

Connection Tracking Implementation and Case

Intro

- Yoga Wahyu Mahendra
- Klaten, 8 September 1999
- MikroTik Certified Trainer (TR0619) at BelajarMikroTik.COM
- Certificate Taken :
 - MTCNA
 - MTCTCE
 - MTCRE
 - MTCWE
 - MTCIPv6E
 - MTCUME
 - MTCINE
 - MTCSE



BelajarMikroTik.COM

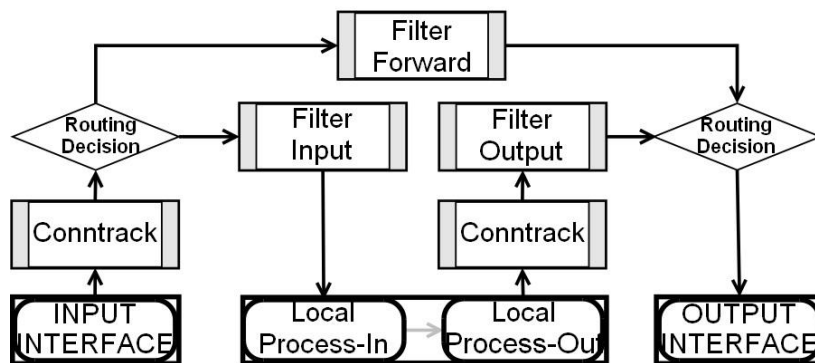
- BelajarMikroTik.COM is the one of MikroTik Training Center in Indonesia
- BelajarMikroTik.COM founded by Herry Darmawan & Akbar Azwir on 2013
- Located in Surabaya but we also hold training around Indonesia even in Australia and Philippines
- Certification that you can take : MTCNA, MTCTCE, MTCRE, MTCUME, MTCWE, MTIPv6E, MTCSE, MTCINE

What is Connection Tracking?

- In Router, all the active traffic will be stored real-time to restored them to the correct request source
- In MikroTik RouterOS, This feature called Connection-Tracking



How Connection Tracking Work?

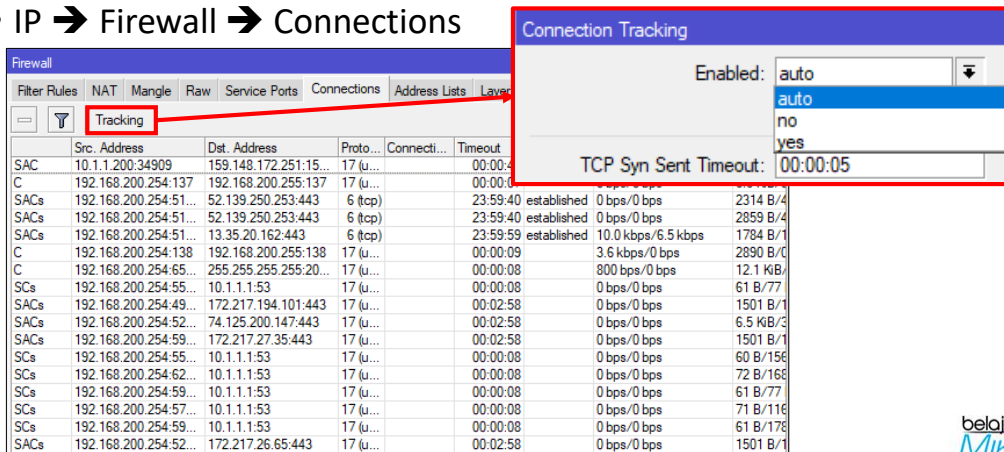


Connection Tracking

- Disabling connection tracking will effect with some Firewall feature
- Feature affected by Connection-Tracking :
 - NAT
 - Connection-bytes
 - Connection-mark
 - Connection-state
 - Connection-limit
 - Connection-rate
 - Layer7-protocol
 - New-connection-mark
 - Tarpit

