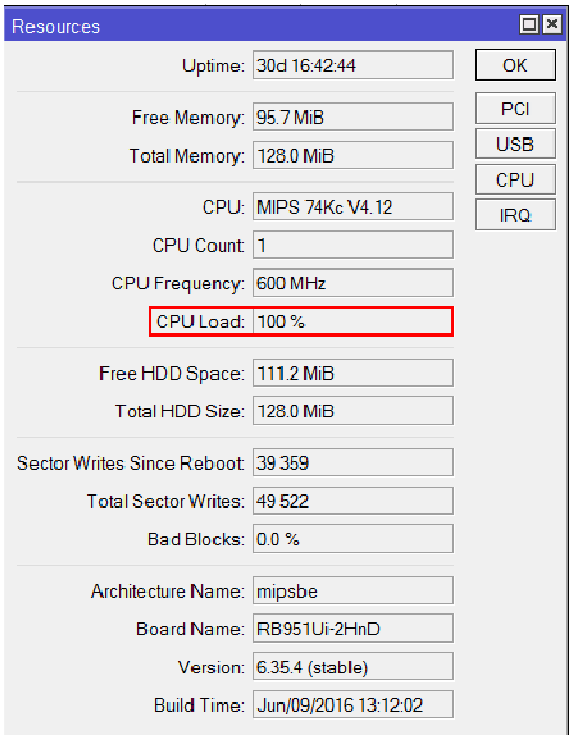
Высокая загрузка процессора Mikrotik. Что делать - DNS flood

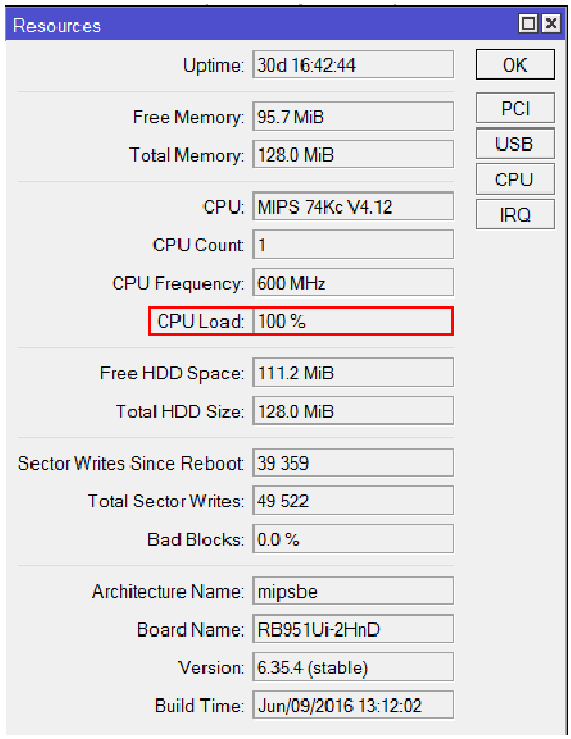
Отражаем атаки

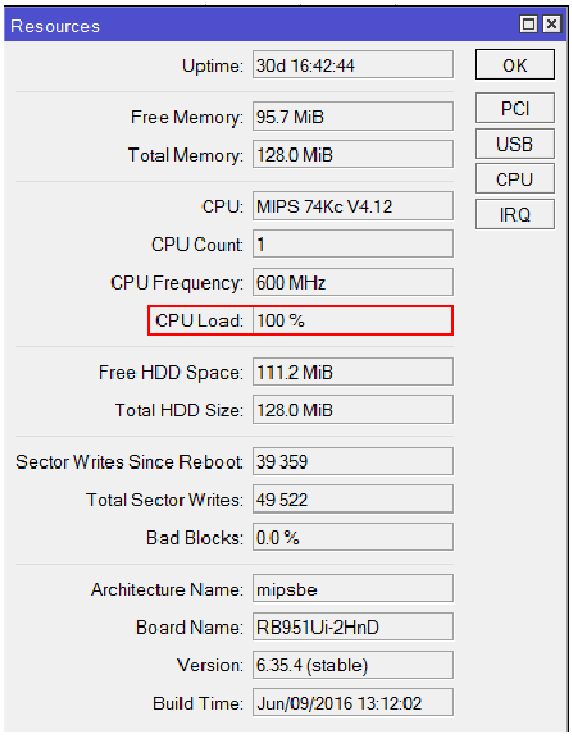
https://wiki.merionet.ru/seti/4/vysokaya-zagruzka-processora-mikrotik-chto-delat/

