Динамические списки в Mikrotik

Для защиты сети и другие полезности.

Обо Мне

- Практикующий администратор сетей и решений с 1996г.
- Учился в TSI Рига и МТИ Москва.
- Работал в компаниях NURON DC, SIA Datagrupa 777, СП Buzton, Novatel, Sonet.
- Сертификатов много, зачем они вам? :)
- Работаю с Микротиком с 2012 года.
- Контакты: timur.hp@gmail.com

Динамические списки безопасности.

- Безопасность общая проблема IT. Вы можете максимально автоматизировать процесс защиты прохождения траффика.
- Как создать правила и где?
- Правила для анализа не благонадежного трафика.
- Добавление источника, ротация данных.
- Другие полезности.

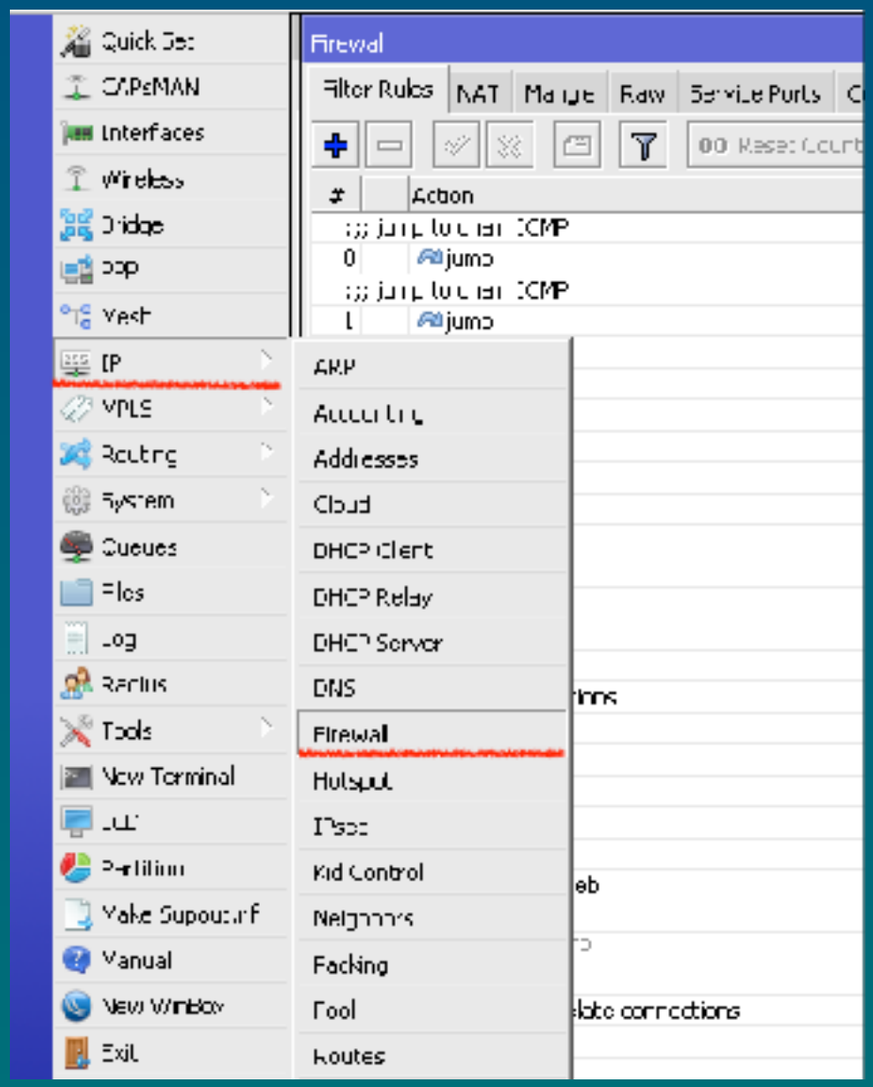
Mikrotik

- Латвийский производитель сетевого оборудования. Компания разрабатывает и продает сетевое оборудование (маршрутизаторы, сетевые коммутаторы, точки достуда и программногое обеспечение).
- Компания основана в 1996 года.
- Основные достоинства:
  - Стоимость - в своей ценовой категории просто нет.
  - Функциональность просто огромная. Можно реализовать любую хотелку.
  - Надежность и стабильность.
  - Документация и обновления.
  - Единая OS и система конфигурирования.
  - Масштабируемость.

Безопасность.

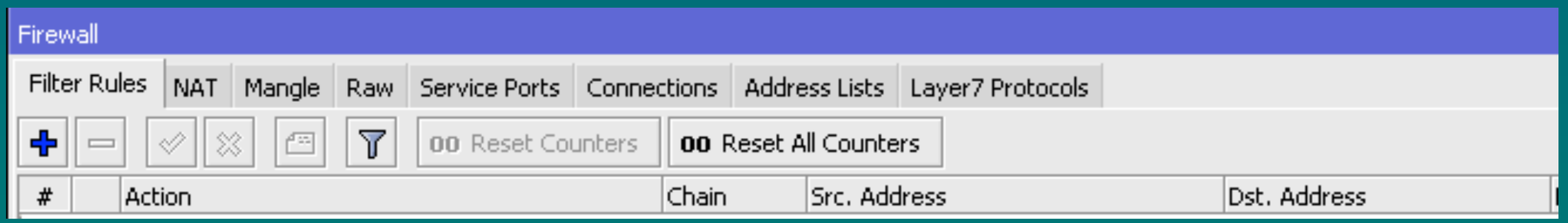
- Как много в этом слове, но мы должны определится, что мы будет защищать.
- Защита канала роутера.
- Защита канала клиентов.
- Защита ресурсов сети.

Начнем с самого простого. У нас уже есть роутер Mikrotik и желание автоматизировать процесс контроля трафика.



