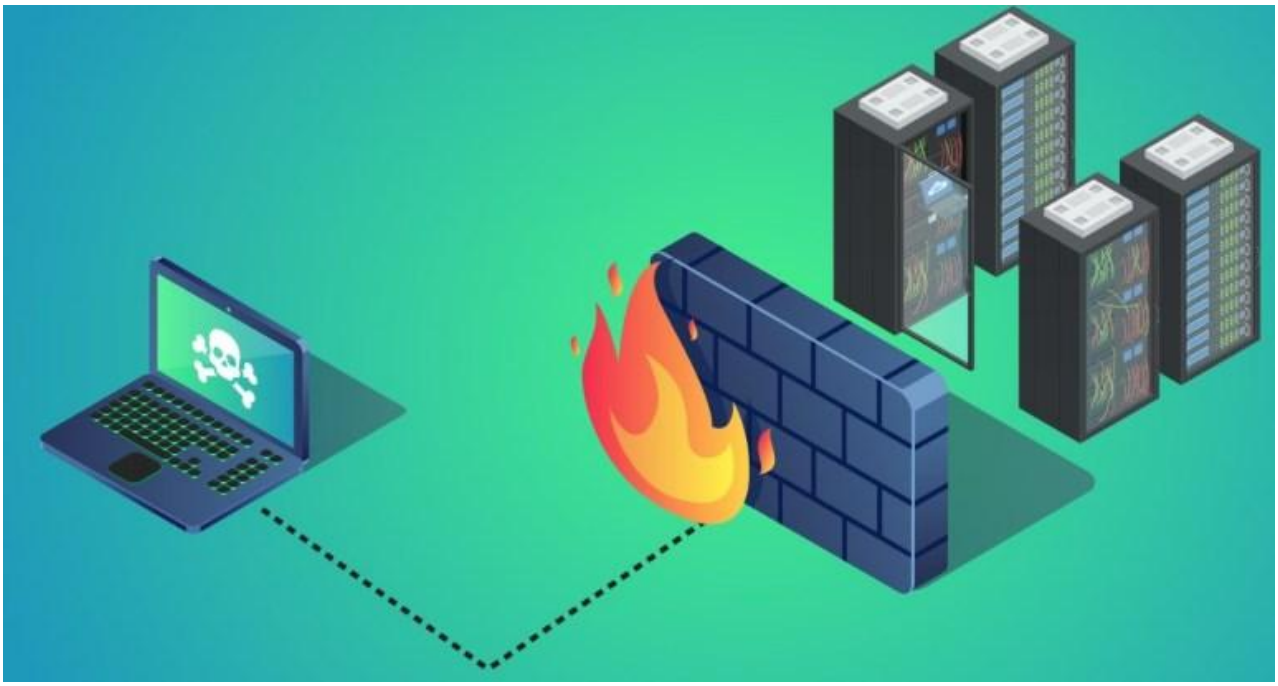
Базовая настройка Firewall на Микротик

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 изучитьНаша 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.

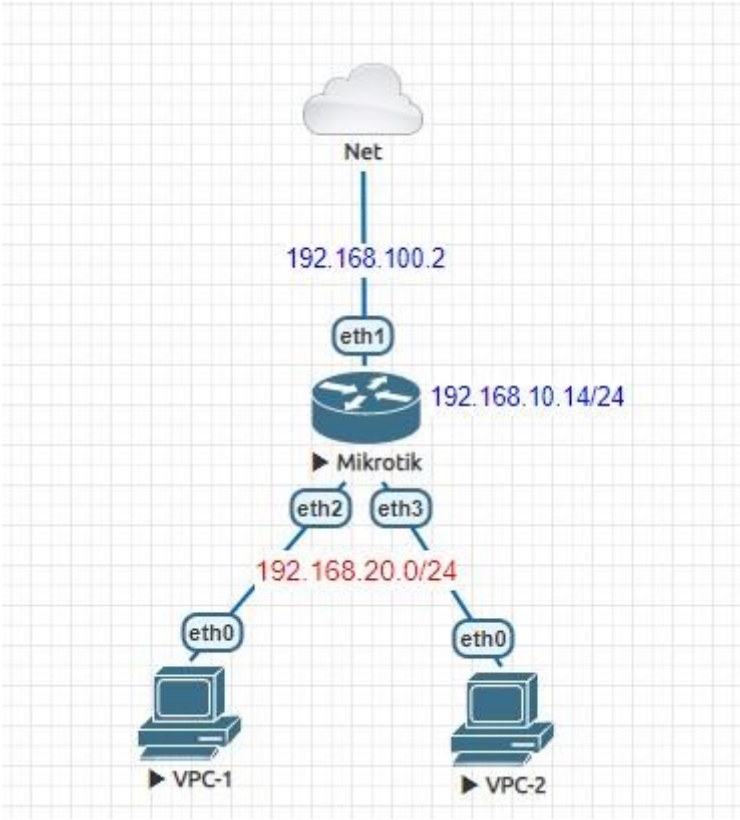
Содержание

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:

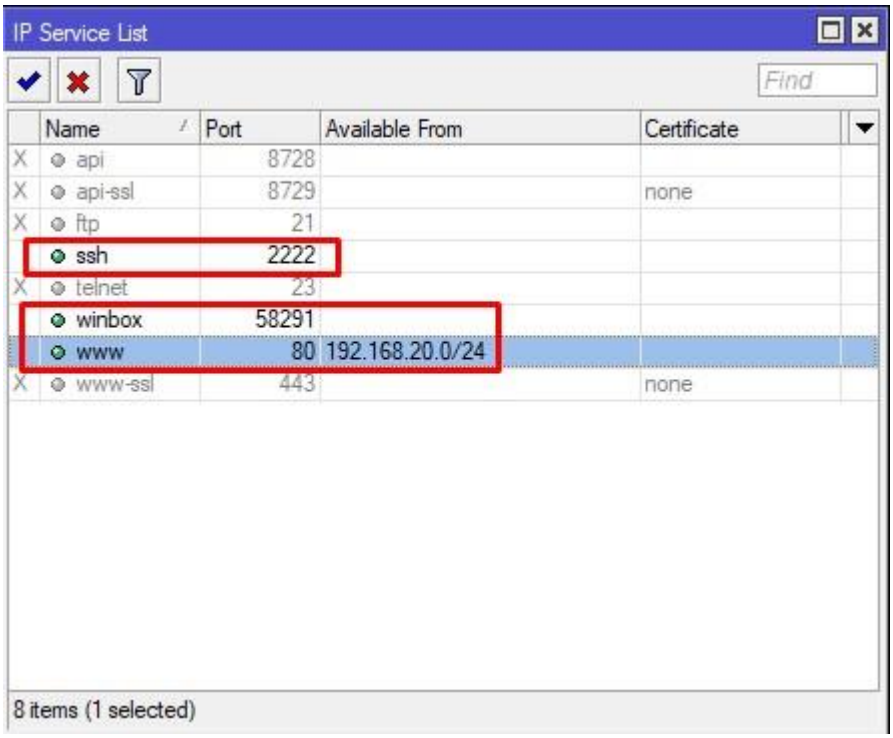
- 168.10.14/24 – адрес роутера в сети провайдера;
- 168.100.2 – провайдер предоставляет доступ в интернет через L2TP, это адрес в туннеле;
- 168.20.1/24 – адрес в локальной сети с DHCP сервером для VPC-1 и VPC-1;
- RouterOS 6.46.



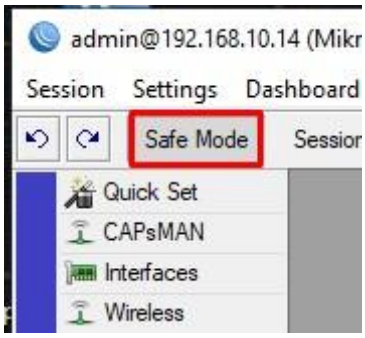
Базовая настройка Firewall

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.