Connection Tracking Menu

- IP → Firewall → Connections



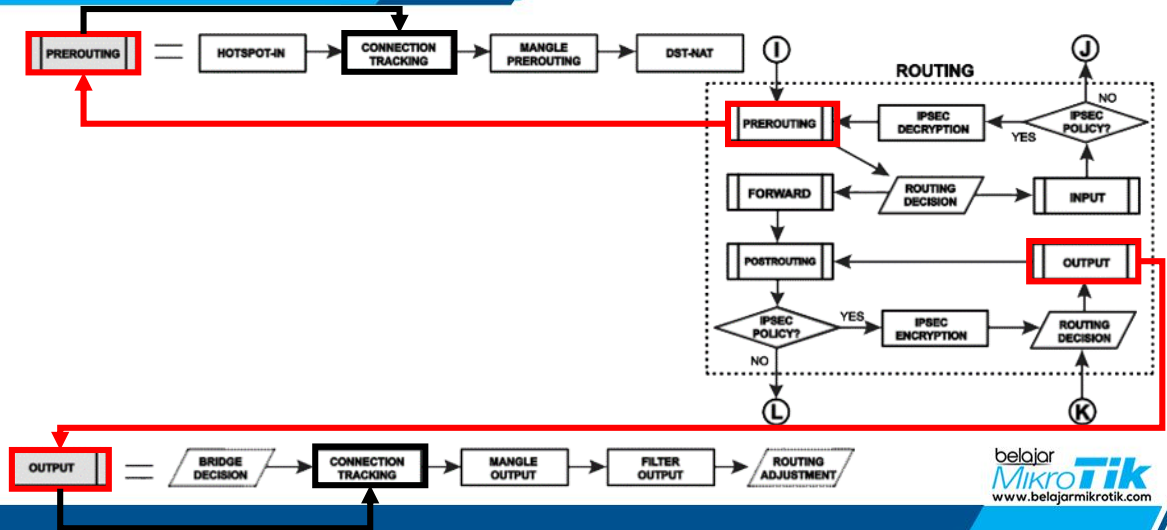
The screenshot shows the Mikrotik WinBox interface. The 'Firewall' menu is open, and the 'Connections' sub-menu is selected. The 'Connection Tracking' sub-menu is also open, showing the following settings:

- Enabled: auto
- TCP Syn Sent Timeout: 00:00:05

The main window displays a table of active connections. The table has the following columns: Src. Address, Dst. Address, Proto..., Connecti..., and Timeout. The table contains several rows of connection data, including source and destination IP addresses, protocols, connection states, and timeouts.

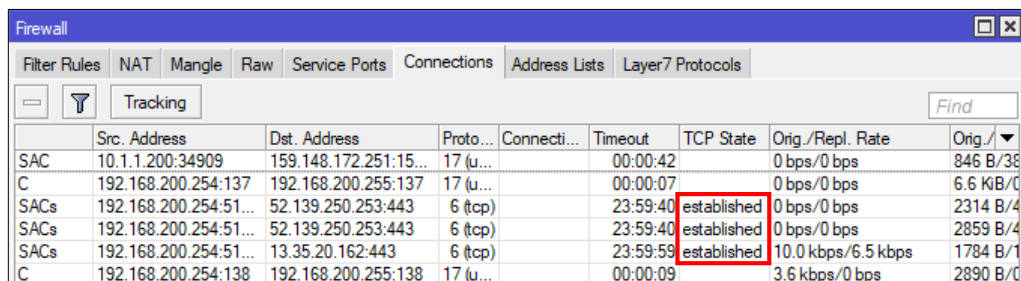
Src. Address	Dst. Address	Proto...	Connecti...	Timeout
SAC 10.1.1.200:34909	159.148.172.251:15...	17 (u...		00:00:05
C 192.168.200.254:137	192.168.200.255:137	17 (u...		00:00:05
SACs 192.168.200.254:51...	52.139.250.253:443	6 (tcp)		23:59:40 established
SACs 192.168.200.254:51...	52.139.250.253:443	6 (tcp)		23:59:40 established
SACs 192.168.200.254:51...	13.35.20.162:443	6 (tcp)		23:59:59 established
C 192.168.200.254:138	192.168.200.255:138	17 (u...		00:00:09
C 192.168.200.254:65...	255.255.255.255:20...	17 (u...		00:00:08
SCs 192.168.200.254:55...	10.1.1.1:53	17 (u...		00:00:08
SACs 192.168.200.254:49...	172.217.194.101:443	17 (u...		00:02:58
SACs 192.168.200.254:52...	74.125.200.147:443	17 (u...		00:02:58
SACs 192.168.200.254:59...	172.217.27.35:443	17 (u...		00:02:58
SCs 192.168.200.254:55...	10.1.1.1:53	17 (u...		00:00:08
SCs 192.168.200.254:62...	10.1.1.1:53	17 (u...		00:00:08
SCs 192.168.200.254:59...	10.1.1.1:53	17 (u...		00:00:08
SCs 192.168.200.254:57...	10.1.1.1:53	17 (u...		00:00:08
SCs 192.168.200.254:59...	10.1.1.1:53	17 (u...		00:00:08
SCs 192.168.200.254:52...	172.217.26.65:443	17 (u...		00:02:58

