

Mangle

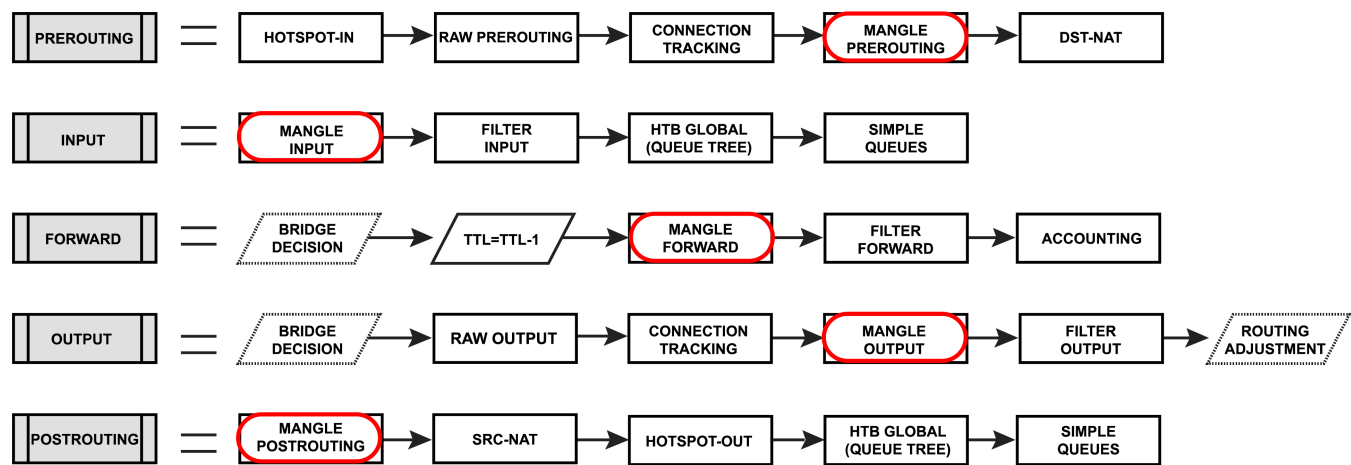
- [Introduction](#)
- [Properties](#)
 - [Stats](#)
- [Configuration example](#)
 - [Change MSS](#)

Introduction

Mangle is a kind of 'marker' that marks packets for future processing with special marks. Many other facilities in RouterOS make use of these marks, e.g. queue trees, NAT, routing. They identify a packet based on its mark and process it accordingly. The mangle marks exist only within the router, they are not transmitted across the network.

Additionally, the mangle facility is used to modify some fields in the IP header, like TOS (DSCP) and TTL fields.

Firewall mangle rules consist of five predefined chains that cannot be deleted:



- The **PREROUTING** chain: Rules in this chain apply to packets as they just arrive on the network interface;
- The **INPUT** chain: Rules in this chain apply to packets just before they're given to a local process;
- The **OUTPUT** chain: The rules here apply to packets just after they've been produced by a process;
- The **FORWARD** chain: The rules here apply to any packets that are routed through the current host;
- The **POSTROUTING** chain: The rules in this chain apply to packets as they just leave the network interface;