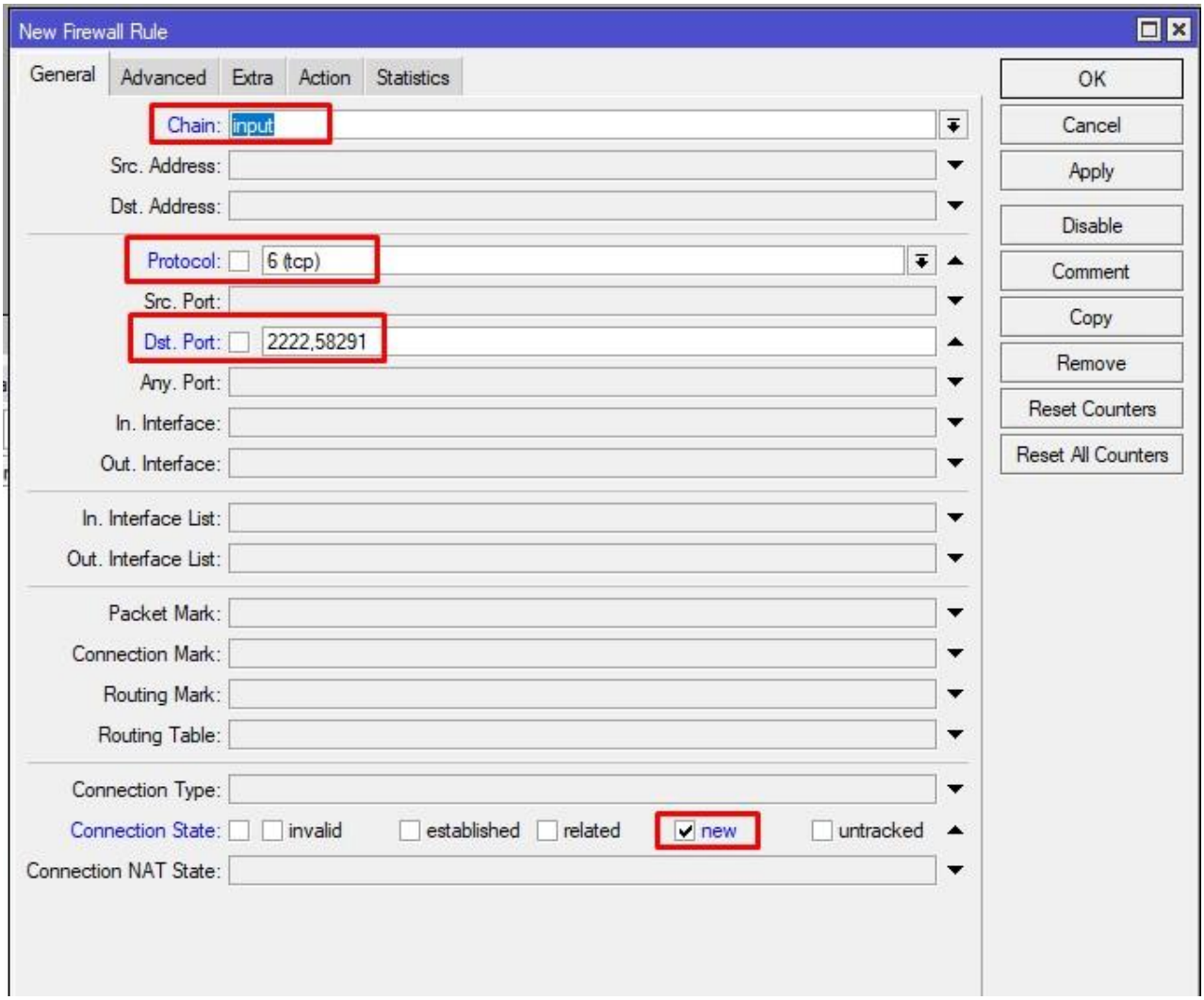
> Рекомендую менять стандартные порты управления и отключать не используемые службы, есть большая вероятность, что начнут брутфорсить ваш девайс. Это можно сделать в IP – Services.



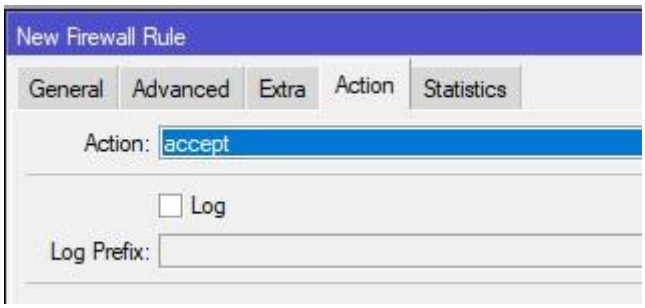
Настройка цепочки input. Не стреляем себе в ногу и жмем на Safe Mode прежде, чем что-либо делать!



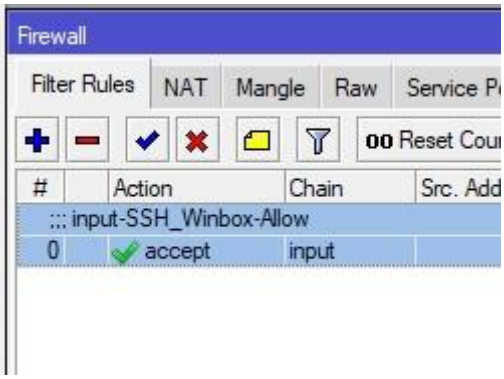
Из примера выше мы изменили стандартные порты для SSH, Winbox и WWW. Все они работают по TCP. Создадим соответствующие правила в фильтре. IP – Firewall – Filter.

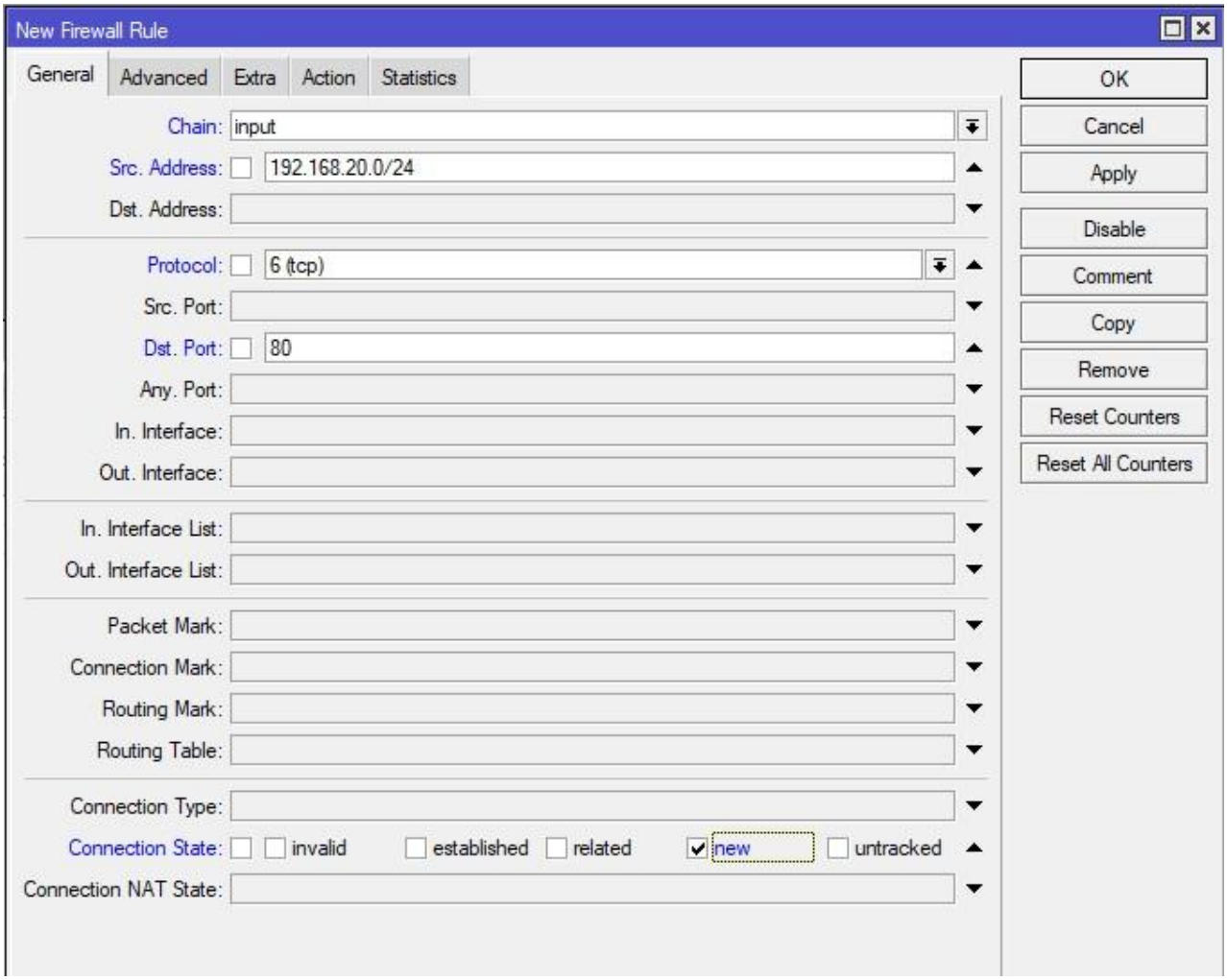


Интерпретируем правило: если есть новое соединение с любого адреса на роутер по протоколу TCP на порт 2222 или 58291 — разрешить. Обязательно комментируем правило в списке правил.Почему именно новое соединение? Ответ узнаем дальше.