Connection Tracking in Packet Flow



Connection State

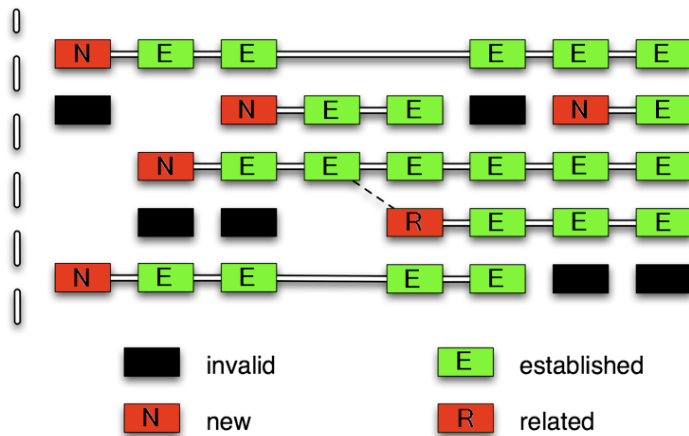
- Each connection has a state
- This state called Connection-state



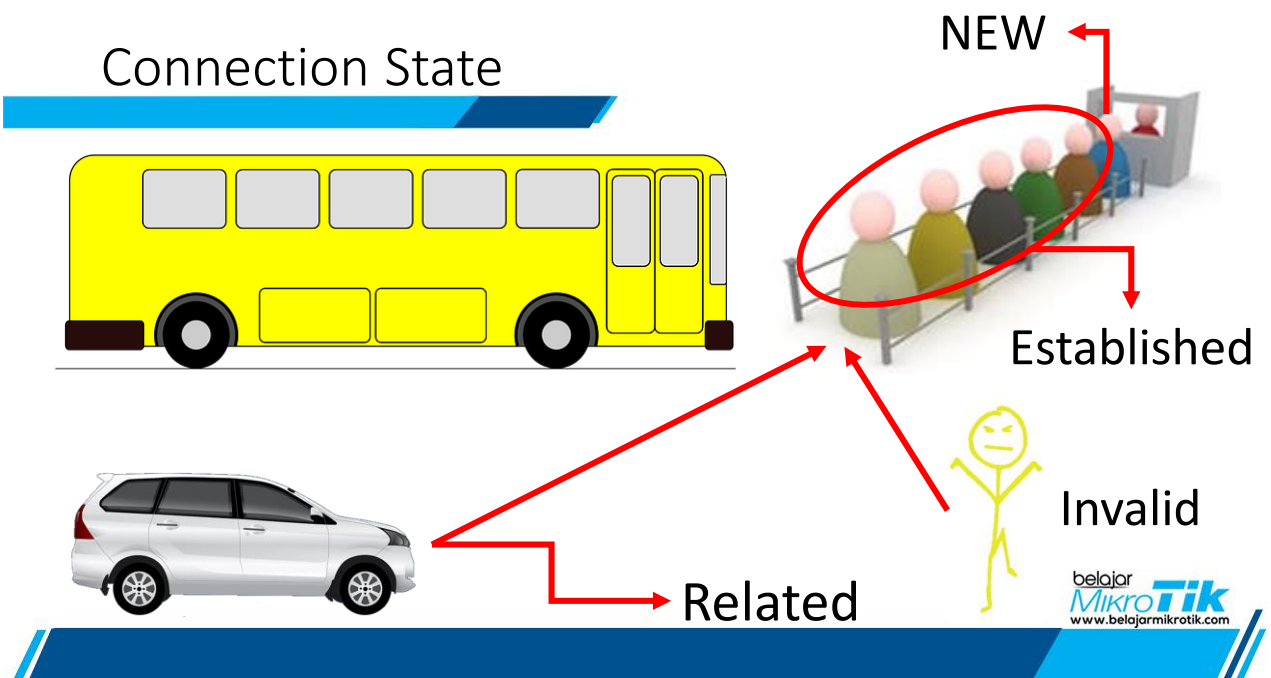
	Src. Address	Dst. Address	Proto...	Connecti...	Timeout	TCP State	Orig./Repl. Rate	Orig./
SAC	10.1.1.200:34909	159.148.172.251:15...	17 (u...		00:00:42		0 bps/0 bps	846 B/38
C	192.168.200.254:137	192.168.200.255:137	17 (u...		00:00:07		0 bps/0 bps	6.6 KiB/0
SACs	192.168.200.254:51...	52.139.250.253:443	6 (tcp)		23:59:40	established	0 bps/0 bps	2314 B/4
SACs	192.168.200.254:51...	52.139.250.253:443	6 (tcp)		23:59:40	established	0 bps/0 bps	2859 B/4
SACs	192.168.200.254:51...	13.35.20.162:443	6 (tcp)		23:59:59	established	10.0 kbps/6.5 kbps	1784 B/1
C	192.168.200.254:138	192.168.200.255:138	17 (u...		00:00:09		3.6 kbps/0 bps	2890 B/0

Connection State

Firewall



