

Mangle

```
: system
: Level1
: /ip firewall mangle
: IP
: mangle
```

Mangle

```
: /ip firewall mangle
```

Mangle " " RouterOS ,
NAT.
mangle ,

action (accept | add-dst-to-address-list | add-src-to-address-list | change-dscp | change-mss | change-ttl | jump | log | mark-connection | mark-packet | mark-routing | passthrough | return | set-priority | strip-ipv4-options; : **accept**) - ,

- **accept** - , . . .
- **add-dst-to-address-list** - IP
address-list
- **add-src-to-address-list** - IP
address-list
- **change-dscp** - **new-dscp** (DSCP)
- **change-mss** - **new-mss**
- **change-ttl** - **new-ttl**
- **jump** - **jump-target**
- **log** -
- **mark-connection** - , **new-connection**
- **mark-packet** - , **new-packet-mark** ,

- **mark-routing** **new-routing-mark.**
- **passthrough** -
- **return** -
- **set-priority** - **new-priority**
- **strip-ipv4-options** - (VLAN WMM-enabled IPv4 IP)

address-list(name) - IP
action=add-dst-to-address **action=add-src-to-address-list.**

address-list-timeout(time; : 00:00:00) - **address-list.**
add-dst-to-address-list **add-src-to-address-**

list

- **00:00:00** -

chain (forward | input | output | postrouting | prerouting) -

comment(text)

connection-bytes(integer-integer) -

- **0** - : **connection-bytes=2000000-0**
2

connection-limit(integer, netmask) -

connection-mark(name) - mangle

connection-state (established | invalid | new | related) -

- **established** -
- **invalid** - ICMP
- **new** -

- **related** - , ICMP , FTP FTP
(
/ip firewall service-port)

connection-type (ftp | gre | h323 | irc | mms | pptp | quake3 | tftp) -

/ip firewall service-port

content(text) -

dscp (integer: 0..63) - DSCP (ex-ToS) - IP

dst-address (IP address/netmask | IP address -IP address) -

IP

address/netmask . 1.1.1.1/24

1.1.1.0/24

dst-address-list(name) -

dst-address-type (unicast | local | broadcast | multicast) -

IP

- **unicast** - IP

- **local** -

- **broadcast** - IP IP

- **multicast** - IP

dst-limit (integer/time{0,1},integer,dst-address | dst-port | src-address{+},time{0,1}) -
IP

):

- **count** - , time -

(pps),

time

- **time** -

- **burst** - -

- **mode** -

- **expire** - IP /

dst-port - (integer: 0..65535-integer: 0..65535{*}) -

fragment (yes | no) - IP (.

hotspot (multiple choice: auth | from-client | http | local-dst | to-client) -
HotSpot.

- **auth** - , HotSpot
- **from-client** - , HotSpot
- **http** - , HotSpot
proxy (Universal Proxy technique) 80
- **local-dst** - , IP
- **to-client** - ,

icmp-options (integer.integer) - ICMP :

in-bridge-port (name) -

(, ,)

in-interface

in-interface (name) -

(,)

ingress-priority (integer: 0..63) - INGRESS() ,

(0) .

VLAN

WMM

ipv4-options (any | loose-source-routing | no-record-route | no-router-alert | no-source-routing | no-timestamp | none | record-route | router-alert | strict-source-routing | timestamp) -
ipv4

- **any** - ipv4
- **loose-source-routing** -
- **no-record-route** -
- **no-router-alert** -
- **no-source-routing** -
- **no-timestamp** - timestamp
- **record-route** -
- **router-alert** -
- **strict-source-routing** -
- **timestamp** - timestamp

jump-target (forward | input | output | postrouting | prerouting name) -
, **action=jump**

layer7-protocol (name) - Layer 7
protocol . :

/ip firewall layer7-

limit (integer/time{0,1},integer) -

- **count** (pps), **time** , -
- **time** - ,
- **burst** - -

log-prefix (text) -

new-dscp (integer: 0..63) - **action=mark-connection**

DSCP

new-mss (integer) - **action=change-dscp**

MSS

action=change-mss

new-packet-mark(name) -

action-mark-packet

new-priority (integer) -

action=set-priority

- **from-dscp** - DSCP
- **from-ingress** - INGRESS(VLAN
- WMM - ; 0)

new-routing-mark (name) -

action=mark-routing

new-ttl (decrement | increment | set:integer) -

TTL

action=change-ttl

- **decrement** - TTL
- **increment** - TTL
- **set:** TTL

nth (integer,integer: 0..15,integer{0,1}) -

Nth

16

- **every** - +1 , +1
- **counter** .
- **packet** (nth) .
0 every

, every+1
0 every

out-bridge-port(name) -

(
out-interface)

out-interface (name) -

(,)

p2p (all-p2p | bit-torrent | direct-connect | edonkey | fasttrack | gnutella | soulseek | warez | winmx) -

