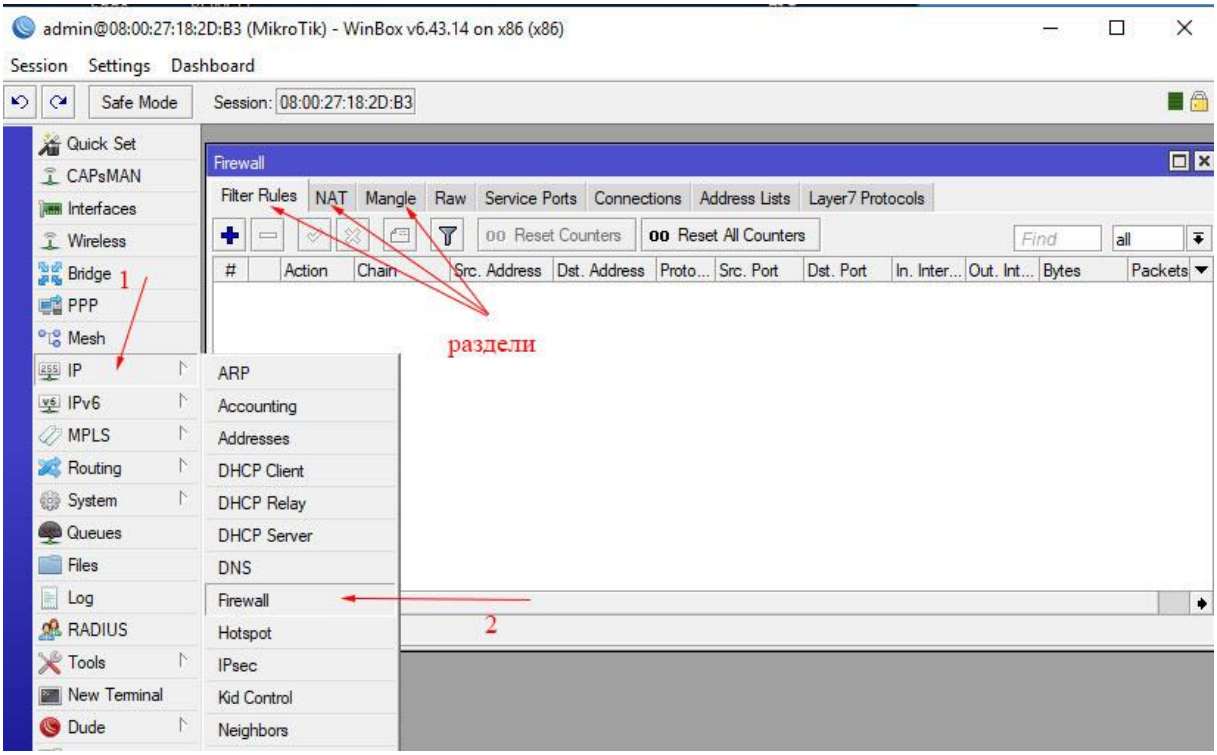
Защитна стена (Firewall)

Защитната стена е услуга, предназначена за проверка на мрежовия трафик, насочен към, напускащ и минаващ през маршрутизатора и налагаща контрол, като разрешава или ограничава достъпа по предварително дефинирани политики. Обикновено тя стои между две мрежи, една от които е вътрешна и се предполага, че е сигурна, а другата външна и е несигурна.

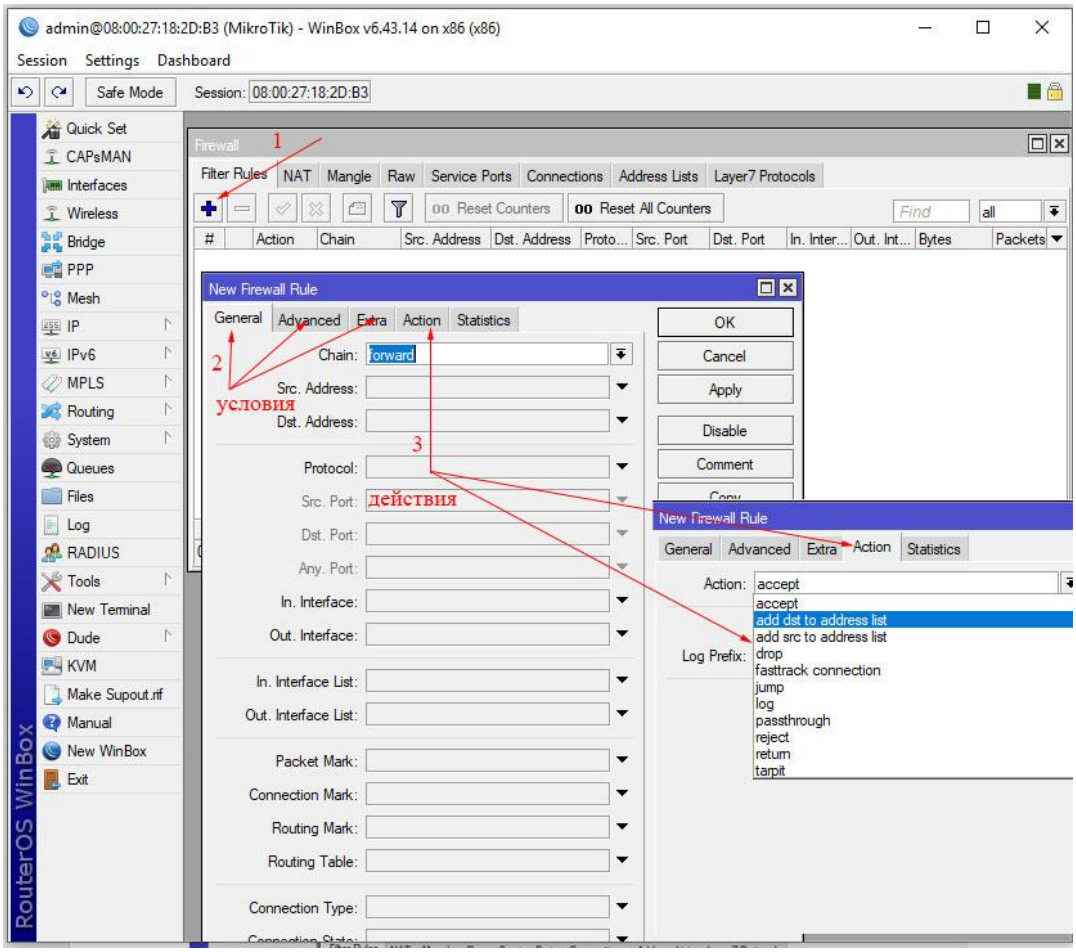
1. Защитна стена на RouterOS.

