



Итрансляция сетевых адресов (NAT) и Firewall filter



Network Address Translation

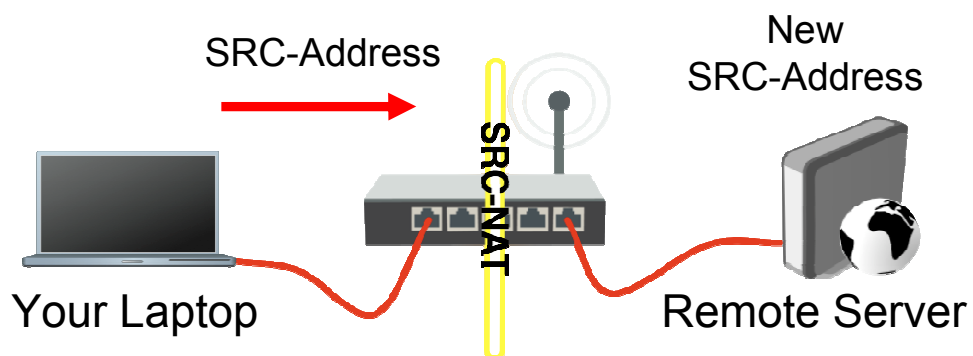
NAT

- Роутер может заменить **Source(источник)** или **Destination(назначение)** адреса когда пакеты следуют ...
- Этот процесс называется **src-nat** или **dst-nat**

3

3

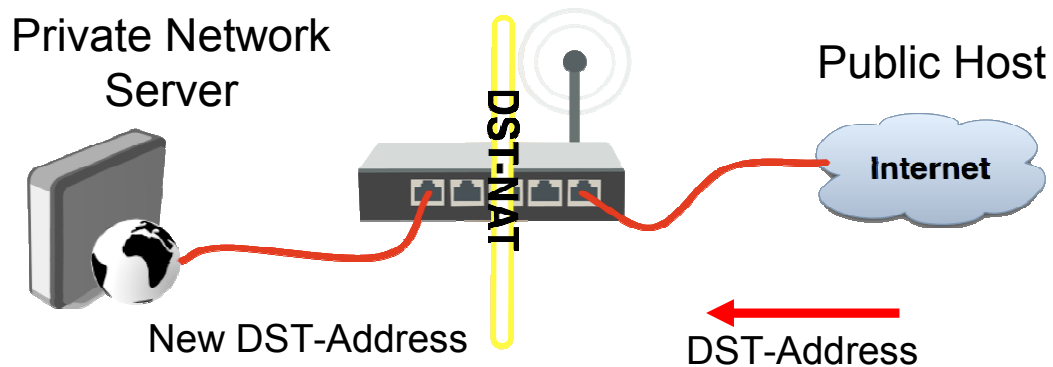
SRC-NAT



4

4

DST-NAT



5

5

NAT Chains (цепи)

- Необходимо выбрать цепочку : **srcnat** или **dstnat**
- NAT правила работают по принципу **IF-THEN** (ЕСЛИ-ТО)

6

6

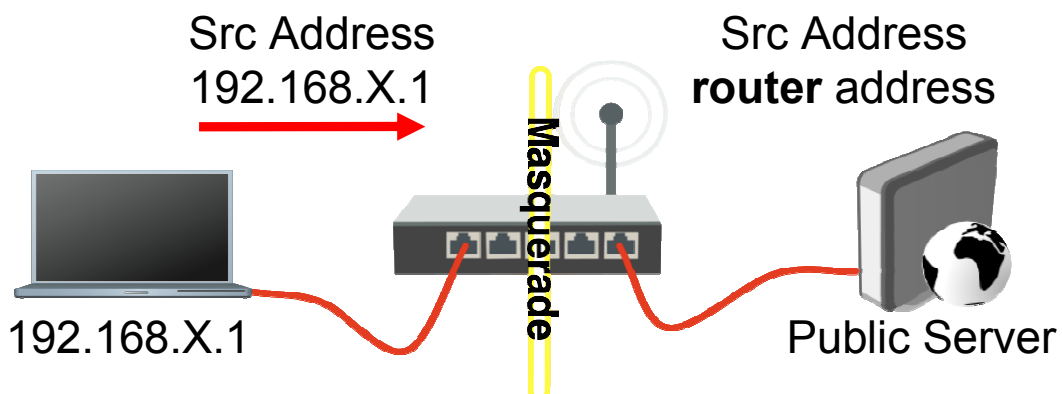
SRC-NAT

- **SRC-NAT** подменяет в packet's (пакетах) source address (адрес источника)
- Вы можете использовать его для подключения вашей приватной сети к Интернету через публичный IP адрес
- **Masquerade** это один из типов SRC-NAT

7

7

Masquerade



8

8

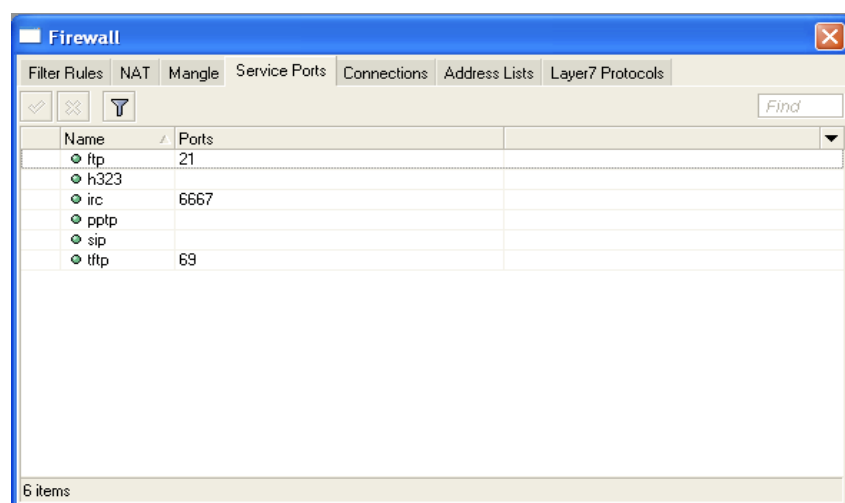
Ограничения SRC-NAT

- Подключение к внутренним серверам из публичной сети невозможно (DST-NAT needed)
- Некоторым протоколам необходимо использовать NAT helpers для правильной работы

9

9

NAT Helpers



1

10

Connection Tracking

- Connection tracking управляет информацией о всех активных соединений.
- Он должен быть включен для Filter и NAT