Properties

Property	Description
----------	-------------

action (<i>action name</i> ; Default: accept)	<p>Action to take if a packet is matched by the rule:</p> <ul style="list-style-type: none"> • accept - accept the packet. A packet is not passed to the next firewall rule. • add-dst-to-address-list - add destination address to address list specified by address-list parameter • add-src-to-address-list - add source address to address list specified by address-list parameter • change-dscp - change the Differentiated Services Code Point (DSCP) field value specified by the new-dscp parameter • change-mss - change the Maximum Segment Size field value of the packet to a value specified by the new-mss parameter • change-ttl - change the Time to Live field value of the packet to a value specified by the new-ttl parameter • clear-df - clear 'Do Not Fragment' Flag • fasttrack-connection - shows fasttrack counters, useful for statistics • jump - jump to the user-defined chain specified by the value of jump-target parameter • log - add a message to the system log containing the following data: in-interface, out-interface, src-mac, protocol, src-ip:port->dst-ip:port and length of the packet. After a packet is matched it is passed to the next rule in the list, similar as passthrough • mark-connection - place a mark specified by the new-connection-mark parameter on the entire connection that matches the rule • mark-packet - place a mark specified by the new-packet-mark parameter on a packet that matches the rule • mark-routing - place a mark specified by the new-routing-mark parameter on a packet. This kind of mark is used for policy routing purposes only. Do not apply any other routing marks besides "main" for the packets processed by FastTrack, since FastTrack can only work in the main routing table. • passthrough - if a packet is matched by the rule, increase the counter and go to the next rule (useful for statistics). • return - pass control back to the chain from where the jump took place • route - forces packets to a specific gateway IP by ignoring normal routing decisions (prerouting chain only) • set-priority - set priority specified by the new-priority parameter on the packets sent out through a link that is capable of transporting priority (VLAN or WMM-enabled wireless interface). Read more • sniff-pc - send a packet to a remote RouterOS CALEA server. • sniff-tzsp - send a packet to a remote TZSP compatible system (such as Wireshark). Set remote target with sniff-target and sniff-target-port parameters (Wireshark recommends port 37008) • strip-ipv4-options - strip IPv4 option fields from IP header, the action does not actually remove IPv4 options but rather replaces all option octets with NOP, further matcher with ipv4-options=any will still match the packet.
address-list (<i>string</i> ; Default:)	Name of the address list to be used. Applicable if action is add-dst-to-address-list or add-src-to-address-list
address-list-timeout (<i>none-dynamic none-static time</i> ; Default: none-dynamic)	<p>Time interval after which the address will be removed from the address list specified by address-list parameter. Used in conjunction with add-dst-to-address-list or add-src-to-address-list actions</p> <ul style="list-style-type: none"> • Value of none-dynamic (00:00:00) will leave the address in the address list till reboot • Value of none-static will leave the address in the address list forever and will be included in the configuration export/backup
chain (<i>name</i> ; Default:)	Specifies to which chain the rule will be added. If the input does not match the name of an already defined chain, a new chain will be created
comment (<i>string</i> ; Default:)	Descriptive comment for the rule.
connection-bytes (<i>integer-integer</i> ; Default:)	Matches packets only if a given amount of bytes has been transferred through the particular connection. 0 - means infinity, for example connection-bytes=2000000-0 means that the rule matches if more than 2MB (upload and download) has been transferred through the relevant connection
connection-limit (<i>integer,netmask</i> ; Default:)	Matches connections per address or address block after a given value is reached