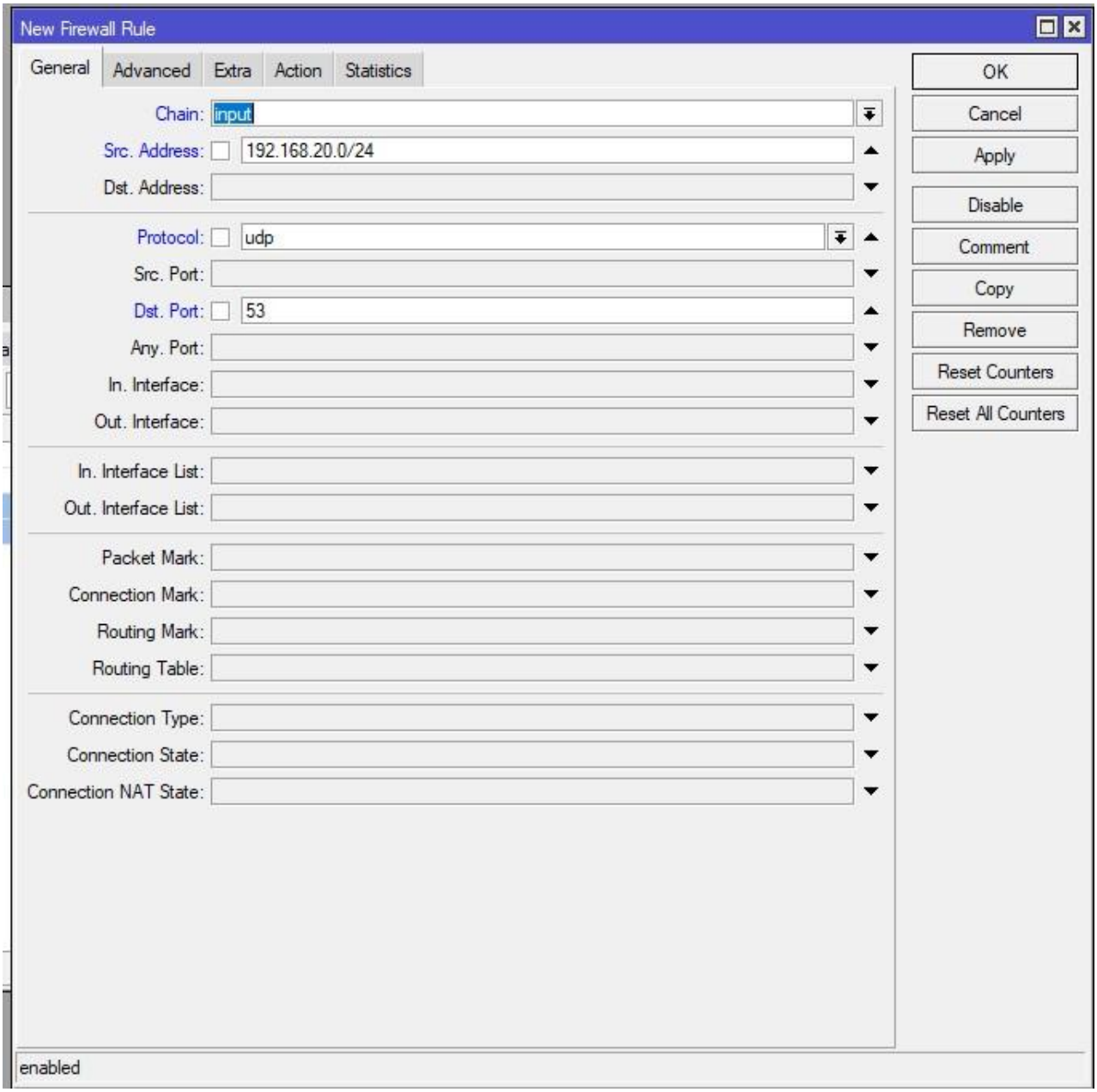


Далее разрешим input на 80 порт с ЛВС.

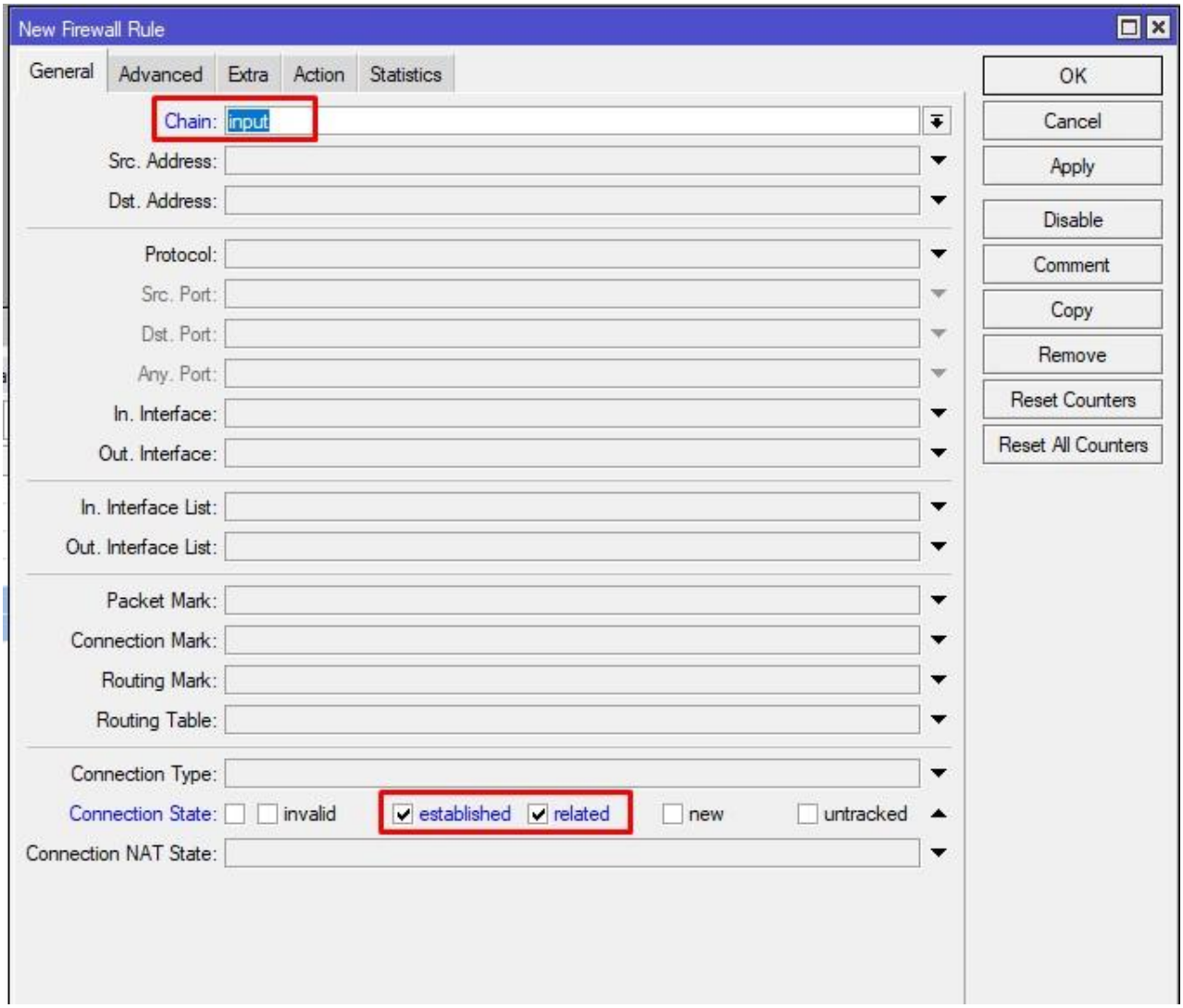




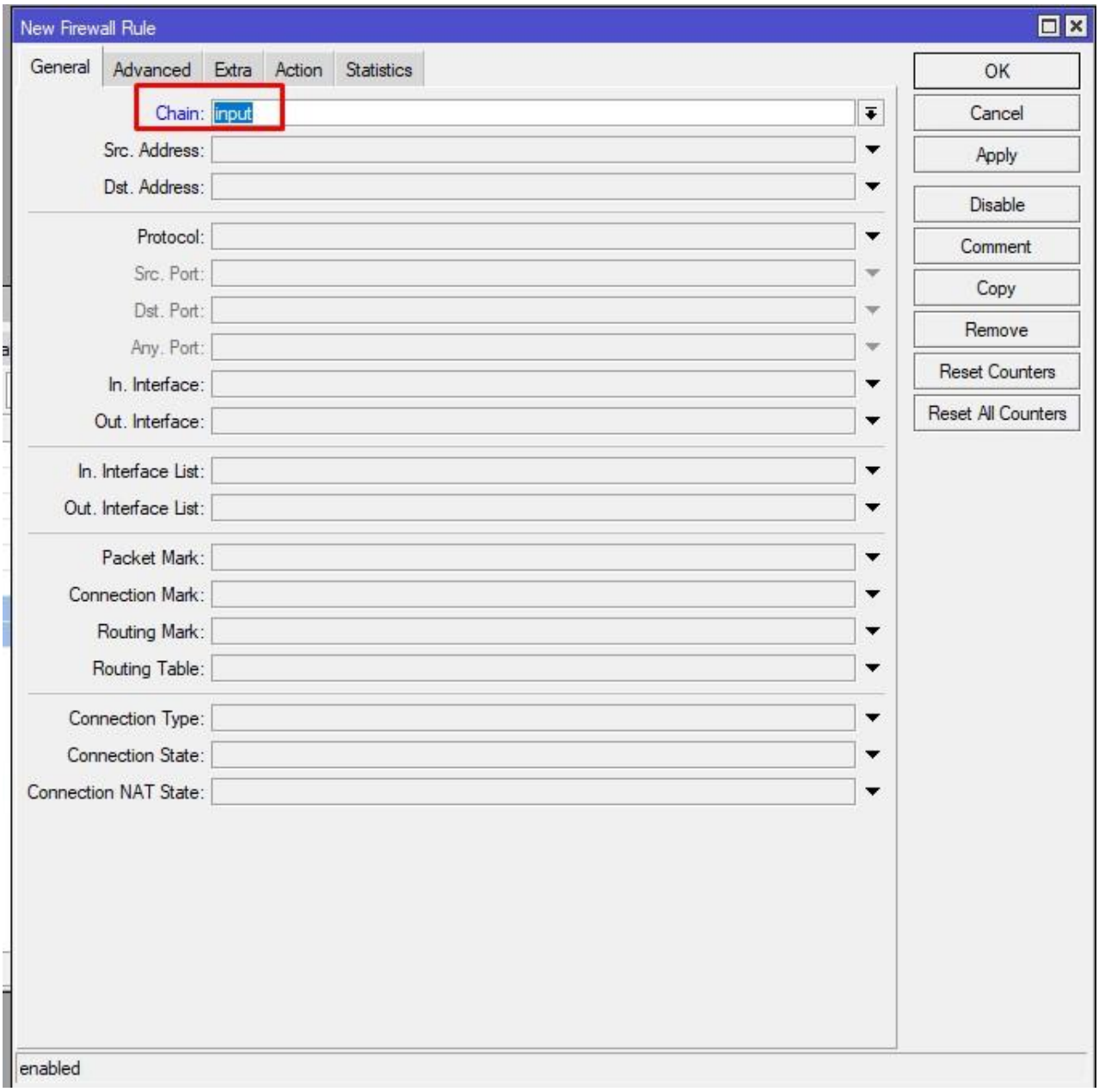
Если новое соединение с 192.168.20.0/24 по TCP на 80 порт – разрешить.Далее нужно разрешить DNS. Он может работать как по TCP, так и по UDP, наш случай это UDP, т.к. запросы на разрешение имен идут именно по UDP.