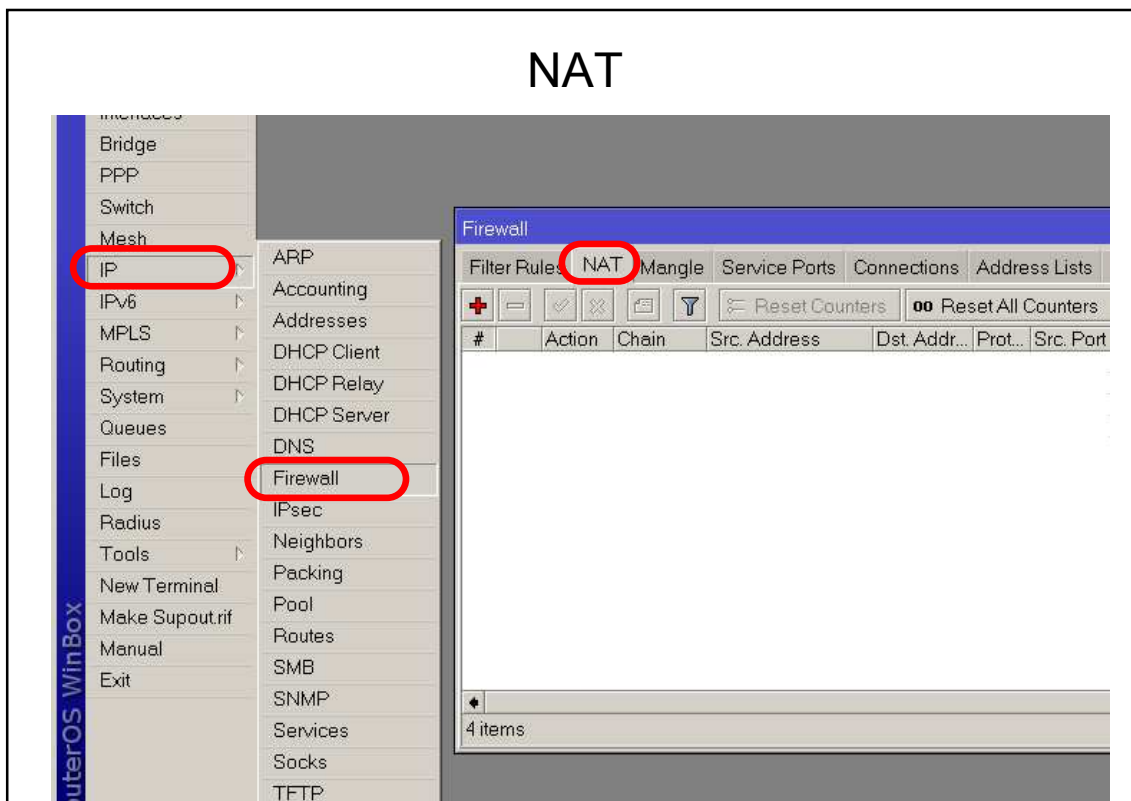
11

1

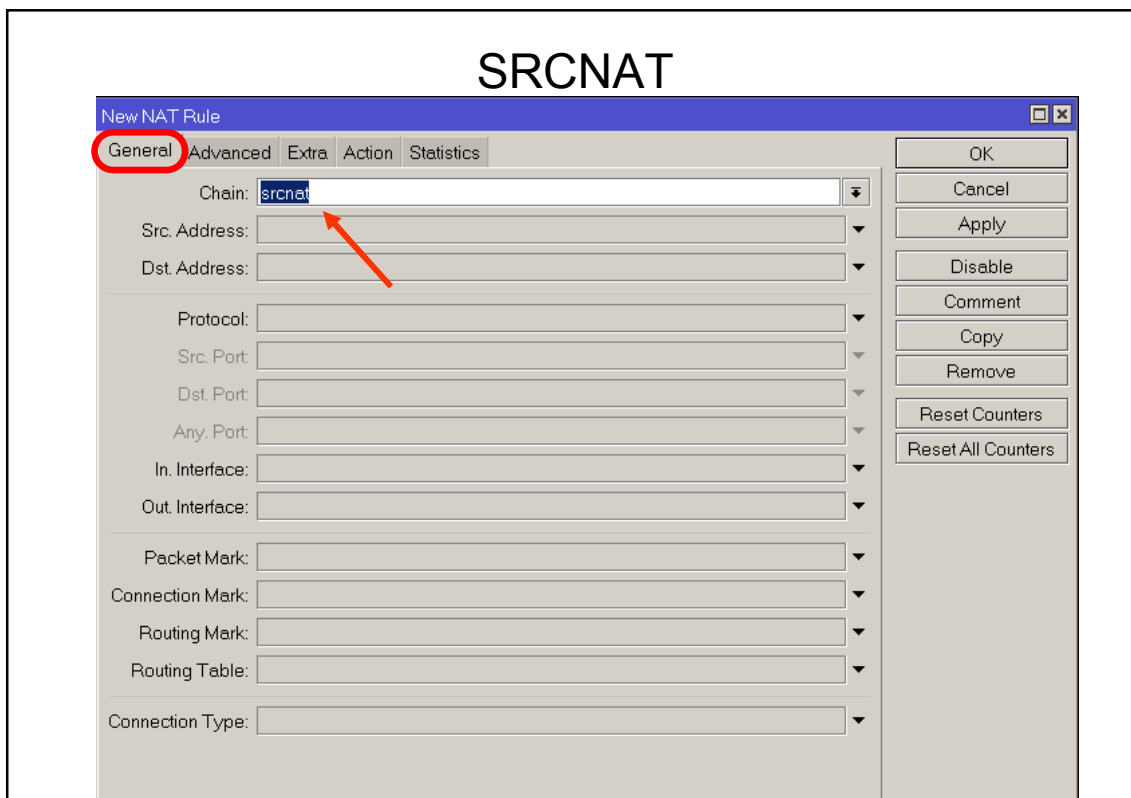
Connection Tracking

The screenshot shows the Mikrotik WinBox interface. On the left, the 'RouterOS WinBox' menu is visible with 'IP' and 'Firewall' highlighted by red circles. The main window displays the 'Firewall' configuration page, with the 'Connections' tab selected and also highlighted by a red circle. Below the 'Connections' tab, the 'Tracking' sub-tab is active. A 'Connection Tracking' dialog box is open, showing the 'Enabled' checkbox checked. The dialog contains various timeout settings for TCP and UDP connections, such as 'TCP Syn Sent Timeout' (00:00:05), 'TCP Established Timeout' (1d 00:00:00), and 'UDP Timeout' (00:00:10).

NAT



SRCNAT



SRCNAT

New NAT Rule

General Advanced Extra Action Statistics

Chain: srcnat

Src. Address:

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

In. Interface:

Out. Interface: ☐ ether10

Packet Mark:

Connection Mark:

Routing Mark:

Routing Table:

Connection Type:

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Reset Counters

Reset All Counters

SRCNAT

New NAT Rule

General Advanced Extra Action Statistics

Action: src-nat

To Addresses: 87.234.54.3

To Ports:

OK

Cancel

Apply

Disable

Comment

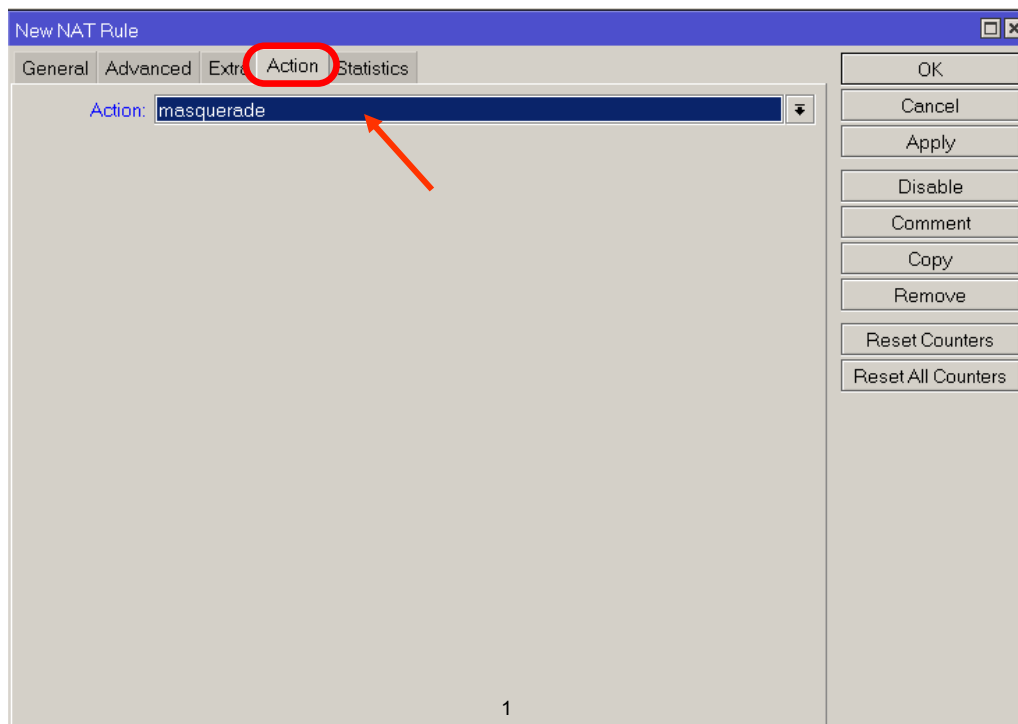
Copy

Remove

Reset Counters

Reset All Counters

Masquerade

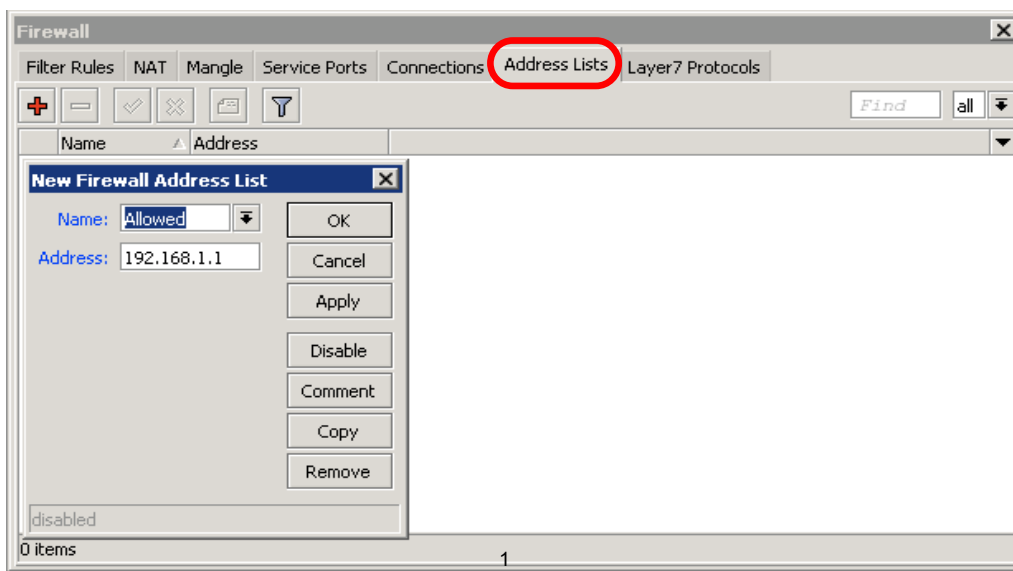


Address-List

- Address-list позволяет вам группировать различные IP адреса IP-сети для дальнейшего применения в правилах
- Автоматически добавлять адреса в address-list и затем блокировать

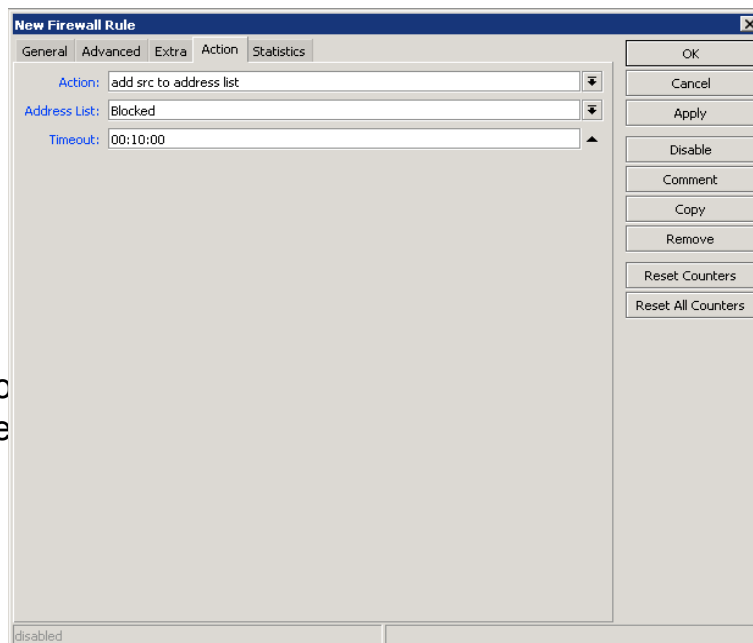
Address-List

- Создавать различные группы
- Подсети, диапазон адресов, или же один хост



Address-List

- Add specific host to address-list
- Specify timeout for temporary service



Address-List

21

- Удалите все правила NAT
- Создайте правило src-nat позволяющее вашей локальной сети выходить в Интернет
- Создайте правило src-nat позволяющее группе IP адресов "internet users" выходить в Интернет (и отключите предыдущее правило)
- Создайте правило src-nat позволяющее выходить в Интернет всем IP кроме определенных IP адресов (и отключите предыдущее правило)
- Создайте правило src-nat позволяющее одному IP выходить в Интернет и только на сайт mail.md (и отключите предыдущее правило)
- Создайте правило src-nat позволяющее вашей локальной сети выходить в интернет, но только на WEB (80 и 443 порты) ресурсы.
- Удалите все правила NAT и создайте правило разрешающее вашей сети выход в интернет

LAB

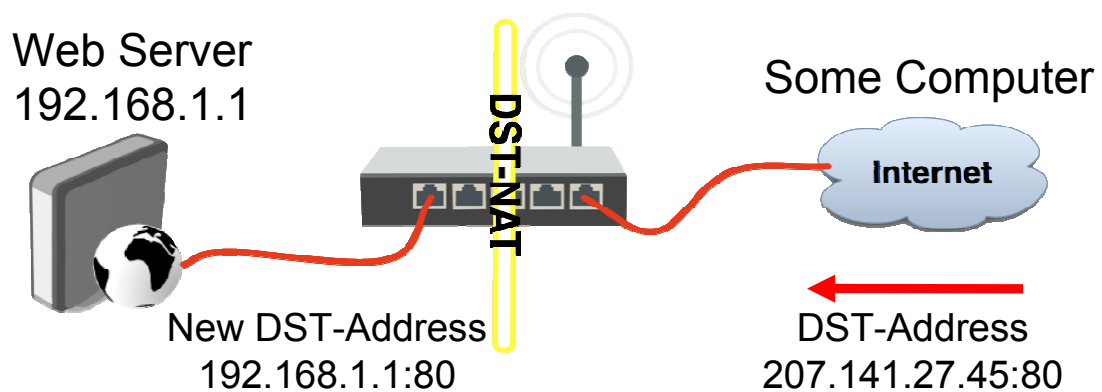
DST-NAT

- DST-NAT подменяет в пакетах destination address(адрес назначения) и port
- Он может быть использован, чтобы направить интернет-пользователей на сервер в вашей локальной сети

