

# MikroTik Certified Security Engineer

MTCSE

## Chapter 2.2: Security Basic Firewall

Filter Rules  
Custom chains

ICMP Filtering

RAW Table

Security Areas

Tracking

Stateful  
Firewall

Default  
Configuration

Management  
access and  
other

Simple Bridge  
Filter  
Rules

Basic Firewall  
Rules



**qualitytraining**  
Succeed with Quality

MTI-GROUP LLC / network academy

V.21-01

# ROUTEROS DEFAULT CONFIGURATION

Когда следует удалить конфигурацию по умолчанию и настроить роутер с нуля?

# ROUTEROS DEFAULT CONFIGURATION

<https://help.mikrotik.com/docs/display/ROS/Default+configurations>

Все RouterBOARDs с завода приходят с дефолтной конфигурацией. Есть несколько разных конфигураций в зависимости от модели:

- CPE router
- LTE CPE AP router
- AP router (single or dual band)
- PTP Bridge (AP or CPE)
- WISP Bridge (AP in ap\_bridge mode)
- Switch
- IP only
- CAP (Controlled Access Point)

## ROUTEROS DEFAULT CONFIGURATION

На платах embedded просто прописан IP-адрес 192.168.88.1/24

На многих бордах(core) один интерфейс выделен под wan (как правило первый) на котором настроен dhcp-client, отключен вход по MAC и MNDP, настроен firewall с мин.конфигурацией, остальные интерфейсы добавлены в бридж, на котором прописан IP 192.168.88.1/24 и настроен dhcp-server

На оборудовании wireless (для мостов, ТД и т.д.) настроен бридж, куда добавлены интерфейсы ether1 и беспроводной модуль



# ROUTEROS DEFAULT CONFIGURATION and IPv6

- Пакет IPv6 по умолчанию отключен в RouterOS v6.
- Если произвести сброс настроек в Default - когда пакет IPv6 был включен то Firewall filter - так же настроится для IPv6

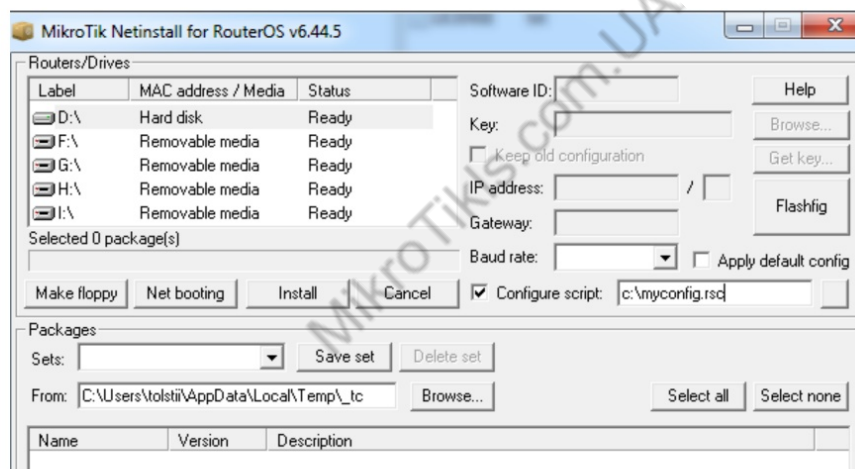
## ROUTEROS DEFAULT CONFIGURATION

посмотреть дефолтную конфигурацию можно:

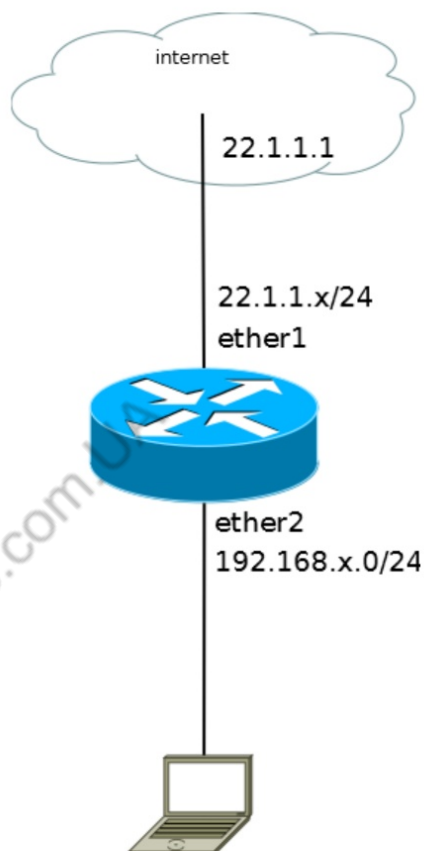
- `/system default-configuration print`

изменить дефолтную конфигурацию можно используя

- `netinstall (mtcna)`
- `/system default-configuration custom-script`



# LAB



- настройте роутер по схеме
- сбросьте маршрутизатор в "нулевую" конфигурацию
- идентификация роутера : X\_YourName
- wan ether1(wlan1 - MikroTik-Ntema) ip 22.1.1.x/24 gw 22.1.1.1 dns 22.1.1.1
- lan ether2 ip 192.168.x.1/24
- обновите RouterOS и FW
- настройте интернет для локальной сети
- создайте пользователя **man** с паролем Man33ioP с правами full

# MikroTik Certified Security Engineer

MTCSE

## Chapter 2.2: Security Basic Firewall

Filter Rules  
Custom chains

ICMP Filtering

RAW Table

Security Areas

Tracking

Stateful  
Firewall

Default  
Configuration

Management  
access and  
other

Simple Bridge  
Filter  
Rules

Basic Firewall  
Rules



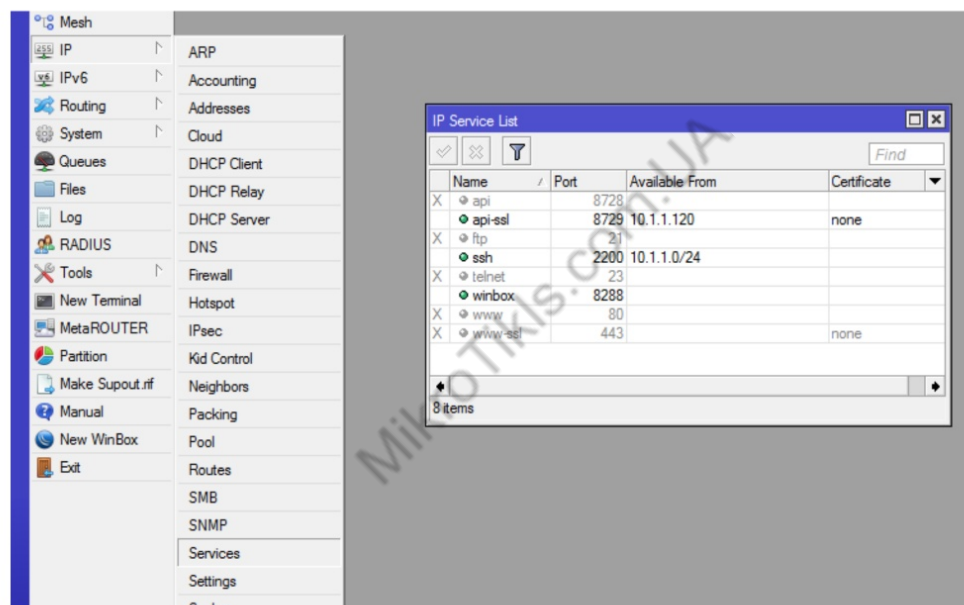
**qualitytraining**  
Succeed with Quality

MTI-GROUP LLC / network academy

V.21-01

# RouterOS services

- Отключайте неиспользуемые сервисы
- Меняйте дефолтные порты
- Ограничивайте доступ к сервисам available-from=10.1.1.0/24\*
- Используйте сертификаты



# RouterOS services

```
/ip service disable telnet,ftp,www,www-ssl,api  
/ip service set winbox port=8288  
/ip service set ssh port=2200 address=10.1.1.0/24  
/ip service set api-ssl port=8729 address=10.1.1.121
```

# RouterOS MAC Access

RouterOS имеет встроенные опции для удобного доступа к устройствам даже без настройки IP адреса.

Этот доступ необходимо ограничить (например, только внутренние интерфейсы) или отключить полностью!

Для ограничения используются interface-list-ы

```
/tool mac-server set allowed-interface-list=none  
/tool mac-server mac-winbox set allowed-interface-list=none  
/tool mac-server ping set enabled=no
```

# RouterOS Bandwidth Test

Bandwidth test server используется для проверки пропускной способности между RouterOS\*.