connection-mark (<i>no-mark</i> / <i>string</i> ; Default:)	Matches packets marked via mangle facility with particular connection mark. If no-mark is set, the rule will match any unmarked connection.
connection-nat-state (<i>srcnat</i> / <i>dstnat</i> ; Default:)	Can match connections that are srcnatted, dstnatted, or both. Note that connection-state=related connections connection-nat-state is determined by the direction of the first packet. and if connection tracking needs to use dst-nat to deliver this connection to the same hosts as the main connection it will be in connection-nat-state=dstnat even if there are no dst-nat rules at all.
connection-rate (<i>Integer 0..4294967295</i> ; Default:)	Connection Rate is a firewall matcher that allows the capture of traffic based on the present speed of the connection.
connection-state (<i>established</i> / <i>invalid</i> / <i>new</i> / <i>related</i> ; Default:)	<p>Interprets the connection tracking analytics data for a particular packet:</p> <ul style="list-style-type: none"> established - a packet that belongs to an existing connection invalid - a packet that does not have a determined state in connection tracking (usually - severe out-of-order packets, packets with wrong sequence/ack number, or in case of a resource over usage on a router), for this reason, an invalid packet will not participate in NAT (as only connection-state=new packets do), and will still contain original source IP address when routed. We strongly suggest dropping all connection-state=invalid packets in the firewall filter forward and input chains new - the packet has started a new connection, or is otherwise associated with a connection that has not seen packets in both directions related - a packet that is related to, but not parts of an existing connection, such as ICMP errors or a packet that begins an FTP data connection untracked - packet which was set to bypass connection tracking in Firewall RAW tables.
connection-type (<i>ftp</i> / <i>h323</i> / <i>irc</i> / <i>pptp</i> / <i>quake3</i> / <i>sip</i> / <i>tftp</i> ; Default:)	Matches packets from related connections based on information from their connection tracking helpers. A relevant connection helper must be enabled under: <code>/ip firewall service-port</code>
content (<i>string</i> ; Default:)	Match packets that contain specified text
dscp (<i>integer: 0..63</i> ; Default:)	Matches DSCP IP header field
dst-address (<i>IP/netmask</i> / <i>IP range</i> ; Default:)	Matches packets where the destination is equal to the specified IP or falls into a specified IP range
dst-address-list (<i>name</i> ; Default:)	Matches the destination address of a packet against a user-defined address list
dst-address-type (<i>unicast</i> / <i>local</i> / <i>broadcast</i> / <i>multicast</i> ; Default:)	<p>Matches destination address type:</p> <ul style="list-style-type: none"> unicast - IP address used for point to point transmission local - if dst-address is assigned to one of the router's interfaces broadcast - packet is sent to all devices in a subnet multicast - packet is forwarded to a defined group of devices
dst-limit (<i>integer[/time]</i> , <i>integer</i> , <i>dst-address</i> / <i>dst-port</i> / <i>src-address[/time]</i> ; Default:)	<p>Matches packets until a given PPS limit is exceeded. As opposed to the limit matcher, every destination IP address/destination port has its own limit. Parameters are written in the following format: <code>count[/time],burst,mode[/expire]</code>.</p> <ul style="list-style-type: none"> count - maximum average packet rate measured in packets per <code>time</code> interval time - specifies the time interval in which the packet rate is measured (optional) burst - number of packets that are not counted by packet rate mode - the classifier for packet rate limiting expire - specifies interval after which recorded ip address /port will be deleted (optional)
dst-port (<i>integer[-integer]</i> : <i>0..65535</i> ; Default:)	List of destination port numbers or port number ranges
fragment (<i>yes/no</i> ; Default:)	Matches fragmented packets. The first (starting) fragment does not count. If connection tracking is enabled there will be no fragments as the system automatically assembles every packet

hotspot (<i>auth / from-client / http / local-dst / to-client</i> ; Default:)	Matches packets received from HotSpot clients against various HotSpot matches. <ul style="list-style-type: none"> auth - matches authenticated HotSpot client packets from-client - matches packets that are coming from the HotSpot client http - matches HTTP requests sent to the HotSpot server local-dst - matches packets that are destined to the HotSpot server to-client - matches packets that are sent to the HotSpot client
icmp-options (<i>integer:integer</i> ; Default:)	Matches ICMP "type:code" fields
in-bridge-port (<i>name</i> ; Default:)	Actual interface the packet has entered the router if the incoming interface is a bridge
in-interface (<i>name</i> ; Default:)	Interface the packet has entered the router
ingress-priority (<i>integer: 0..63</i> ; Default:)	Matches ingress the priority of the packet. Priority may be derived from VLAN, WMM, or MPLS EXP bit. Read more
ipsec-policy (<i>in / out, ipsec / none</i> ; Default:)	Matches the policy used by IPsec. Value is written in the following format: direction, policy . The direction is Used to select whether to match the policy used for decapsulation or the policy that will be used for encapsulation. <ul style="list-style-type: none"> in - valid in the PREROUTING, INPUT, and FORWARD chains out - valid in the POSTROUTING, OUTPUT, and FORWARD chains ipsec - matches if the packet is subject to IPsec processing; none - matches packet that is not subject to IpSec processing (for example, IpSec transport packet). <p>For example, if a router receives an IPsec encapsulated Gre packet, then rule ipsec-policy=in, ipsec will match Gre packet, but a rule ipsec-policy=in,none will match the ESP packet.</p>
ipv4-options (<i>any / loose-source-routing / no-record-route / no-router-alert / no-source-routing / no-timestamp / none / record-route / router-alert / strict-source-routing / timestamp</i> ; Default:)	Matches IPv4 header options. <ul style="list-style-type: none"> any - match packet with at least one of the ipv4 options loose-source-routing - match packets with a loose source routing option. This option is used to route the internet datagram based on information supplied by the source no-record-route - match packets with no record route option. This option is used to route the internet datagram based on information supplied by the source no-router-alert - match packets with no router alter option no-source-routing - match packets with no source routing option no-timestamp - match packets with no timestamp option record-route - match packets with record route option router-alert - match packets with router alter option strict-source-routing - match packets with strict source routing option timestamp - match packets with a timestamp
jump-target (<i>name</i> ; Default:)	Name of the target chain to jump to. Applicable only if action=jump
layer7-protocol (<i>name</i> ; Default:)	Layer7 filter name defined in layer7 protocol menu .
limit (<i>integer,time,integer</i> ; Default:)	Matches packets until a given PPS limit is exceeded. Parameters are written in the following format: count[/time],burst . <ul style="list-style-type: none"> count - maximum average packet rate measured in packets per time interval time - specifies the time interval in which the packet rate is measured (optional, 1s will be used if not specified) burst - number of packets that are not counted by packet rate
log (<i>yes / no</i> ; Default: no)	Add a message to the system log containing the following data: in-interface, out-interface, src-mac, protocol, src-ip:port->dst-ip:port, and length of the packet.
log-prefix (<i>string</i> ; Default:)	Adds specified text at the beginning of every log message. Applicable if action=log or log=yes configured.
new-dscp (<i>integer: 0..63</i> ; Default:)	Sets a new DSCP value for a packet