23

2

DST-NAT Example

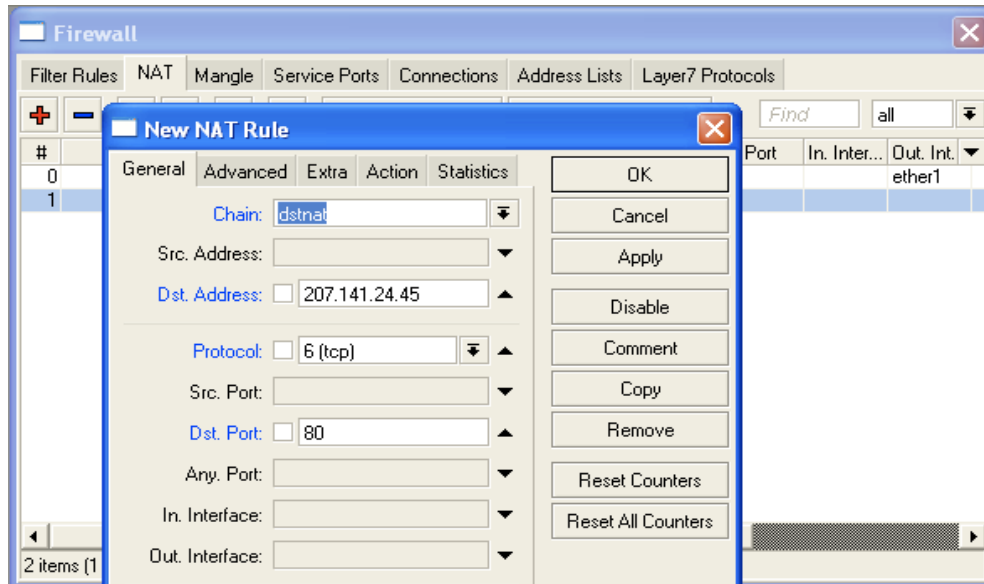


24

2

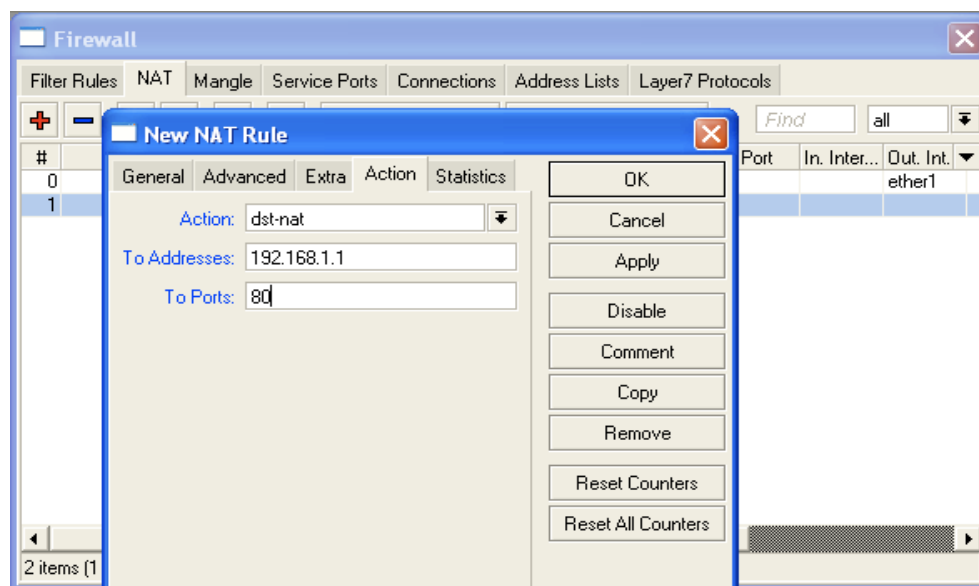
DST-NAT Example

- Создадим правило которое позволит пробросить трафик до WEB сервера в приватной сети



DST-NAT Example

- Создадим правило которое позволит пробросить трафик до WEB сервера в приватной сети



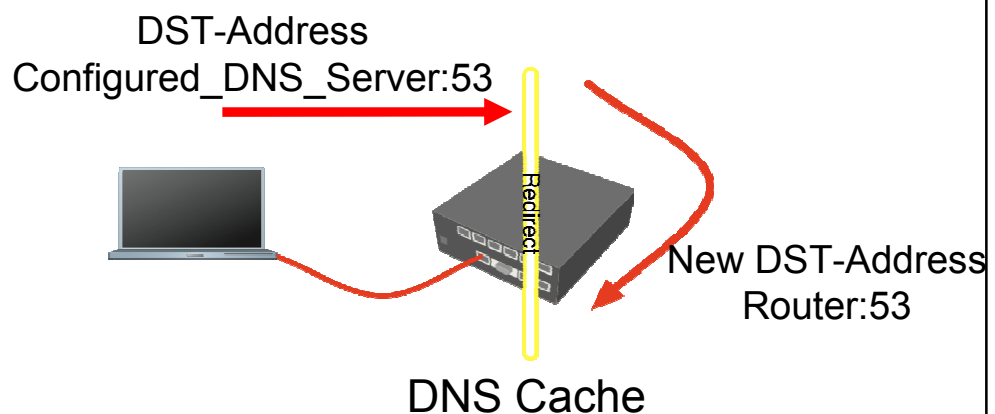
Redirect

- Специальный тип DST-NAT
- Это действие перенаправляет пакеты на сам роутер
- Данное действие можно применять для проксирования таких сервисов (DNS, HTTP)

27

2

Redirect example



28

2

Redirect Example

- Let's make local users to use Router DNS cache
- Also make rule for **udp** protocol

New NAT Rule

General | Advanced | Extra | Action | Statistics

Chain: dstnat

Src. Address:

Dst. Address:

Protocol: ☐ udp

Src. Port:

Dst. Port: 53

Any. Port:

In. Interface:

Out. Interface:

Packet Mark:

Connection Mark:

Routing Mark:

Connection Type:

Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove, Reset Counters, Reset All Counters

29

Redirect Example

- Let's make local users to use Router DNS cache
- Also make rule for **udp** protocol

New NAT Rule

General | Advanced | Extra | Action | Statistics

Action: redirect

To Ports: 53

Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove, Reset Counters, Reset All Counters

30

NAT Actions

- Accept
- DST-NAT/SRC-NAT
- Redirect
- Masquerade
- Netmap

31

3

LAB

- Перенаправьте все запросы на внешние DNS сервера на свой роутер
- У вас в локальной сети имеется почтовый сервер (который использует порты 110,25,143,80), создайте правило которое позволит пробросить трафик до вашего почтового сервера

Firewall

33

Firewall

- Защищает Ваш роутер и Ваших клиентов (сети) от несанкционированного доступа
- Это можно сделать путем создания правил в Firewall Filter и NAT

34

Firewall Filter

- Состоит из пользовательских правил которые работают по принципу **IF-Then** (если-то)
- Эти правила упорядочены в цепочки (Chains)
- Имеются predetermined цепочки (Chains), и цепочки (Chans) созданные пользователем

35

3

Filter Chains

- Правила могут быть помещены в 3 цепочки по умолчанию
 - input (**to** router (на роутер))
 - output (**from** router (с роутера))
 - forward (**through** the router(через роутер))

