Manual:Connection Rate

From MikroTik Wiki

Contents

Applies to RouterOS: 3, v4

Introduction

Connection Rate is a firewall matcher that allow to capture traffic based on present speed of the connection.

Theory

Each entry in connection tracking table represents bidirectional communication. Every time packet gets associated to particular entry, packet size value (including IP header) is added to "connection-bytes" value for this entry. (in another words "connection-bytes" includes both - upload and download)

Connection Rate calculates speed of connection based on change of "connection-bytes". Connection Rate is recalculated every second and does not have any averages.

Both options "connection-bytes" and "connection-rate" work only with TCP and UDP traffic. (you need to specify protocol to activate these options)

In "connection-rate" you can specify range of speed that you like to capture.

```
ConnectionRate ::= [!]From-To
  From,To ::= 0..4294967295    (integer number)
```

Example

These rules will capture TCP/UDP traffic that was going trough the router when connection speed was below 100kbps

```
/ip firewall filter
add action=accept chain=forward connection-rate=0-100k protocol=tcp
add action=accept chain=forward connection-rate=0-100k protocol=udp
```

Notes

Connection Rate is available in RouterOS since v3.30. This option was introduced to allow capture traffic intensive connections.

Application Example - Traffic Prioritization

Connection-rate can be used in various different ways, that still need to be realized, but most common setup will be to detect and set lower priorities to the "heavy connections" (connections that maintain fast rate for long periods of time (such as P2P,HTTP,FTP downloads). By doing this you can prioritize all other traffic that usually includes VOIP and HTTP browsing and online gaming.

Method described in this example can be used together with other ways to detect and prioritize traffic

As connection-rate option does not have any averages we need to determine what will be the margin that identifies "heavy connections". If we assume that normal HTTP browsing connection is less than 500kB (4Mb) long and VOIP requires no more than 200kbps speed, then every connection that after first 500kB still have more than 200kbps speed can be assumed as "heavy".

(You might have different "connection-bytes" for HTTP browsing and differenet "connection-rate" for VOIP in your network - so, please, do your own research before applying this example)

For this example lets assume that we have 6Mbps upload and download connection to ISP.

Quick Start for Impatient

```
/ip firewall mangle
add chain=forward action=mark-connection connection-mark=!heavy_traffic_conn \
    new-connection-mark=all_conn
add chain=forward action=mark-connection connection-bytes=500000-0 \
    connection-mark=all_conn connection-rate=200k-100M \
    new-connection-mark=heavy_traffic_conn protocol=tcp
add chain=forward action=mark-connection connection-bytes=500000-0 \
    connection-mark=all_conn connection-rate=200k-100M \
    new-connection-mark=heavy_traffic_conn protocol=udp
add chain=forward action=mark-packet connection-mark=heavy_traffic_conn \
    new-packet-mark=heavy_traffic passthrough=no
add chain=forward action=mark-packet connection-mark=all_conn \
    new-packet-mark=other_traffic passthrough=no

/queue tree
add name=upload parent=public max-limit=6M
add name=other_upload parent=upload limit-at=4M max-limit=6M \
    packet-mark=other_traffic priority=1
add name=heavy_upload parent=upload limit-at=2M max-limit=6M \
    packet-mark=heavy_traffic priority=8
add name=download parent=local max-limit=6M
add name=other_download parent=download limit-at=4M max-limit=6M \
    packet-mark=other_traffic priority=1
add name=heavy_download parent=download limit-at=2M max-limit=6M \
    packet-mark=heavy_traffic priority=8
```

Explanation

In mangle we need to separate all connections into two groups, then mark packets from there 2 groups. As we are talking about client's traffic most logical place for marking would be mangle chain forward.

Keep in mind that as soon as "heavy" connection will have lower priority and queue will hit max-limit - heavy connection will drop speed, and connection-rate will be lower. This will result in a change to higher priority and connection will be able to get more traffic for a short while, when again connection-rate will raise and that again will result in change to lower priority). To avoid this we must make sure that once detected "heavy connections" will remain marked as "heavy connections" for all times.

IP Firewall mangle

```
/ip firewall mangle
add chain=forward action=mark-connection connection-mark=!heavy_traffic_conn \
    new-connection-mark=all_conn
```

This rule will ensure that that "heavy" connections will remain heavy". and mark rest of the connections with default connection mark.

```
add chain=forward action=mark-connection connection-bytes=500000-0 \
    connection-mark=all_conn connection-rate=200k-100M \
    new-connection-mark=heavy_traffic_conn protocol=tcp
add chain=forward action=mark-connection connection-bytes=500000-0 \
    connection-mark=all_conn connection-rate=200k-100M \
    new-connection-mark=heavy_traffic_conn protocol=udp
```

These two rules will mark all heavy connections based on our standarts, that every connection that after first 500kB still have more than 200kbps speed can be assumed as "heavy"

```
add chain=forward action=mark-packet connection-mark=heavy_traffic_conn \
    new-packet-mark=heavy_traffic passthrough=no
add chain=forward action=mark-packet connection-mark=all_conn \
    new-packet-mark=other_traffic passthrough=no
```

Last two rules in mangle will simple mark all traffic from corresponding connections.

Queue

This is a simple queue tree that is placed on the Interface HTB - "public" is interface where your ISP is connected, "local" where are your clients. If you have more than 1 "public" or more than 1 "local" you will need to mangle upload and download separately and place queue tree in global-out.

```
/queue tree
add name=upload parent=public max-limit=6M
add name=other_upload parent=upload limit-at=4M max-limit=6M \
    packet-mark=other_traffic priority=1
add name=heavy_upload parent=upload limit-at=2M max-limit=6M \
    packet-mark=heavy_traffic priority=8
add name=download parent=local max-limit=6M
add name=other_download parent=download limit-at=4M max-limit=6M \
    packet-mark=other_traffic priority=1
add name=heavy_download parent=download limit-at=2M max-limit=6M \
    packet-mark=heavy_traffic priority=8
```


Categories: Manual | IP | Examples | Firewall