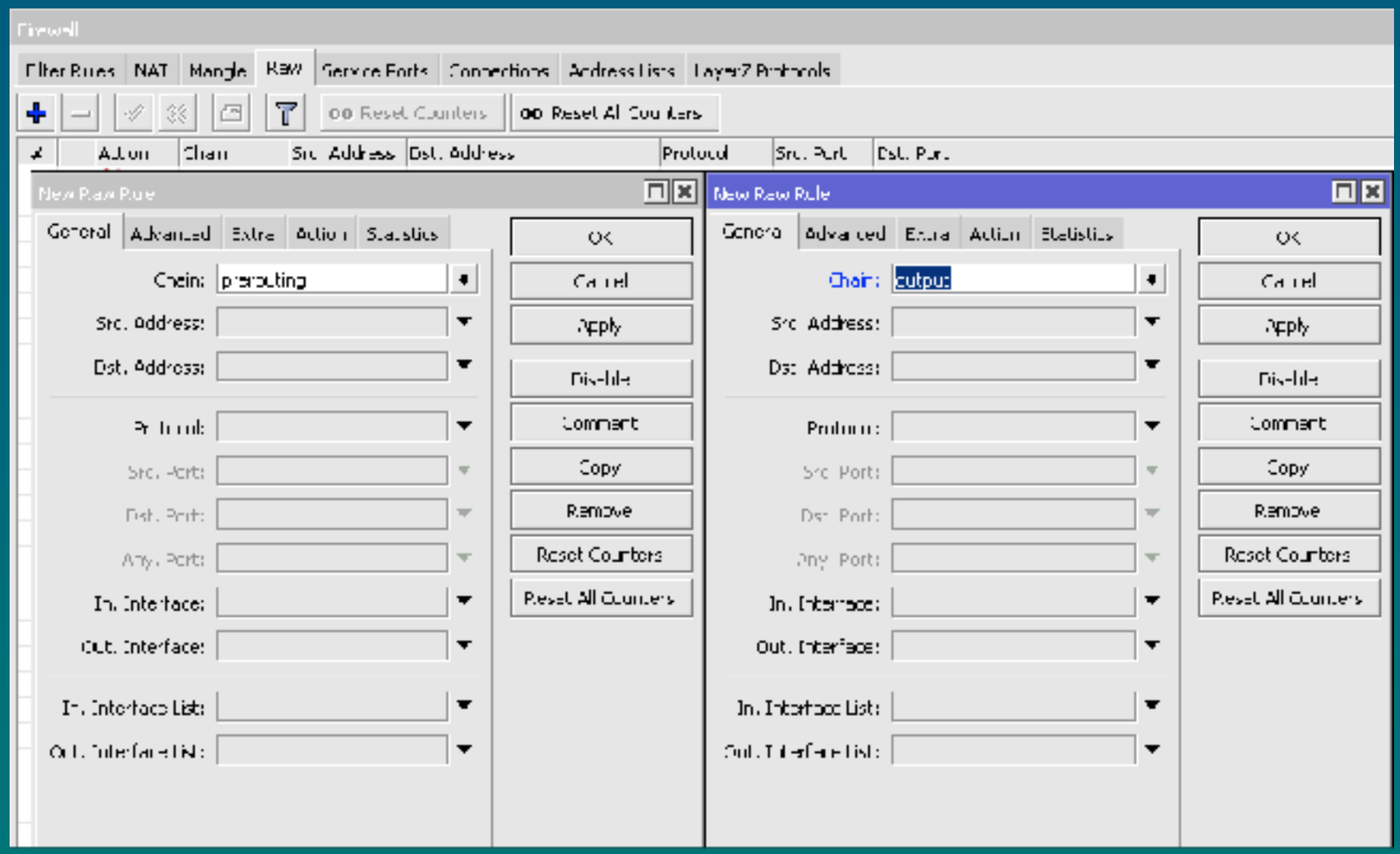
В Микротике начиная с версии 6.36, в разделе firewall есть четыре основные ветки таблиц:

- **Filter Rules**
- **Nat**
- **Mangle**
- **Raw**



Нам необходима ветка RAW, данная ветка сильно разгружает CPU маршрутизатора, так как работает до отслеживания соединения. Этим она и полезна. У данной ветки есть два направления:

- **prerouting - ветка для любого пакета вошедшего.**
- **output - ветка для любого пакета вышедшего.**



Составляем список что будем контролировать.

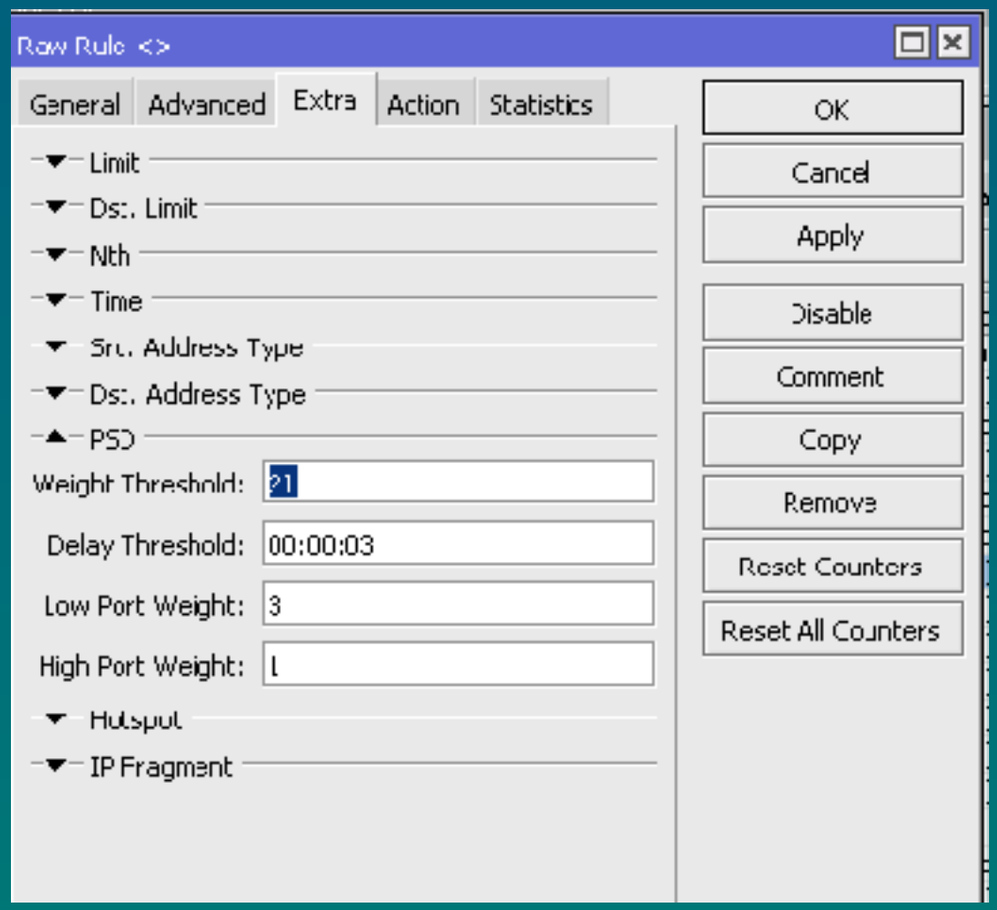
- направление входящего трафика, источник.
- tcp соединение.
- основные сервисные порты tcp/udp.
- время в карантине, источника проблем.

Определяем не желательную последовательность tcp флагов.