36

3

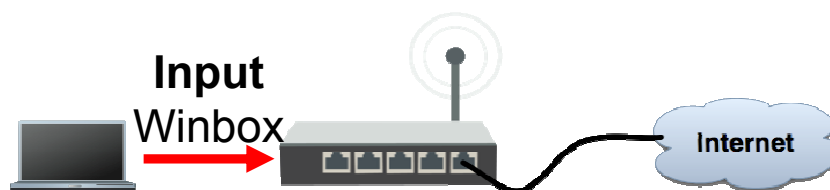
Firewall Chains



37

3

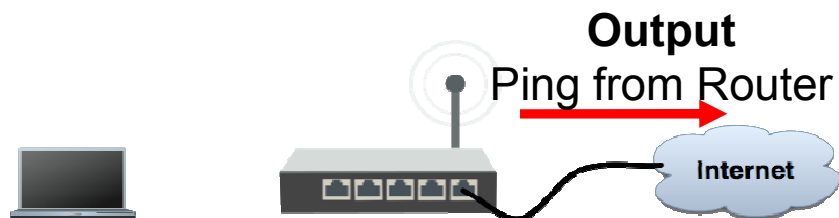
Firewall Chains



38

3

Firewall Chains



39

3

Firewall Chains

Firewall

Filter Rules NAT Mangle Service Ports Connections Address Lists Layer7 Protocols

Reset Counters Reset All Counters Find all

#	Action	Chain	Src. Address	Dst. Address	Prot...	Src. Port	Dst. Port	In. Int...	Out. I...	Byte...
0 items										

40

4

Input

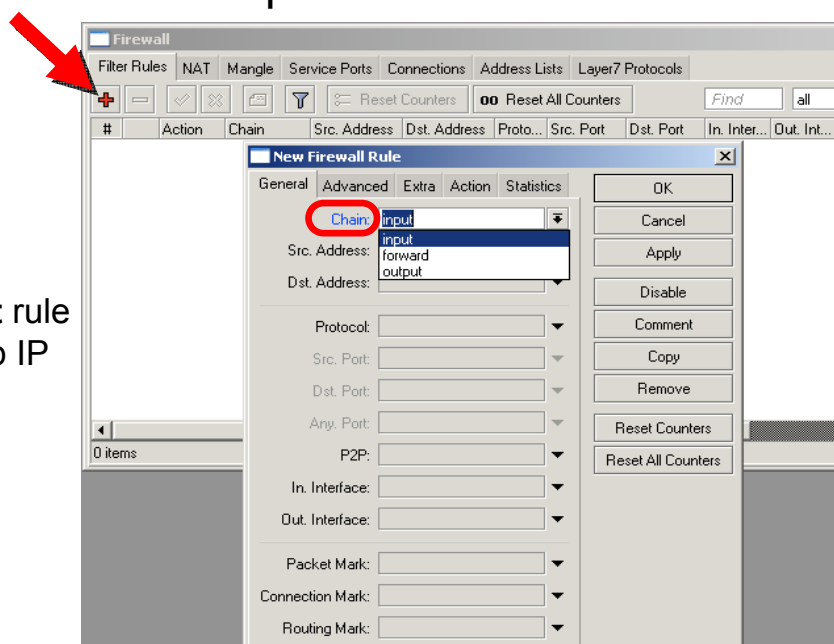
- Правила которые защищают сам роутер
- Давайте заблокируем всем доступ к роутеру кроме вашего ноутбука

41

4

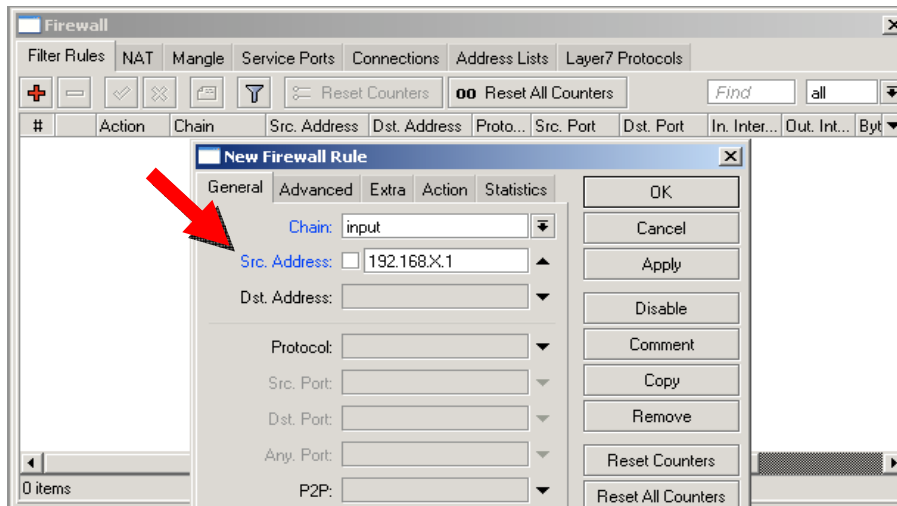
Input

- Add an **accept** rule for your Laptop IP address



4

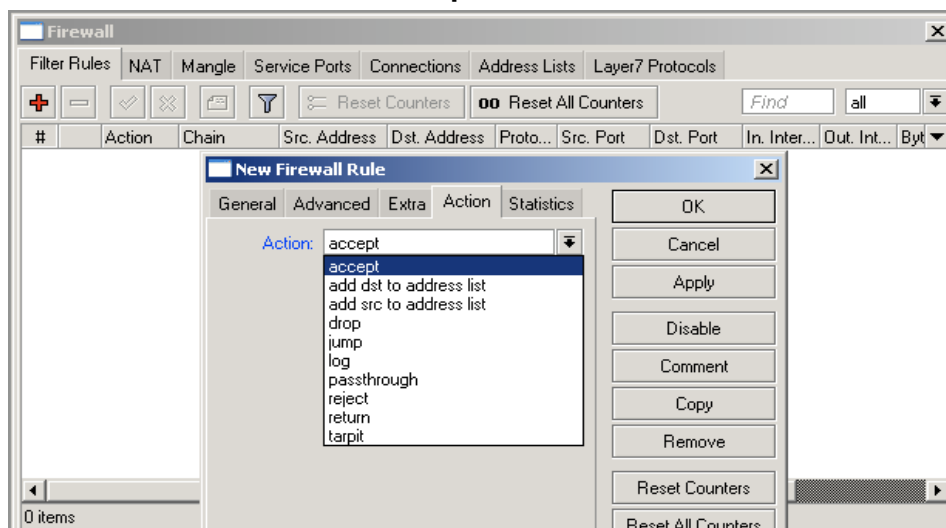
Input



- Add an **accept** rule for your Laptop IP address

43

Input

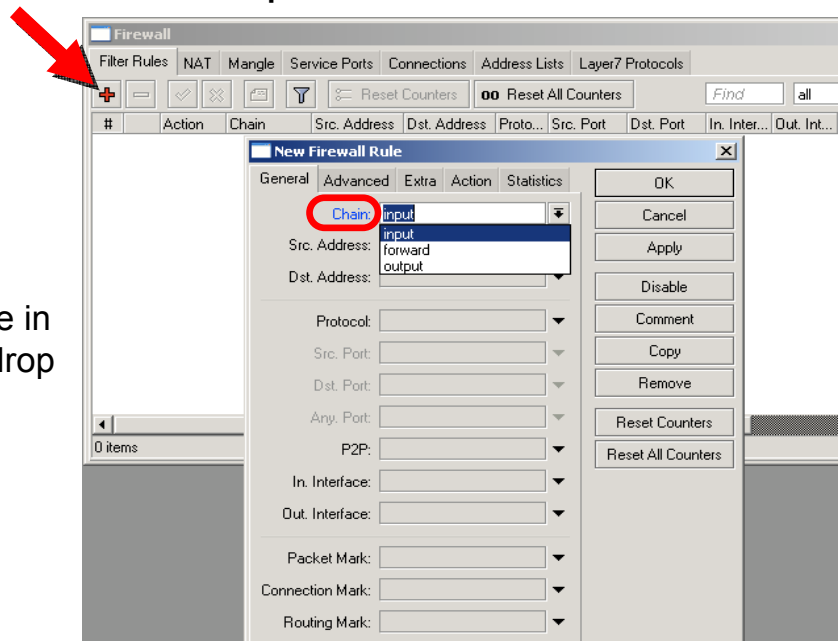


- Add an **accept** rule for your Laptop IP address

44

Input

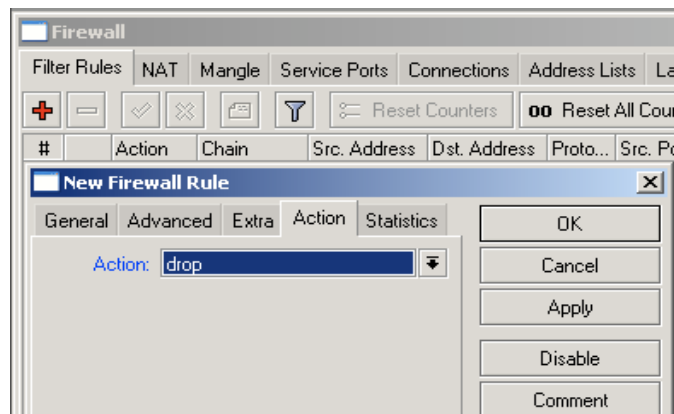
- Add a **drop** rule in input chain to drop everyone else