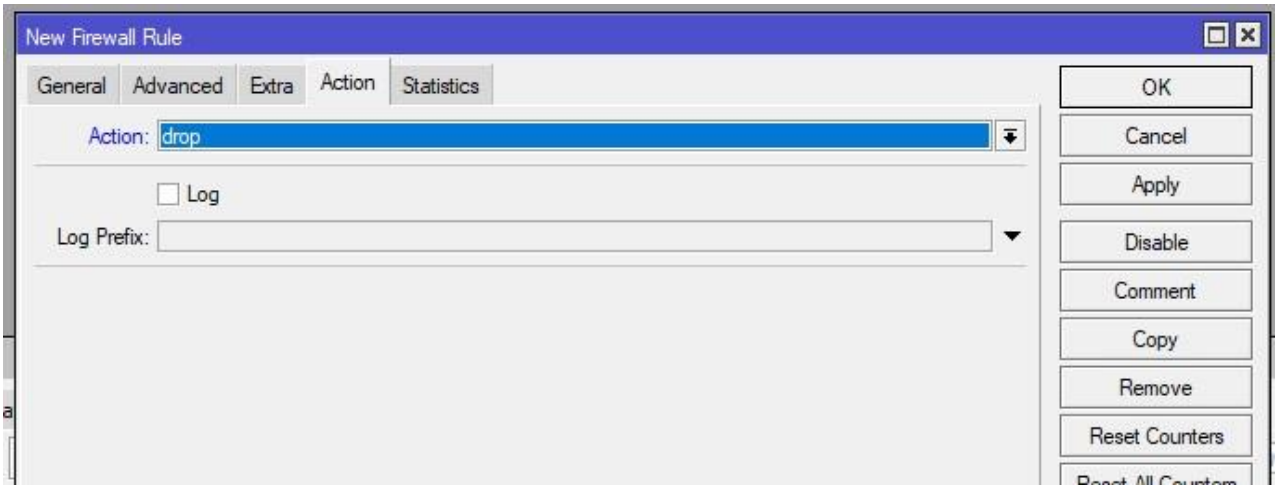


Обратите внимание, что мы разрешаем весь трафик по UDP:53 с 192.168.20.0/24, это связанно с тем, что данный протокол не поддерживает установку соединения и подтверждение получения каждого пакета, поэтому ставить Connection State – New бессмысленно.Создаем следующее правило.

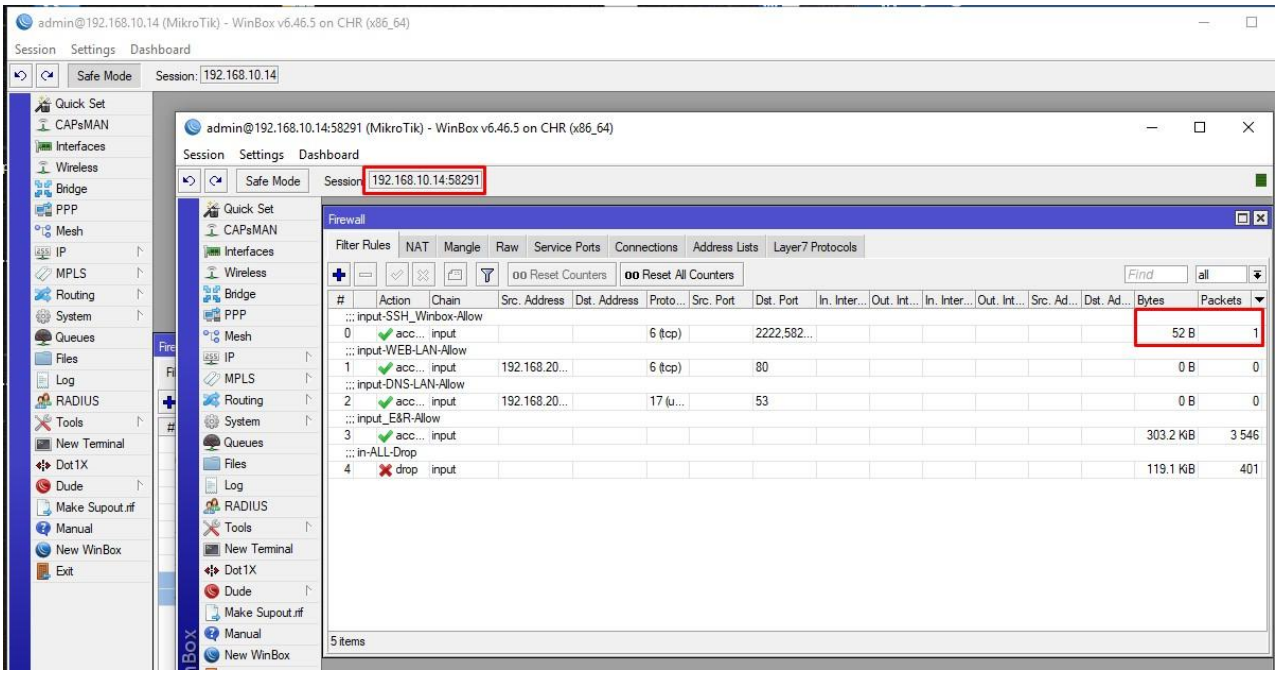


Любое связанное и установившееся входящее соединение разрешить. Дело все в том, что Mikrotik понимает все входящие, исходящие и транзитные соединения. Т.к. мы хотим оптимизировать нагрузку на устройство, то создаем данное правило, иначе ранее созданные правила будут работать только на новые соединения, 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.