Защитната стена на RouterOS е достъпна от менюто **IP->Firewall**. Включва раздели, обособени като отделни табове (фигура 1), като всеки от тях управлява специфични функции от нея. Резултатът от приложени функции в един раздел може да се използва в друг раздел. Защитната стена работи на база последователно изпълнение на правила. Те са съставени от две части (фигура 2):

- Условие – за проверка на удовлетворени съответствия. Проверяват се параметри като: MAC адрес на подател; IP адрес; тип на комуникацията (broadcast, unicast, local, multicast); портове; протокол и опции; входящ или изходящ интерфейс.
- Действие – изпълнява се при удовлетворено условие, определя живота на пакета и последващата му обработка.



фигура 1



фигура 2

Правилата се групират и подреждат във вериги (chains). Съществуват предварително дефинирани вериги. Могат да бъдат създадени и допълнителни от администратора.

2. Проследяване на връзките (connection tracking)

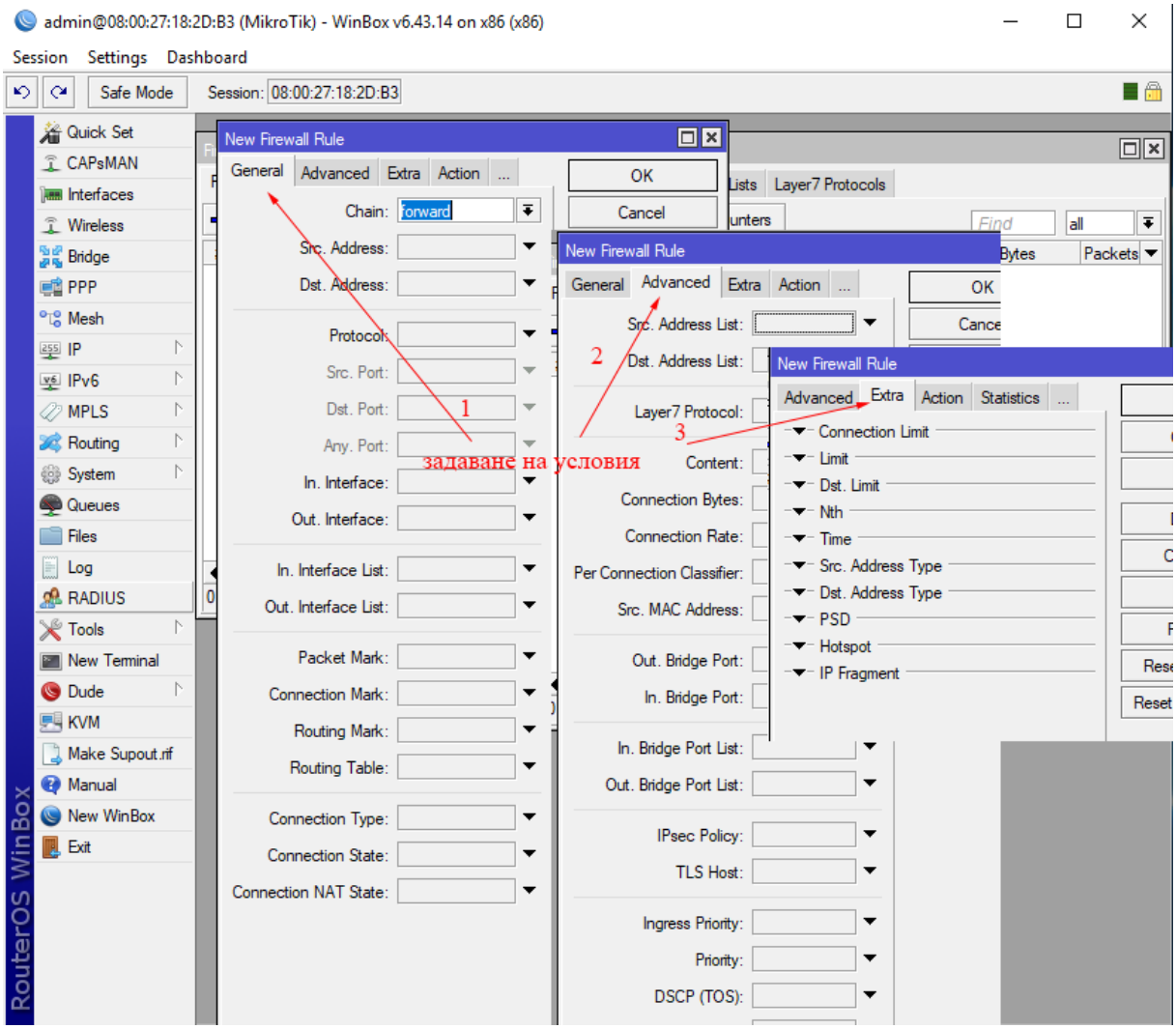
Системата за проследяване на връзките е част от защитната стена на RouterOS. Достъпът до нея може да се направи от секцията **Connections**. Не е желателно да се правят дори опити за изключване. Проследяването разчита на механизмите за установяване на сесия (*3-way handsh*ake), прехвърляне на данни и прекратяване на сесия (*4-way disconnect*) при TCP. Логическата последователност на TCP състоянията е: *syn-sent*, *syn-recv*, *established*, *listen*, *fin-wait*, *time-wait*, *close-wait*, *last-ack*, *close*, *none*. Разработен е собствен механизъм за проследяване и на UDP връзките (UDP е безвръзков протокол). Първият пакет е със състояние NEW. Всички останали могат да се тълкуват като вече установени, докато не се достигне стойност за *udp-timeout*, която по подразбиране е 10 секунди.