Этот доступ необходимо ограничить или отключить полностью!

```
/tool bandwidth-server set enabled=no
```



# RouterOS Other client services

```
/ip proxy set enabled=no  
/ip socks set enabled=no  
/ip upnp set enabled=no  
/ip cloud set ddns-enabled=no update-time=no
```

# RouterOS more secure ssh

```
/ip ssh set strong-crypto=yes
```

Introduces following changes in the SSH configuration:

- Prefer 256 and 192 bit encryption instead of 128 bits
- Disable null encryption
- Prefer sha256 for hashing instead of sha1
- Disable md5
- Use 2048bit prime for Diffie Hellman exchange instead of 1024bit

# RouterOS unuser interfaces

хорошая практика отключать не используемые интерфейсы

# MikroTik Certified Security Engineer

MTCSE

## Chapter 2.2: Security Basic Firewall

Filter Rules  
Custom chains

ICMP Filtering

RAW Table

Security Areas

Tracking

Stateful  
Firewall

Default  
Configuration

Management  
access and  
other

Simple Bridge  
Filter  
Rules

Basic Firewall  
Rules



**qualitytraining**  
Succeed with Quality

MTI-GROUP LLC / network academy

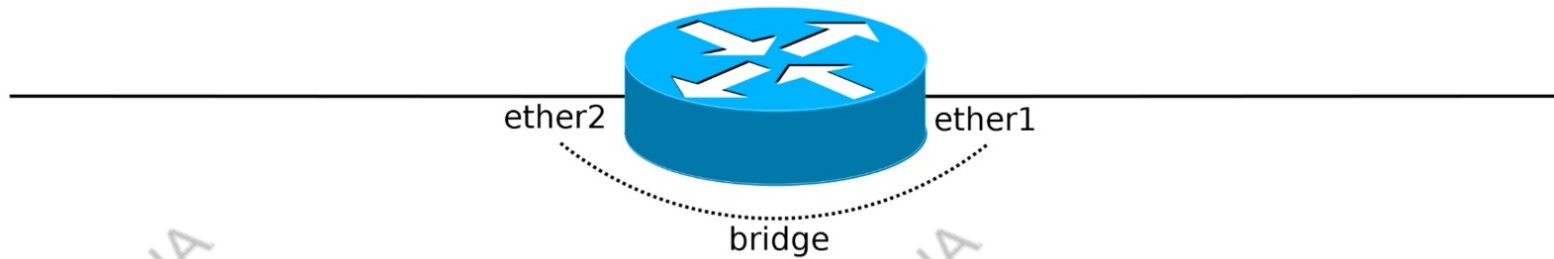
V.21-01

# RouterOS Bridge Filter

The bridge firewall implements packet filtering and there by provides security functions that are used to manage data flow to, from and through bridge.

/interface bridge filter

## sample - Only PPPoE Traffic



```
/interface bridge filter
add action=accept chain=forward mac-protocol=pppoe
add action=accept chain=forward mac-protocol=pppoe-discovery
add action=drop chain=forward
```

# MikroTik Certified Security Engineer

MTCSE

## Chapter 2.2: Security Basic Firewall

Default  
Configuration

Management  
access and  
other

Simple Bridge  
Filter  
Rules

Basic Firewall  
Rules

Filter Rules  
Custom chains

ICMP Filtering

RAW Table

Security Areas

Tracking

Stateful  
Firewall



**qualitytraining**  
Succeed with Quality

MTI-GROUP LLC / network academy

V.21-01

# Firewall Basic (mtcna)

- Работайте с новыми соединениями для снижения нагрузки на CPU маршрутизатора
- Для доступа к роутеру используйте address-list и по возможности логируйте все события
- Enable ICMP access (optionally) и только нужные типы и коды;
- Блокируйте все остальное
  - Блокируйте попытки доступа из локальных сетей через внешний интерфейс на приватные адреса (rfc1918) (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16)
  - Блокируйте проходящие пакеты в локальные сети (new) - кроме dnat (логируйте) - я не рекомендую
  - Отбрасывать входящие пакеты из интернета, SRC которые не являются публичными IP адреса (rfc1918),



# Firewall Basic (mtcna)

# LAB

- Защитите ваш маршрутизатор и ваши локальные сети, используя информацию из предыдущих слайдов.
- Настройте Firewall в минимально-оптимальной конфигурации
- откройте доступ по api-ssl, winbox с хоста 22.1.1.133

# Firewall Basic (mtcna)

# LAB

- Не меняйте настройки ваших маршрутизаторов
- Тренер производит аудит firewall у 2х добровольцев.
- Добровольцы (3) произвести аудит случайно выбранных маршрутизаторов из класса (по предыдущей лабе)

# Firewall Basic (mtcna)

super minimum but optional configuration

/ip firewall filter

add action=accept chain=input connection-state=established,related

add action=drop chain=input in-interface=ether1

add action=accept chain=forward connection-state=established,related

add action=drop chain=forward in-interface=ether1

# Firewall Basic (mtcna)

Firewall

Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols

00 Reset Counters00 Reset All Counters

#	Action	Chain	Src. Address	Dst. A...	Protocol	Src. Port	Dst. Port	In. Inter...	Out. Int...	In. Inter...	Out. Int...	Src. Address List	Dst. Address List
0	acc...	input											
1	drop	input						ether1				not_in_intemet	
2	acc...	input			1 (icmp)								
3	acc...	input			6 (tcp)		8291					myGroup	
4	drop	input						ether1					
5	acc...	forward											
6	drop	forward	192.168.88.0/24						ether1				not_in_internet
7	drop	forward						ether1				not_in_intemet	
8	drop	forward						ether1					

9 items

# MikroTik Certified Security Engineer

MTCSE

## Chapter 2.2: Security Basic Firewall

Filter Rules  
Custom chains

ICMP Filtering

RAW Table

Security Areas

Tracking

Stateful  
Firewall

Default  
Configuration

Management  
access and  
other

Simple Bridge  
Filter  
Rules

Basic Firewall  
Rules



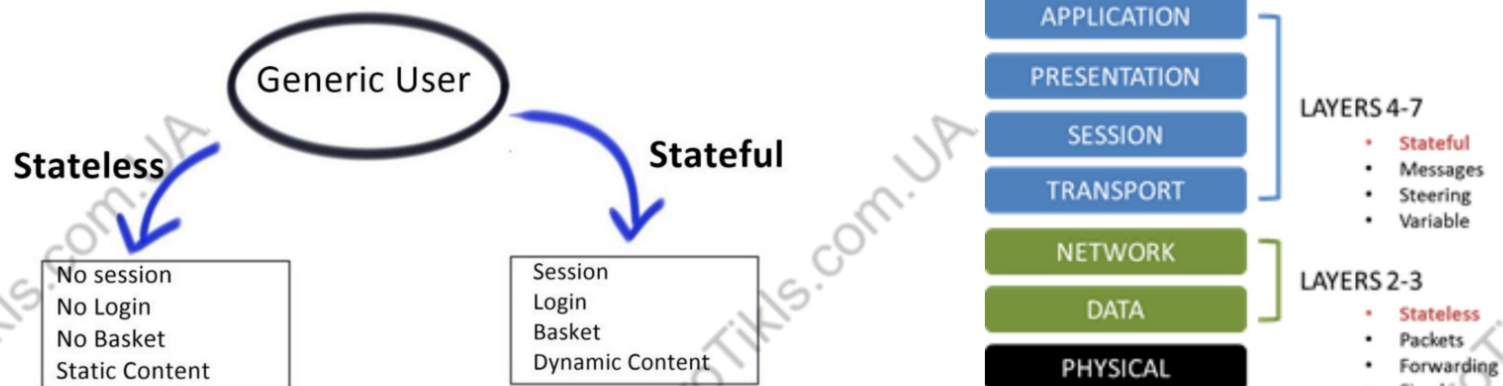
**qualitytraining**  
Succeed with Quality

MTI-GROUP LLC / network academy

V.21-01

# FIREWALL

## Stateful vs Stateless



# Stateless Firewall

Stateless брандмауэры отслеживают сетевой трафик и ограничивают или блокируют пакеты на основе адресов источника и получателя или других статических значений.

Они не «осведомлены» о трафике или потоках данных.

Брандмауэры такого типа используют простые наборы правил, которые не учитывают возможность того, что пакет может быть получен при попытке симулирования настоящего источника пакетов.

Брандмауэры stateless обычно быстрее и лучше работают при более тяжелых нагрузках, но менее гибкие.

Connaction Tracking - не нужен

# Stateful Firewall

Stateful Брандмауэры могут наблюдать потоки трафика от начала до конца.

Они знают о различных способах прохождения трафика и могут реализовывать различные функции IP-безопасности (IPsec), такие как туннели и шифрование.

В технических терминах это означает, что брандмауэры стэйтфул могут определить, на какой стадии подключено TCP-соединение, он может определить, изменилось ли MTU, были ли фрагменты фрагментированы и т. д.

Брандмауэры с активными состояниями лучше идентифицируют несанкционированные и поддельные источники, хоть и требуют больше ресурсов.

Connaction Tracking - должен быть включен



# FIREWALL

## Stateful vs Stateless

Parameters	Stateless	Stateful
Philosophy	Treats each packet in isolation and does not relates to connection state	Stateful firewalls maintain context about active sessions and use "state information" to speed packet processing
Filtering decision	Based on information in packet headers	Based on flows
Memory and CPU intensive	Low	High
Security	Low	High
Connection Status	Unknown	Known
Performance	Fast	Slower
Related terms	Header info, IP address, port no etc.	State information, pattern matching etc.

# Stateful Firewall in RouterOS

- RouterOS реализует межсетевой экран с отслеживанием состояния. Stateful-firewall - это межсетевой экран, способный отслеживать ICMP, UDP и TCP соединения.
- Это означает, что брандмауэр может определить взаимосвязь пакета с предыдущим пакетом.
- Firewall can track operating state.