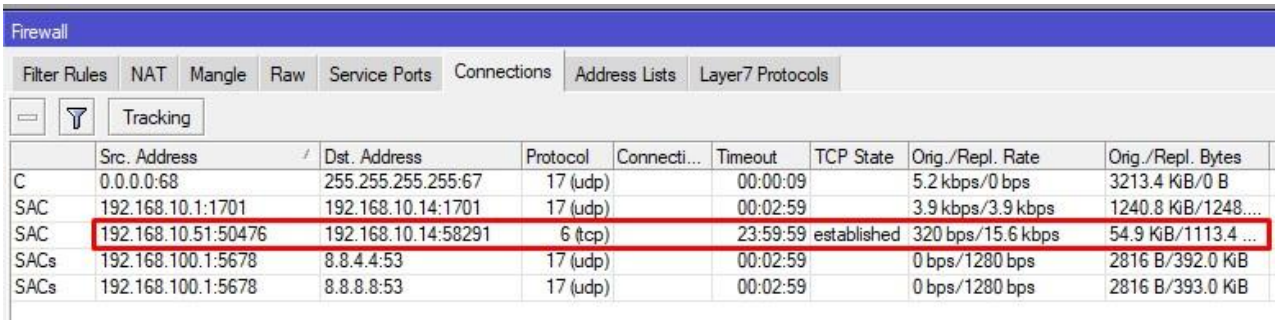




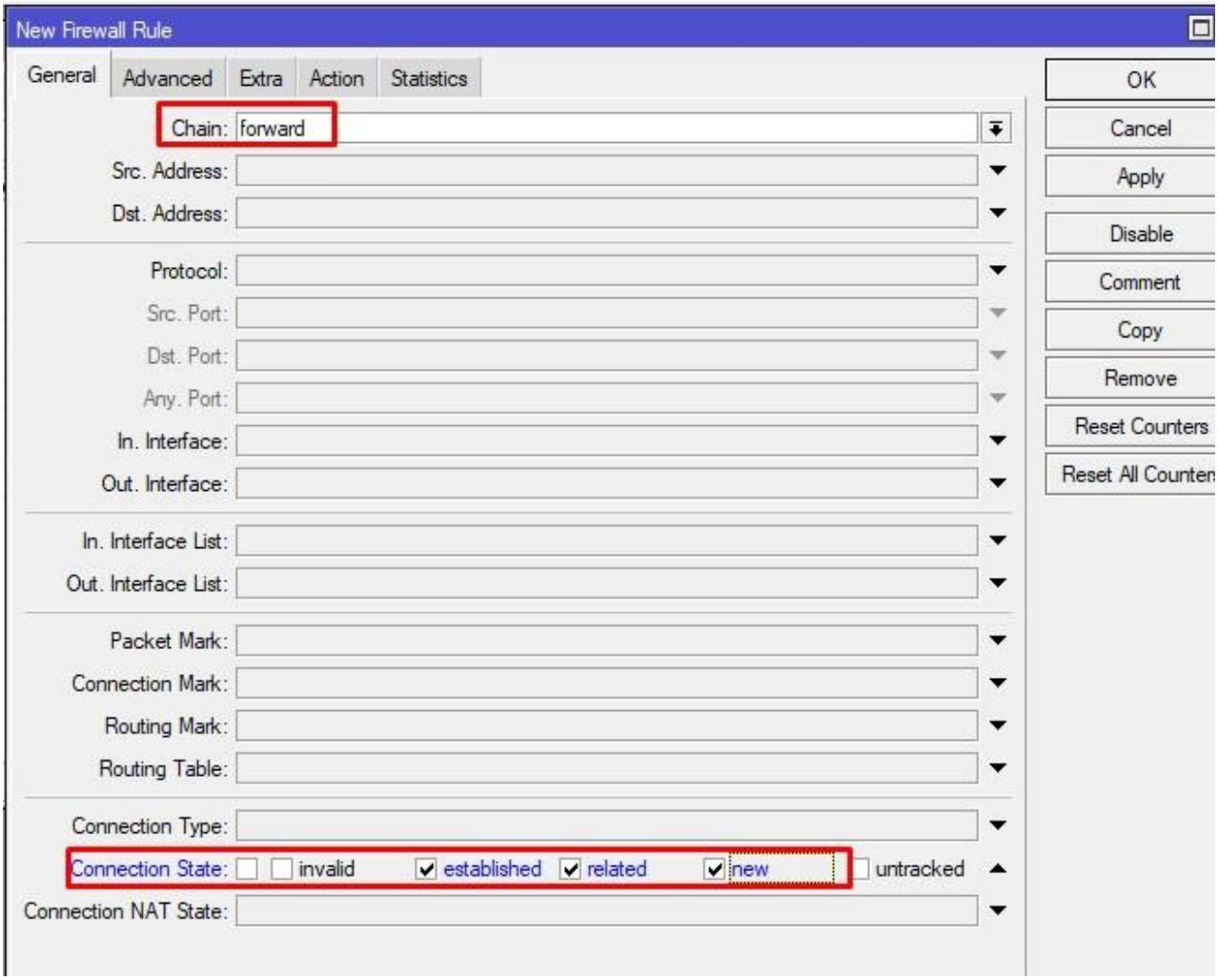
Попробуем подключиться к устройству по нестандартным портам Winbox не отпуская Safe Mode.



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 помешало подключению (подошел логин пароль, нет запрещающих правил и др.) соединение превратилось в устоявшееся.

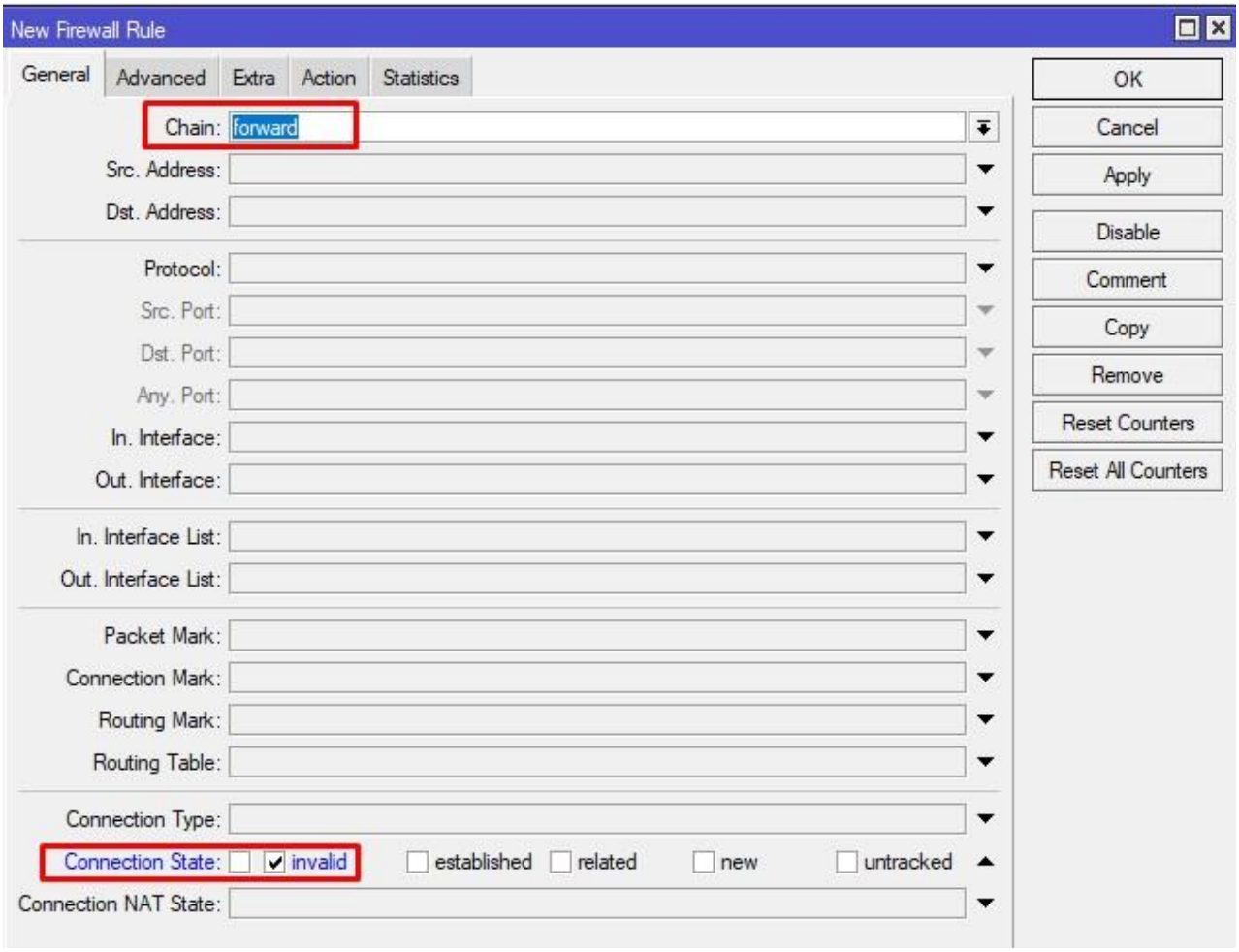


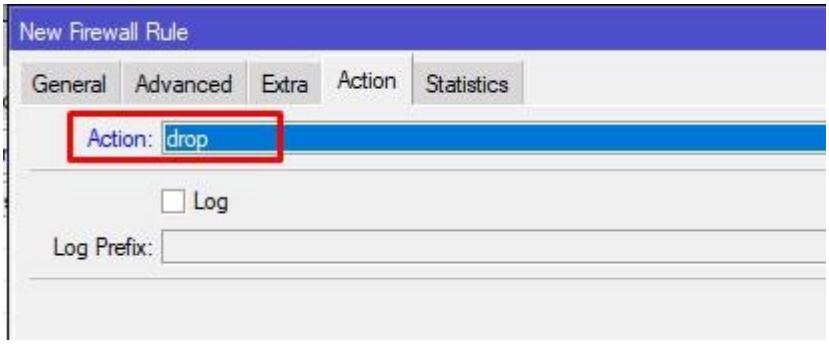
Настроим правила пересылки. Если у вас нет особенных требования для этого, то будет достаточно двух правил. Разрешим новые, устоявшиеся и зависимые соединения.



