

Mangle

Document revision 2.8 (Tue Jul 12 09:18:22 GMT 2005)

Table of Contents

[Table of Contents](#)

[Summary](#)

[Specifications](#)

[Related Documents](#)

[Mangle](#)

[Description](#)

[Property Description](#)

[Description](#)

[Peer-to-Peer Traffic Marking](#)

[Mark by MAC address](#)

[Change MSS](#)

General Information

Summary

The mangle facility allows to mark IP packets with special marks. These marks are used by various other router facilities to identify the packets. Additionally, the mangle facility is used to modify some fields in the IP header, like TOS (DSCP) and TTL fields.

Specifications

Packages required: *system*

License required: *level1*

Home menu level: */ip firewall mangle*

Standards and Technologies: [IP](#)

Hardware usage: *Increases with count of mangle rules*

Related Documents

- [Software Package Management](#)
- [IP Addresses and ARP](#)
- [Routes, Equal Cost Multipath Routing, Policy Routing](#)
- [NAT](#)
- [Filter](#)
- [Packet Flow](#)

Mangle

chain (*forward | input | output | postrouting | prerouting*) - specify the chain to put a particular rule into. As the different traffic is passed through different chains, always be careful in choosing the right chain for a new rule. If the input does not match the name of an already defined chain, a new chain will be created

comment (*text*) - free form textual comment for the rule. A comment can be used to refer the particular rule from scripts

connection-bytes (*integer | integer*) - match packets only if a given amount of bytes has been transferred through the particular connection

- **0** - means infinity, exempli gratia: `connection-bytes=2000000-0` means that the rule matches if more than 2MB has been transferred through the relevant connection

connection-limit (*integer | netmask*) - restrict connection limit per address or address block

connection-mark (*name*) - match packets marked via mangle facility with particular connection mark

connection-type (*ftp | gre | h323 | irc | mms | pptp | quake3 | tftp*) - match packets from related connections based on information from their connection tracking helpers. A relevant connection helper must be enabled under `/ip firewall service-port`

content (*text*) - the text packets should contain in order to match the rule

dst-address (*IP address | netmask | IP address | IP address*) - specify the address range an IP packet is destined to. Note that console converts entered address/netmask value to a valid network address, i.e.: `1.1.1.1/24` is converted to `1.1.1.0/24`

dst-address-list (*name*) - match destination address of a packet against user-defined address list

dst-address-type (*unicast | local | broadcast | multicast*) - match destination address type of the IP packet, one of the:

- **unicast** - IP addresses used for one point to another point transmission. There is only one sender and one receiver in this case
- **local** - match addresses assigned to router's interfaces
- **broadcast** - the IP packet is sent from one point to all other points in the IP subnetwork
- **multicast** - this type of IP addressing is responsible for transmission from one or more points to a set of other points

dst-limit (*integer | time | integer | dst-address | dst-port | src-address | time*) - limit the packet per second (pps) rate on a per destination IP or per destination port base. As opposed to the limit match, every destination IP address / destination port has it's own limit. The options are as follows (in order of appearance):

- **Count** - maximum average packet rate, measured in packets per second (pps), unless followed by Time option
- **Time** - specifies the time interval over which the packet rate is measured
- **Burst** - number of packets to match in a burst
- **Mode** - the classifier(-s) for packet rate limiting
- **Expire** - specifies interval after which recorded IP addresses / ports will be deleted

dst-port (*integer: 0..65535 | integer: 0..65535*) - destination port number or range

hotspot (*multiple choice: from-client | auth | local-dst | http*) - match packets received from clients against various Hot-Spot. All values can be negated

- **from-client** - true, if a packet comes from HotSpot client
-

- **auth** - true, if a packet comes from authenticated client
- **local-dst** - true, if a packet has local destination IP address
- **hotspot** - true, if it is a TCP packet from client and either the transparent proxy on port 80 is enabled or the client has a proxy address configured and this address is equal to the address:port pair of the IP packet

icmp-options (*integer | integer*) - match ICMP Type:Code fields

in-interface (*name*) - interface the packet has entered the router through

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*) - match ipv4 header options

- **any** - match packet with at least one of the ipv4 options
- **loose-source-routing** - match packets with 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 timestamp

jump-target (*forward | input | output | postrouting | prerouting | name*) - name of the target chain to jump to, if the action=jump is used

limit (*integer | time | integer*) - restrict packet match rate to a given limit. Usefull to reduce the amount of log messages

- **Count** - maximum average packet rate, measured in packets per second (pps), unless followed by Time option
- **Time** - specify the time interval over which the packet rate is measured
- **Burst** - number of packets to match in a burst

log-prefix (*text*) - all messages written to logs will contain the prefix specified herein. Used in conjunction with action=log

new-connection-mark (*name*) - specify the new value of the connection mark to be used in conjunction with action=mark-connection

new-mss (*integer*) - specify MSS value to be used in conjunction with action=change-mss

new-packet-mark (*name*) - specify the new value of the packet mark to be used in conjunction with action=mark-packet

new-routing-mark (*name*) - specify the new value of the routing mark used in conjunction with action=mark-routing

new-tos (*max-reliability | max-throughput | min-cost | min-delay | normal | integer*) - specify TOS value to be used in conjunction with action=change-tos