P2P

packet-mark (name) -

mangle

packet-mark

packet-size (integer: 0..65535-integer: 0..65535{0,1})-

min -

max -

passthrough (yes | no; : yes) -

()

port (port{0-16}) -

()
()

src-port

dst-port)

protocol (ddp | egp | encap | ggp | gre | hmp | icmp | idrp -cmtip | igmp | ipencap | ipip | ipsec-ah | ipsec-esp | iso-tp4 | ospf | pup | rdp | rspf | st | tcp | udp | vmtip | xns -idp | xtp | integer) -

psd (integer,time,integer,integer) -

TCP UDP

FTP

- **WeightThreshold** -

TCP/UDP

- **DelayThreshold** -

- **LowPortWeight** -

(1024)

- **HighPortWeight** -

random (integer: 1..99) -

routing-mark (name) -

src-address (IP address/netmask | IP address-IP address) -

IP

. 1.1.1.1/24

1.1.1.0/24

address/netmask

src-address-list (name) -

src-address-type (unicast | local | broadcast | multicast) -

IP

- **unicast** - IP

- **local** -

- **broadcast** - IP

- **multicast** - IP

IP

src-mac-address (MAC address) - MAC

src-port (integer: 0..65535-integer: 0..65535{*}) -

tcp-flags (multiple choice: ack | cwr | ece | fin | psh | rst | syn | urg)

tcp

- **ack** -

- **cwr** -

- **ece** - ECH-echo ()

- **fin** -

- **psh** -

- **rst** -

- **syn** -

- **urg** -

tcp-mss (integer: 0..65535) -

IP

TCP MSS

time (time-time,sat | fri | thu | wed | tue | mon | sun{+}) -

mangle

(
passthrough
),
P2P,
P2P

mangle

Peer-to-Peer Traffic Marking

VoIP HTTP
, peer-to-peer. RouterOS QOS

P2P
1 Mbps
:

```
[admin@MikroTik] > /ip firewall mangle add chain=forward
... p2p=all-p2p action=mark-connection new-connection-mark=p2p_conn
[admin@MikroTik] > /ip firewall mangle add chain=forward
... connection-mark=p2p_conn action=mark-packet new-packet-mark=p2p
[admin@MikroTik] > /ip firewall mangle add chain=forward
... connection-mark=!p2p_conn action=mark-packet new-packet-mark=other
[admin@MikroTik] > /ip firewall mangle print
Flags: X - disabled, I - invalid, D - dynamic
 0 chain=forward p2p=all-p2p action=mark-connection new-connection-
mark=p2p_conn
 1 chain=forward connection-mark=p2p_conn action=mark-packet new-packet-
mark=p2p
 2 chain=forward packet-mark=!p2p_conn action=mark-packet new-packet-
mark=other
[admin@MikroTik] >
[admin@MikroTik] > /queue tree add parent=Public packet-mark=p2p limit-
at=1000000
... max-limit=100000000 priority=8
[admin@MikroTik] > /queue tree add parent=Local packet-mark=p2p limit-
at=1000000
... max-limit=100000000 priority=8
[admin@MikroTik] > /queue tree add parent=Public packet-mark=other limit-
at=1000000
... max-limit=100000000 priority=1
[admin@MikroTik] > /queue tree add parent=Local packet-mark=other limit-
at=1000000
... max-limit=100000000 priority=1
```

MAC

:

/


```
[admin@MikroTik] > / ip firewall mangle add chain=prerouting
... src-mac-address=00:01:29:60:36:E7 action=mark-connection new-connection-
mark=known_mac_conn
[admin@MikroTik] > / ip firewall mangle add chain=prerouting
... connection-mark=known_mac_conn action=mark-packet new-packet-
mark=known_mac
```

MSS

VPN
MSS

MSS VPN

DF,

MTU (PMTUD)

FTP HTTP

PTUMD,

MSS

VPN

MSS

mangle

```
[admin@MikroTik] > /ip firewall mangle add out-interface=pppoe-out
... protocol=tcp tcp-flags=syn action=change-mss new-mss=1300 chain=forward
[admin@MikroTik] > /ip firewall mangle print
Flags: X - disabled, I - invalid, D - dynamic
0 chain=forward out-interface=pppoe-out protocol=tcp tcp-flags=syn
action=change-mss new-mss=1300
[admin@MikroTik] >
```