- Определяем последовательность флагов от сканирования tcp.
  - NMAP FIN scan - tcp-flags=fin,!syn,!rst,!psh,!ack,!urg
  - SYN/FIN scan - tcp-flags=fin,syn
  - SYN/RST scan - tcp-flags=syn,rst
  - FIN/PSH/URG scan - tcp-flags=fin,psh,urg,!syn,!rst,!ack
  - ALL/ALL scan - tcp-flags=fin,syn,rst,psh,ack,urg
  - NMAP Null scan - tcp-flags=!fin,!syn,!rst,!psh,!ack,!urg

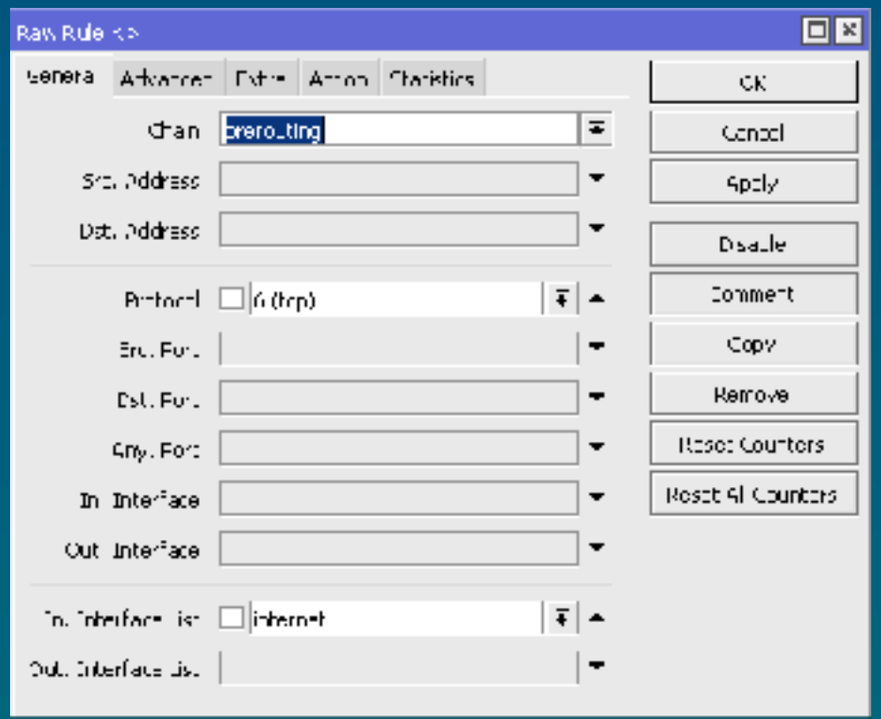
Пытаемся определить сканирование TCP, средствами firewall.

- в разделе Extra, PSD параметр (Port Scan Detection):
  - *psd (integer,time,integer,integer)* – попытка определения сканирования TCP и UDP портов. Необходимо назначить меньшее значение портам с высокими номерами для того, чтобы уменьшить количество ложных срабатываний. К примеру, при использовании пассивного режима FTP.

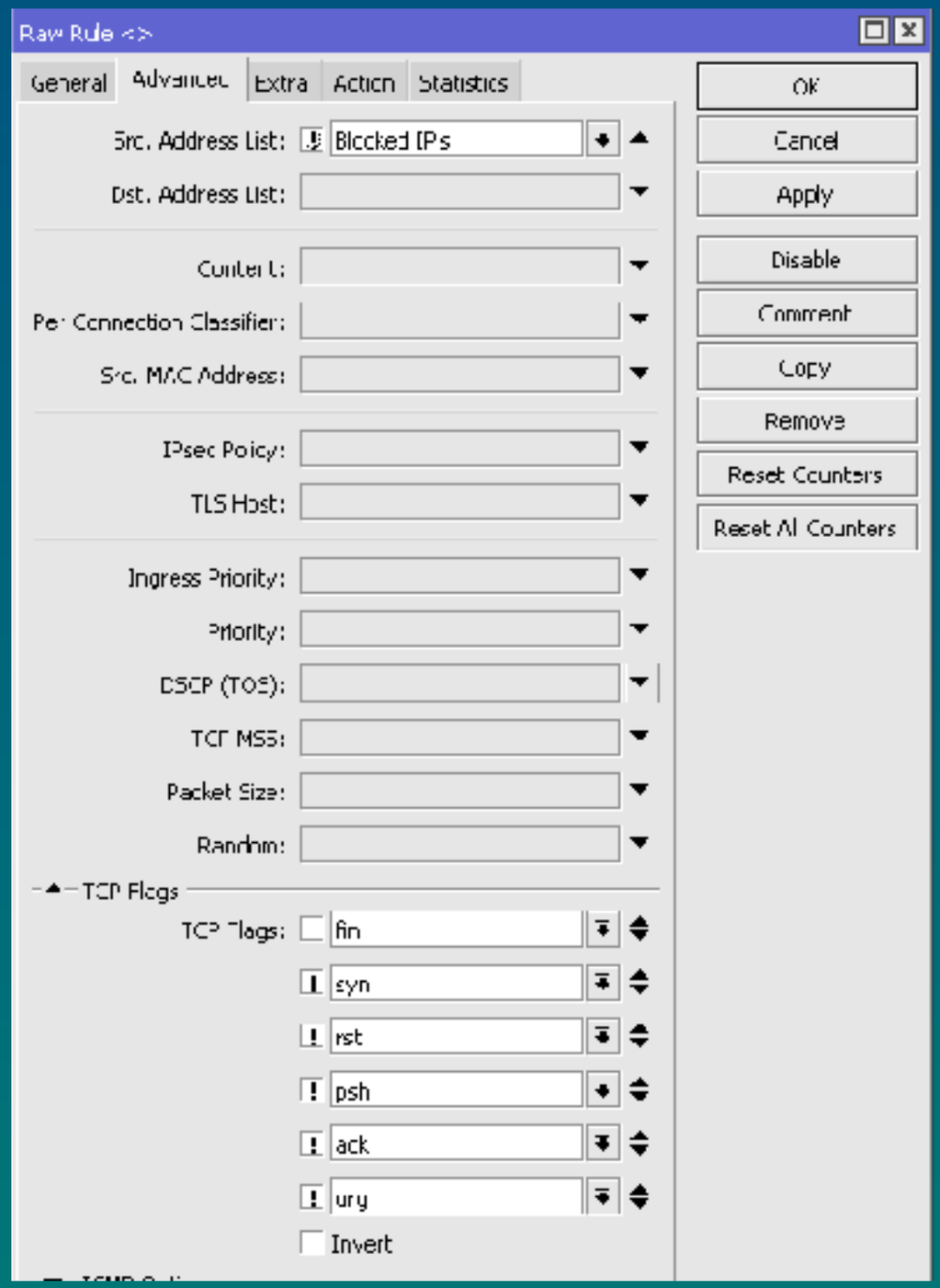


Создания правил для добавления источника проблема по src в динамический список.