Connection State



Tips for connection state

- DROP Invalid Packet
- ACCEPT Established and Related Packet
- Another rule will only check the NEW Packet
- Less Check = Less CPU Load

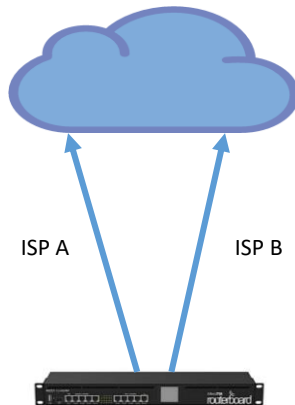
Implementation

Filter Rules										
NAT Mangle Service Ports Connections Address Lists Layer7 Protocols										
+ - ✓ ✗ 📄 🔍 🔄 Reset Counters 🔢 Reset All Counters Find										
#	Action	Chain	S...	D...	Protocol	S...	Dst. Port	In. ...	Out. I...	Connection State
0	✗ drop	input								invalid
1	✓ accept	input								established
2	✓ accept	input								related
3	🔗 jump	input								
4	🔗 jump	input								
5	📄 log	input			6 (tcp)		8291			
6	✓ accept	input			17 (udp)	53				
7	✓ accept	input			17 (udp)		20561,5678			
8	✓ accept	input								

This Rule only checking the NEW
PACKET

Connection Tracking Stuck?

- For some case we need to mark other connection.