# Stateful Firewall in RouterOS

contrack должен быть включен

admin@172.20.1.8:8233 (MTI-CCR-Internet) - WinBox v6.44.5 on CCR1036-8G-2S+ (tile)

Session Settings Dashboard

Safe Mode Session: 172.20.1.8:8233

Firewall

Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols

Tracking

	Src. Address	Dst. Address	Proto...	Connecti...	Timeout	TCP State	Orig./Repl. R...
C	0.0.0.0/68	255.255.255.255/67	17 (u...		00:00:09		18.4 kbps/0 b
C	0.0.0.0/5678						0 bps
C	2.17.169.138/443						0 bps
C	2.17.169.138/443						0 bps
SAC	10.9.9.3/54016						0 bps
SAC	10.9.9.3/54017						0 bps/17.5
C	10.172.192.33/138						0 bps
SACs	10.172.192.33/1695						0 bps
SACs	10.172.192.33/3074						0 bps/1096
SACs	10.172.192.33/36813						0 bps
SACs	10.172.192.33/36814						0 bps
SACs	10.172.192.33/36815						0 bps
SACs	10.172.192.33/36816						0 bps
SACs	10.172.192.33/36817						0 bps
SACs	10.172.192.33/36818						0 bps
SACs	10.172.192.33/37766						0 bps
SACs	10.172.192.33/38757						0 bps
SACs	10.172.192.33/41482						0 bps
SACs	10.172.192.33/43544						0 bps
SACs	10.172.192.33/47050						0 bps

1212 items

Connection Tracking

Enabled: yes

☒ Loose TCP Tracking

TCP Syn Sent Timeout: 00:00:05

TCP Syn Received Timeout: 00:00:05

TCP Established Timeout: 1d 00:00:00

TCP Fin Wait Timeout: 00:00:10

TCP Close Wait Timeout: 00:00:10

TCP Last Ack Timeout: 00:00:10

TCP Time Wait: 00:00:10

TCP Close: 00:00:10

TCP Max Retransmit Timeout: 00:05:00

TCP Unacked Timeout: 00:05:00

# MikroTik Certified Security Engineer

MTCSE

## Chapter 2.2: Security Basic Firewall

Filter Rules  
Custom chains

ICMP Filtering

RAW Table

Security Areas

Tracking

Stateful  
Firewall

Default  
Configuration

Management  
access and  
other

Simple Bridge  
Filter  
Rules

Basic Firewall  
Rules



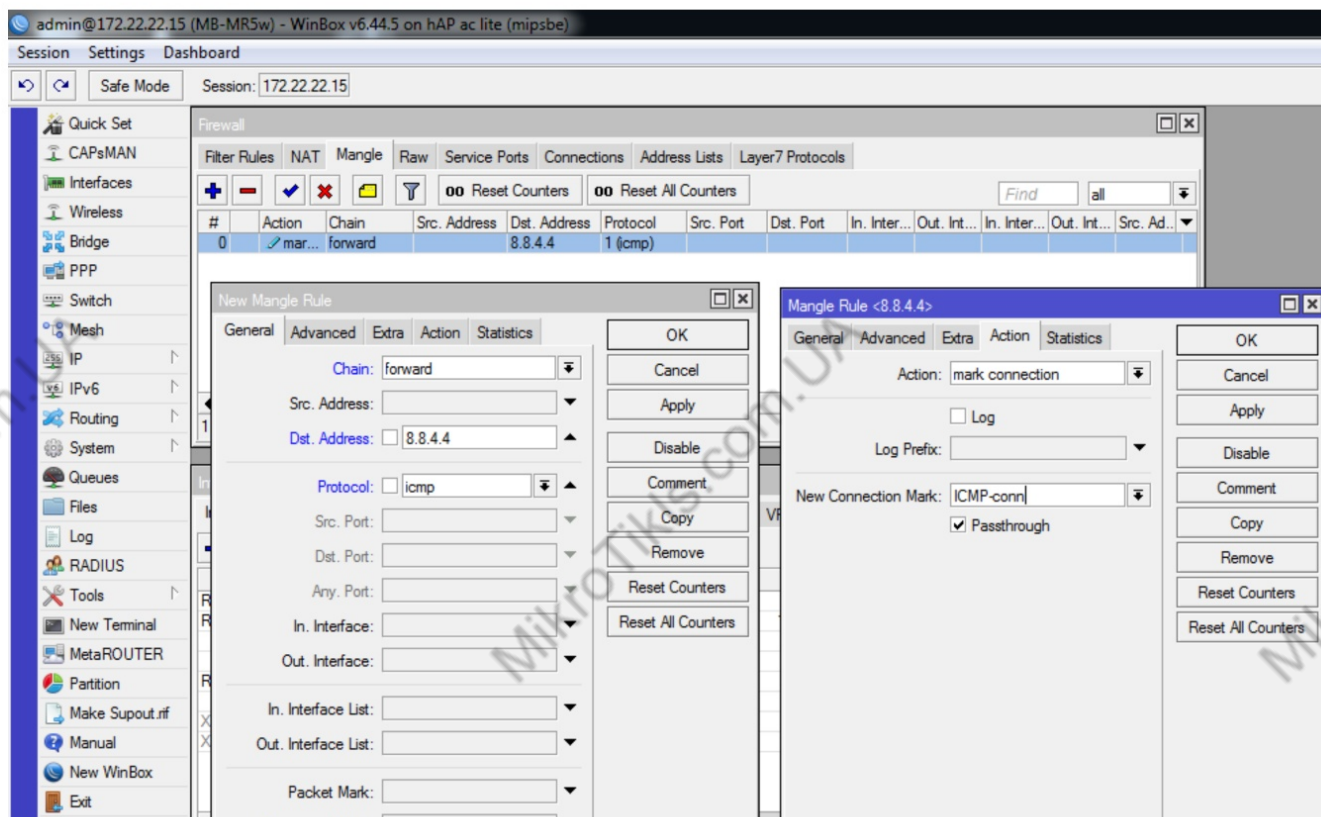
**qualitytraining**  
Succeed with Quality

MTI-GROUP LLC / network academy

V.21-01

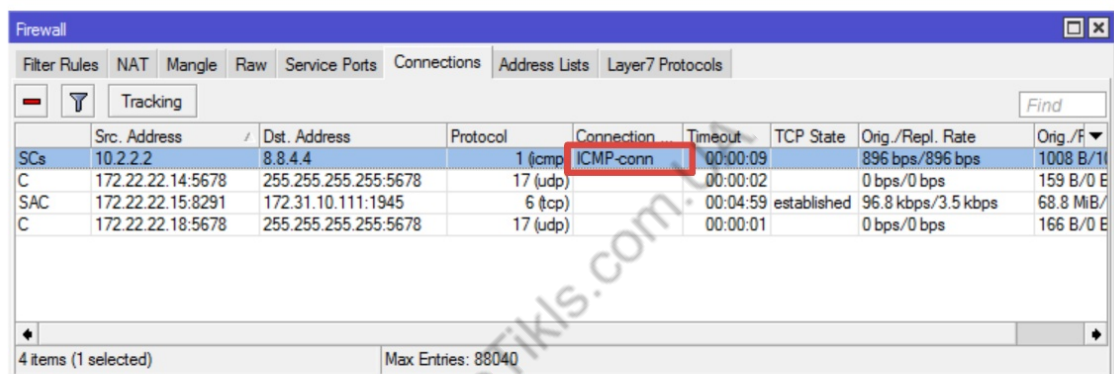
# ICMP Tracking use contrack

chain=forward action=mark-connection new-connection-mark=ICMP-conn  
passthrough=yes protocol=icmp dst-address=8.8.4.4



# ICMP Tracking

## Мониторинг соединений

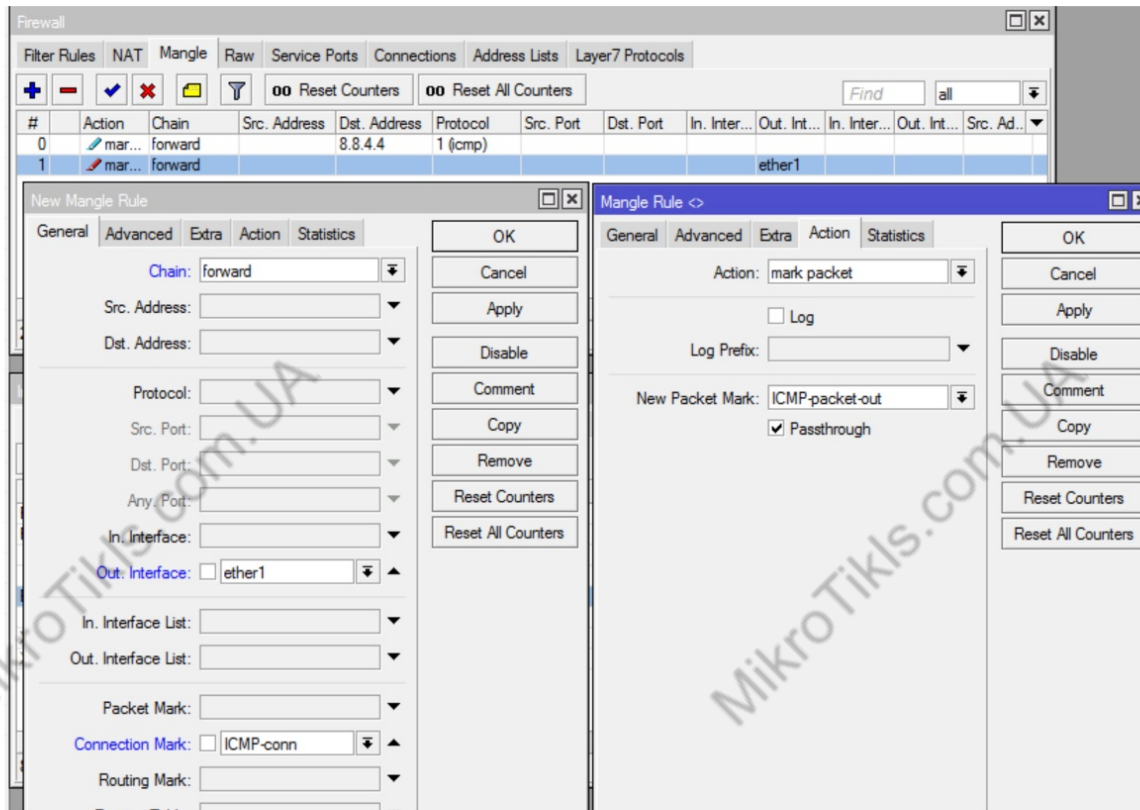


The screenshot shows the Mikrotik WinBox Firewall Connections tab. The 'Tracking' button is active. The table displays four entries. The first entry, 'SCs', is selected and has a red box around its 'Connection' value 'ICMP-conn'. The status bar at the bottom indicates '4 items (1 selected)' and 'Max Entries: 88040'.