3. Филтър в защитната стена (Filter Rules)

Стандартните вериги, които обслужват условията във филтъра са:

- **forward** – обработва трафика, преминаващ през маршрутизатора;
- **input** - обработва трафика, предназначен за самия маршрутизатор;
- **output** – обхваща трафика, генериран от самия маршрутизатор.

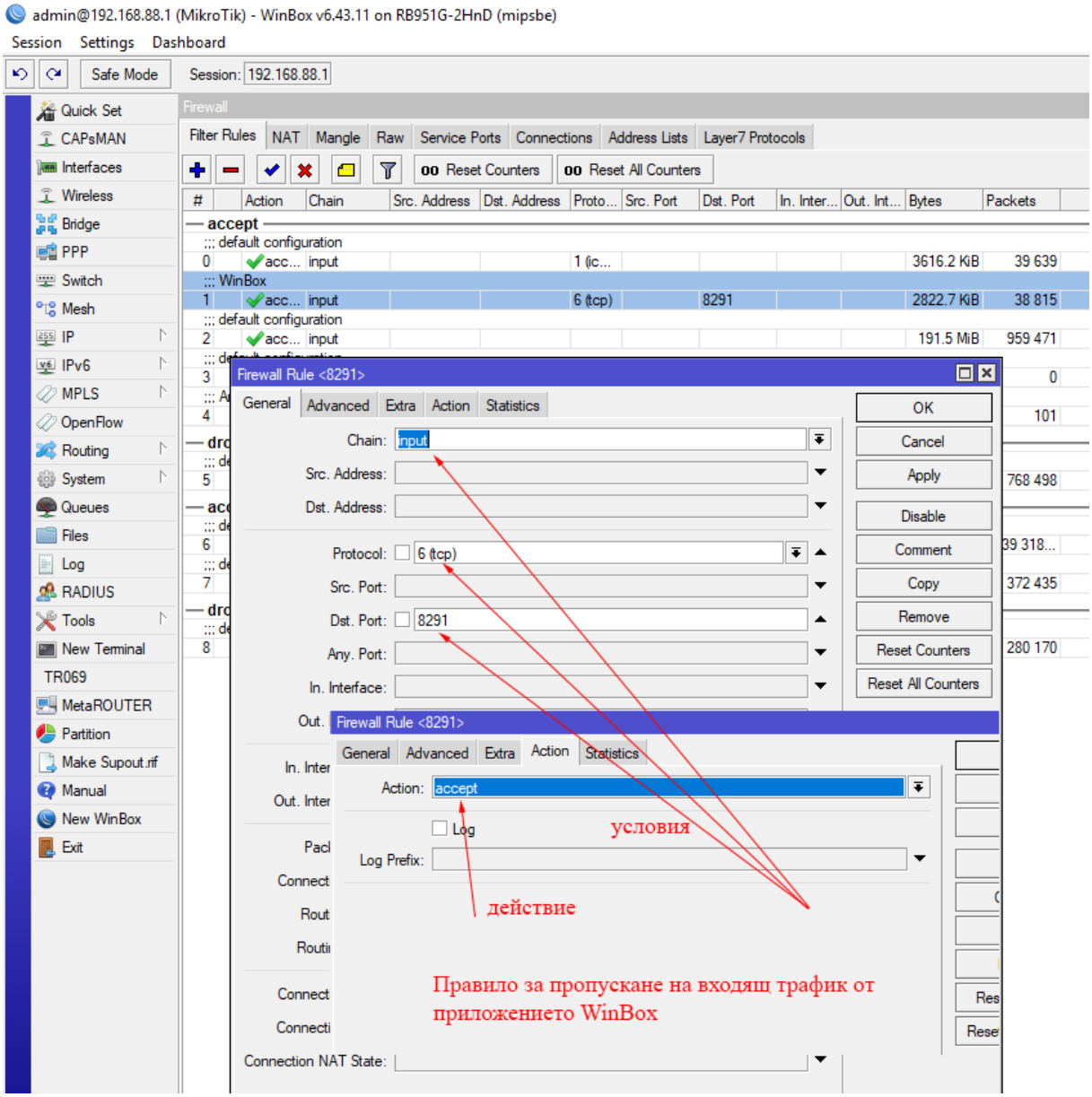
Условията във филтъра се обслужват от разделите: *General*, *Advanced* и *Extra* (фигура 3).