new-mss (<i>integer</i> ; Default:)	<p>Sets a new MSS for a packet.</p> <div>  Clamp-to-pmtu feature sets (DF) bit in the IP header to dynamically discover the PMTU of a path. Host sends all datagrams on that path with the DF bit set until receives ICMP Destination Unreachable messages with a code meaning "fragmentation needed and DF set". Upon receipt of such a message, the source host reduces its assumed PMTU for the path. </div>
new-packet-mark (<i>string</i> ; Default:)	Sets a new packet-mark value
new-priority (<i>integer from-dscp from-dscp-high-3-bits from-ingress</i> ; Default:)	Sets a new priority for a packet. This can be the VLAN, WMM, DSCP or MPLS EXP priority Read more . This property can also be used to set an internal priority.
new-routing-mark (<i>string</i> ; Default:)	Sets a new routing-mark value (in RouterOS v7 routing mark must be created before as a new Routing table)
new-ttl (<i>decrement increment set: integer</i> ; Default:)	Sets a new Time to live value
nth (<i>integer, integer</i> ; Default:)	Matches every nth packet: nth=2, 1 rule will match every first packet of 2, hence, 50% of all the traffic that is matched by the rule
out-bridge-port (<i>name</i> ; Default:)	Actual interface the packet is leaving the router if the outgoing interface is a bridge
out-interface (; Default:)	Interface the packet is leaving the router
packet-mark (<i>no-mark string</i> ; Default:)	Matches packets marked via mangle facility with particular packet mark. If no-mark is set, the rule will match any unmarked packet
packet-size (<i>integer[-integer]: 0..65535</i> ; Default:)	Matches packets of specified size or size range in bytes
passthrough (<i>yes/no</i> ; Default: yes)	whether to let the packet to pass further (like action passthrough) into the firewall or not (property only valid for some actions)
per-connection-classifier (<i>ValuesToHash:Denominator/Remainder</i> ; Default:)	PCC matcher allows the division of traffic into equal streams with the ability to keep packets with a specific set of options in one particular stream
port (<i>integer[-integer]: 0..65535</i> ; Default:)	Matches if any (source or destination) port matches the specified list of ports or port ranges. Applicable only if protocol is TCP or UDP
protocol (<i>name or protocol ID</i> ; Default: tcp)	Matches particular IP protocol specified by protocol name or number
psd (<i>integer, time, integer, integer</i> ; Default:)	<p>Attempts to detect TCP and UDP scans. Parameters are in the following format WeightThreshold, DelayThreshold, LowPortWeight, HighPortWeight</p> <ul style="list-style-type: none"> • WeightThreshold - total weight of the latest TCP/UDP packets with different destination ports coming from the same host to be treated as port scan sequence • DelayThreshold - delay for the packets with different destination ports coming from the same host to be treated as possible port scan subsequence • LowPortWeight - the weight of the packets with privileged (<1024) destination port • HighPortWeight - the weight of the packet with a non-privileged destination port
random (<i>integer: 1..99</i> ; Default:)	Matches packets randomly with a given probability.
routing-mark (<i>string</i> ; Default:)	Matches packets marked by mangle facility with particular routing mark
route-dst (<i>IP</i> ; Default:)	Matches packets with a specific gateway
priority (<i>integer: 0..63</i> ; Default:)	Matches the packet's priority after a new priority has been set. Priority may be derived from VLAN, WMM, DSCP, MPLS EXP bit, or from the internal priority that has been set using the set-priority action
src-address (<i>IP/Netmask, IP range</i> ; Default:)	Matches packets where the source is equal to a specified IP or falls into a specified IP range.