Сетевое оборудование вендора **Mikrotik** является весьма любопытным и привлекательным продуктом в сегменте SOHO (Small office/home office). Соотношение цены, качества, функционала и стабильности обеспечивает все большее распространение небольших белых коробочек в офисах небольших компаний.

Но спустя какое-то время беззаботного пользования, пользователи начинают жаловаться. Администратор, открыв **Winbox**, переходит в раздел **System** → **Resources** и видит, что загрузка процессора 100%:



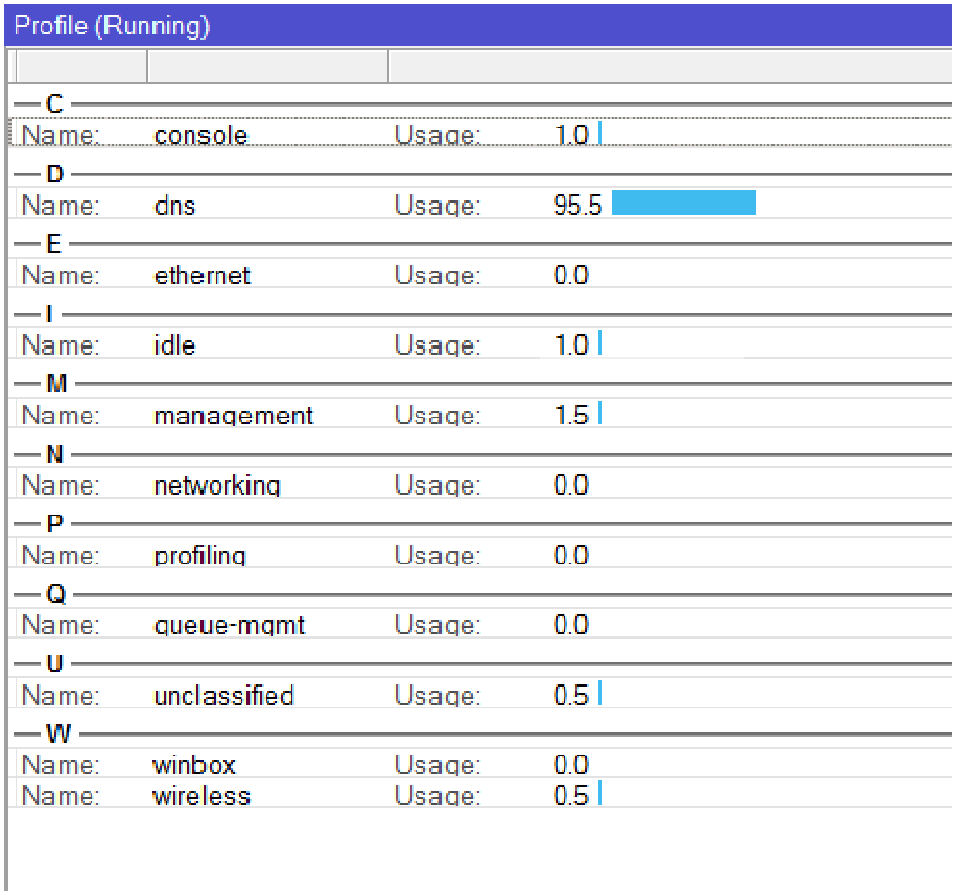