4

Input

- Add a **drop** rule in input chain to drop everyone else



46

4

Input Lab

LAB

- Поменяйте на вашем ноутбуке IP address, 192.168.x.**y**
- Проверьте подключение. Убедитесь в работе firewall
- Вы можете подключиться по MAC-address, Firewall Filter только для IP

47

4

Input

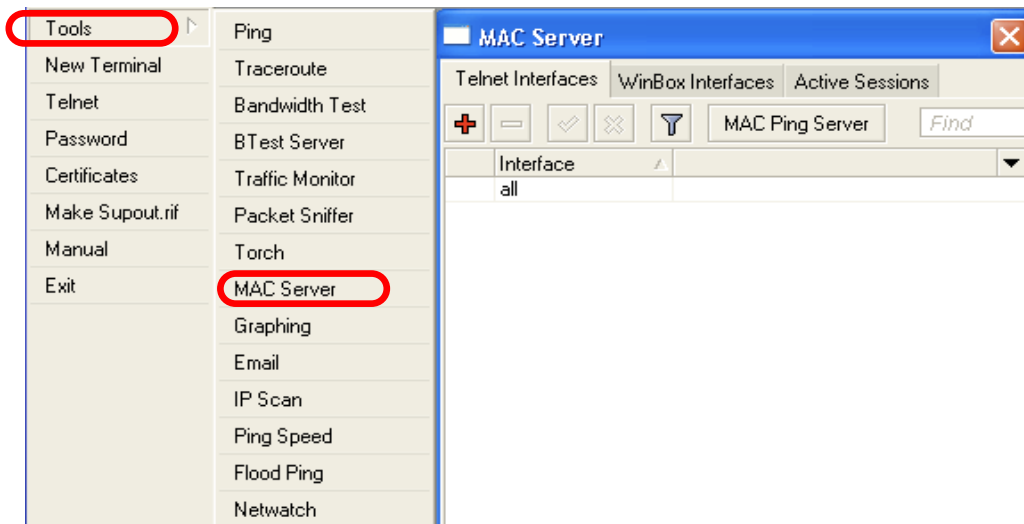
LAB

- Доступ к вашему роутеру заблокирован (кроме вашего IP)
- Интернет не работает
- Отключите правила Filter rules что бы у вас появился интернет
- Подключитесь к роутеру по IP

48

4

Input



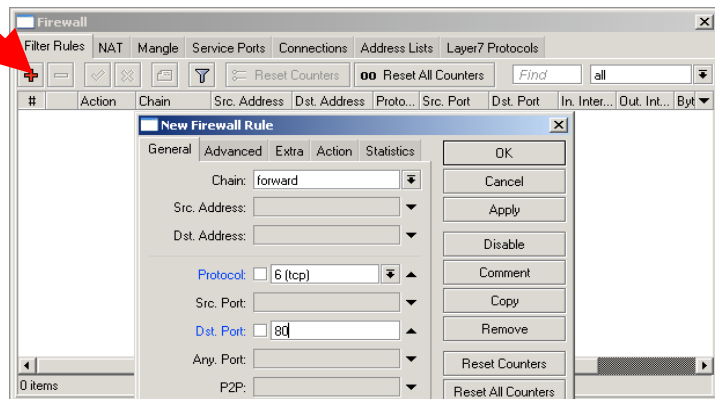
- Вы можете отключить доступ по MAC в меню **MAC Server**

Forward

- Цепочки правил которые контролируют пакеты проходящие **через** роутер
- Контроль трафика **до и от клиентов**

Forward

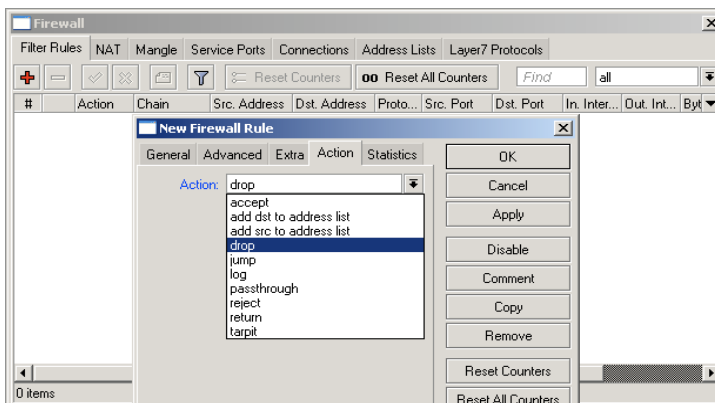
- Создадим правило которое заблокирует TCP port 80 (web browsing)
- Must select protocol to block ports



51

Forward

- Создадим правило которое заблокирует TCP port 80 (web browsing)
- Must select protocol to block ports



52

Forward

- Заблокируйте Web browsing
- Попробуйте открыть www.aitec.md
- Попробуйте открыть <http://192.168.X.1>
- web страница роутера работает потому что наше правило работает для блокировки **chain=forward** трафика

53

5

List of well-known ports

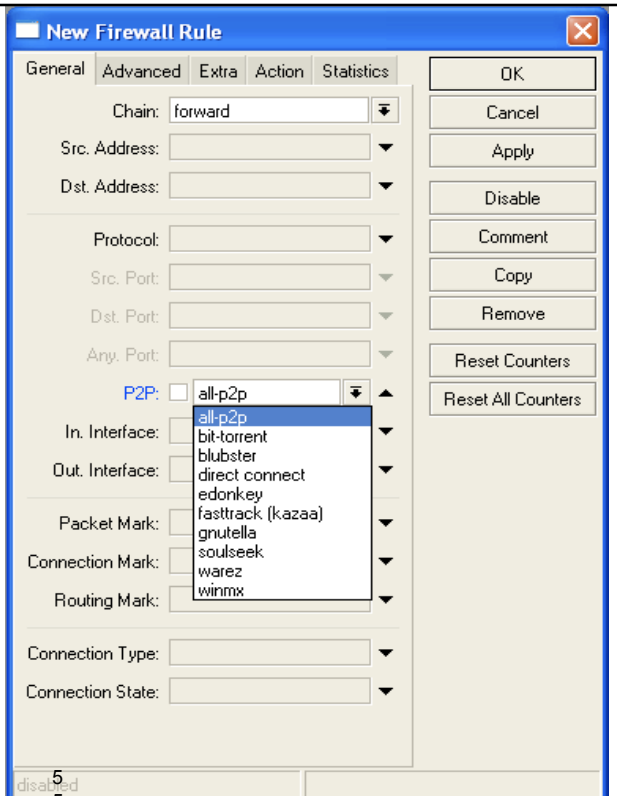
Port	Protocol	Service
80	TCP	WWW, HTTP
22	TCP	SSH
23	TCP	Telnet
53	TCP/UDP	DNS
21,20	TCP	FTP
8291	TCP	Winbox
123	UDP	NTP
443	TCP	HTTPS, SSL
5678	UDP	MNDP
8080	TCP	MikroTik Proxy
20561	UDP	MAC-Winbox
/1	ICMP	Pings