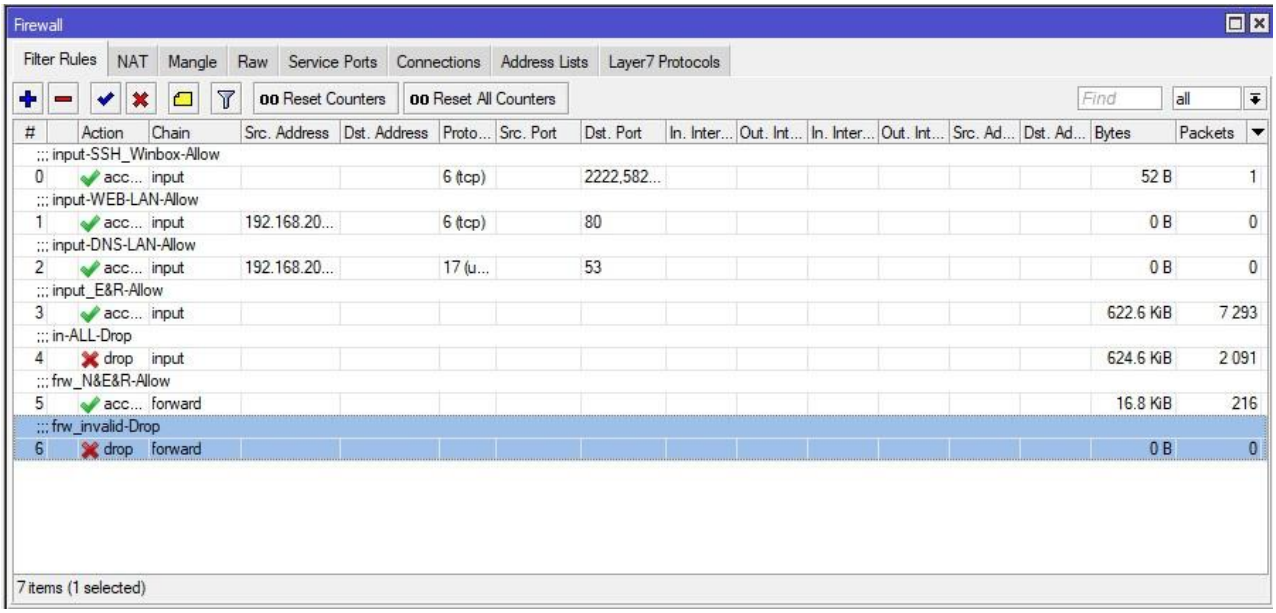
Запретим invalid.

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





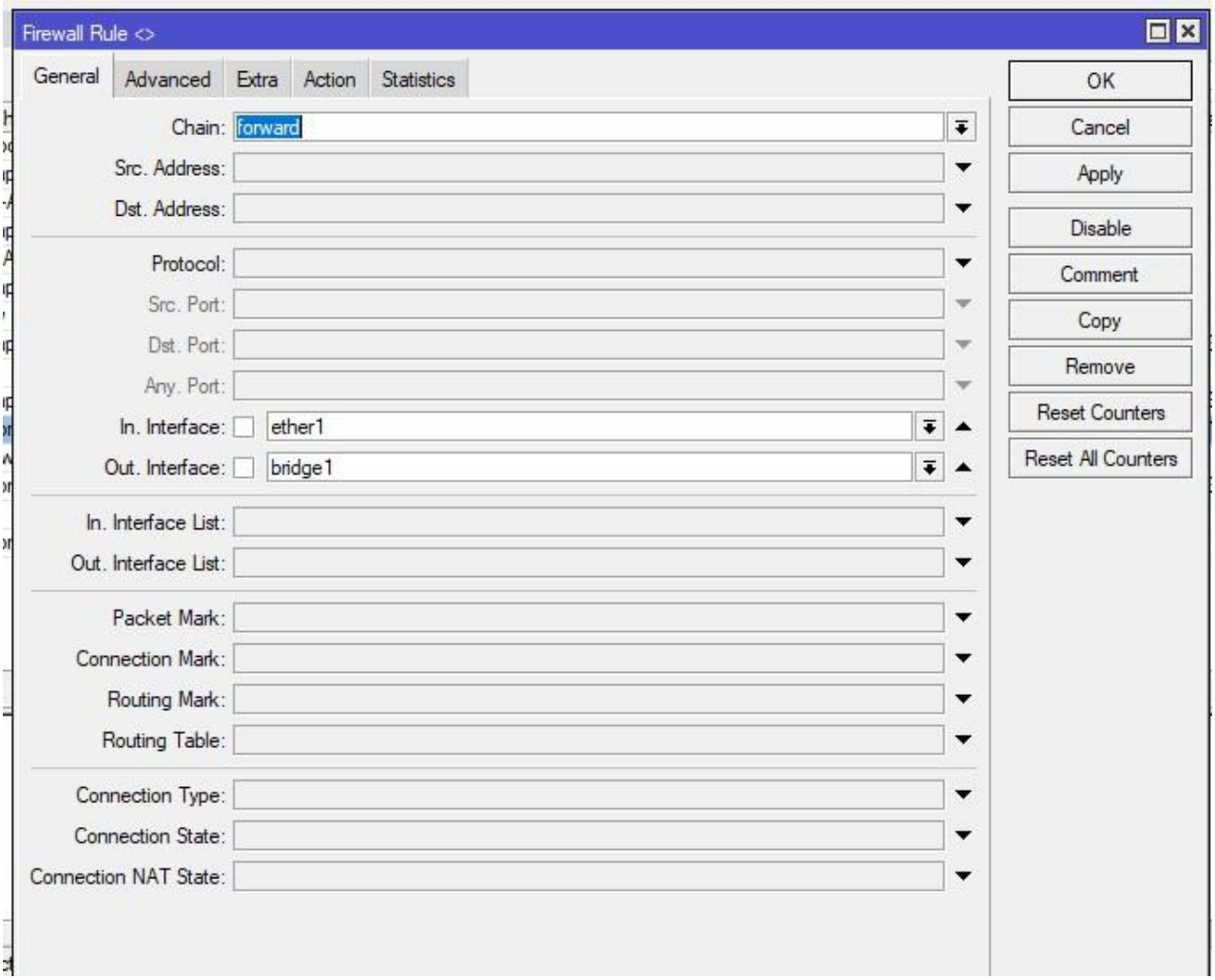
Давайте взглянем на список созданных правил.

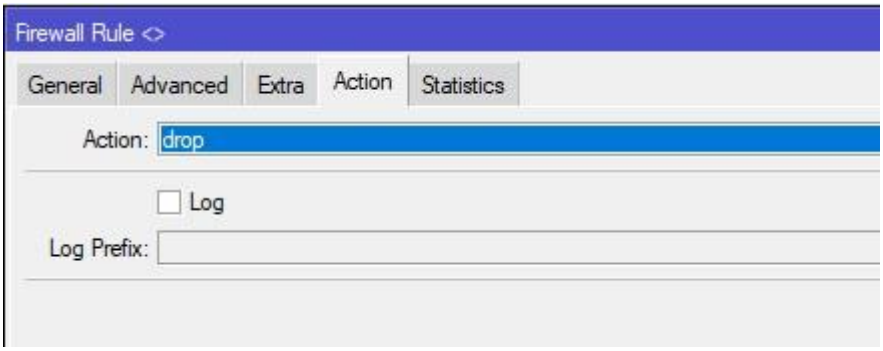


Читая комментарии, можно примерно понять, что настроено. Используйте их, если конечно не хотите усложнять жизнь себе и другим.

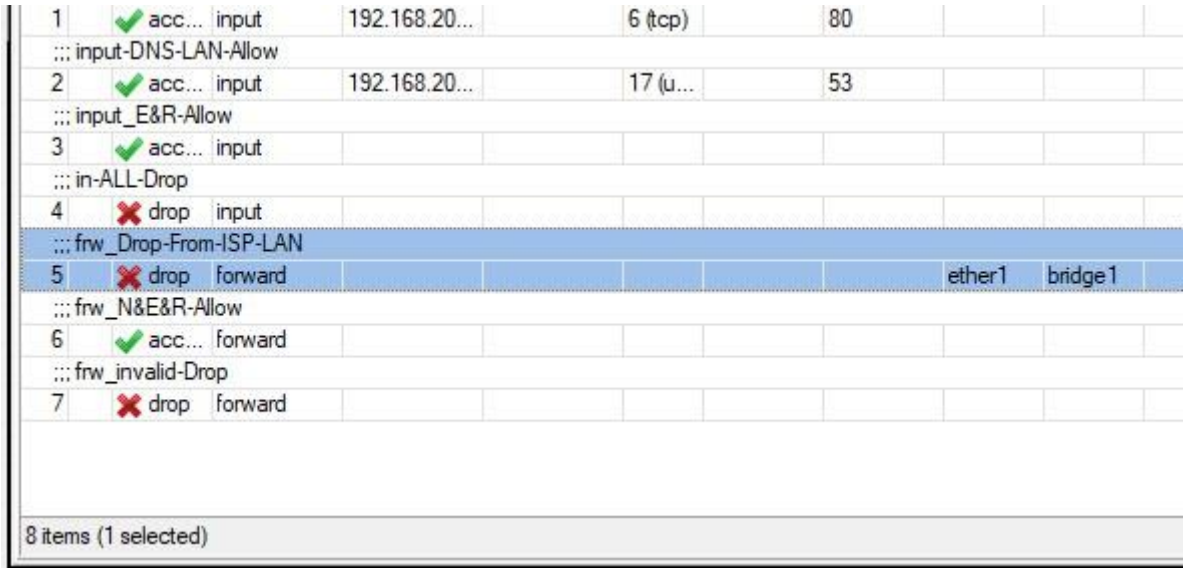
Защита локальной сети от атак из сети провайдера

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.