src-address-list (<i>name</i> ; Default:)	Matches the source address of a packet against a user-defined address list
src-address-type (<i>unicast</i> <i>local</i> <i>broadcast</i> <i>multicast</i> ; Default:)	Matches source address type: <ul style="list-style-type: none"> • <i>unicast</i> - IP address used for point-to-point transmission • <i>local</i> - if an address is assigned to one of the router's interfaces • <i>broadcast</i> - packet is sent to all devices in a subnet • <i>multicast</i> - packet is forwarded to a defined group of devices
src-port (<i>integer</i> [- <i>integer</i>]: 0..65535; Default:)	List of source ports and ranges of source ports. Applicable only if a protocol is TCP or UDP.
src-mac-address (<i>MAC address</i> ; Default:)	Matches the source MAC address of the packet
tcp-flags (<i>ack</i> <i>cwr</i> <i>ece</i> <i>fin</i> <i>psh</i> <i>rst</i> <i>syn</i> <i>urg</i> ; Default:)	Matches specified TCP flags <ul style="list-style-type: none"> • <i>ack</i> - acknowledging data • <i>cwr</i> - congestion window reduced • <i>ece</i> - ECN-echo flag (explicit congestion notification) • <i>fin</i> - close connection • <i>psh</i> - push function • <i>rst</i> - drop connection • <i>syn</i> - new connection • <i>urg</i> - urgent data
tcp-mss (<i>integer</i> [- <i>integer</i>]: 0..65535; Default:)	Matches the TCP MSS value of an IP packet
time (<i>time-time,sat</i> <i>fri</i> <i>thu</i> <i>wed</i> <i>tue</i> <i>mon</i> <i>sun</i> ; Default:)	Allows creation of a filter based on the packets' arrival time and date or, for locally generated packets, departure time and date
tls-host (<i>string</i> ; Default:)	Allows matching traffic based on TLS hostname. Accepts GLOB syntax for wildcard matching. Note that the matcher will not be able to match the hostname if the TLS handshake frame is fragmented into multiple TCP segments (packets).
ttl (<i>equal</i> <i>greater-than</i> <i>less-than</i> <i>not-equal</i> : <i>integer</i> (0..255); Default:)	Matches packets TTL value.

Stats

To show additional *read-only* properties:

Property	Description
bytes (<i>integer</i>)	The total amount of bytes matched by the rule
packets (<i>integer</i>)	The total amount of packets matched by the rule

To print out stats:

```
[admin@MikroTik] > ip firewall mangle print stats all
Flags: X - disabled, I - invalid, D - dynamic
# CHAIN ACTION BYTES PACKETS
0 D ;; special dummy rule to show fasttrack counters
prerouting passthrough 18 176 176 30 562
1 D ;; special dummy rule to show fasttrack counters
forward passthrough 18 176 176 30 562
2 D ;; special dummy rule to show fasttrack counters
postrouting passthrough 18 176 176 30 562
3 forward change-mss 18 512 356
```

Configuration example

Change MSS

It is a known fact that VPN links have a smaller packet size due to encapsulation overhead. A large packet with MSS that exceeds the MSS of the VPN link should be fragmented before sending it via that kind of connection. However, if the packet has a *Don't Fragment* flag set, it cannot be fragmented and should be discarded. On links that have broken path MTU discovery (PMTUD), it may lead to a number of problems, including problems with FTP and HTTP data transfer and e-mail services.

In the case of a link with broken PMTUD, a decrease of the MSS of the packets coming through the VPN link resolves the problem. The following example demonstrates how to decrease the MSS value via mangle:

```
/ip firewall mangle add out-interface=pppoe-out protocol=tcp tcp-flags=syn action=change-mss new-mss=1300  
chain=forward tcp-mss=1301-65535
```