Mark Connection

- To know which connection that we have to delete we can mark that connection

The image displays two overlapping Mikrotik WinBox windows for configuring a Mangle Rule.

Left Window: Mangle Rule <10.5.255.0/24->192.168.1.1>

- Chain: prerouting
- Src. Address: 10.5.255.0/24
- Dst. Address: 192.168.1.1
- Protocol: (empty)
- Src. Port: (empty)
- Dst. Port: (empty)
- Any. Port: (empty)
- In. Interface: ether2-ISP-A

Right Window: Mangle Rule <>

- Action: mark connection
- ☐ Log
- Log Prefix: (empty)
- New Connection Mark: via-ISP-A
- ☒ Passthrough

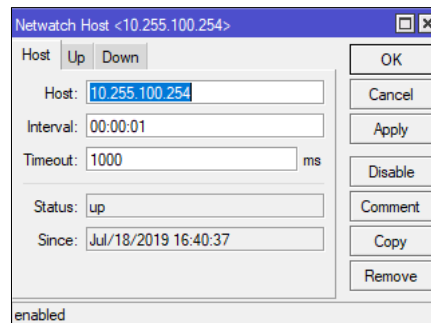
Delete the Conn-Track

Firewall							
Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols							
Tracking							
	Src. Address	/	Dst. Address	Proto...	Connection Mark	Timeout	TCP State
SC	10.255.100.100		10.255.100.254	1 (ic...	via-ISP-A	00:00:09	896 bps/896 bps
SCs	192.168.99.2		10.255.100.254	1 (ic...		00:00:09	960 bps/960 bps
SACs	192.168.99.2:53417		172.217.27.46:443	17 (u...		00:01:53	0 bps/0 bps
SCs	192.168.99.2:53421		10.5.255.140:161	17 (u...		00:00:09	0 bps/0 bps
SACs	192.168.99.2:61701		74.125.68.188:5228	6 (tcp)		23:59:30	established 0 bps/0 bps
SACs	192.168.99.2:61705		40.90.189.152:443	6 (tcp)		23:43:01	established 0 bps/0 bps
SACs	192.168.99.2:61732		103.20.90.197:8290	6 (tcp)		23:59:59	established 1760 bps/17.6 kbps
SACs	192.168.99.2:61734		10.5.255.125:8291	6 (tcp)		23:59:59	established 640 bps/7.8 kbps
SACs	192.168.99.2:61853		104.244.42.8:443	6 (tcp)		23:59:17	established 0 bps/0 bps
SACs	192.168.99.2:61856		103.20.90.211:443	6 (tcp)		23:59:17	established 0 bps/0 bps
C	192.168.99.2:63641		255.255.255.255:20...	17 (u...		00:00:10	8.4 kbps/0 bps

This Connection that we should Delete!!

Ensure Gateway is reachable

- To ensure that gateway always reachable we can use Tools → Netwatch



PROBLEM SOLVED?

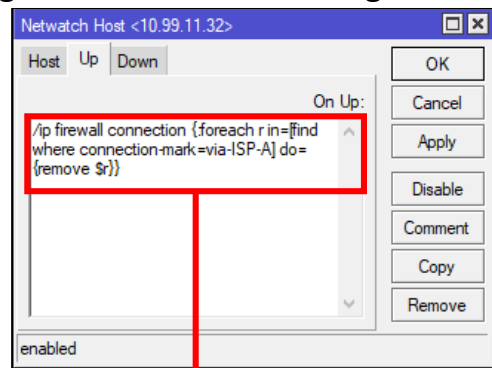
NO

How if the problems always come?

Solution

- We can use Script in Netwatch deleting the connection tracking automatically

```
/ip firewall connection  
{:foreach r in=[find where  
connection-mark=via-ISP-A]  
do={remove $r}}
```





Thanks!

Any questions?

You can find me at :

 Yoga Wahyu Mahendra
 @yogawhyme
 yoga@belajarmikrotik.com

belajar
MikroTik
www.belajarmikrotik.com