RouterOS — сетевая операционная система на базе Linux установлена на всех маршрутизаторах Mikrotik.
Устройства компании Mikrotik стали широко распространены из-за своей цены по отношению к функционалу. Но и ошибки в программном обеспечении никто не отменял.

Инструкция как закрыть самые опасные уязвимости RouterOS.

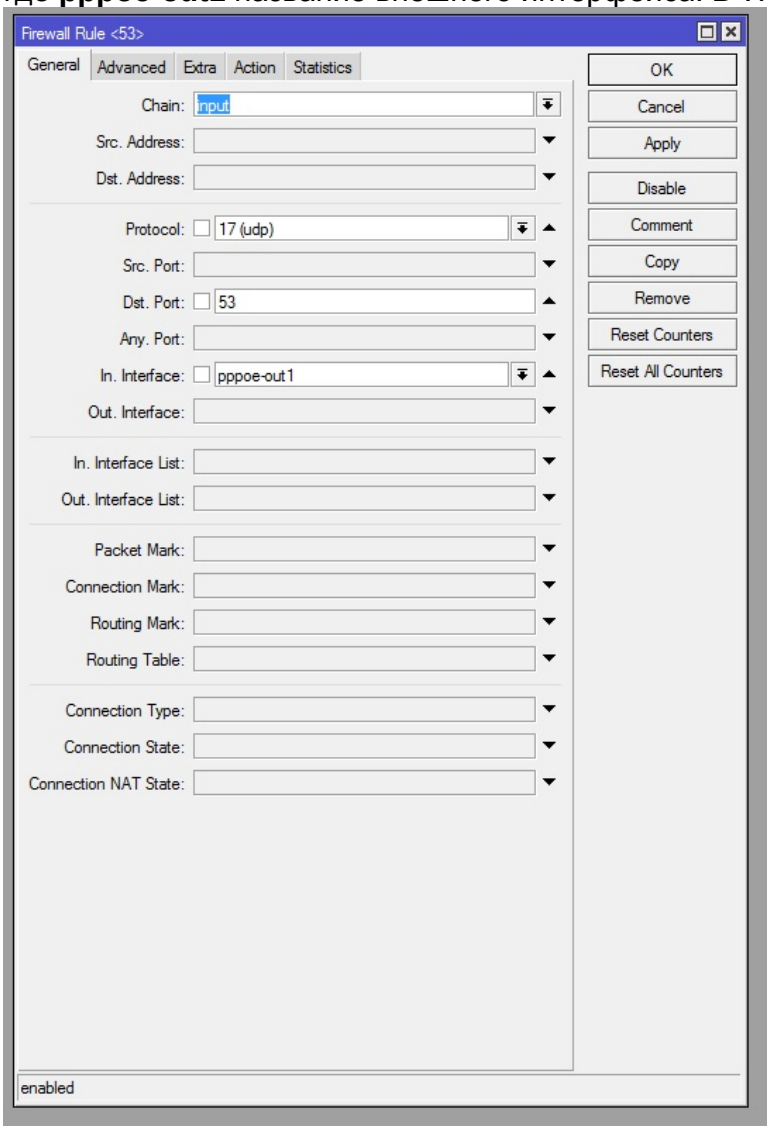
1. DNS-UDP-53порт:

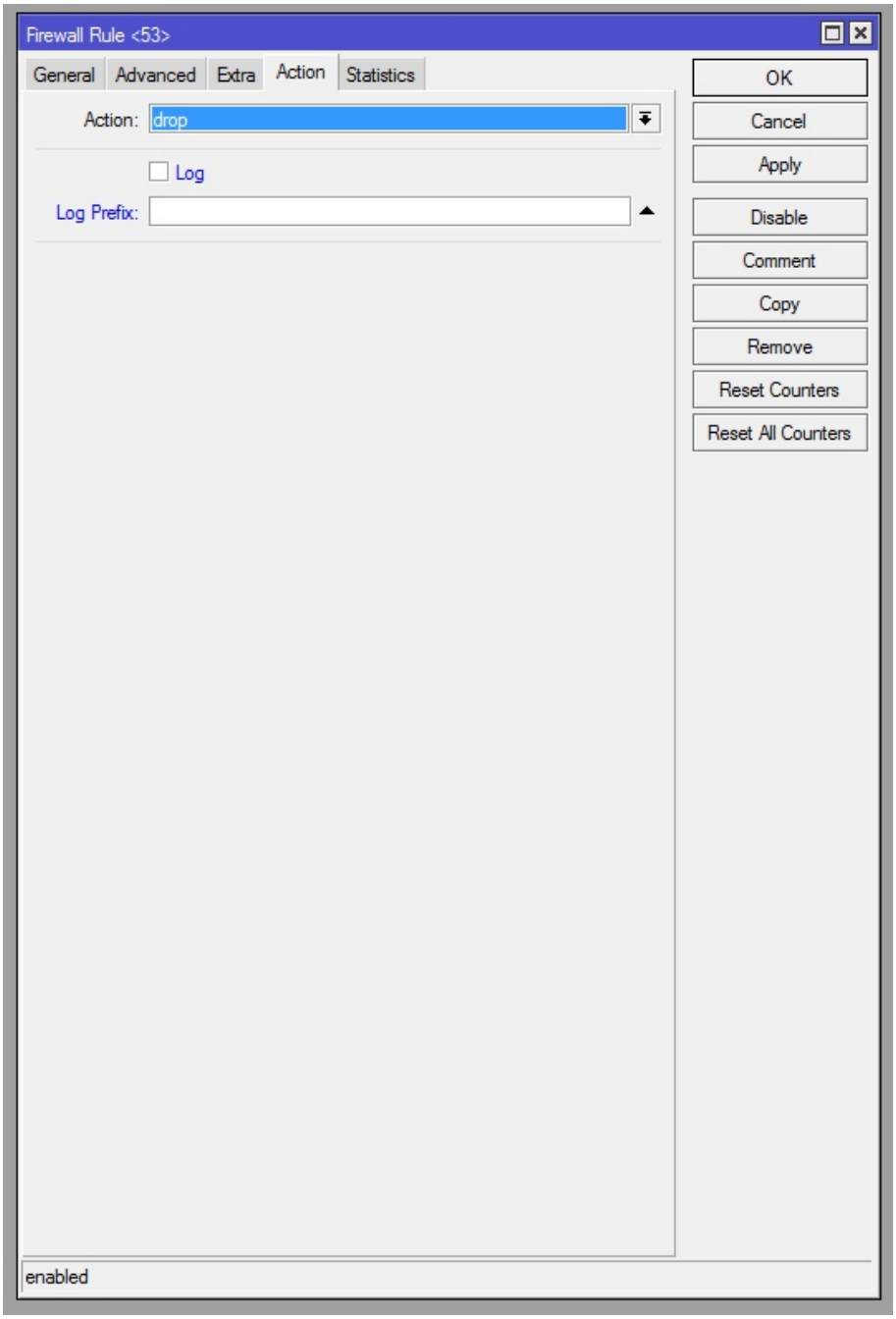
По умолчанию 53 порт открыт на ВСЕХ интерфейсах, в том числе из глобального интернета. Рано или поздно, у Mikrotik с белым ip адресом, можно заметить нагрузку на процессор и утечку трафика, которая вызвана внешними запросами к Вашему DNS серверу.