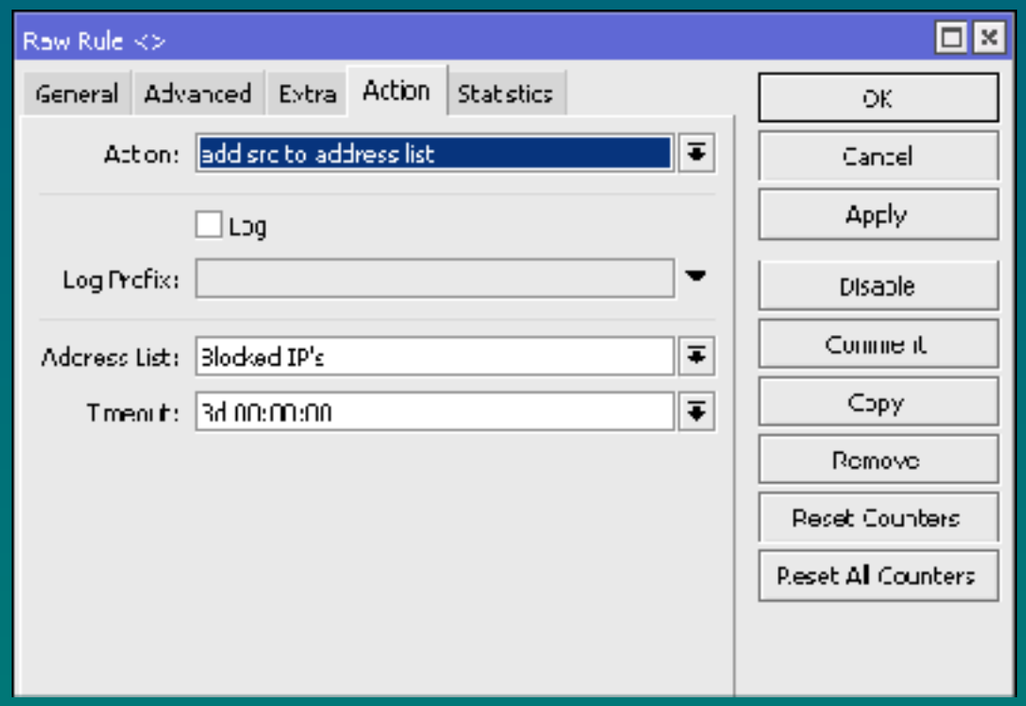
1



2



3



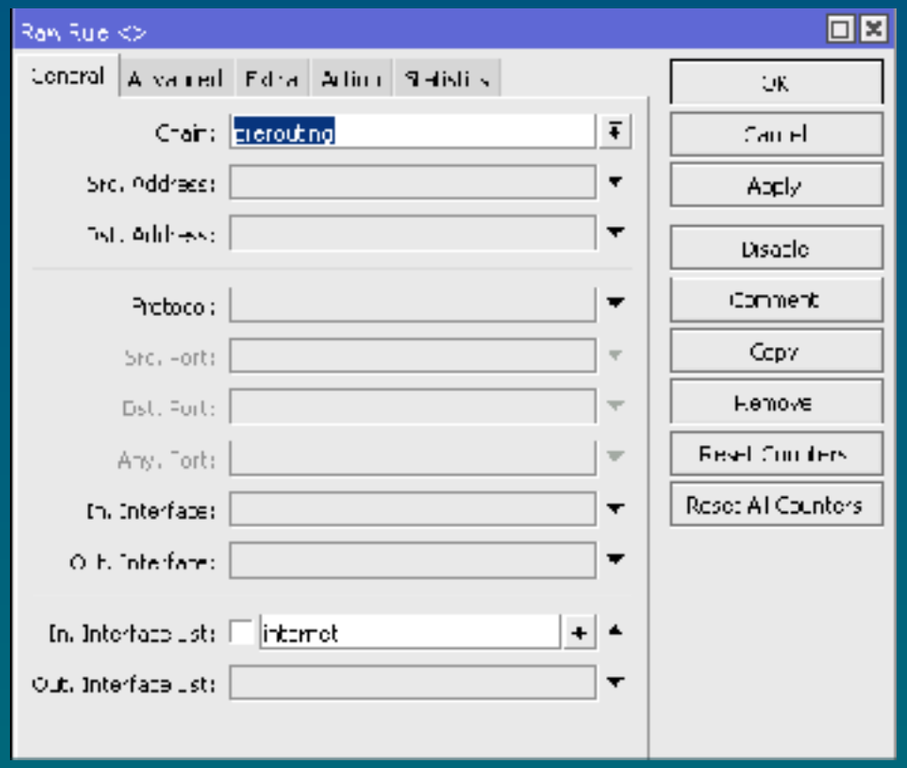
Правила реагирующие на сканирование.

```
;;; Port scanners to list
    chain=prerouting action=add-src-to-address-list in-interface-list=internet log=no log-prefix="" protocol=tcp psd=21,3s,3,1 src-address-list=!
Blocked IP's
    address-list=Blocked IP's address-list-timeout=3d

  chain=prerouting action=add-src-to-address-list tcp-flags=fin,!syn,!rst,!psh,!ack,!urg in-interface-list=internet log=no log-prefix="" protocol=tcp
    src-address-list=!Blocked IP's address-list=Blocked IP's address-list-timeout=3d

  chain=prerouting action=add-src-to-address-list tcp-flags=fin,syn in-interface-list=internet log=no log-prefix="" protocol=tcp src-address-list=!
Blocked IP's
    address-list=Blocked IP's address-list-timeout=3d

  chain=prerouting action=add-src-to-address-list tcp-flags=syn,rst in-interface-list=internet log=no log-prefix="" protocol=tcp src-address-list=!
Blocked IP's
    address-list=Blocked IP's address-list-timeout=3d

  chain=prerouting action=add-src-to-address-list tcp-flags=fin,psh,urg,!syn,!rst,!ack in-interface-list=internet log=no log-prefix="" protocol=tcp src-
address-list=!Blocked IP's
    address-list=Blocked IP's address-list-timeout=3d

  chain=prerouting action=add-src-to-address-list tcp-flags=fin,syn,rst,psh,ack,urg in-interface-list=internet log=no log-prefix="" protocol=tcp src-
address-list=!Blocked IP's
    address-list=Blocked IP's address-list-timeout=3d

  chain=prerouting action=add-src-to-address-list tcp-flags=!fin,!syn,!rst,!psh,!ack,!urg in-interface-list=internet log=no log-prefix="" protocol=tcp
    src-address-list=!Blocked IP's address-list=Blocked IP's address-list-timeout=3d
```