фигура 3

Чрез тях се търси съответствие в пакетите по множество критерии като IP адрес на получателя и подателя (Src. Address или Dst. Address), протокол (като *tcp*, *udp*, *icmp*, *gre* и други), по входящи и изходящи мрежови интерфейси или списъци с такива (In./Out. Interface, In./Out. Interface List), адресни списъци (Src. /Dst. Address List) и други.

На фигура 4 е представен пример за разрешаване на входящ трафик от приложението WinBox.



фигура 4

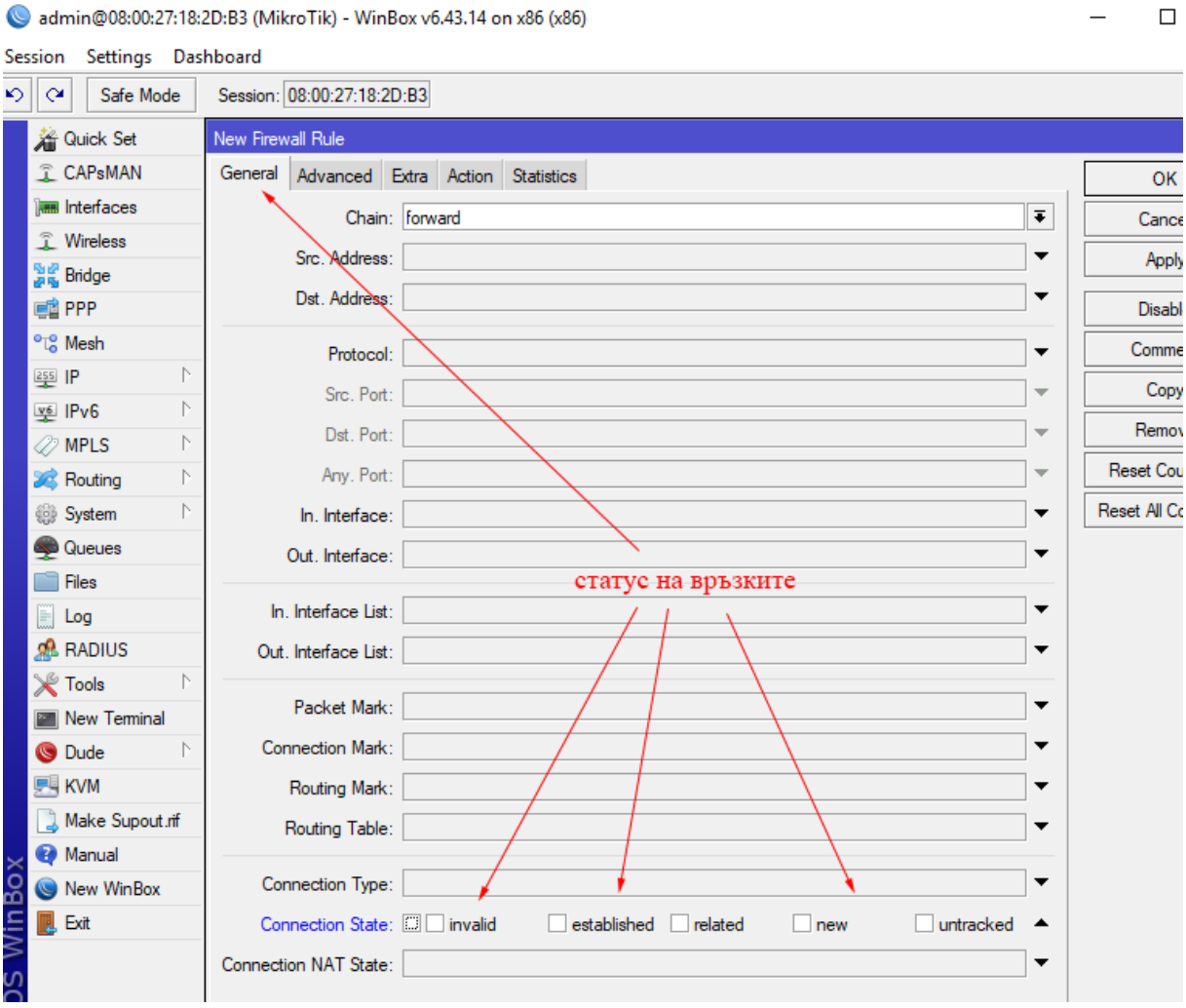
4. Статус на връзките (Connection State)