	Src. Address	/	Dst. Address	Protocol	Connection	Timeout	TCP State	Orig./Repl. Rate	Orig./F
SCs	10.2.2.2		8.8.4.4	1 (icmp)	ICMP-conn	00:00:09		896 bps/896 bps	1008 B/1
C	172.22.22.14:5678		255.255.255.255:5678	17 (udp)		00:00:02		0 bps/0 bps	159 B/0 E
SAC	172.22.22.15:8291		172.31.10.111:1945	6 (tcp)		00:04:59	established	96.8 kbps/3.5 kbps	68.8 MiB/
C	172.22.22.18:5678		255.255.255.255:5678	17 (udp)		00:00:01		0 bps/0 bps	166 B/0 E

4 items (1 selected) Max Entries: 88040

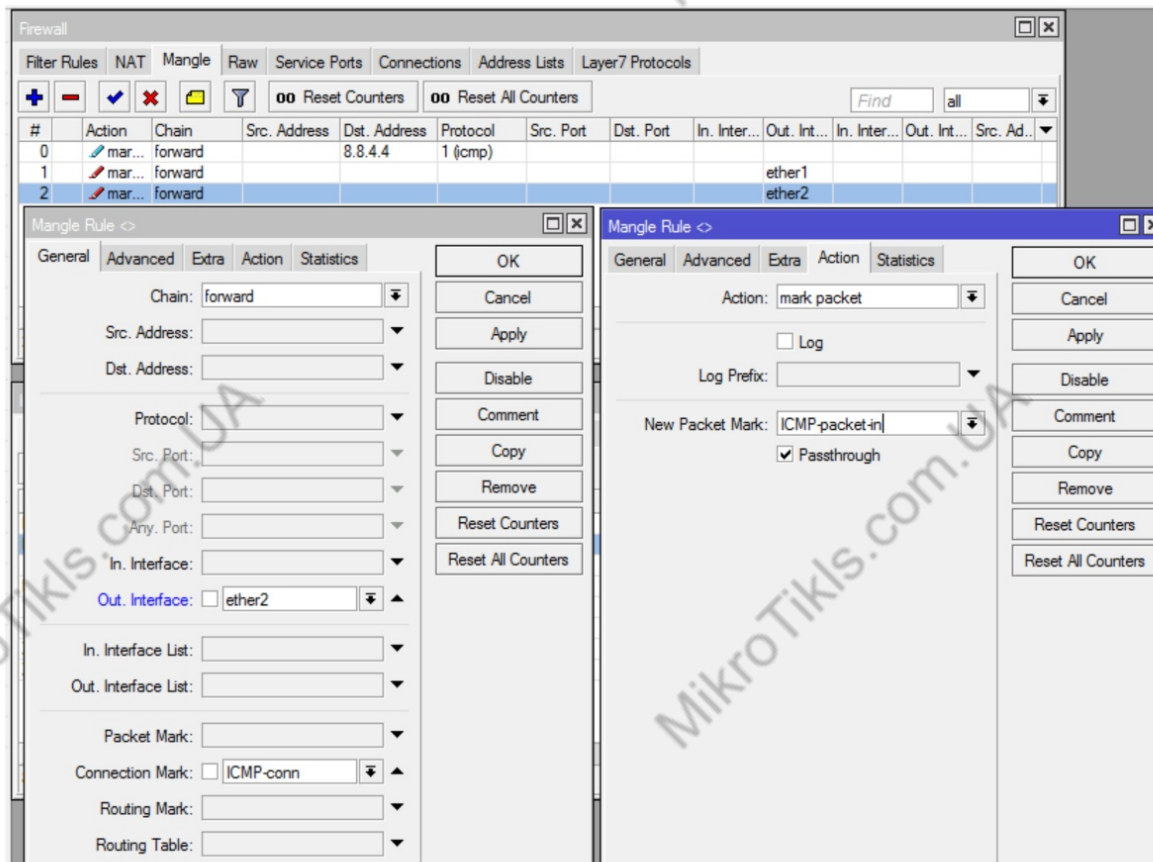
# ICMP Tracking



Отслеживать  
пакеты OUT



# ICMP Tracking

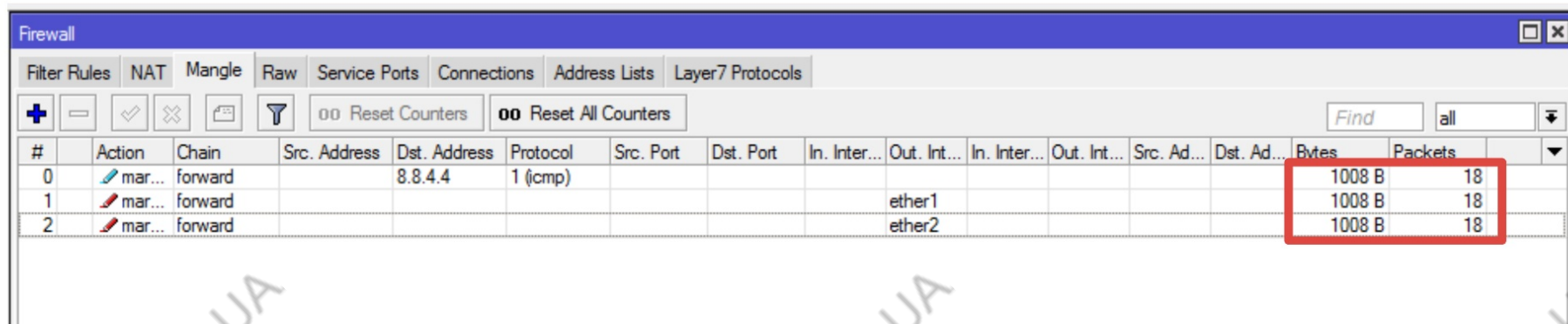


Отслеживать  
пакеты IN



# ICMP Tracking

Отслеживать  
пакеты IN/OUT



The screenshot shows the Mikrotik WinBox Firewall configuration window. The 'Filter Rules' tab is active. Three rules are listed, all with the action 'mark-connection' and chain 'forward'. Rule 0 targets destination 8.8.4.4. Rule 1 targets out-interface ether1. Rule 2 targets out-interface ether2. The statistics for these rules are shown in the bottom right, with a red box highlighting the 'Bytes' and 'Packets' columns.

#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Inter...	Out. Int...	In. Inter...	Out. Int...	Src. Ad...	Dst. Ad...	Bytes	Packets
0	mar...	forward		8.8.4.4	1 (icmp)									1008 B	18
1	mar...	forward							ether1					1008 B	18
2	mar...	forward							ether2					1008 B	18

chain=forward action=mark-connection new-connection-mark=ICMP-conn  
passthrough=yes protocol=icmp dst-address=8.8.4.4 log=no

chain=forward action=mark-packet new-packet-mark=ICMP-packet-out  
passthrough=yes connection-mark=ICMP-conn out-interface=ether1 log=no

chain=forward action=mark-packet new-packet-mark=ICMP-packet-in  
passthrough=yes connection-mark=ICMP-conn out-interface=ether2 log=no