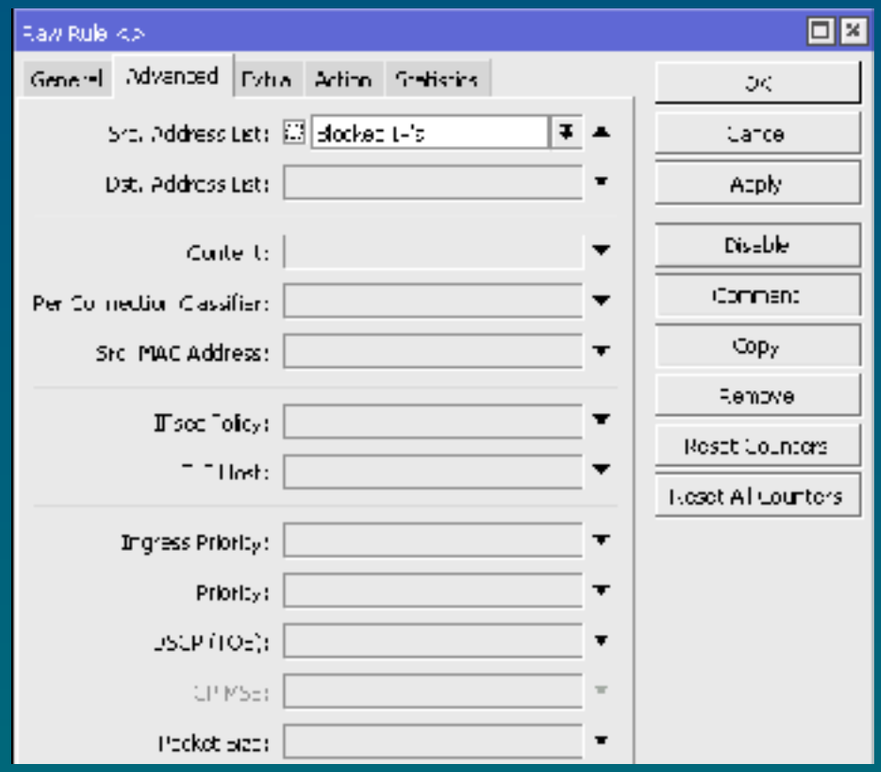
;;; Port scanners to list							
13		ad...	prerouting	6 (tcp)		0 B	0
14		ad...	prerouting	6 (tcp)	fin, !syn, !rst, !psh, !ack, !urg	0 B	0
15		ad...	prerouting	6 (tcp)	fin, syn	0 B	0
16		ad...	prerouting	6 (tcp)	syn, rst	0 B	0
17		ad...	prerouting	6 (tcp)	fin, !syn, !rst, psh, !ack, urg	0 B	0
18		ad...	prerouting	6 (tcp)	fin, syn, rst, psh, ack, urg	0 B	0
19		ad...	prerouting	6 (tcp)	!fin, !syn, !rst, !psh, !ack, !urg	0 B	0

Заключительное правило блокирует доступ по динамическому списку.