Статусите на връзките във филтъра (фигура 5) на защитната стена имат следния смисъл:

- **New** - първият пакет за една връзка (съвпада с TCP Syn пакета). При UDP е отново първият пакет;
- **Established** - това са всички останали пакети след *New* от същата връзка. При UDP - останалите при стойност по подразбиране от

10 сек. Това са вече познати връзки. Добра е за тези пакети да се създаде правило с действие **Accept** (да се приемат);

- **Related** - връзка, създадена от вече съществуваща връзка. Подходящ пример за такива връзки е FTP протоколът, който установява връзка на 21 порт, но за прехвърляне на данни отваря друг порт (20) и съответно нова връзка, създадена от вече установената такава. Добра практика е за тези пакети да се приемат;
- **Invalid** - TCP сегмент, без установено състояние. Добра практика е за тези пакети да се създаде правило с действие **Drop** (да се изхвърлят).

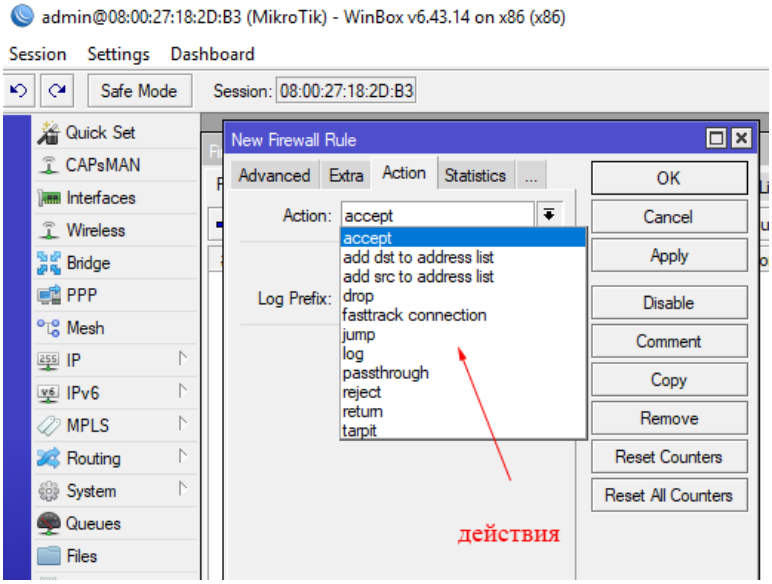


фигура 5

5. Действия във филтър

Действията (фигура 6), които могат да се изпълнят при открито съответствие с условието на правилото са:

- **Accept** - действие по подразбиране за всяко правило. При него пакетът се приема и не се препраща към следващите правила на защитната стена;
- **Add-dst-to-address-list** - IP адресът на получателя се добавя в адресен списък и пакетът продължава обработка от следващите правила на защитната стена;
- **Add-src-to-address-list** - IP адресът на подателя се добавя в адресен списък и пакетът продължава обработка от следващите правила на защитната стена;
- **Drop** - пакетът се изхвърля (без отговор на подателя) и повече не се предава към следващите правила на защитната стена;
- **Fasttrack-connection** - маркира пакетите с цел използване на по-малко процесорни ресурси и ускоряване на работата като съкращава техния път за обработка. Работи само с TCP и UDP връзки;
- **Jump** - пакетът се прехвърля към потребителска верига, като се предава към първото правило в нея (потребителската верига);
- **Log** - добавя съобщение към лога (преглед чрез */log print* или в прозореца от меню Log). Пакетът се предава към следващото правило;
- **Passthrough** - игнорира текущото правило и преминава към следващото (подходящо за статистика);
- **Reject** - пакетът се изхвърля и като отговор се изпраща ICMP съобщение на подателя. Пакетът не се проверява от следващите правила;
- **Return** - връщане назад към веригата преди изпълнение на **Jump**. Пакетът се предава към следващото правило (в основната верига, ако пътят му не е прекратен от правило в потребителската верига);
- **Tarpit** - улавяне и задържане на TCP връзката (отговор със SYN/ACK на входящите TCP SYN пакети). Пакетът не се предава за проверка от следващите правила в защитната стена. Възможно е да се използва за забавяне на атакуващия при атаки за отказ на услуга.