- **max-reliability** - maximize reliability (ToS=4)
-

- **max-throughput** - maximize throughput (ToS=8)
- **min-cost** - minimize monetary cost (ToS=2)
- **min-delay** - minimize delay (ToS=16)
- **normal** - normal service (ToS=0)

new-ttl (*decrement* | *increment* | *set* | *integer*) - specify the new TTL field value used in conjunction with action=change-ttl

- **decrement** - the value of the TTL field will be decremented for value
- **increment** - the value of the TTL field will be incremented for value
- **set:** - the value of the TTL field will be set to value

nth (*integer* | *integer: 0..15* | *integer*) - match a particular Nth packet received by the rule. One of 16 available counters can be used to count packets

- **Every** - match every Nth packet
- **Counter** - specifies which counter to use
- **Packet** - match on the given packet number. The value by obvious reasons must be between 0 and Every-1. If this option is used for a given counter, then there must be at least Every rules with this option, covering all values between 0 and Every-1 inclusively.

out-interface (*name*) - match the interface name a packet left the router through

p2p (*all-p2p* | *bit-torrent* | *direct-connect* | *edonkey* | *fasttrack* | *gnutella* | *soulseek* | *warez* | *winmx*) - match packets belonging to connections of the above P2P protocols

packet-mark (*name*) - match the packets marked in mangle with specific packet mark

packet-size (*integer: 0..65535* | *integer: 0..65535*) - matches packet of the specified size or size range in bytes

- **Min** - specifies lower boundary of the size range or a standalone value
- **Max** - specifies upper boundary of the size range

phys-in-interface (*name*) - matches the bridge port physical input device added to a bridge device. It is only useful if the packet has arrived through the bridge

protocol (*ddp* | *egp* | *encap* | *ggp* | *gre* | *hmp* | *icmp* | *idrp-cmt* | *igmp* | *ipencap* | *ipip* | *ipsec-ah* | *ipsec-esp* | *iso-tp4* | *ospf* | *pup* | *rdp* | *rspf* | *st* | *tcp* | *udp* | *vmtp* | *xns-idp* | *xtp* | *integer*) - matches particular IP protocol specified by protocol name or number. You should specify this setting if you want to specify ports

psd (*integer* | *time* | *integer* | *integer*) - attempts to detect TCP and UDP scans. It is advised to assign lower weight to ports with high numbers to reduce the frequency of false positives, such as from passive mode FTP transfers

- **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** - weight of the packets with privileged (<=1024) destination port
- **HighPortWeight** - weight of the packet with non-privileged destination port

random (*integer: 1..99*) - matches packets randomly with given probability

routing-mark (*name*) - matches packets marked with the specified routing mark

src-address (*IP address | netmask | IP address | IP address*) - specifies the address range an IP packet is originated from. Note that console converts entered address/netmask value to a valid network address, i.e.:1.1.1.1/24 is converted to 1.1.1.0/24

src-address-list (*name*) - matches source address of a packet against user-defined address list

src-address-type (*unicast | local | broadcast | multicast*) - matches source address type of the IP packet, one of the:

- **unicast** - IP addresses used for one point to another point transmission. There is only one sender and one receiver in this case
- **local** - matches addresses assigned to router's interfaces
- **broadcast** - the IP packet is sent from one point to all other points in the IP subnetwork
- **multicast** - this type of IP addressing is responsible for transmission from one or more points to a set of other points

src-mac-address (*MAC address*) - source MAC address

src-port (*integer: 0..65535 | integer: 0..65535*) - source port number or range

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

- **ack** - acknowledging data
- **cwr** - congestion window reduced
- **ece** - ECN-echo flag (explicit congestion notification)
- **fin** - close connection
- **psh** - push function
- **rst** - drop connection
- **syn** - new connection
- **urg** - urgent data

tcp-mss (*integer: 0..65535*) - matches TCP MSS value of an IP packet

time (*time | time | sat | fri | thu | wed | tue | mon | sun*) - allows to create filter based on the packets' arrival time and date or, for locally generated packets, departure time and date

tos (*max-reliability | max-throughput | min-cost | min-delay | normal*) - specifies a match for the value of Type of Service (ToS) field of an IP header

- **max-reliability** - maximize reliability (ToS=4)
- **max-throughput** - maximize throughput (ToS=8)
- **min-cost** - minimize monetary cost (ToS=2)
- **min-delay** - minimize delay (ToS=16)
- **normal** - normal service (ToS=0)

General Information

Description

The following section discusses some examples of using the mangle facility.

Peer-to-Peer Traffic Marking