Есть отличное решение данной проблемы. Необходимо добавить правило в **IP — Firewall — Filter Rules**:

/ip firewall filter
add chain=input action=drop in-interface=**pppoe-out1** protocol=udp dst-port=53

где **pppoe-out1** название внешнего интерфейса. В Winbox это делается так:

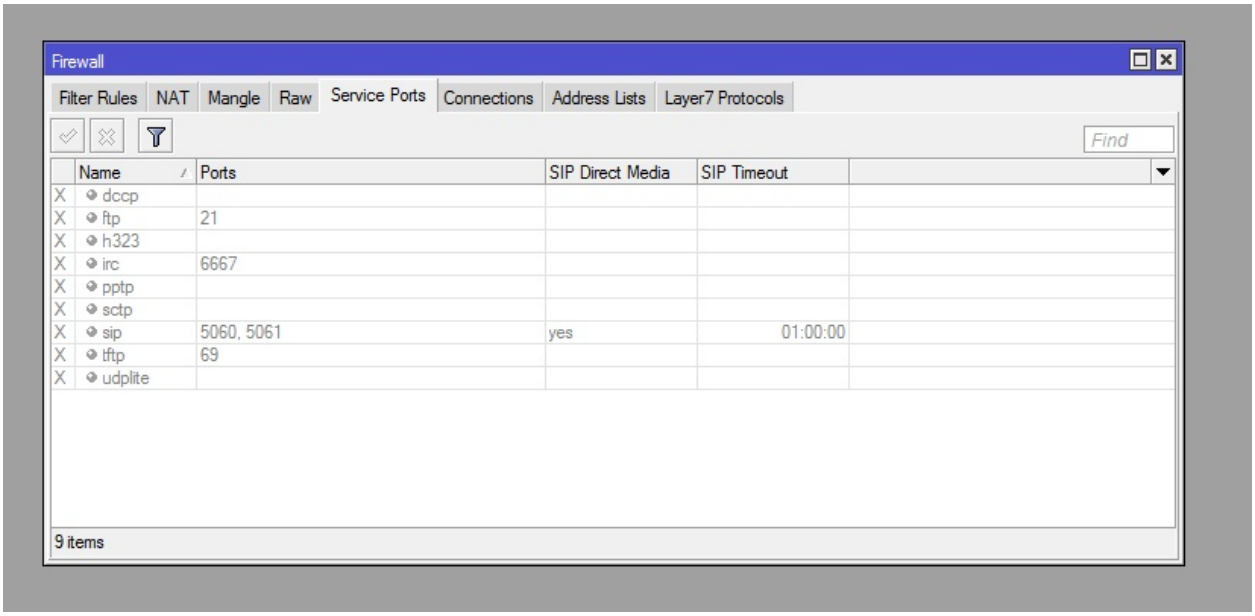




После чего нагрузка на процессор пропадёт, ваш DNS прекратят использовать для DDoS-атак (DNS Amplification).

2. Закрыть все открытые служебные порты которыми вы не пользуетесь.

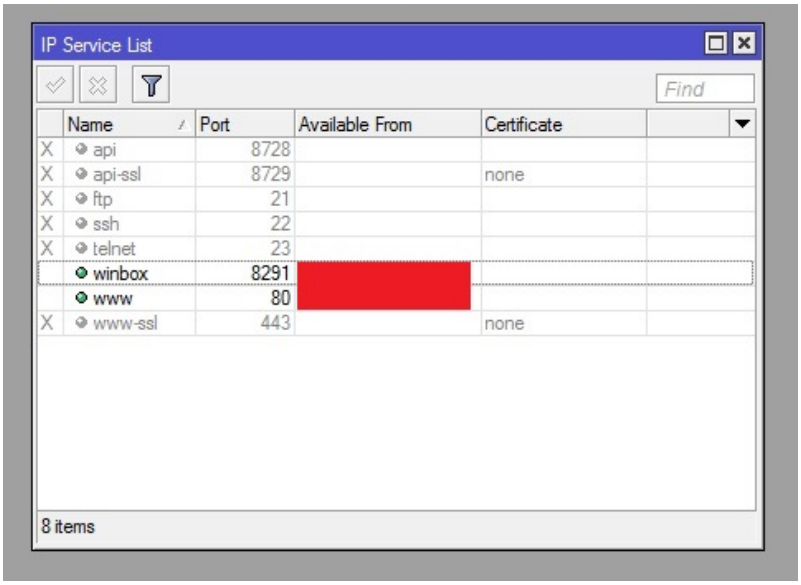
IP — Firewall — Service Port, выключить все:



3. Как защитить Mikrotik Routerboard от внешних вторжений ?