фигура 6

От изброените действия:

- **Accept**, **Add-dst-to-address-list**, **Add-src- to-address-list**, **Jump**, **Log**, **Passthrough** и **Return**, не прекратяват обработката на пакетите и ги предават към следващите по ред правила, в същата или друга верига, или ги връщат обратно;
- при **Fasttrack-connection**, **Drop**, **Reject** и **Tarpit**, пакетите се изхвърлят и проверката от следващи правила не се извършва.

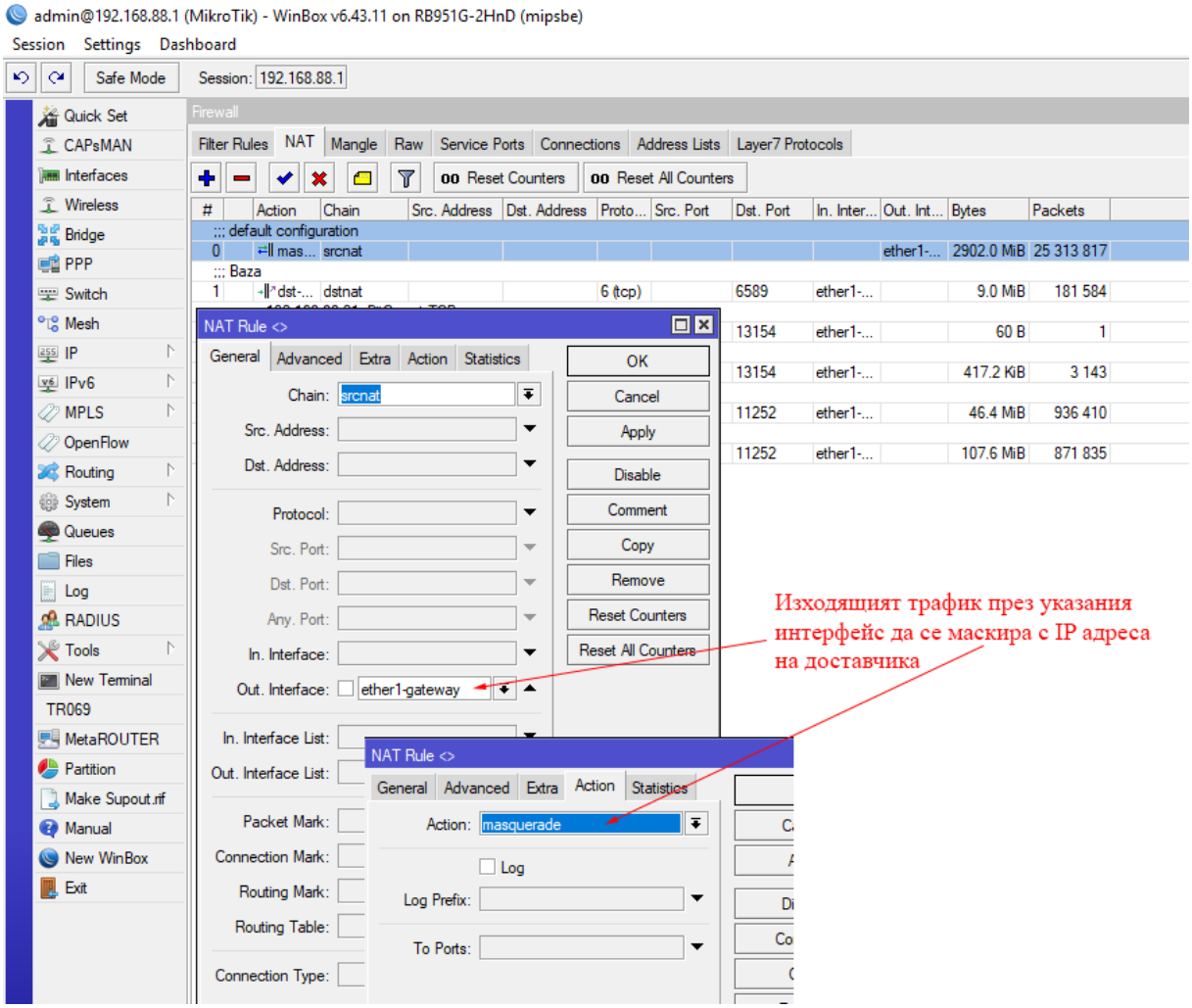
6. Транслиране на мрежови връзки (Network Address Translation, NAT)

Вторият раздел в защитната стена е наречен NAT. Стандартните вериги за този раздел са:

- **Srcnat** (source NAT) - маршрутизаторът подменя ***IP адреса*** и **порта** (TCP/UDP) **на подателя**, когато пакета идва от **мрежата, върху която се прилага NAT**. Обратната процедура се прилага, когато пакетите се връщат в обратната посока;
- **Dstnat** (destination NAT) - маршрутизаторът подменя **IP адреса на получателя**, когато пакета е предназначен за **мрежата, върху която се прилага NAT**. Обратната процедура се прилага върху пакетите „отговори“ при изход от мрежата зад NAT.