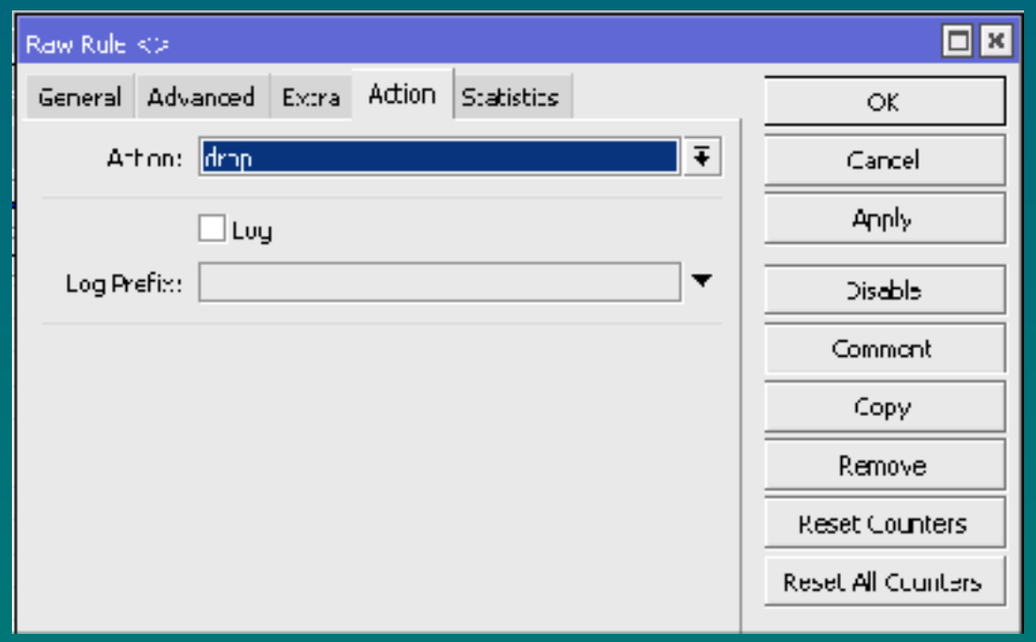
1



2



3

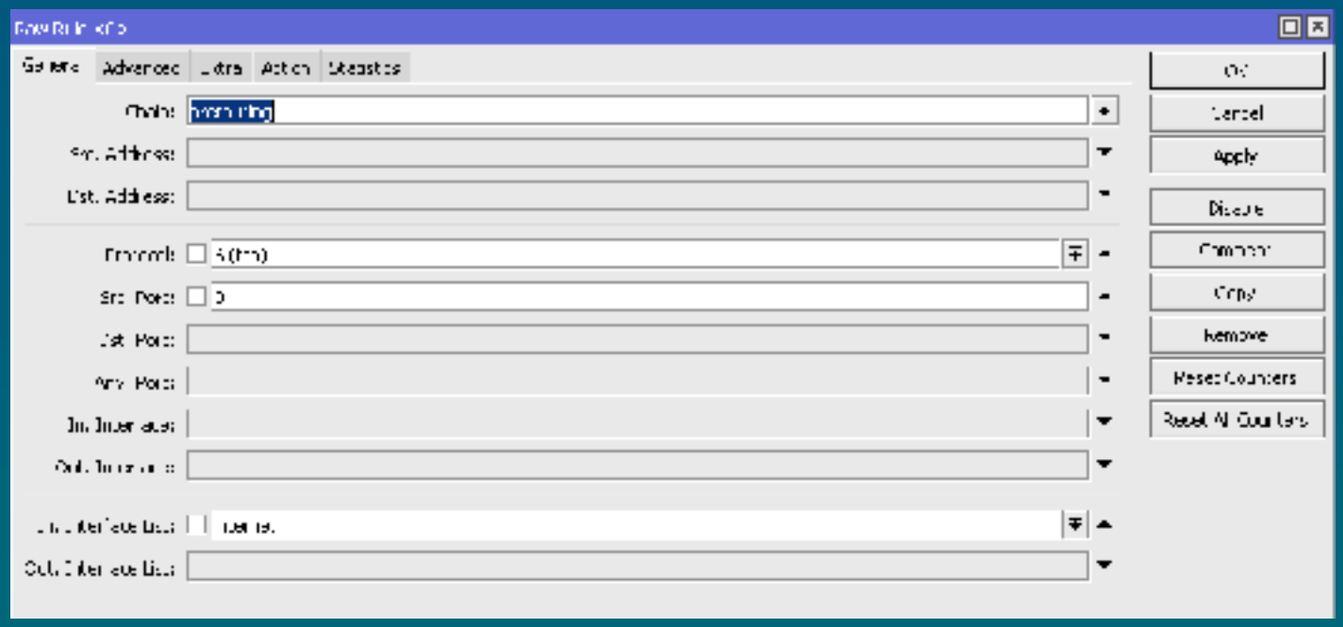


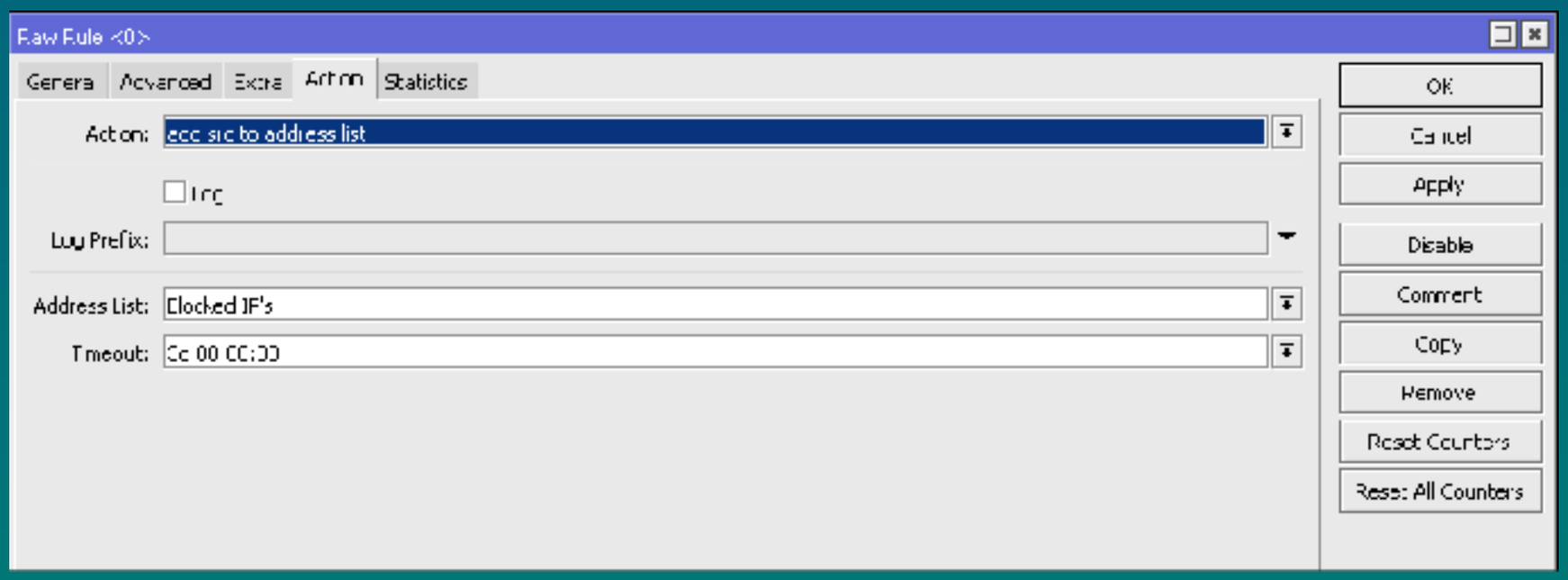
Список портов, на которые возможны атаки, а так же усиление атак.

- 53 tcp/udp - dns
- 123 udp - ntp
- 69 tcp/udp - tfts
- 111 tcp/udp - portmapper rcp
- 135-139,445 tcp/udp - netbios and etc.
- 161 tcp/udp - snmp
- 548 tcp/udp - afp
- 520,1900 udp - RIP, SSDP
- 5060 udp/tcp - SIP
- 4569 udp/tcp - IAX2
- 3128,1080 tcp - proxy, sock
- 8291,8728,8729 tcp - mikrotik access, api and etc
- 20-25,110,993,587 tcp - ftp, ftp-data, smtp, pop3, imap, smtps and etc.
- 3389,11211 - rdp, memory cache

Примеры заполнения списка.