# MikroTik Certified Security Engineer

MTCSE

## Chapter 2.2: Security Basic Firewall

Filter Rules  
Custom chains

ICMP Filtering

RAW Table

Security Areas

Tracking

Stateful  
Firewall

Default  
Configuration

Management  
access and  
other

Simple Bridge  
Filter  
Rules

Basic Firewall  
Rules

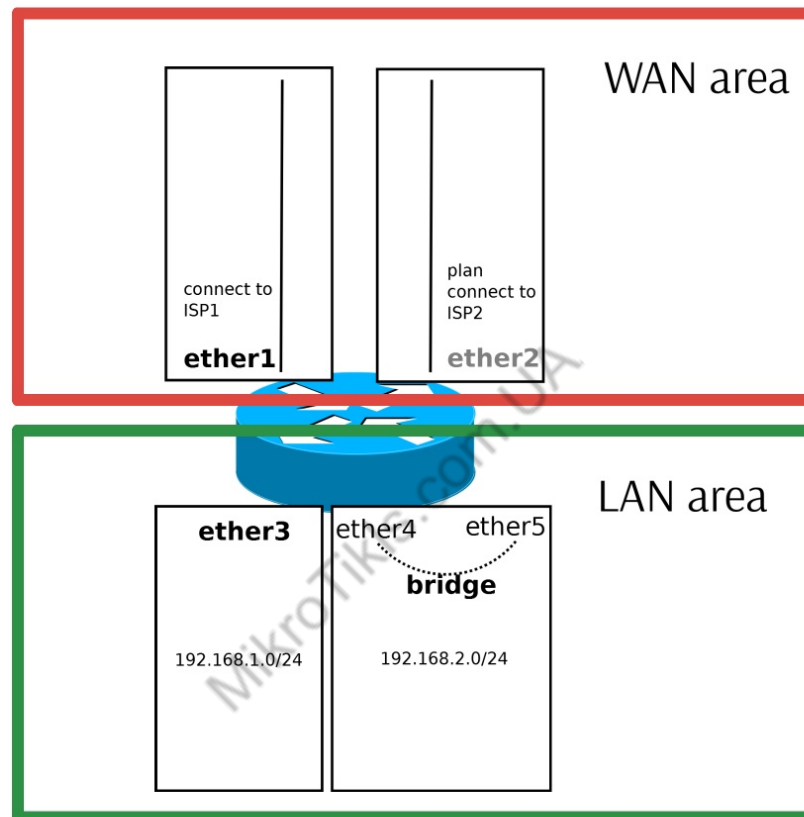


**qualitytraining**  
Succeed with Quality

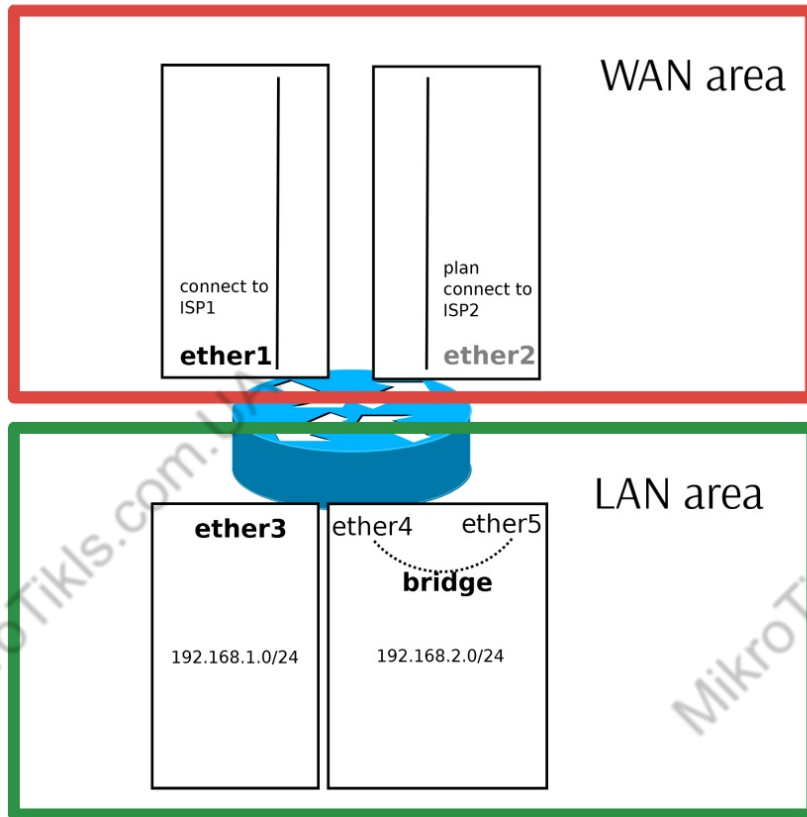
MTI-GROUP LLC / network academy

V.21-01

# Security Areas - Области безопасности



# Области безопасности



```
/interface list  
add name=WAN  
add name=LAN
```

```
/interface bridge  
add name=bridge1
```

```
/interface bridge port  
add bridge=bridge1 interface=ether4  
add bridge=bridge1 interface=ether5
```

```
/interface list member  
add interface=ether1 list=WAN  
add interface=ether2 list=WAN  
add interface=bridge1 list=LAN  
add interface=ether3 list=LAN
```

# Области безопасности

- отключайте неиспользуемые интерфейсы
- конфигурируйте правила Firewall filter, nat, mangle и т.д с листами интерфейсов, это упростит конфигурацию(меньше правил), снизит нагрузку с маршрутизатора.
- отпадет необходимость перенастраивать правила в случае изменений областей безопасности

# Interface Lists

# LAB

- Перенастройте ваш маршрутизатор используя Листы Интерфейсов

# MikroTik Certified Security Engineer

MTCSE

## Chapter 2.2: Security Basic Firewall

Filter Rules  
Custom chains

ICMP Filtering

RAW Table

Security Areas

Tracking

Stateful  
Firewall

Default  
Configuration

Management  
access and  
other

Simple Bridge  
Filter  
Rules

Basic Firewall  
Rules



**qualitytraining**  
Succeed with Quality

MTI-GROUP LLC / network academy

V.21-01

# RAW Table

RAW таблицы предлагают две цепочки - prerouting и output

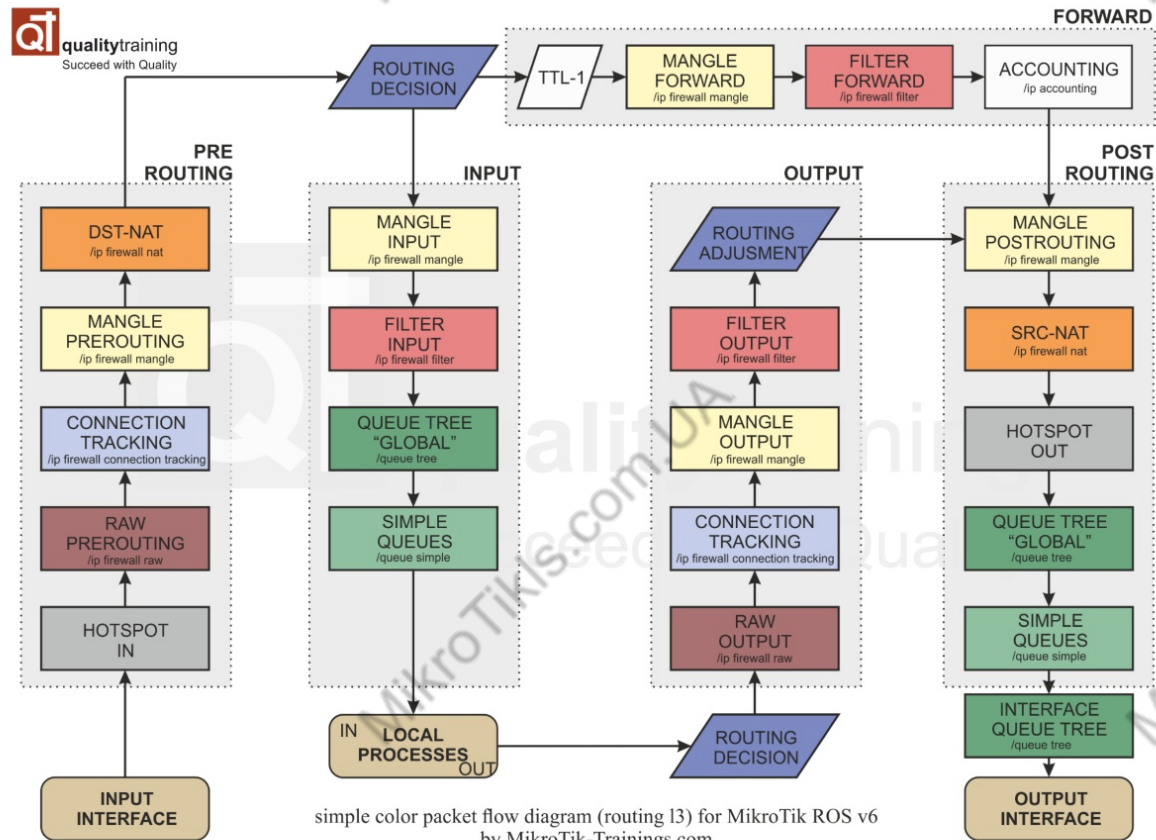
Цель использования таблицы RAW заключается в обработке пакетов **до connection tracking**, что значительно поможет снизить нагрузку на процессор

Это гораздо эффективнее чем использовать другие цепочки firewall filter .

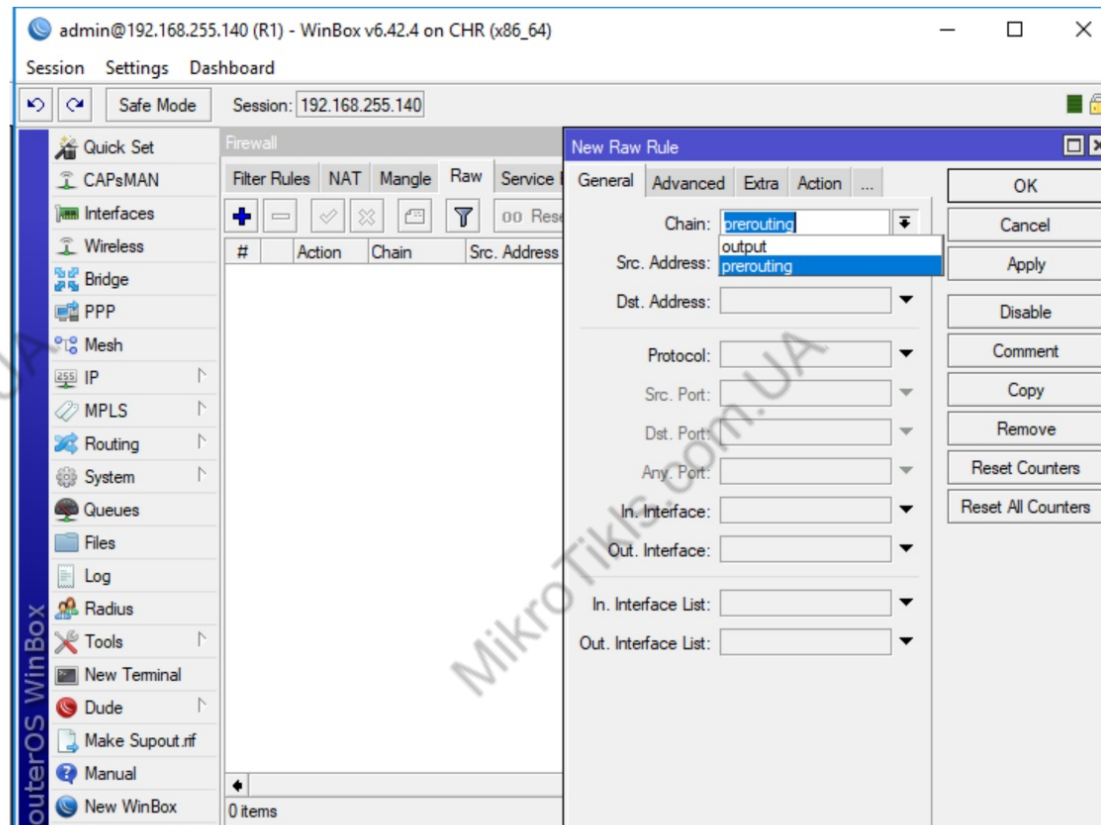
В других цепочках используя contrack можно делать гибкий анализ и определять аномалии, формировать адрес листы, а блокировать уже в RAW