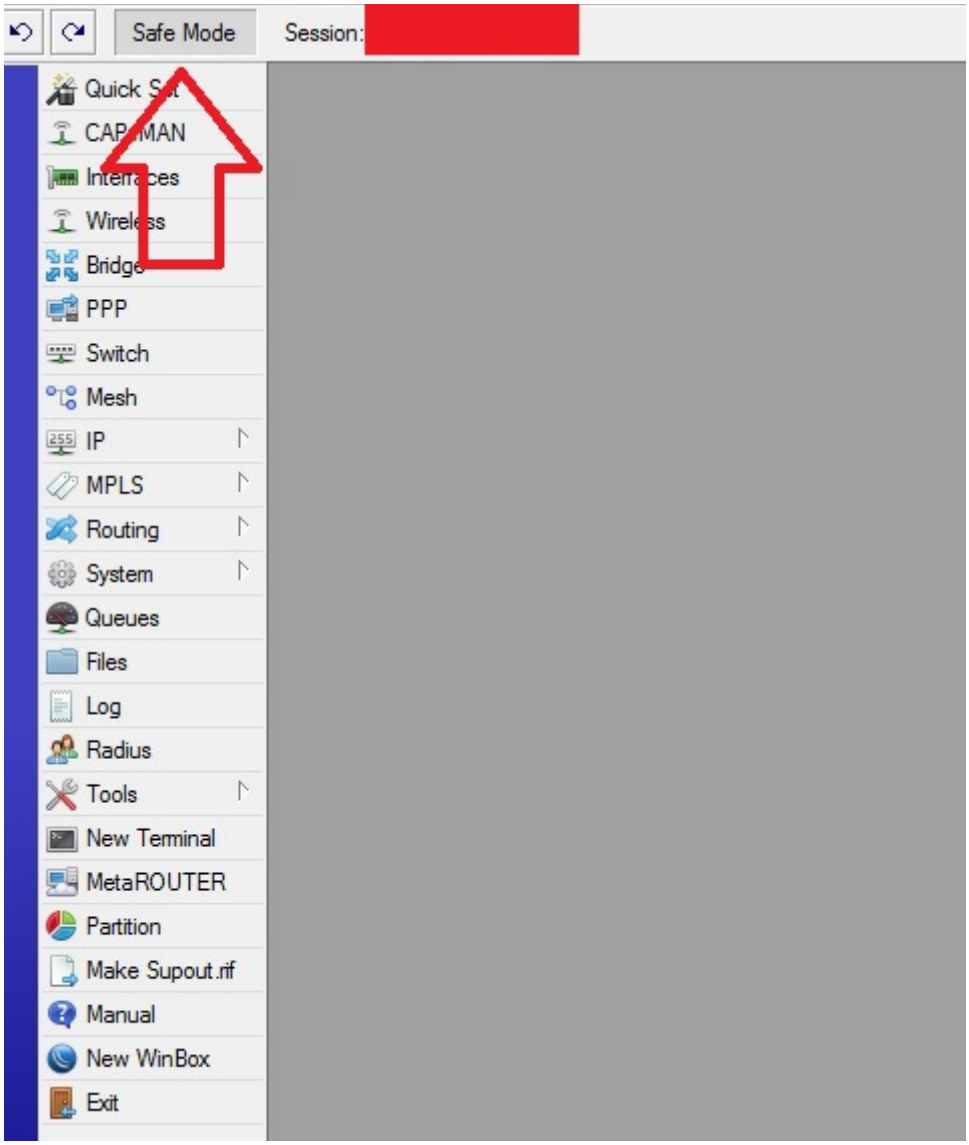
Это можно сделать так, Переходим в раздел **IP — Service**.