Поради спецификата на NAT, хостовете, които са разположени зад тази услуга се сблъскват с някои ограничения, поради което е възможно някои интернет протоколи да не работят коректно. За решаване на тези проблеми се използват така наречените NAT помощници (*NAT helpers*). Чрез тях се

осигуряват работа на редица протоколи през NAT. В менюто **Service Ports** на защитната стена е достъпен списък на всички NAT помощници в RouterOS.



фигура 7

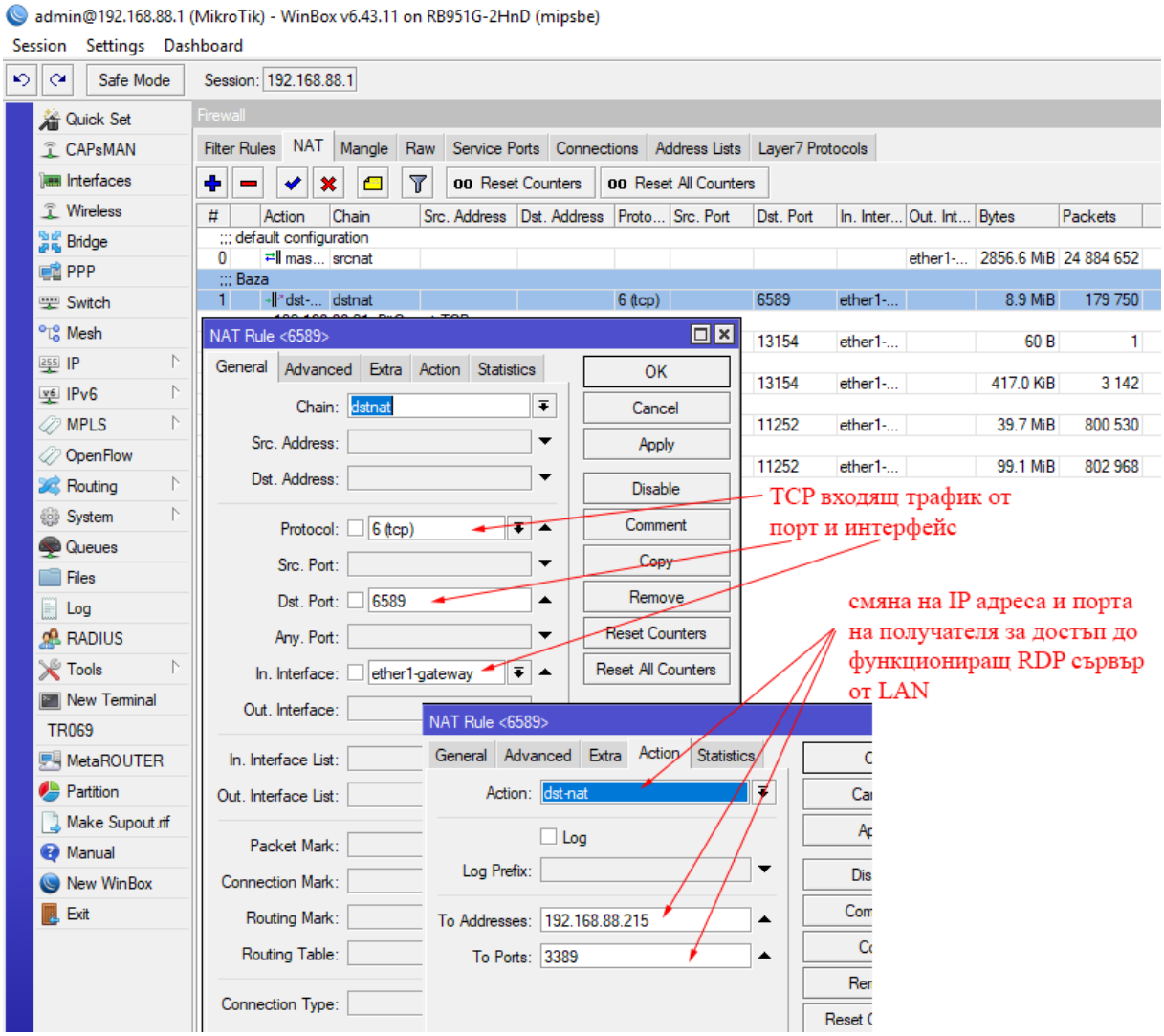
Четирите основни действия за двата типа NAT са:

- **masquerade** и **src-nat** – използват се, когато в условието бъде избрана веригата **srcnat**. Резултатът от прилагане на тези действия се изразява в подмяната на IP адреса и порта на подателя, когато пакетите напускат мрежата и обратно, когато се връщат. Разликата между masquerade (фигура 7) и src-nat е, че при действието src-nat е възможно да бъде определен кой точно IP адрес и порт на маршрутизатора да се поставя в пакетите, вместо тези на подателя.