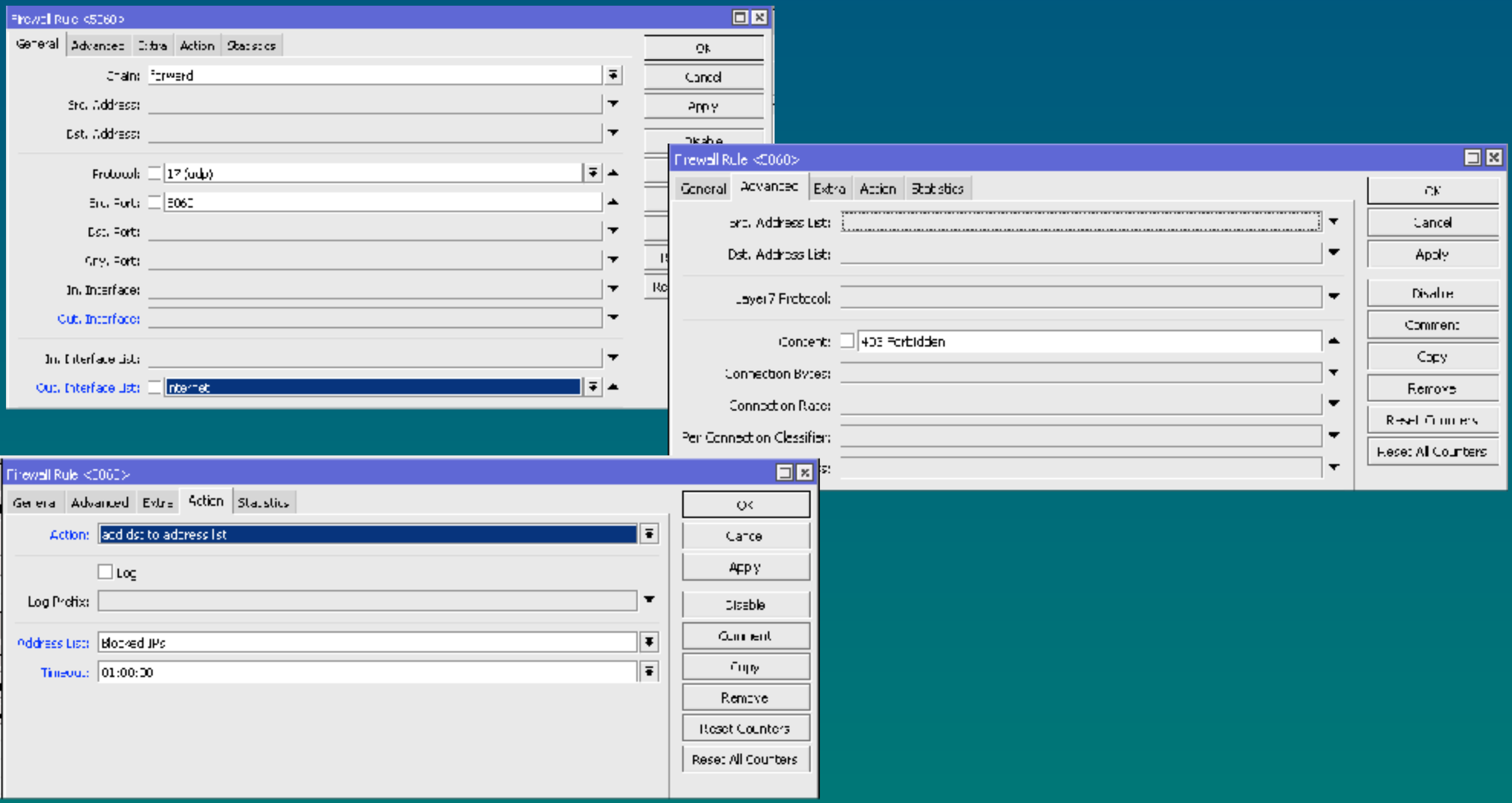
- 0 порт tcp/udp источник или назначение.





Примеры заполнения списка.

- 5060 порт udp, защита телефонии.
- все ответы sip порта, можно найти на https://wiki.sipnet.ru/index.php/SIP_ответы_и_их_значения

