Connection Tracking and Service Ports

Document revision 1.0 (Fri Mar 05 08:34:03 GMT 2004)
This document applies to V2.8

Table of Contents

General Information

Summary

Connection tracking or conntrack provides a facility for monitoring connections made through the router and respective state information.In turn, service port submenu allows to configure conntrack 'helpers' for various protocols. They are used to provide correct NAT traversal for these protocols.

Specifications

Packages required: ***system***
License required: ***level1***
Home menu level: ***/ip firewall connection, /ip firewall service-port***
Standards and Technologies: ***IP***
Hardware usage: *Increases with connections count*

Related Documents

- IP Addresses and ARP
- Routes, Equal Cost Multipath Routing, Policy Routing
- Network Address Translation

Notes

Connection tracking must be enabled in order to use NAT.

Copyright 1999-2006, MikroTik. All rights reserved. Mikrotik, RouterOS and RouterBOARD are trademarks of Mikrotikls SIA.
Other trademarks and registred trademarks mentioned herein are properties of their respective owners.

Connection Tracking

Home menu level: ***/ip firewall connection***

Description

Using Connection Tracking, you can observe connections passing through the router.

Connection Timeouts

Here comes a list of connection timeouts:

- **TCP SYN sent** - (first stage in establishing a connection) = 2min
- **TCP SYN recvd** - (second stage in establishing a connection) = 60sec
- **Established TCP connections** - (third stage) = 5 days
- **TCP FIN wait** - (connection termination) = 2min
- **TCP TIME wait** - (connection termination) = 2min
- **TCP CLOSE** - (remote party sends RTS) = 10sec
- **TCP CLOSE wait** - (sent RTS) = 60sec
- **TCP LAST ACK** - (received ACK) = 30sec
- **TCP Listen** - (ftp server waiting for client to establish data connection) = 2min
- **UDP timeout** - 30sec
- **UDP with reply timeout** - (remote party has responded) = 180sec
- **ICMP timeout** - 30sec
- **All other** - 10min

Property Description

dst-address (*read-only: IP address:port*) - the destination address and port the connection is established to

src-address (*read-only: IP address:port*) - the source address and port the connection is established from

protocol (*read-only: text*) - IP protocol name or number

tcp-state (*read-only: text*) - the state of TCP connection

timeout (*read-only: time*) - the amount of time until the connection will be timed out

reply-src-address (*read-only: IP address:port*) - the source address and port the reply connection is established from

reply-dst-address (*read-only: IP address:port*) - the destination address and port the reply connection is established to

assured (*read-only: true | false*) - shows whether the connection is assured

icmp-id (*read-only: integer*) - contains the ICMP ID. Each ICMP packet gets an ID set to it when it is sent, and when the receiver gets the ICMP message, it sets the same ID within the new ICMP message so that the sender will recognize the reply and will be able to connect it with the

Copyright 1999-2006, MikroTik. All rights reserved. Mikrotik, RouterOS and RouterBOARD are trademarks of Mikrotikls SIA.
Other trademarks and registred trademarks mentioned herein are properties of their respective owners.

appropriate ICMP request

icmp-option (*read-only: integer*) - the ICMP type and code fields

reply-icmp-id (*read-only: integer*) - contains the ICMP ID of received packet

reply-icmp-option (*read-only: integer*) - the ICMP type and code fields of received packet

unreplied (*read-only: true | false*) - shows whether the request was unreplied

Example

```
[admin@test_1] ip firewall connection> print
Flags: U - unreplied, A - assured
  #    SRC-ADDRESS           DST-ADDRESS           PR.. TCP-STATE   TIMEOUT
  0 U  0.0.0.0:5678          255.255.255.255:5678  udp              1s
  1 U  1.1.1.1:49679         255.255.255.255:69    udp              11s
  2 U  1.1.1.1:56635         255.255.255.255:69    udp              27s
  3  A 10.1.0.128:2413       10.10.1.1:23          tcp  established 4d22h24m14s
  4 U  10.1.0.157:5678       255.255.255.255:5678  udp              0s
  5 U  10.1.0.172:5678       255.255.255.255:5678  udp              24s
  6 U  10.1.0.175:5678       255.255.255.255:5678  udp              25s
  7 U  10.1.0.209:5678       255.255.255.255:5678  udp              25s
  8 U  10.1.0.212:5678       255.255.255.255:5678  udp              22s
  9  A 10.5.7.242:32846      10.10.1.1:23          tcp  established 4d23h59m59s
 10  A 10.5.7.242:32933      10.10.1.1:23          tcp  established 4d23h59m59s
 11 U  10.10.1.11:5678       255.255.255.255:5678  udp              12s
 12 U  10.10.10.1:5678       255.255.255.255:5678  udp              24s

[admin@test_1] ip firewall connection>
```

Service Ports

Home menu level: ***/ip firewall service-port***

Description

Some network protocols require direct two-sided connection between endpoints. This is not always possible, as network address translation is widely used to connect clients to the network. This submenu allows to configure Connection Tracking 'helpers' for above mentioned protocols. These 'helpers' are used to provide correct NAT traversal.

Property Description

name - protocol name

ports (*read-only: integer*) - port range that is used by the protocol

Example

Suppose we want to disable **h323**service port:

```
[admin@test_1] ip firewall service-port> set h323 disabled=yes
[admin@test_1] ip firewall service-port> print
Flags: X - disabled
  #   NAME                                                    PORTS
  0   ftp                                                     21
  1   pptp
  2   gre
  3 X h323
  4   mms
  5   irc                                                     6667
```


Copyright 1999-2006, MikroTik. All rights reserved. Mikrotik, RouterOS and RouterBOARD are trademarks of Mikrotikls SIA.
Other trademarks and registred trademarks mentioned herein are properties of their respective owners.

```
  6   quake3
[admin@test_1] ip firewall service-port>
```


Copyright 1999-2006, MikroTik. All rights reserved. Mikrotik, RouterOS and RouterBOARD are trademarks of Mikrotikls SIA.
Other trademarks and registred trademarks mentioned herein are properties of their respective owners.