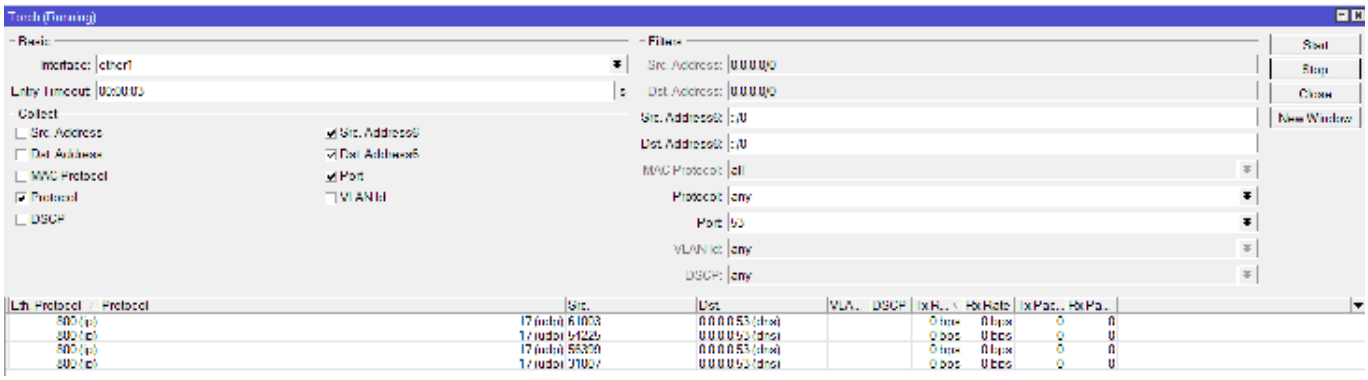
Не стоит волноваться. У нас есть решение. Все настройки и «траблшутинг» будем осуществлять с помощью Winbox.

Настройка Firewall в Mikrotik

Первым делом давайте проверим службу, которая больше всего «отъедает» ресурсов процессор. Для этого, перейдем в раздел **Tools** → **Profile**:



Как видно из скриншота, львиную долю ресурсов нашего процессора занимает служба DNS. Давайте посмотрим, что происходит на уровне обмена пакетами на основном интерфейс ether1. Для этого воспользуемся утилитой **Tools** → **Torch**:

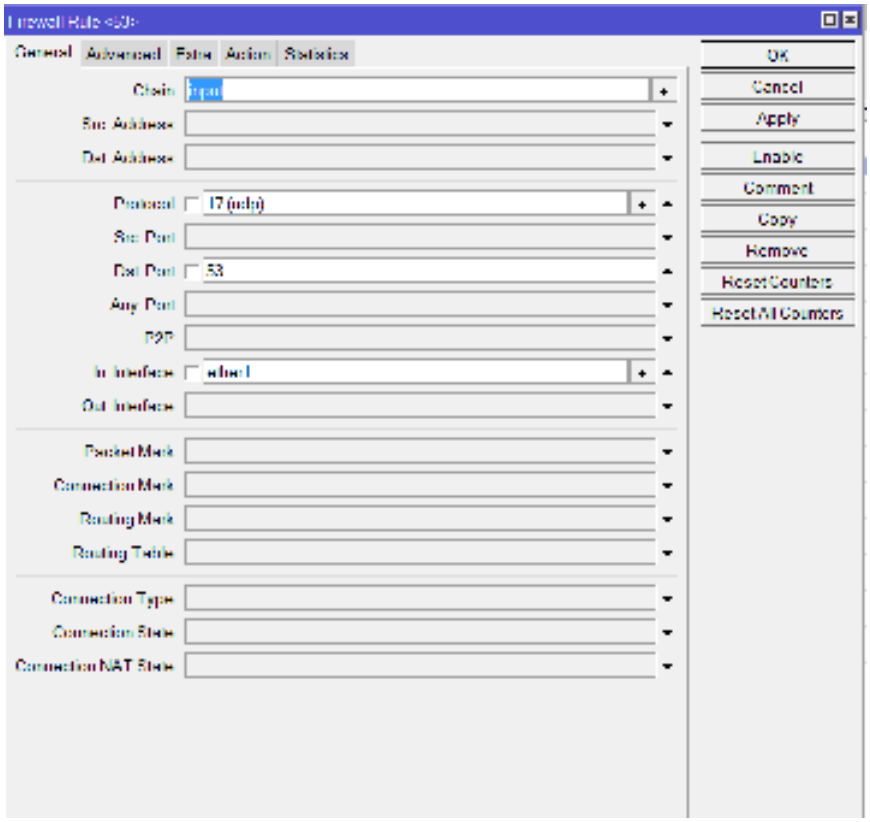


Мы видим большое количество пакетов с различных IP – адресов на 53 порт. Наш Mikrotik отвечает на каждый из таких запросов, тем самым, нерационально используя ресурсы процессора и повышая температуру.

Эту проблему надо решать. Судя по снятому дампу, пакеты приходят с частотой 10-20 секунд с одного IP – адреса. Добавим в наш Firewall два правила:

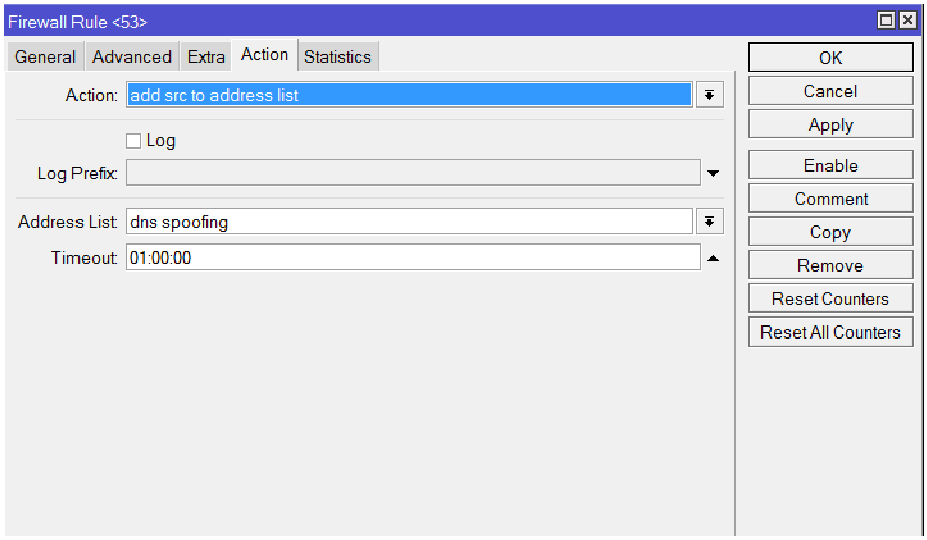
1. Все IP – адреса, пакеты с которых приходят на 53 порт нашего Микротика будут помещаться в специальный лист с названием **dns spoofing** на 1 час.
2. Каждый IP – адрес, с которого будет поступать запрос на 53 порт будет проверяться на предмет нахождения в списке dns spoofing . Если он там есть, мы будем считать, что это DNS – спуфинг с частотой реже чем раз в час и будем дропать данный пакет.

Переходим к настройке. В разделе **IP** → **Firewall** → **Filter Rules** создаем первое правило нажав на значок «+». Во кладке **General** указываем следующие параметры:



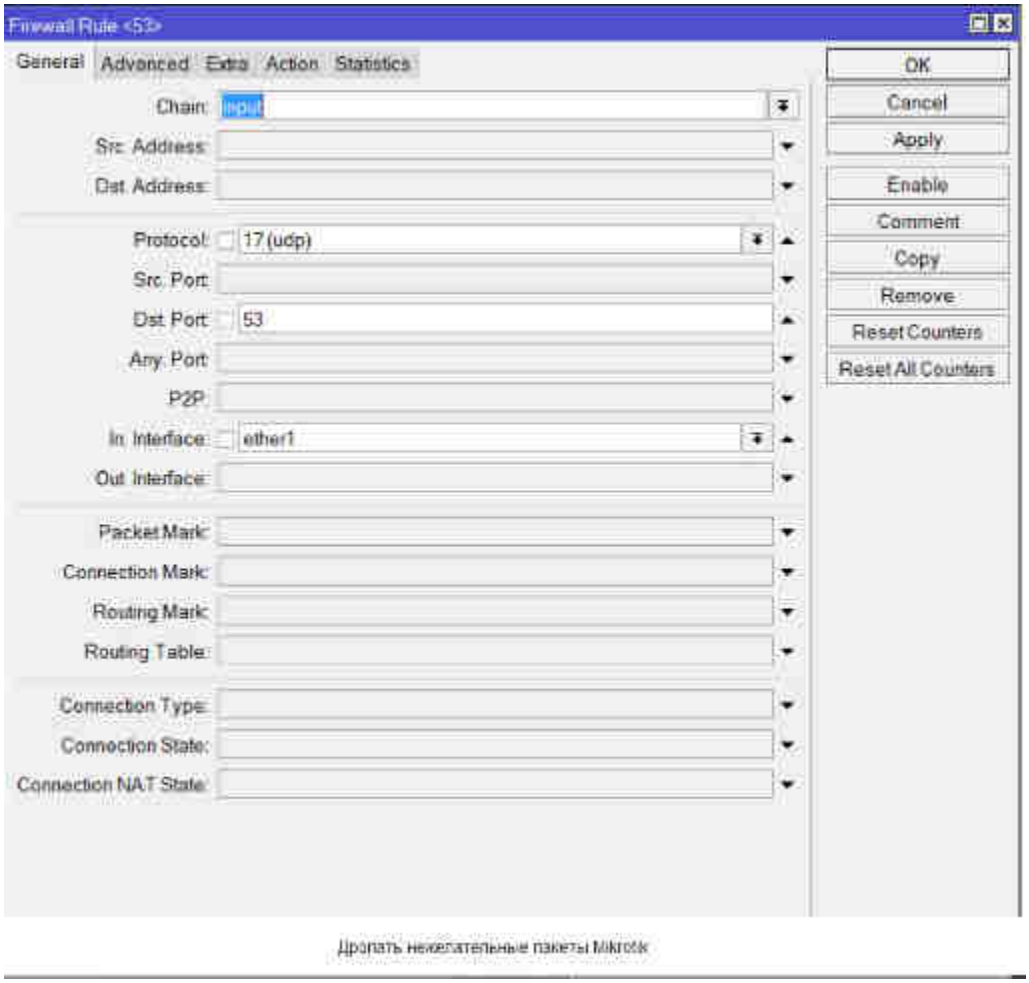
- **Chain = input** - обрабатываем приходящие пакеты
- **Protocol = UDP** - нас интересуют пакеты, у которых в качестве транспорта используется UDP
- **Dst. Port = 53** - портом назначения должен быть 53 порт, то есть DNS служба
- **In. Interface = ether1** - проверка подвергаются все пакеты, которые приходят на интерфейс ether1, который смотрит в публичную сеть.

Переходим во вкладку **Action**:



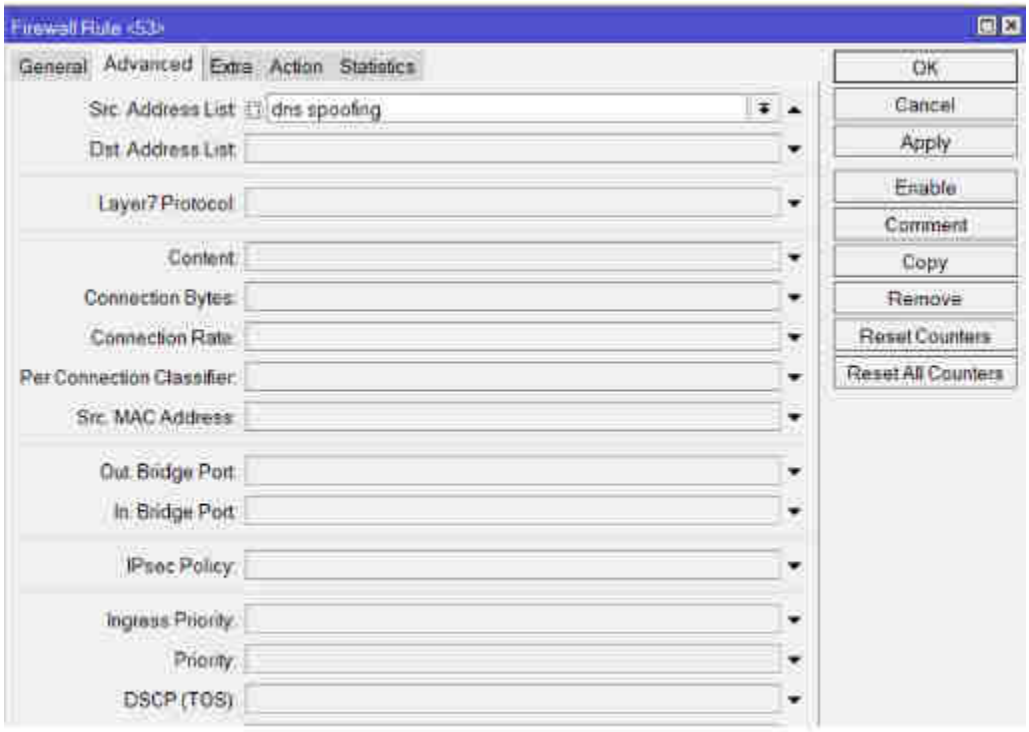
- **Action = add src to address list** - в качестве действия, мы будем добавлять IP – адрес источника в специальный лист
- **Address List = dns spoofing** - указываем имя листа, в который добавляем IP
- **Timeout = 01:00:00** - добавляем на 1 час

Нажимаем **Apply** и **OK**. Настроим второе правило, так же нажав на «+»:



Дропать нежелательные пакеты Mikrotik

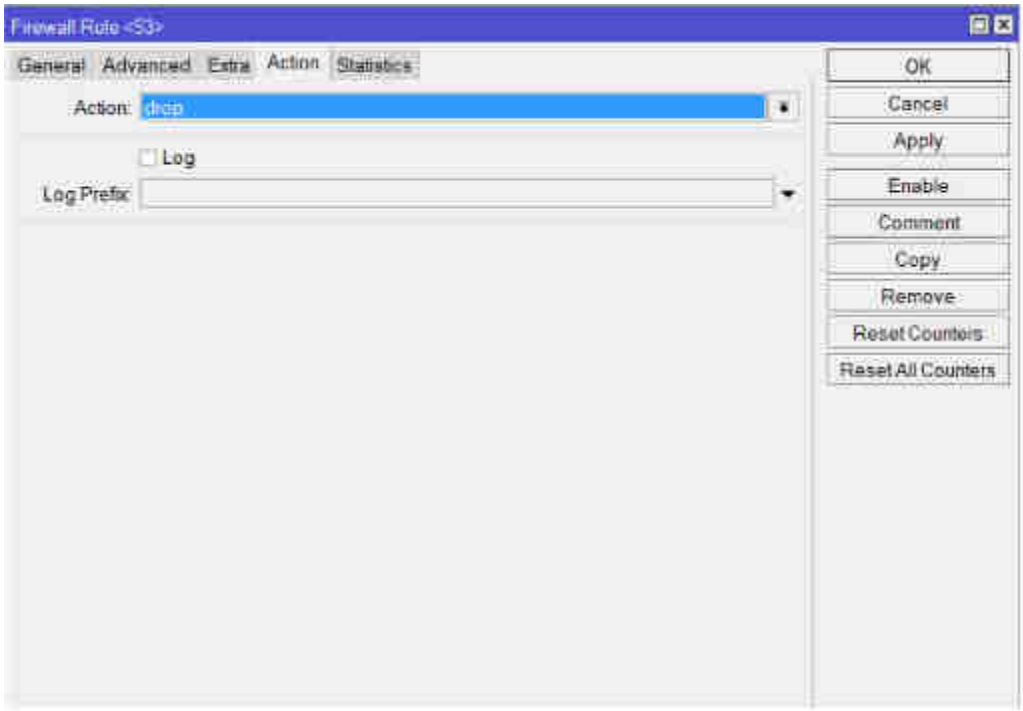
Как видно, настройки во вкладке **General** в данной вкладке идентичны первому правилу. Нажимаем на вкладку **Advanced**:



Action Drop Mikrotik

- **Src. Address List= dns spoofing** - указываем Микротику, производить проверку приходящего пакета на предмет нахождения в указанном листе

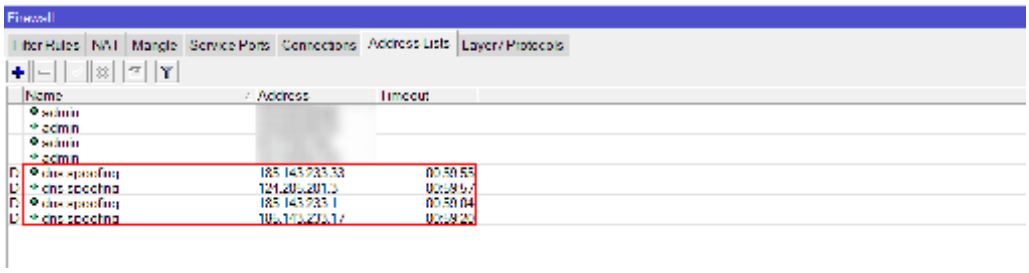
Переходим во вкладку **Action**:



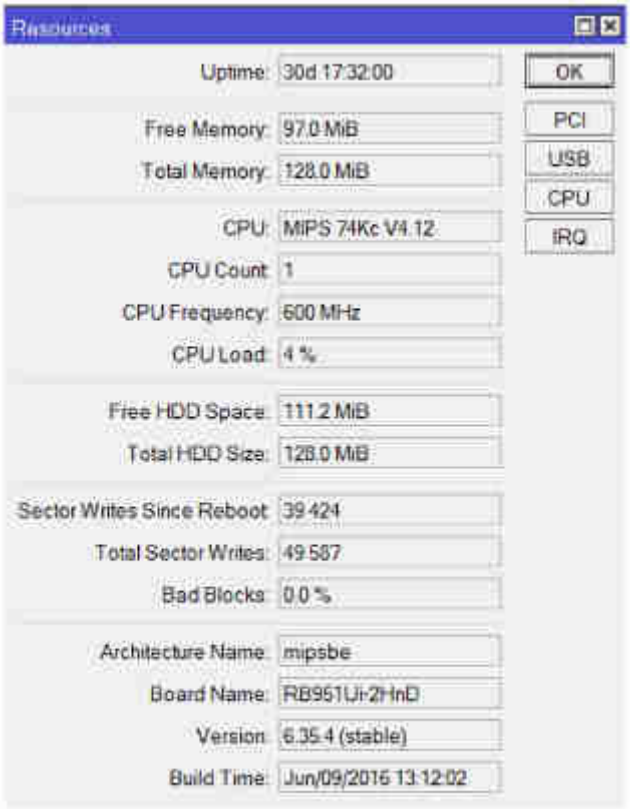
Action Drop Mikrotik

- **Action = drop** - если IP – адрес пакета есть в указанном списке, то дропаем этот пакет.

После того, как оба правила стали активны переходи во вкладку **IP** → **Firewall** → **Address Lists**:



Как видно, адреса стали добавляться в список на 1 час. Теперь давайте проверим загрузку процессора:



Проблема с загрузкой процессора на Mikrotik решена

Теперь загрузка процессора в пределах нормы. Проблема решена.