- **dst-nat** се използва за осигуряване на достъп до услуги на сървъри от LAN зад NAT (например уеб сървър, пощенски сървър, файлов сървър). Достъп до RDP сървър от локалната

мрежа с IP адрес 192.168.88.215 и стандартен за услугата порт 3389 е показан на фигура 8.

- **redirect** – използва се за улавяне и препращане на трафика към услуга на самия маршрутизатор (например при пренасочване на DNS заявките към рекурсивния DNS сървъра в маршрутизатора или използване на прозрачно прокси).



фигура 8

7. Маркиране на пакети (Mangle)

Третият раздел в защитната стена се нарича Mangle. Основните функции, които са налични там се изразяват в поставяне на специални маркери към пакетите или връзките. В зависимост от **типа маркиране**, маркерите могат да се използват при **други услуги в самия маршрутизатор**. Например **маркиране на пакети, връзки** и **маршрутни маркери** може да се използва като условия във филтър, **маркирането на**

пакетите - при управление на качеството на услугите (QoS) в опашки (Queues), **маршрутните маркери** в маршрутните таблици.

При условията в правилата в Mangle също са налични предварително дефинирани вериги, които определят кога да се постави маркера. Веригите са, както следва:

- **Forward** - извършва се маркиране преди филтър във верига forward;
- **Input** - извършва се маркиране преди филтър във верига input;
- **Output** - извършва се маркиране преди филтър във верига output;
- **Postrouting** - извършва се маркиране преди действието src-nat;
- **Prerouting** - извършва се маркиране преди действието dst-nat.

Действията, които поставят маркери са:

- **mark-connection** - поставя маркер, който се задава на параметъра ***new-connection-mark***, на цялата връзка, за което е открито съответствие в условията;
- **mark-packet** - поставя маркер, който се задава на параметъра ***new-packet-mark***, на всеки пакет, за който е открито съответствие в условията;
- **mark-routing** - поставя маркер, който се задава на параметъра ***new-routing-mark***. Такива маркери се използват при управление на процеса на маршрутизация чрез политики.

Добра практика при използване на **mark-connection** и **mark- packet** е, първо да се приложат правила, с който да се маркират необходимите връзки, а след това да се изпълни правило, което да маркира пакетите в тях. Така няма да бъде необходимо целия трафик да се обработва от правилото за маркиране на пакети.

Най-новото действие, добавено от MikroTik в Mangle се нарича **route** - неговата функция е да пренасочва пакетите към зададен в правилото IP адрес на следващ маршрутизатор (Gateway), като игнорира нормалния процес на маршрутизация. Действието **route** може да се използва само с веригата prerouting, защото тя се работи преди процесът на маршрутизация да вземе решение.

8. Ранна обработка на пакети (RAW)

Най-новите функции, свързани с работата на защитната стена в RouterOS, са разположени в таба RAW. Работата с него наподобява до голяма степен тази на филтър, въпреки че условията и действията са значително по-малко.

Причина за това е, че правилата в RAW таба, позволяват селектирано пропускане или прекратяване на пакети, **преди те да попаднат в системата за проследяване на връзките**. Поради тази причина в правилата няма условия, които зависят от системата за проследяване на връзките. Ако даден пакет е маркиран да заобиколи системата за проследяване на връзки, той ще продължи своя път без да бъде дефрагментиран. Действията на правилата могат осезаемо да намалят натоварването на централния процесор. Правилата са особено подходящи **за борба с атаки за отказ на услуга**.

При правилата са налични две вериги по подразбиране:

- **prerouting** - използва се за обработка на всеки пакет, който постъпва в маршрутизатора;
- **output** - използва се за обработка на пакетите, произхождащи от маршрутизатора и напускащи през някой от неговите мрежови интерфейси. Пакетите, които преминават през маршрутизатора не попадат на правилата от веригата.

При създаване на правила възможните действия са следните: **accept**, **add-dst-to-address-list**, **add-src-to-address-list**, **drop, jump**, **log**, **notrack, passthrough**, **return**.

Единственото различно действие спрямо тези във филтъра е **notrack**. Пакетите, които попаднат на правило с това действие няма да бъдат препращани към системата за проследяване на връзките.

9. Списъци с адреси

Списъците с адреси (раздел **Address Lists**) в защитната стена предоставят възможност за групиране на IP адреси и мрежи под общо име. Тези списъци могат да се използват като условия за търсене на съответствие при създаване на правила в филтър, транслиране на мрежови връзки, при маркиране или при ранна обработка на пакетите (в разделите Filter Rules, NAT, Mangle, RAW)

Списъците с адреси могат да се създават, както ръчно, така и динамично с действието **add-dst-to-address-list** или **add-src-to-address-list**.

Чрез списъците с адреси могат да бъдат обозначавани и идентифицирани (техните IP адреси): администратори, които да получат специфични права; хакери; мрежи на държави; безжични клиенти; IP адресите на социални мрежи и много други.

Списъците с адреси помагат за оптимално решаване на ситуации, които например изискват да бъдат създадени 100 правила за да бъдат блокирани 100 IP адреса. Вместо това е възможно да бъде създаден един списък от 100 IP адреса и само с едно правило в защитната стена всички да бъдат блокирани.