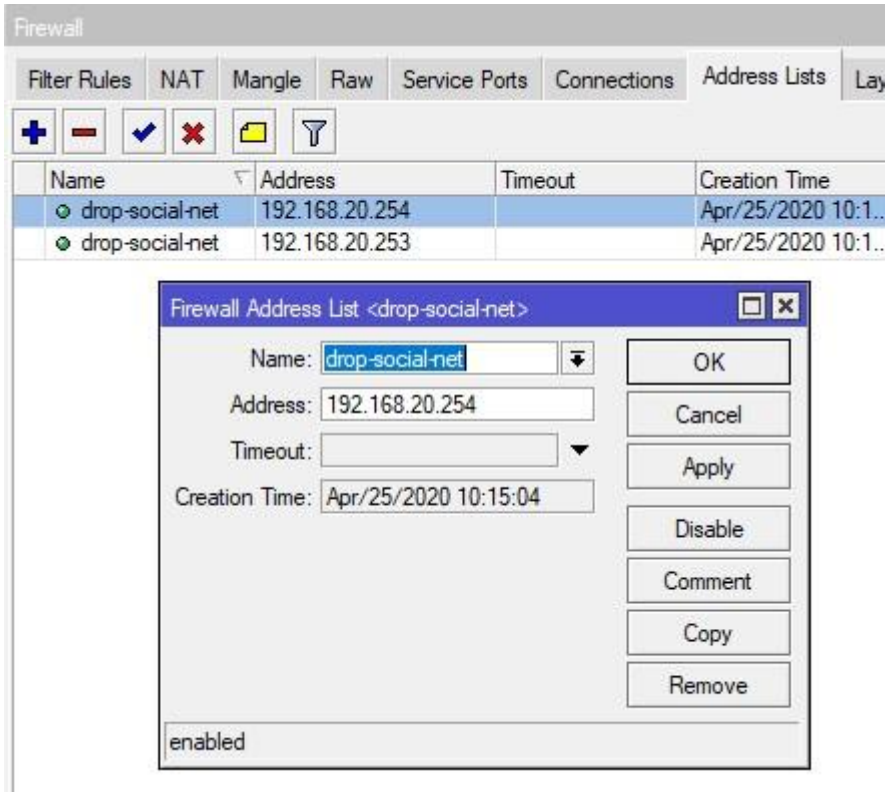


Поместим его выше разрешающего правила пересылки.

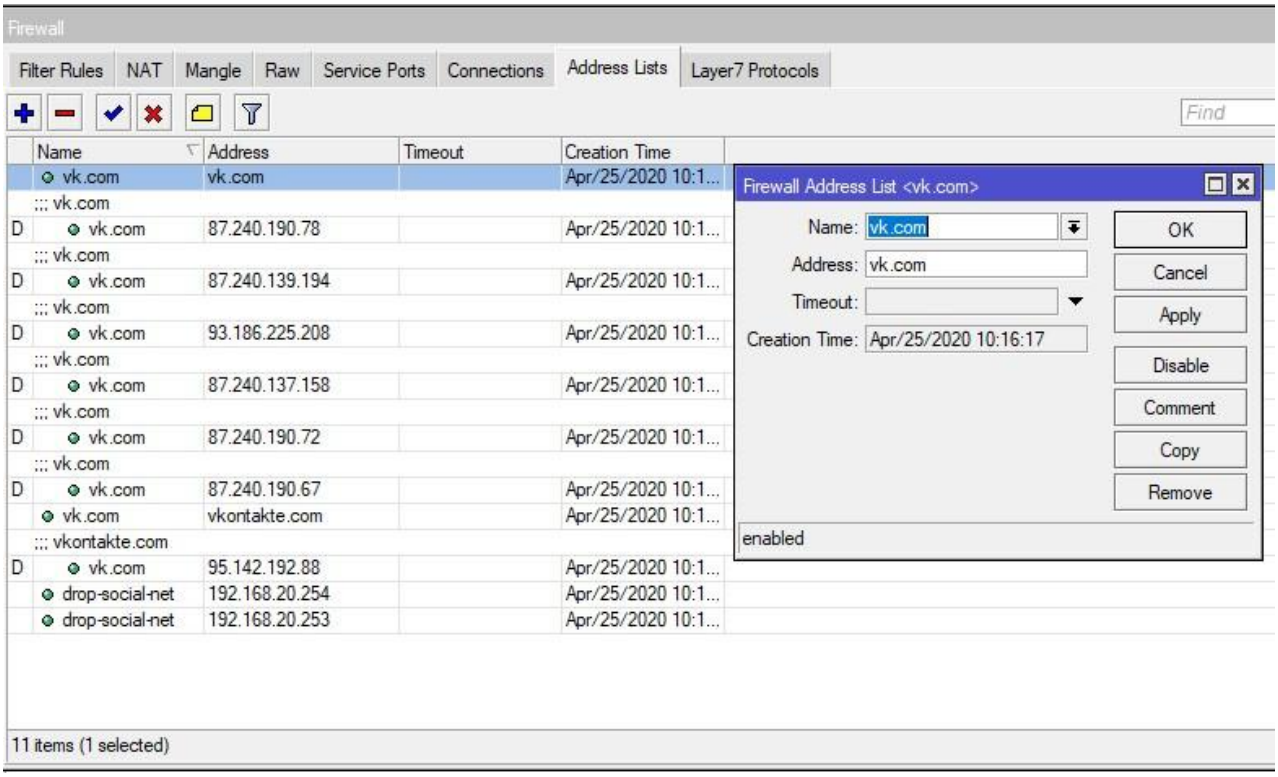


Блокировка соц сетей на Mikrotik с помощью Address List и Firewall

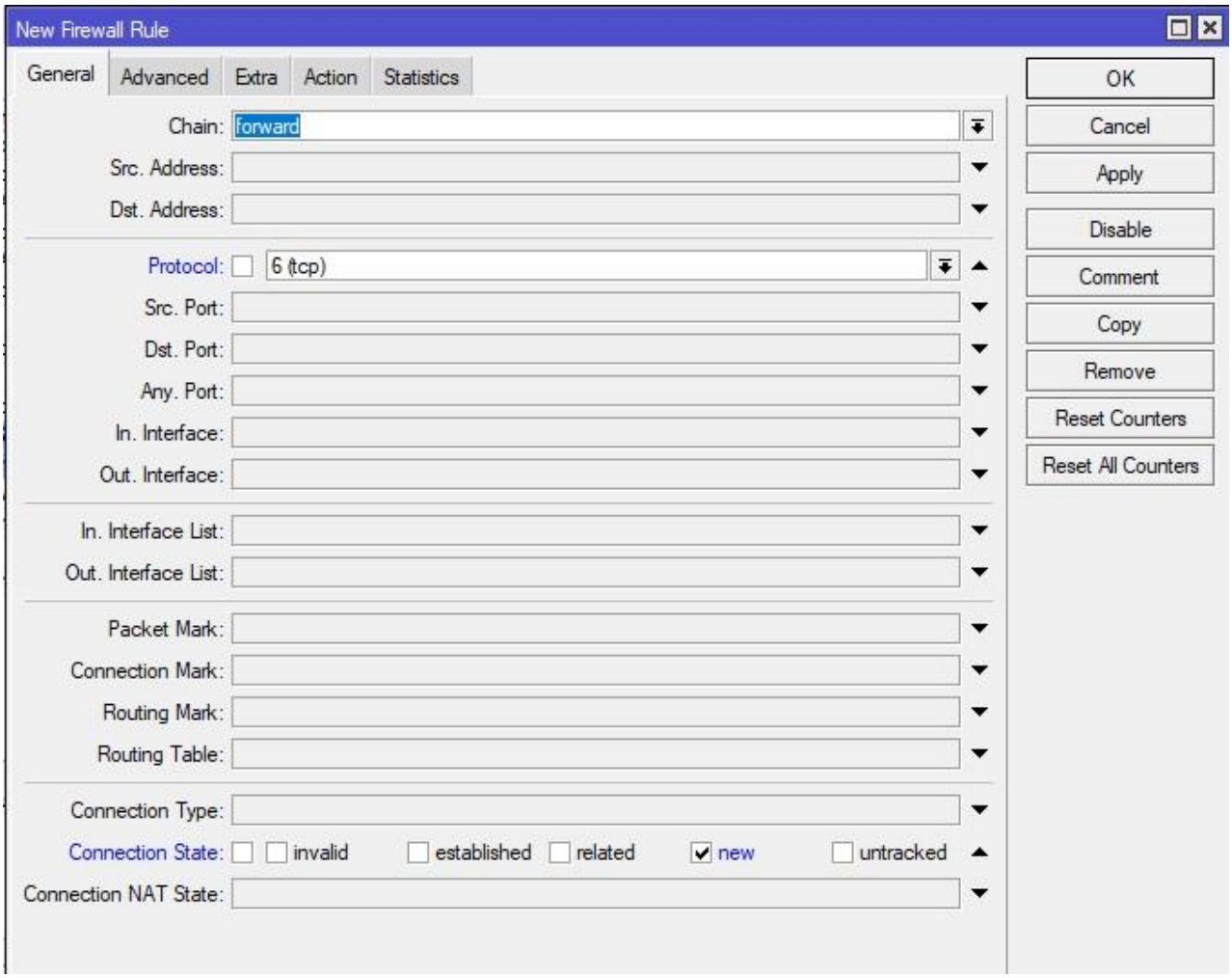
RouterOS есть функционал Address List. Он может содержать подсеть, конкретный адрес или доменное имя. Ниже я покажу как заблокировать vk.com. Есть условие, заблокировать доступ с 192.168.20.254 и 192.168.20.253. Открываем IP – Firewall – Address List. Создадим новые листы.Первый лист, будет содержать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