IP — Service, в появившемся окне мы видим список запущенных сервисов.
WINBOX – это графический интерфейс для управления Mikrotik RouterBoard
WWW – это Веб сервер, который дает возможность с помощью браузера подключится к Mikrotik RouterBoard.
Port – это порт, на котором сервисы ожидают подключения.
Available From – указывает, для какого ip адреса или подсети разрешен доступ. 0.0.0.0/0 разрешает доступ с любого IP адреса.



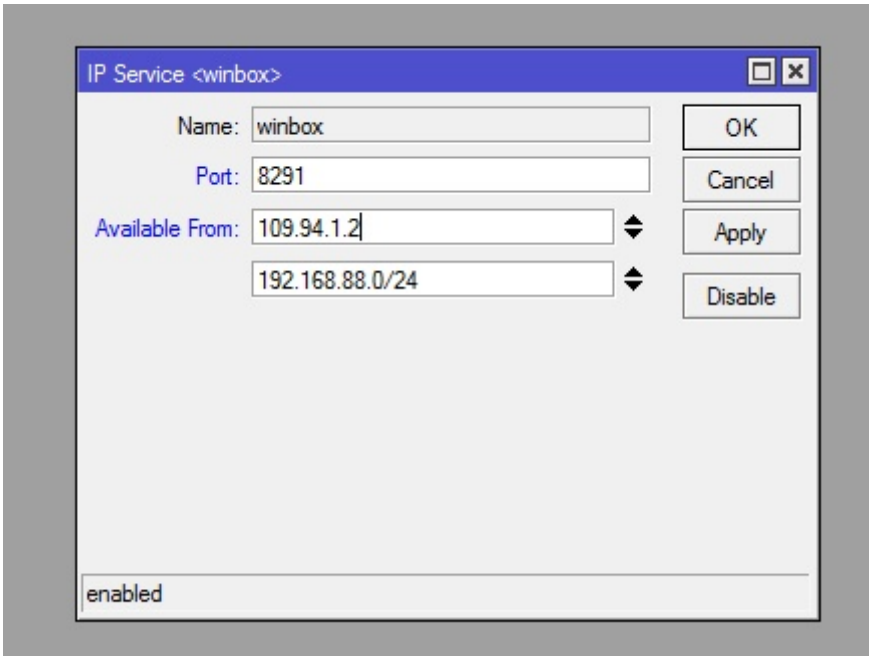
Для управления микротиком нужно оставить WWW и WINBOX, все остальные рекомендуется выключить.

Будьте осторожны с изменениями в WWW и WINBOX, если вы сделаете что-то не так, можете навсегда потерять доступ к роутеру, рекомендуем включить "Безопасный режим прежде чем вносить там изменения". Безопасный режим в WINBOX включается так:



после чего вы можете ограничить подсети для доступа к микротику, в первую очередь там нужно прописать локальную подсеть, по умолчанию это 192.168.88.0/24 и внешние ип адреса откуда будет разрешено подключатся, алогично для WWW.

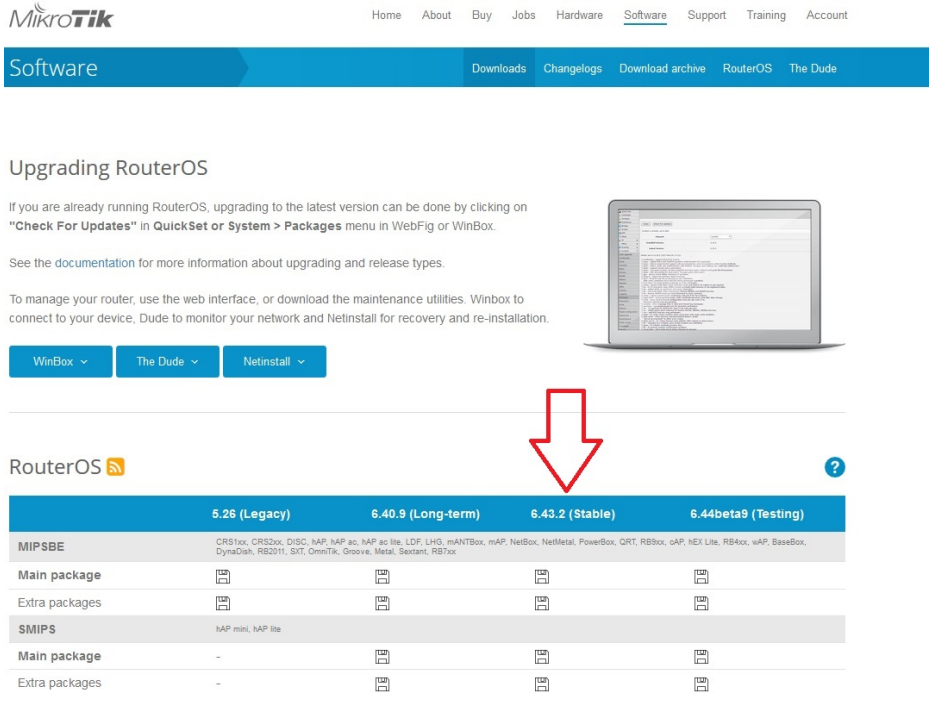
Пример:



Возможно эти настройки вам нетребуются, но все равно мы рекомендуем их сделать. Дело в то что в настройках вашего **Firewall** уже может быть заблокирован доступ из вне, но так бывает не всегда.

4. Рекомендуем как можно чаще обновлять RouterOS, обновления П.О. можно скачать с официального сайта:

https://mikrotik.com/download
Нужное П.О. (Main package) загружается в зависимости от модели вашего маршрутизатора, рекомендуется версия Stable.



5. Как определить что ваш был Mikrotik ВЗЛОМАН.
Если в логах вы видите подобную запись:

Jul/22/2018 22:06:10	memory	info	fetch: file "mikrotik.php" downloaded
Jul/22/2018 22:07:42	memory	info	fetch: file "mikrotik.php" downloaded
Jul/22/2018 22:09:15	memory	info	fetch: file "mikrotik.php" downloaded
Jul/22/2018 22:09:45	memory	info	fetch: file "mikrotik.php" downloaded
Jul/22/2018 22:31:11	memory	info	fetch: file "mikrotik.php" downloaded
Jul/22/2018 22:34:45	memory	info	fetch: file "mikrotik.php" downloaded
Jul/22/2018 22:37:42	memory	info	fetch: file "mikrotik.php" downloaded
Jul/22/2018 22:38:17	memory	info	fetch: file "mikrotik.php" downloaded
Jul/22/2018 23:50:43	memory	info	fetch: file "mikrotik.php" downloaded
Jul/22/2018 23:51:43	memory	info	fetch: file "mikrotik.php" downloaded
Jul/22/2018 23:52:14	memory	info	fetch: file "mikrotik.php" downloaded
Jul/22/2018 23:54:43	memory	info	fetch: file "mikrotik.php" downloaded
Jul/22/2018 23:55:19	memory	info	fetch: file "mikrotik.php" downloaded
Jul/22/2018 23:56:12	memory	info	fetch: file "mikrotik.php" downloaded
Jul/22/2018 23:57:13	memory	info	fetch: file "mikrotik.php" downloaded
Jul/22/2018 23:59:41	memory	info	fetch: file "mikrotik.php" downloaded
Jul/23/2018 00:00:41	memory	info	fetch: file "mikrotik.php" downloaded
Jul/23/2018 00:01:18	memory	info	fetch: file "mikrotik.php" downloaded
Jul/23/2018 00:02:10	memory	info	fetch: file "mikrotik.php" downloaded
Jul/23/2018 00:03:18	memory	info	fetch: file "mikrotik.php" downloaded
Jul/23/2018 00:03:40	memory	info	fetch: file "mikrotik.php" downloaded

значит микротик был взломан, файл mikrotik.php вы найдете в каталоге **Files** .

Единственное 100% рабочее решение на данный момент это полный сброс маршрутизатора, обновление П.О. и рекомендации из этой инструкции.