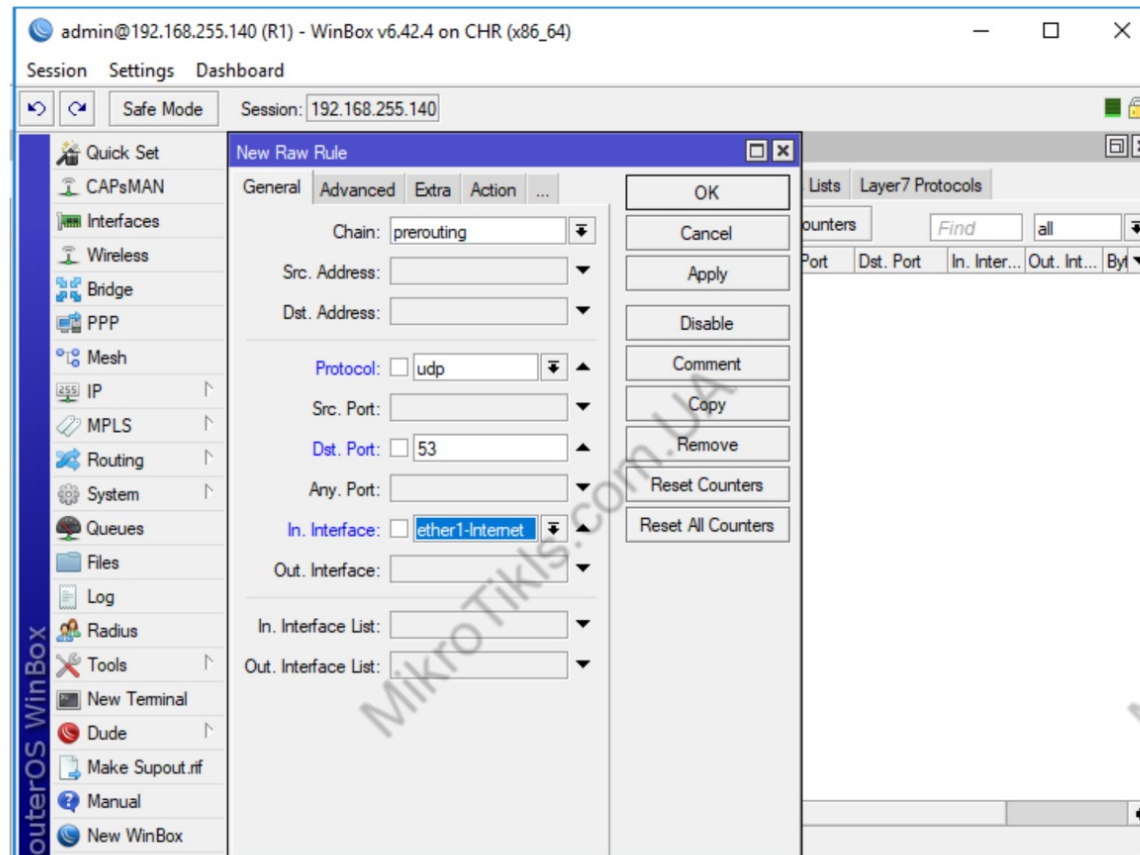
# RAW Table



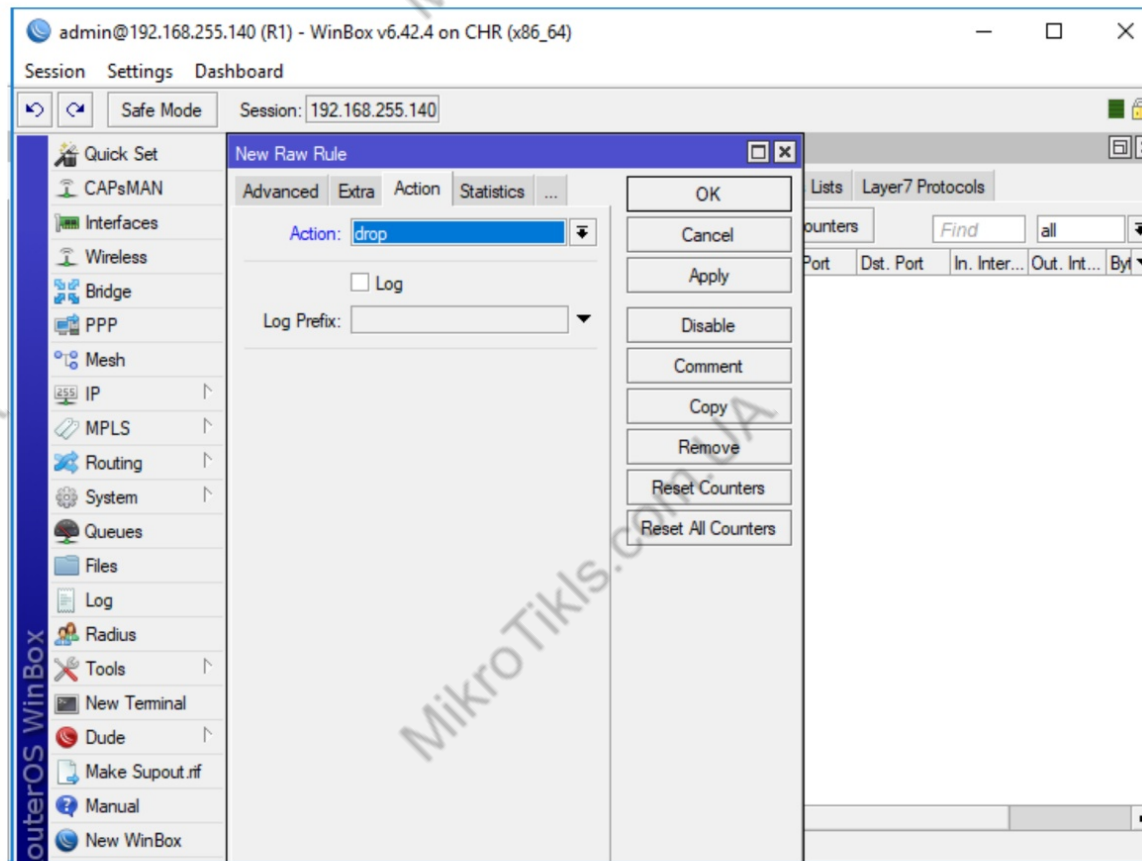
# RAW Table



# RAW Table - sample filter



# RAW Table - sample filter



# RAW Table - sample filter

```
/ip firewall filter
add chain=input action=drop protocol=tcp tcp-
flags=syn in-interface=ether1
```

VS

```
/ip firewall raw
add chain=prerouting action=drop protocol=tcp tcp-
flags=syn in-interface=ether1
```

Session: 192.168.255.140 CPU: 35%

Firewall

Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols

00 Reset Counters 00 Reset All Counters Find all

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
0	drop	prerouting			6 (tcp)			ether1		10.9 MB	286 767

admin@192.168.255.140 (R1) - WinBox v6.42.4 on CHR (x86\_64)

Session Settings Dashboard

Safe Mode Session: 192.168.255.140 CPU: 100%

Quick Set CAPsMAN Interfaces Wireless Bridge PPP Mesh IP MPLS Routing System Queues Files Log Radius Tools New Terminal Dude Make Supout.rf Manual New WinBox Exit

Resources

Uptime: 00:08:12 OK

Free Memory: 1171.5 MB PCI

Total Memory: 1203.2 MB USB

CPU: QEMU CPU

CPU Count: 1 IRQ

CPU Frequency: 2299 MHz RPS

CPU Load: 100 % Hardware

Free HDD Space: 69.3 MB

Total HDD Size: 95.3 MB

Sector Writes Since Reboot: 1 456

Total Sector Writes: 1 457

Architecture Name: x86\_64

Board Name: CHR

Version: 6.42.4 (stable)

Build Time: Jun/15/2018 14:14:17

# MikroTik Certified Security Engineer

MTCSE

## Chapter 2.2: Security Basic Firewall

Filter Rules  
Custom chains

ICMP Filtering

RAW Table

Security Areas

Tracking

Stateful  
Firewall

Default  
Configuration

Management  
access and  
other

Simple Bridge  
Filter  
Rules

Basic Firewall  
Rules



**qualitytraining**  
Succeed with Quality

MTI-GROUP LLC / network academy

V.21-01

# ICMP Filtering

- ICMP (Internet Control Message Protocol – протокол межсетевых управляющих сообщений) – сетевой протокол, входящий в стек протоколов TCP/IP.
- В основном ICMP используется для передачи сообщений об ошибках и других исключительных ситуациях, возникших при передаче данных
- Также на ICMP возлагаются некоторые сервисные функции.
- Нет метода аутентификации - следовательно могут быть использованы хакерами для сбоя
- Брандмауэр / фильтр пакетов должен быть в состоянии определять пакеты основываясь на его тип-код сообщения и принимать решения следует ли разрешить пакету ICMP проходить