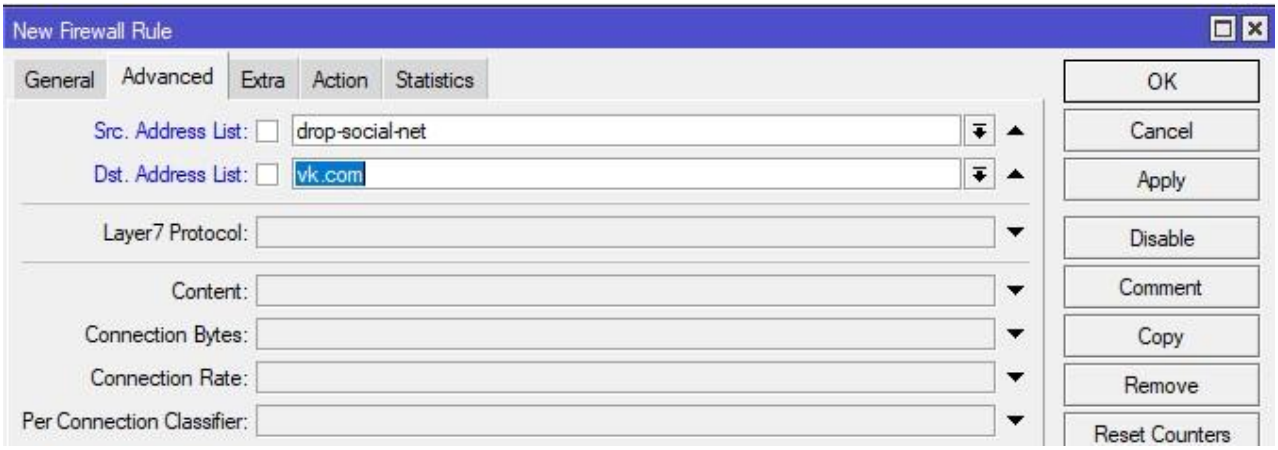
Вторым, vk.com. Задаем доменные имена.



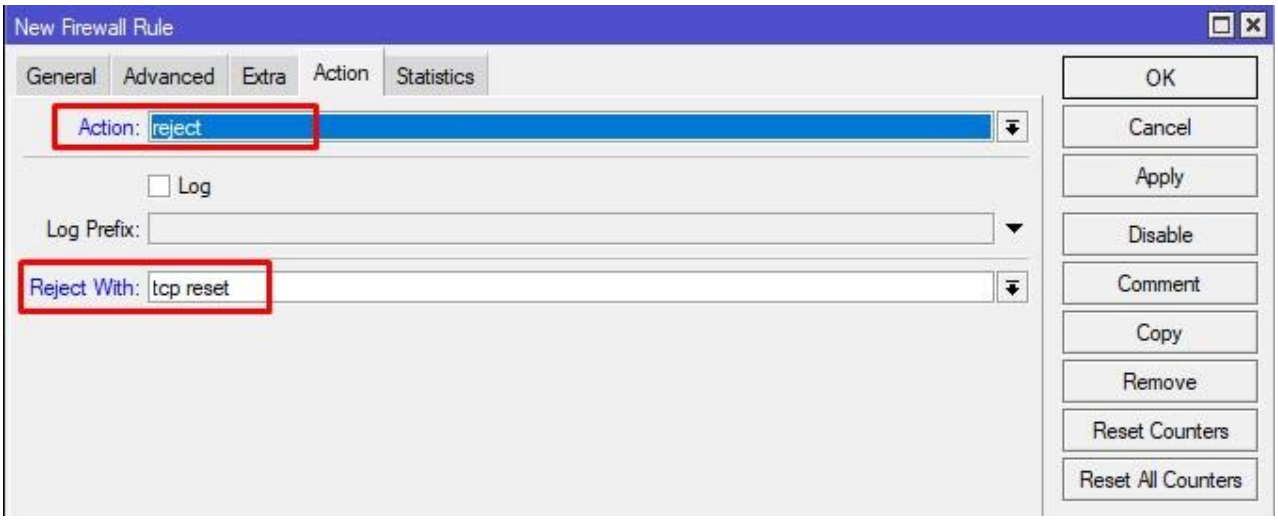
После создания, роутер отрезолвит имя на тех серверах, что указаны в DNS и добавит в адрес лист. Далее простым правилом цепочки forward запрещаем пересылку из одного листа в другой. Чтобы пользователь не ждал долго, а получал отбойник что соединение разорвано укажем некоторые уточнения. Если новый транзитный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



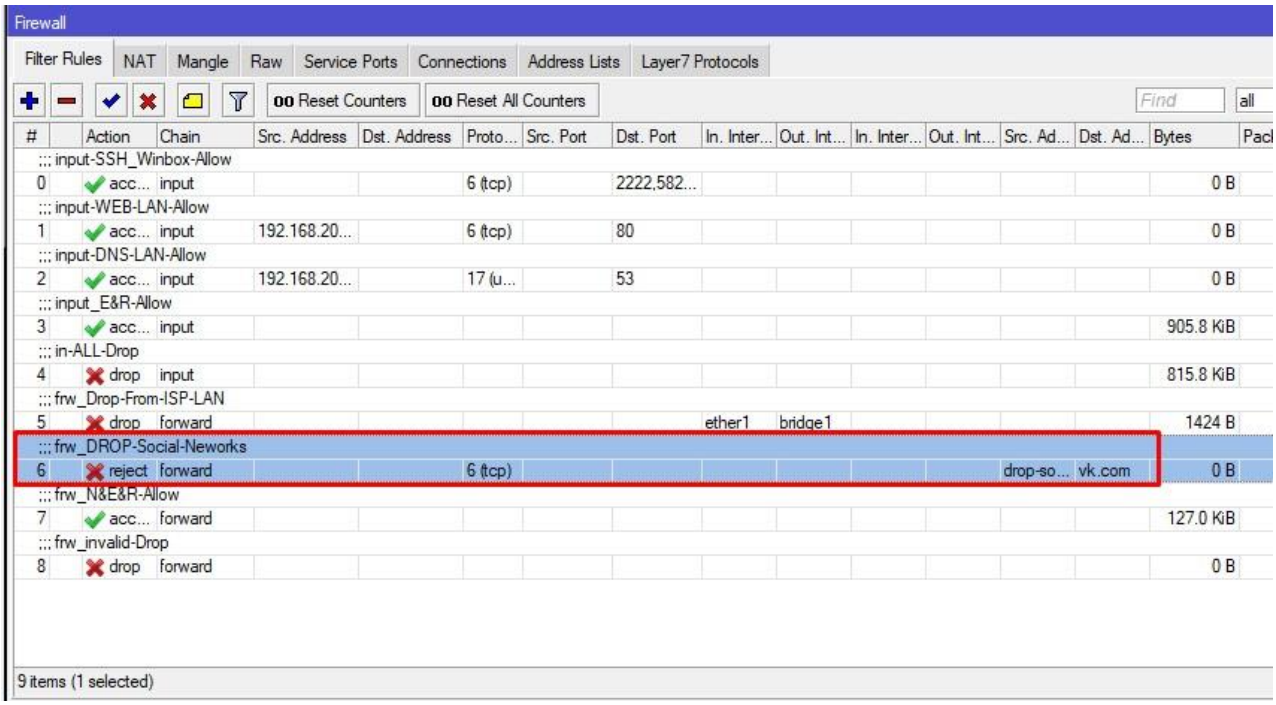
И пересылка происходит из одного листа в другой.



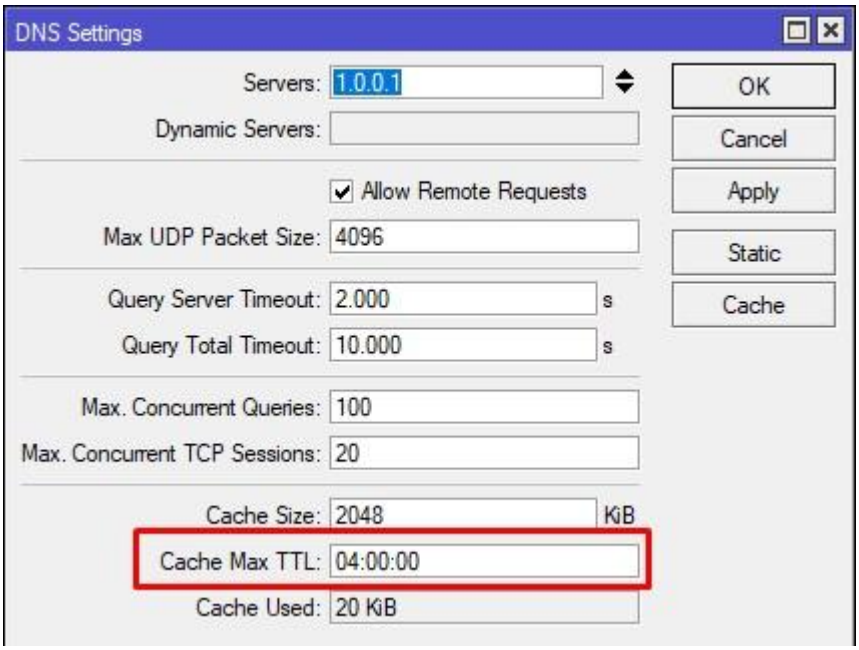
То говорим, что соединение было сброшено.



Не забываем поместить его выше разрешающего правила пересылки.



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.



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.