54

5

Forward

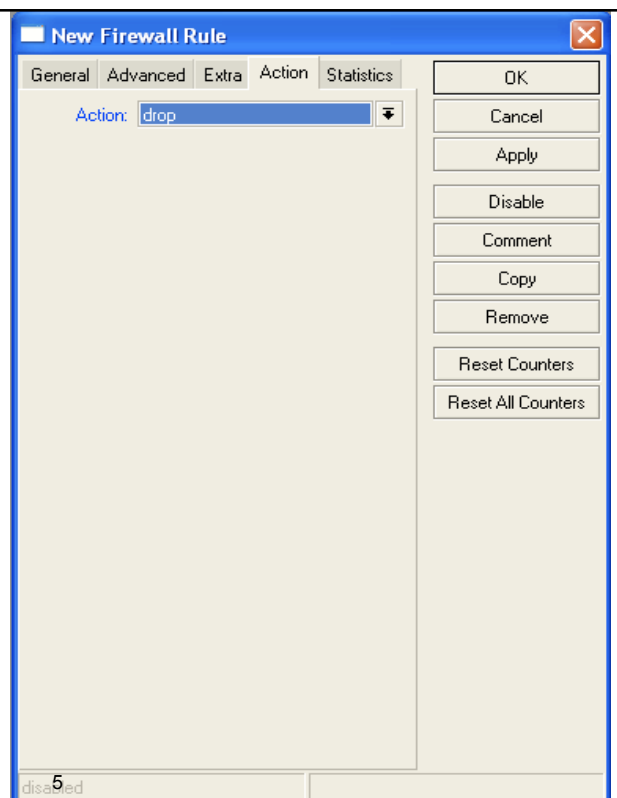
- Create a rule that will block client's p2p traffic



The 'New Firewall Rule' dialog box is shown with the 'General' tab selected. The 'Chain' is set to 'forward'. The 'Src. Address' and 'Dst. Address' fields are empty. The 'Protocol' is set to 'all'. The 'Src. Port' and 'Dst. Port' fields are empty. The 'Any. Port' field is empty. The 'P2P' checkbox is checked, and a dropdown menu is open showing a list of P2P protocols: all-p2p, bit-torrent, blubster, direct connect, edonkey, fasttrack (kazaa), gnutella, soulseek, warez, and winmx. The 'In. Interface' and 'Out. Interface' fields are empty. The 'Packet Mark', 'Connection Mark', and 'Routing Mark' fields are empty. The 'Connection Type' and 'Connection State' fields are empty. The 'Action' field is set to 'drop'. The 'Statistics' tab is selected. The 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', 'Remove', 'Reset Counters', and 'Reset All Counters' buttons are visible on the right.

Forward

- Create a rule that will block client's p2p traffic



The 'New Firewall Rule' dialog box is shown with the 'Action' tab selected. The 'Action' field is set to 'drop'. The 'Statistics' tab is selected. The 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', 'Remove', 'Reset Counters', and 'Reset All Counters' buttons are visible on the right.

Firewall Log

- Let's log client pings to the router
- Log rule should be added before other **action**

New Firewall Rule

General | Advanced | Extra | Action | Statistics

Chain: input

Src. Address:

Dst. Address:

Protocol: ☐ icmp

Src. Port:

Dst. Port:

Any. Port:

P2P:

In. Interface:

Out. Interface:

Packet Mark:

Connection Mark:

Routing Mark:

Connection Type:

Connection State:

Action: log

Log Prefix: ICMP

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Reset Counters

Reset All Counters

disabled

Firewall Log

- Let's log client pings to the router
- Log rule should be added before other **action**

New Firewall Rule

General | Advanced | Extra | Action | Statistics

Chain: input

Src. Address:

Dst. Address:

Protocol: ☐ icmp

Src. Port:

Dst. Port:

Any. Port:

P2P:

In. Interface:

Out. Interface:

Packet Mark:

Connection Mark:

Routing Mark:

Connection Type:

Connection State:

Action: log

Log Prefix: ICMP

OK

Cancel

Apply

Disable

Comment

Copy

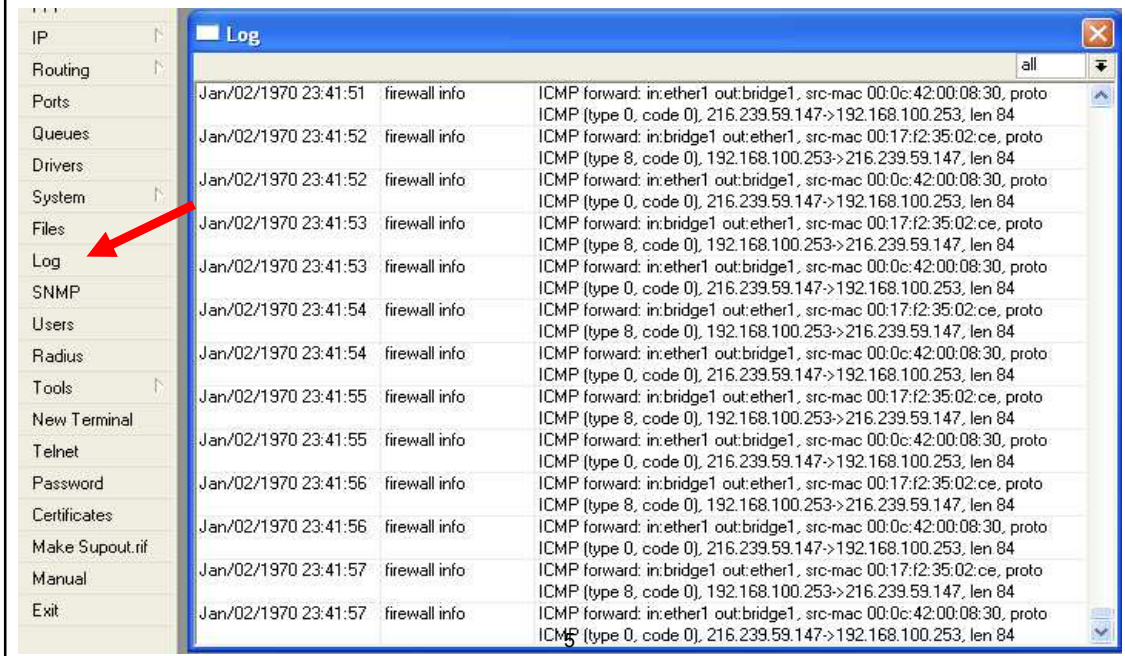
Remove

Reset Counters

Reset All Counters

disabled

Firewall Log



Time	Event	Details
Jan/02/1970 23:41:51	firewall info	ICMP forward: in:ether1 out:bridge1, src-mac 00:0c:42:00:08:30, proto
Jan/02/1970 23:41:52	firewall info	ICMP (type 0, code 0), 216.239.59.147->192.168.100.253, len 84
Jan/02/1970 23:41:52	firewall info	ICMP forward: in:bridge1 out:ether1, src-mac 00:17:f2:35:02:ce, proto
Jan/02/1970 23:41:52	firewall info	ICMP (type 8, code 0), 192.168.100.253->216.239.59.147, len 84
Jan/02/1970 23:41:53	firewall info	ICMP forward: in:ether1 out:bridge1, src-mac 00:0c:42:00:08:30, proto
Jan/02/1970 23:41:53	firewall info	ICMP (type 0, code 0), 216.239.59.147->192.168.100.253, len 84
Jan/02/1970 23:41:53	firewall info	ICMP forward: in:bridge1 out:ether1, src-mac 00:17:f2:35:02:ce, proto
Jan/02/1970 23:41:53	firewall info	ICMP (type 8, code 0), 192.168.100.253->216.239.59.147, len 84
Jan/02/1970 23:41:54	firewall info	ICMP forward: in:ether1 out:bridge1, src-mac 00:0c:42:00:08:30, proto
Jan/02/1970 23:41:54	firewall info	ICMP (type 0, code 0), 216.239.59.147->192.168.100.253, len 84
Jan/02/1970 23:41:54	firewall info	ICMP forward: in:bridge1 out:ether1, src-mac 00:17:f2:35:02:ce, proto
Jan/02/1970 23:41:54	firewall info	ICMP (type 8, code 0), 192.168.100.253->216.239.59.147, len 84
Jan/02/1970 23:41:55	firewall info	ICMP forward: in:ether1 out:bridge1, src-mac 00:0c:42:00:08:30, proto
Jan/02/1970 23:41:55	firewall info	ICMP (type 0, code 0), 216.239.59.147->192.168.100.253, len 84
Jan/02/1970 23:41:55	firewall info	ICMP forward: in:bridge1 out:ether1, src-mac 00:17:f2:35:02:ce, proto
Jan/02/1970 23:41:55	firewall info	ICMP (type 8, code 0), 192.168.100.253->216.239.59.147, len 84
Jan/02/1970 23:41:56	firewall info	ICMP forward: in:ether1 out:bridge1, src-mac 00:0c:42:00:08:30, proto
Jan/02/1970 23:41:56	firewall info	ICMP (type 0, code 0), 216.239.59.147->192.168.100.253, len 84
Jan/02/1970 23:41:56	firewall info	ICMP forward: in:bridge1 out:ether1, src-mac 00:17:f2:35:02:ce, proto
Jan/02/1970 23:41:56	firewall info	ICMP (type 8, code 0), 192.168.100.253->216.239.59.147, len 84
Jan/02/1970 23:41:57	firewall info	ICMP forward: in:ether1 out:bridge1, src-mac 00:0c:42:00:08:30, proto
Jan/02/1970 23:41:57	firewall info	ICMP (type 0, code 0), 216.239.59.147->192.168.100.253, len 84

Firewall chain Lab

- Удалите все правила firewall
- Закройте доступ на роутер с внешнего интерфейса(wlan1) по winbox
- Закройте доступ в Интернет “плохим” пользователям (192.168.x.34 ; 192.168.x.54; 192.168.x.65 – 89)
- Ваш роутер будет выполнять функции VPN сервера, откройте порты для доступа к нему (UDP 1701,TCP 1723)
- Закройте одноклассников (по контенту)
- Закройте ping до сайта aitec.md
- Заблокируйте порт на роутере telnet (TCP – 23) т.к это не безопасно
- Пользователям 192.168.x.24, 192.168.x.25 – нужно закрыть доступ на сервер 212.0.3.43 на порты 110,25,143,80
- Ваш роутер не должен пинговать 212.0.200.1

60

Firewall chain Lab

LAB

- Удалите все правила firewall
- Вам необходимо сделать группу пользователей Group1 (IP – x.43, x.56, x89, x.2) которым разрешенно пользоваться только WEB траффиком в интернете (остальной внешний траффик блокировать), так же на компьютере x.2 стоит сервис на порту 888, нужно дать доступ к этому локальному серверу с Интернета на указанный порт.

61

6

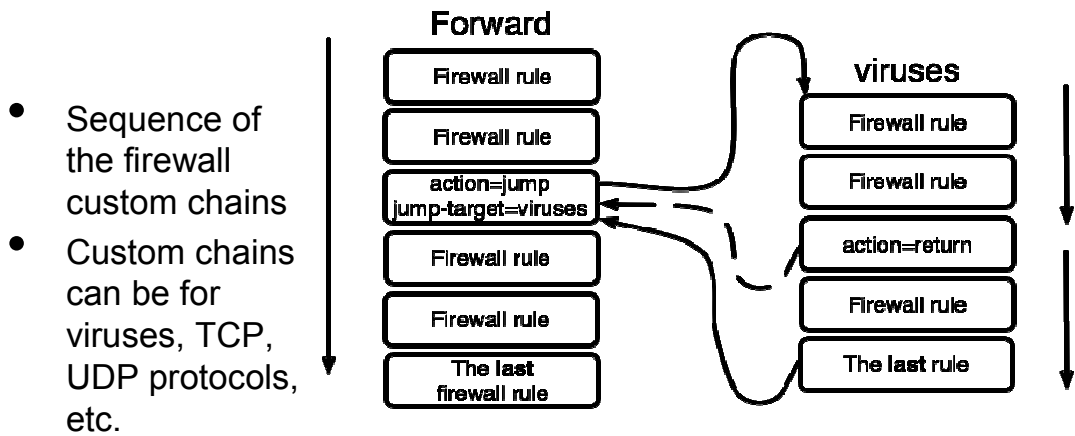
Firewall chains

- Помимо стандартных цепочек (input, forward, output), пользователи могут создавать свои
- Это помогает упростить структуру firewall
- И снижает нагрузку на роутер

62

6

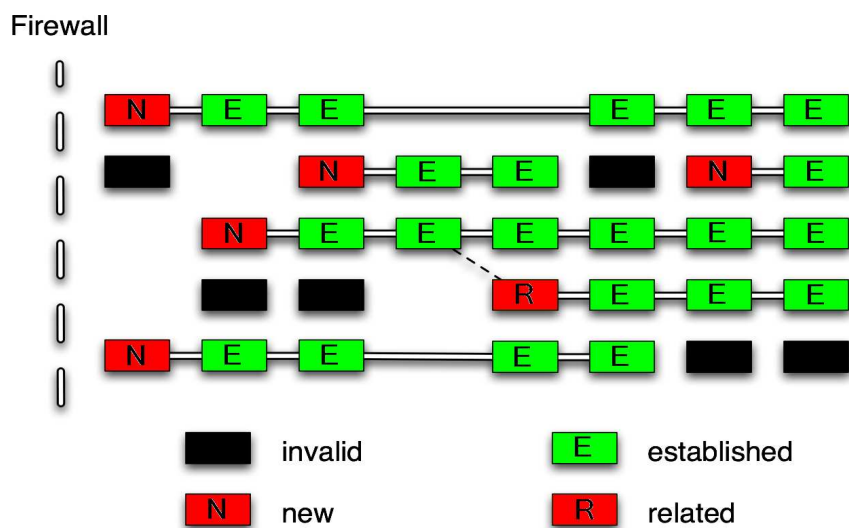
Firewall chains in Action



63

6

Connections (Соединения)



64

6

Connection State

- Рекомендуем, блокировать invalid соединения
- Firewall должен работать только с новыми пакетами, и рекомендуется пропускать остальные состояния пакетов
- Правила фильтрации имеют “connection state”

65

6

Connection State

LAB

- Удалите все правила firewall
- Добавьте правило drop invalid packets
- Добавьте правило accept established packets
- Добавьте правило accept related packets
- Дайте Firewall работать **только** с **new** пакетами

66

6

Firewall Actions

- Accept
- Drop
- Reject
- Tarpit
- log
- add-src-to-address-list(dst)
- Jump, Return
- Passthrough

67