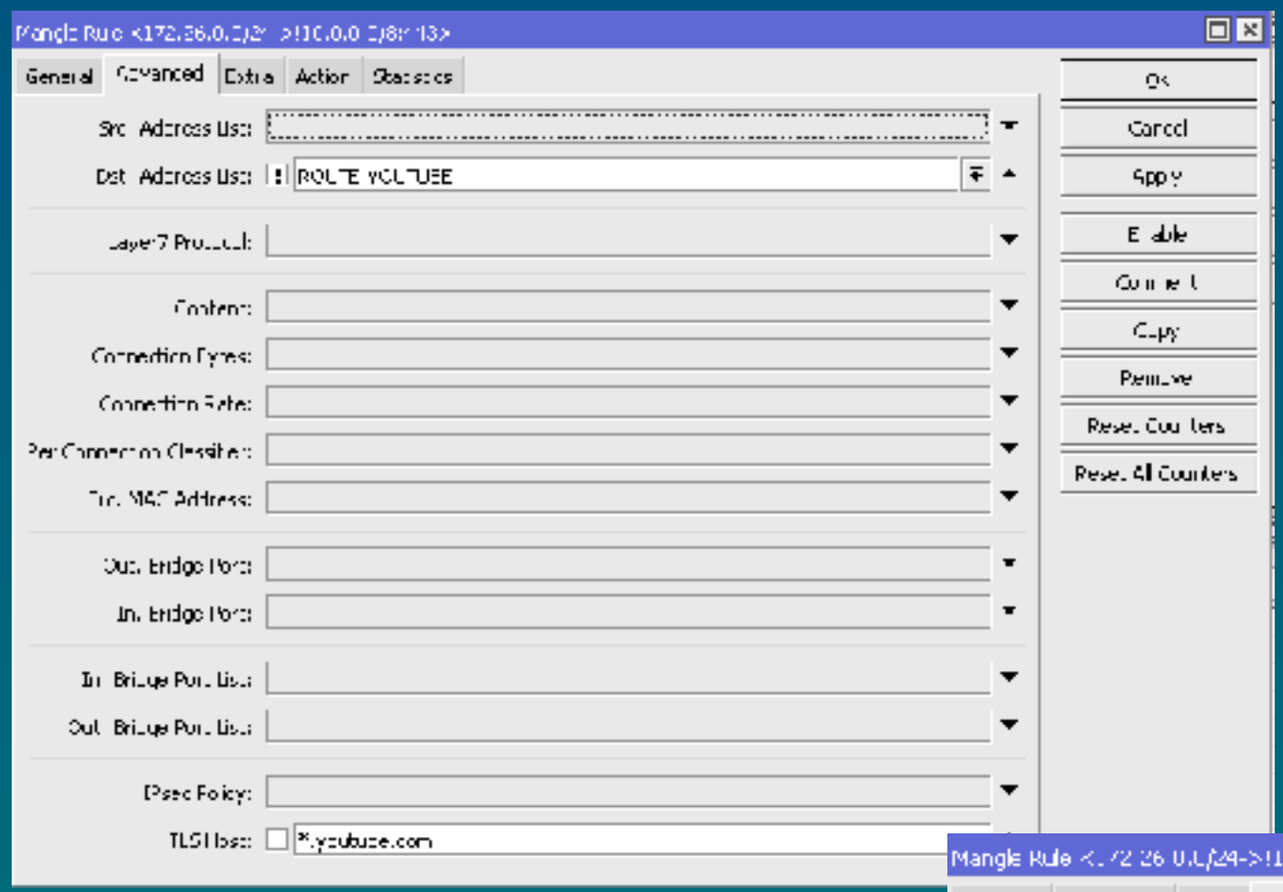


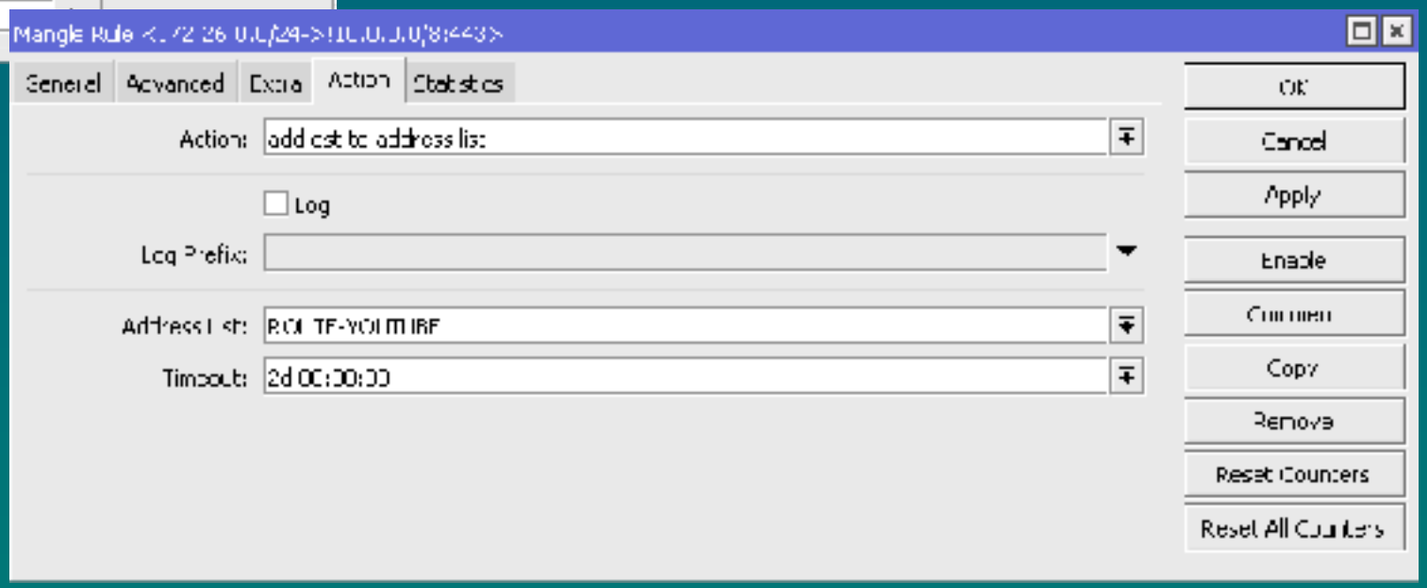
В дополнении…

- Динамические списки дают гибкий инструмент манипулирования трафиком.
- На основе ветки Mangle, можем пометить необходимое нам направление, допустим - youtube.com, в динамический список по dst ip.
- Следующее правила будет перенаправлять в VPN или запрещать доступ до этого ресурса. Можно использовать L7 фильтры, но это накладывает ограничение на CPU.

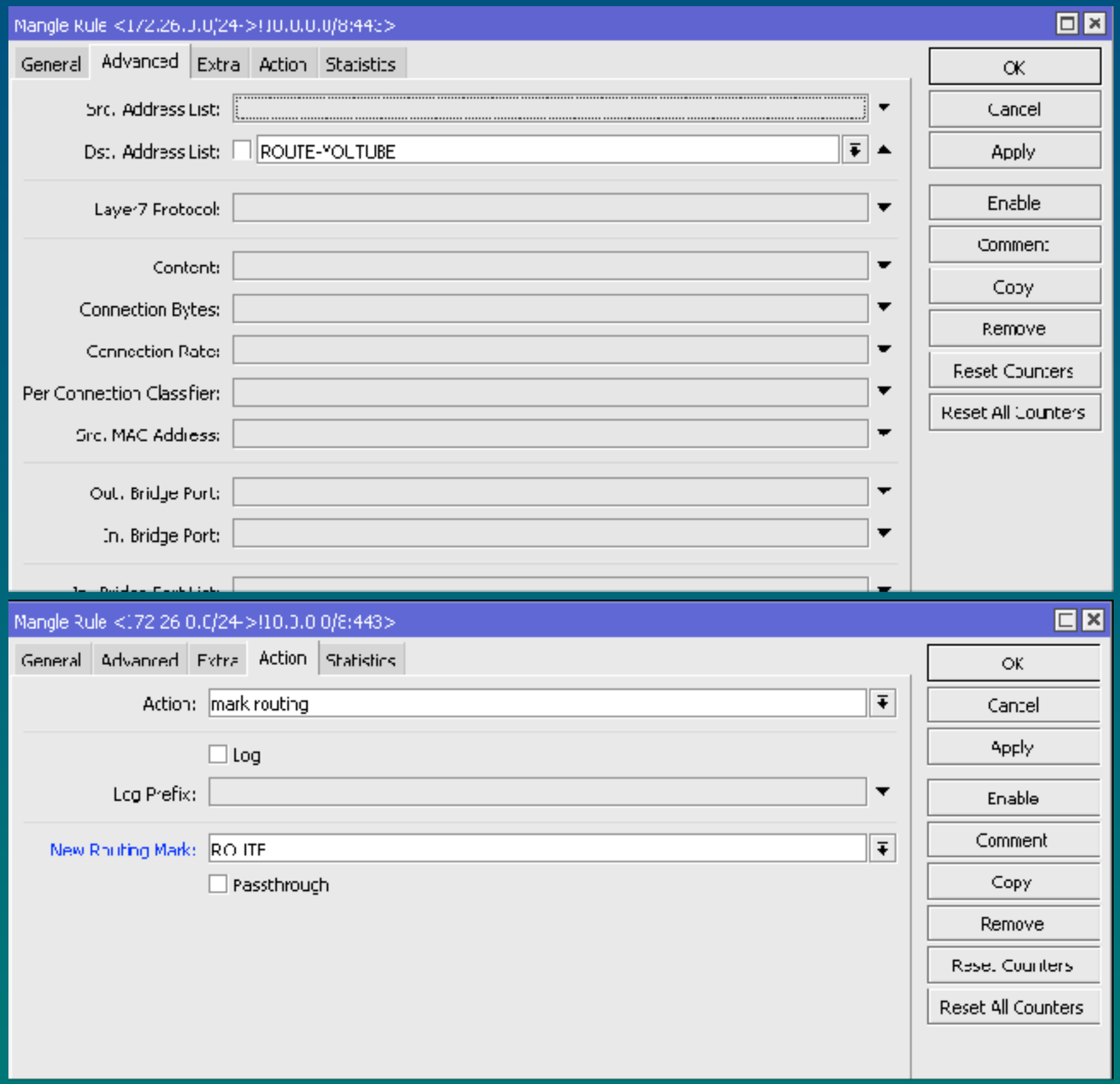
На основе tls рукопожатия.

- Ловим направление по tls handshake, и записываем в динамический список:





Далее направляем или блокируем список.



Вопросы?

Спасибо за внимание!