# ICMP Filtering

Типы пакетов ICMPv4

<https://ru.wikipedia.org/wiki/ICMP>



# ICMPv4

Filtering Recommendations\*\*\*

ICMPv4 Message	Sourced from Device	Through Device	Destined to Device
ICMPv4-unreach-net	Limit rate	Limit rate	Limit rate
ICMPv4-unreach-host	Limit rate	Limit rate	Limit rate
ICMPv4-unreach-proto	Limit rate	Deny	Limit rate
ICMPv4-unreach-port	Limit rate	Deny	Limit rate
ICMPv4-unreach-frag-needed	Send	Permit	Limit rate
ICMPv4-unreach-src-route	Limit rate	Deny	Limit rate
ICMPv4-unreach-net-unknown ( <i>Depr</i> )	Deny	Deny	Deny
ICMPv4-unreach-host-unknown	Limit rate	Deny	Ignore
ICMPv4-unreach-host-isolated ( <i>Depr</i> )	Deny	Deny	Deny
ICMPv4-unreach-net-tos	Limit rate	Deny	Limit rate

# ICMPv4

Filtering Recommendations\*\*\*

ICMPv4 Message	Sourced from Device	Through Device	Destined to Device
ICMPv4-unreach-host-tos	Limit rate	Deny	Limit rate
ICMPv4-unreach-admin	Limit rate	Limit rate	Limit rate
ICMPv4-unreach-prec-violation	Limit rate	Deny	Limit rate
ICMPv4-unreach-prec-cutoff	Limit rate	Deny	Limit rate
ICMPv4-quench	Deny	Deny	Deny
ICMPv4-redirect-net	Limit rate	Deny	Limit rate
ICMPv4-redirect-host	Limit rate	Deny	Limit rate
ICMPv4-redirect-tos-net	Limit rate	Deny	Limit rate
ICMPv4-redirect-tos-host	Limit rate	Permit	Limit rate
ICMPv4-timed-ttl	Limit rate	Permit	Limit rate

# ICMPv4

Filtering Recommendations\*\*\*

ICMPv4 Message	Sourced from Device	Through Device	Destined to Device
ICMPv4-timed-reass	Limit rate	Permit	Limit rate
ICMPv4-parameter-pointer	Limit rate	Deny	Limit rate
ICMPv4-option-missing	Limit rate	Deny	Limit rate
ICMPv4-req-echo-message	Limit rate	Permit	Limit rate
ICMPv4-req-echo-reply	Limit rate	Permit	Limit rate
ICMPv4-req-router-sol	Limit rate	Deny	Limit rate
ICMPv4-req-router-adv	Limit rate	Deny	Limit rate
ICMPv4-req-timestamp-message	Limit rate	Deny	Limit rate
ICMPv4-req-timestamp-reply	Limit rate	Deny	Limit rate
ICMPv4-info-message ( <i>Depr</i> )	Deny	Deny	Deny

# ICMPv4

Filtering Recommendations\*\*\*

ICMPv4 Message	Sourced from Device	Through Device	Destined to Device
ICMPv4-info-reply (Depr)	Deny	Deny	Deny
ICMPv4-mask-request	Limit rate	Deny	Limit rate
ICMPv4-mask-reply	Limit rate	Deny	Limit rate

# ICMPv4

Sample Filtering icmp

Firewall										
Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols										
<div> <div>+</div> <div>-</div> <div>✓</div> <div>✗</div> <div>📁</div> <div>🔍</div> <div>00 Reset Counters</div> <div>00 Reset All Counters</div> <div>Find</div> <div>all</div> <div>▼</div> </div>										
#	Action	Chain	Src. Address	Dst. Address	Protocol	ICMP Options/ICMP Type	IC...	Bytes	Packets	
0	jump	forward						0 B	0	
::: echo reply										
1	✓ accept	icmp			1 (icmp)	0 (echo reply)	0	0 B	0	
::: net unreachable										
2	✓ accept	icmp			1 (icmp)	3 (destination unreachable)	0	0 B	0	
::: host unreachable										
3	✓ accept	icmp			1 (icmp)	3 (destination unreachable)	1	0 B	0	
::: host unreachable fragmentation required										
4	✓ accept	icmp			1 (icmp)	3 (destination unreachable)	4	0 B	0	
::: allow source quench										
5	✓ accept	icmp			1 (icmp)	4 (source quench)	0	0 B	0	
::: allow echo request										
6	✓ accept	icmp			1 (icmp)	8 (echo request)	0	0 B	0	
::: allow time exceed										
7	✓ accept	icmp			1 (icmp)	11 (time exceeded)	0	0 B	0	
8	✓ accept	icmp			1 (icmp)	12 (parameter problem)	0	0 B	0	
::: deny all other types										
9	✗ drop	icmp						0 B	0	
10 items										

# ICMPv4

Sample Filtering icmp

New Firewall Rule

General Advanced Extra Action Statistics

Src. Address List:

Dst. Address List:

Layer7 Protocol:

Content:

Connection Bytes:

Connection Rate:

Per Connection Classifier:

Src. MAC Address:

Out. Bridge Port:

In. Bridge Port:

In. Bridge Port List:

Out. Bridge Port List:

IPsec Policy:

TLS Host:

Ingress Priority:

Priority:

DSCP (TOS):

TCP MSS:

Packet Size:

Random:

TCP Flags

ICMP Options

IPv4 Options:

TTL:

OK Cancel Apply Disable Comment Copy Remove Reset Counters Reset All Counters

enabled

NOT ICMP  
OPTIONS

New Firewall Rule

General Advanced Extra Action Statistics

Src. Address List:

Dst. Address List:

Layer7 Protocol:

Content:

Connection Bytes:

Connection Rate:

Per Connection Classifier:

Src. MAC Address:

Out. Bridge Port:

In. Bridge Port:

In. Bridge Port List:

Out. Bridge Port List:

IPsec Policy:

TLS Host:

Ingress Priority:

Priority:

DSCP (TOS):

TCP MSS:

Packet Size:

Random:

TCP Flags

ICMP Options

ICMP Type:

ICMP Code:

IPv4 Options:

TTL:

OK Cancel Apply Disable Comment Copy Remove Reset Counters Reset All Counters

enabled

ICMP OPTIONS



# MikroTik Certified Security Engineer

MTCSE

## Chapter 2.2: Security Basic Firewall

Filter Rules  
Custom chains

ICMP Filtering

RAW Table

Security Areas

Tracking

Stateful  
Firewall

Default  
Configuration

Management  
access and  
other

Simple Bridge  
Filter  
Rules

Basic Firewall  
Rules



**qualitytraining**  
Succeed with Quality

MTI-GROUP LLC / network academy

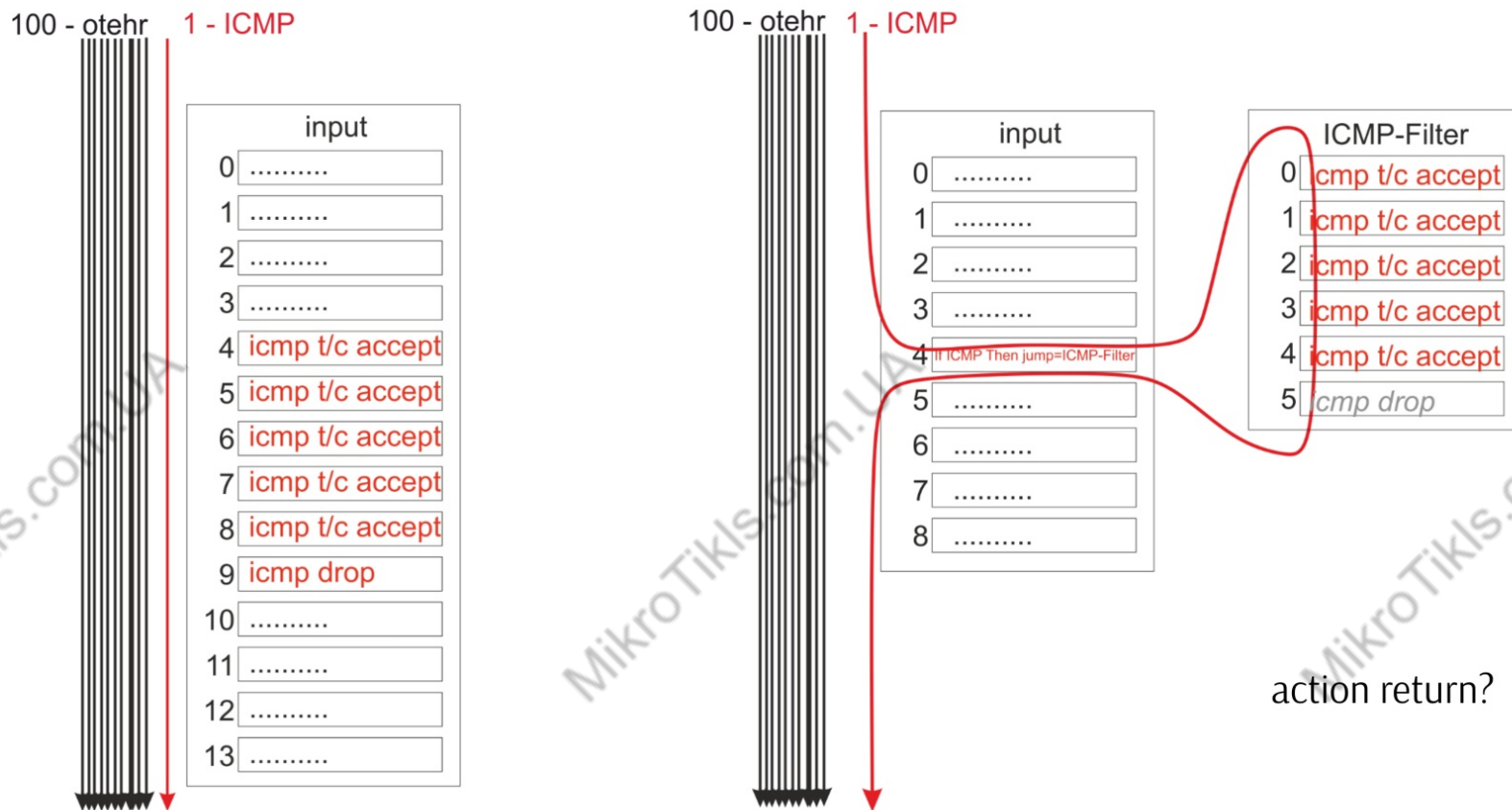
V.21-01

# Firewall filter - custom chains

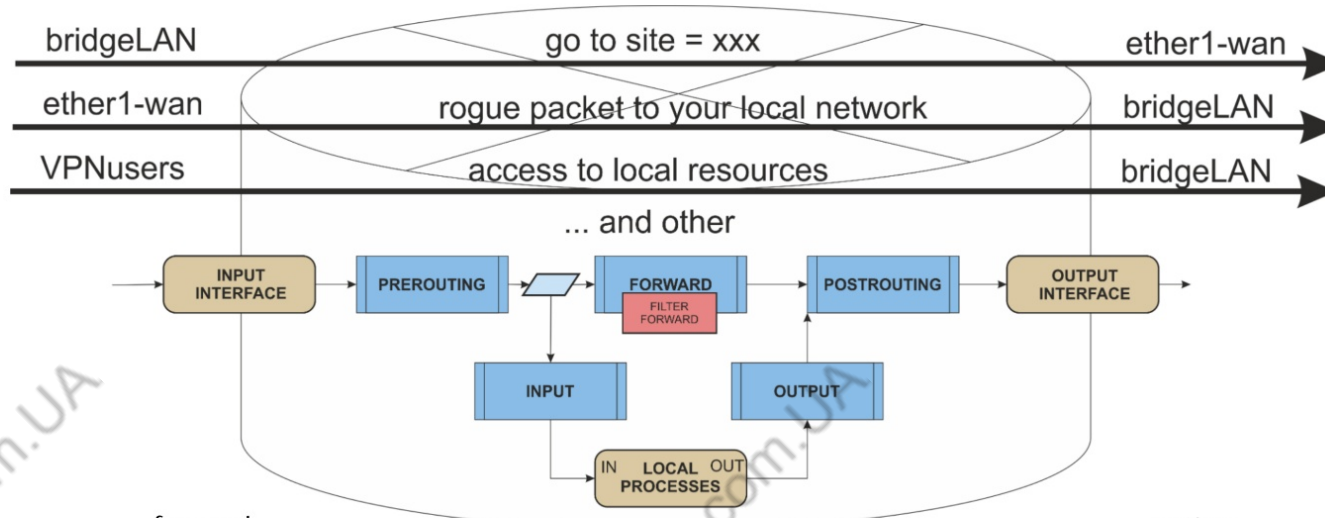
- В IP Firewall Filter - три встроенные цепочки input, forward, output
- Мы можем создавать свои цепочки как в Firewall Filter, так и NAT, Mangle с целью:
  - снижения нагрузки с CPU
  - упрощения структуры filter, nat, mangle



# Firewall filter - custom chains

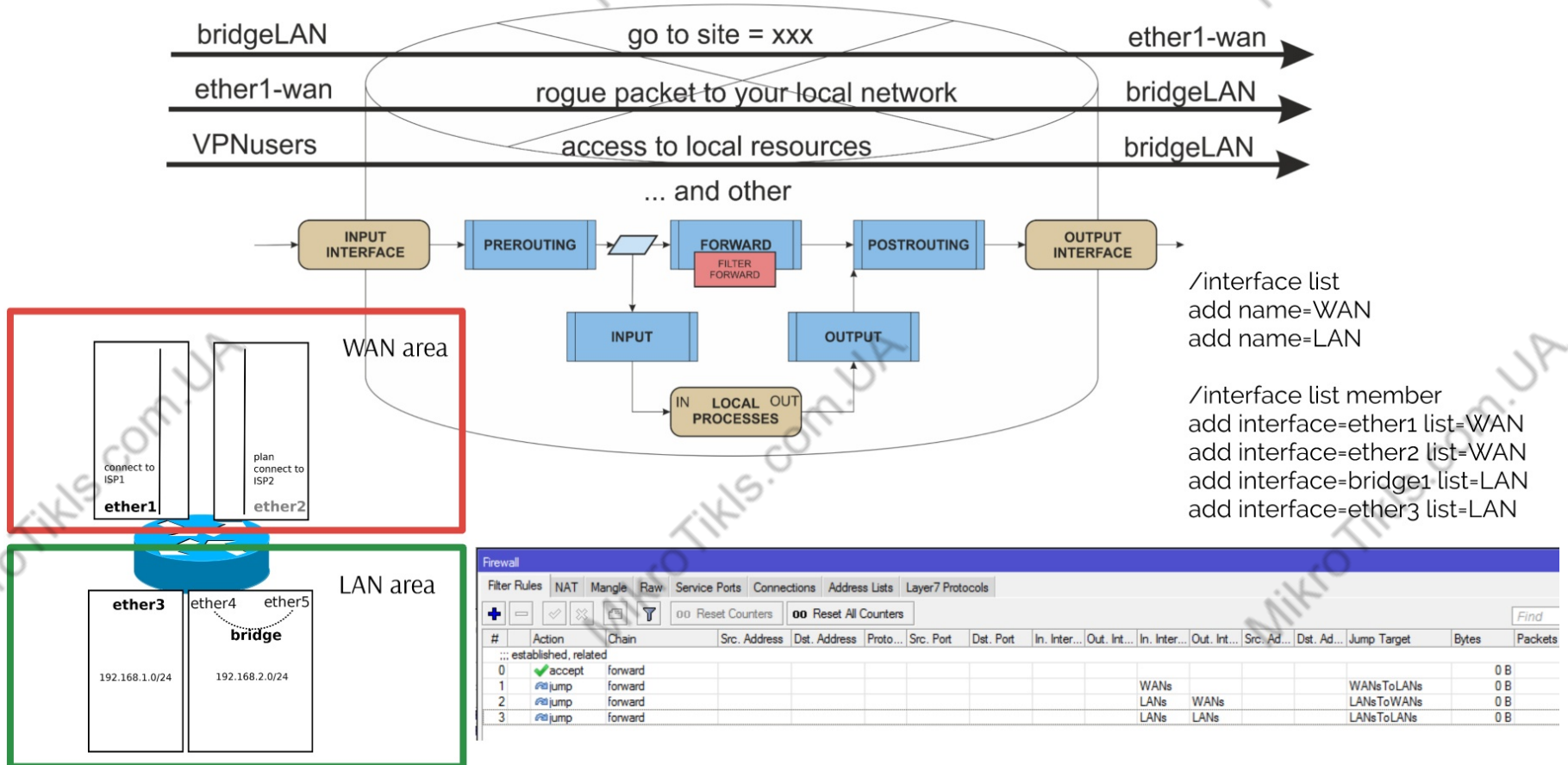


# Firewall filter - custom chains



forward .....	action
forward ..... защищает локалку?	action
forward ..... фильтр публичных сервисов?	action
forward ..... доступ между сетями?	action
forward ..... защита локальный ресурсов?	action
forward ..... VPN пользователи кому куда можно?	action
forward .....	action
forward .....	action
1000 .....	

# Firewall filter - custom chains



Firewall

Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols

00 Reset Counters 00 Reset All Counters

Find forward

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	In. Inter...	Out. Int...	Src. Ad...	Dst. Ad...	Jump Target	Bytes	Packets
... established, related																
0	✓ accept	forward													0 B	0
1	⚡ jump	forward								WANs				WANsToLANs	0 B	0
2	⚡ jump	forward								LANs	WANs			LANsToWANs	0 B	0
3	⚡ jump	forward								LANs	LANs			LANsToLANs	0 B	0

Firewall

Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols

00 Reset Counters 00 Reset All Counters

Find WANsToLANs

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	In. Inter...	Out. Int...	Src. Ad...	Dst. Ad...	Jump Target	Bytes	Packets
4	✓ accept	WANsToLANs		192.168.33.100	6 (tcp)		3389					GOODI...			0 B	0
5	✓ accept	WANsToLANs		192.168.33.220	6 (tcp)		80,110								0 B	0
6	✓ accept	WANsToLANs		192.168.33.200	6 (tcp)		443								0 B	0
7	✗ drop	WANsToLANs													0 B	0

Firewall

Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols

00 Reset Counters 00 Reset All Counters

Find LANsToWANs

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	In. Inter...	Out. Int...	Src. Ad...	Dst. Ad...	Jump Target	Bytes	Packets
8	✗ drop	LANsToWANs	192.168.33.10	4.5.6.7											0 B	0
9	✗ drop	LANsToWANs	192.168.33.10		6 (tcp)		678								0 B	0
10	✗ drop	LANsToWANs	192.168.33.10		6 (tcp)		555								0 B	0
11	✗ drop	LANsToWANs													0 B	0

Firewall

Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols

00 Reset Counters 00 Reset All Counters

Find LANsToLANs

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	In. Inter...	Out. Int...	Src. Ad...	Dst. Ad...	Jump Target	Bytes	Packets
---	--------	-------	--------------	--------------	----------	-----------	-----------	--------------	-------------	--------------	-------------	------------	------------	-------------	-------	---------

# Firewall Basic Custom Chains

# LAB

- Перенастройте Firewall таким образом, что бы логическое движение трафика было распределено по цепочкам (custom)
- Разрешите только необходимые типы и коды ICMP (сделайте это в custom chain)

# MikroTik Certified Security Engineer

MTCSE

## Chapter 2.2: Security Basic Firewall

Filter Rules  
Custom chains

ICMP Filtering

RAW Table

Security Areas

Tracking

Stateful  
Firewall

Default  
Configuration

Management  
access and  
other

Simple Bridge  
Filter  
Rules

Basic Firewall  
Rules



**qualitytraining**  
Succeed with Quality

MTI-GROUP LLC / network academy

V.21-01