

# FIREWALL

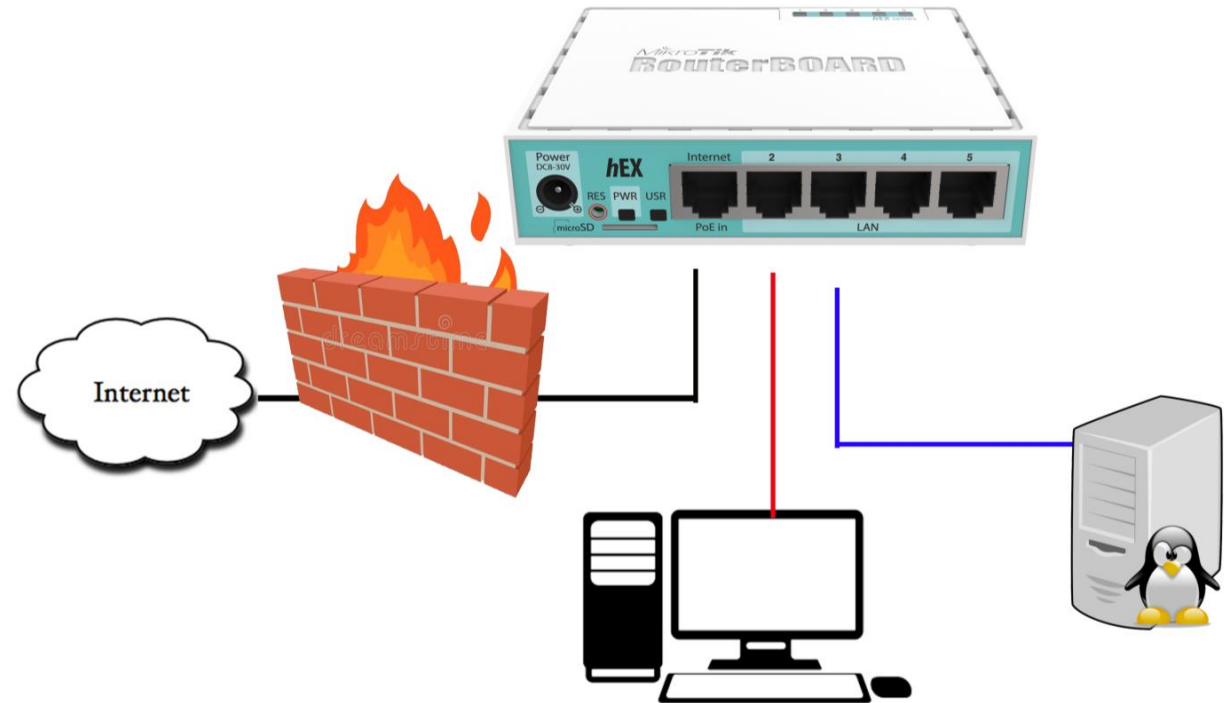
## ADMINISTRASI INFRASTRUKTUR JARINGAN

### TUJUAN:

1. Mampu memahami fungsi firewall dalam jaringan
2. Mampu melakukan konfigurasi firewall jaringan
3. Mampu melakukan troubleshooting firewall dalam jaringan

# KONSEP Firewall

- Layanan yang melakukan pengecekan atau modifikasi paket data yang menuju atau melewati router
- Tujuannya adalah untuk pngamanan jaringan
- Contoh: firewall diantara jaringan internet dengan LAN

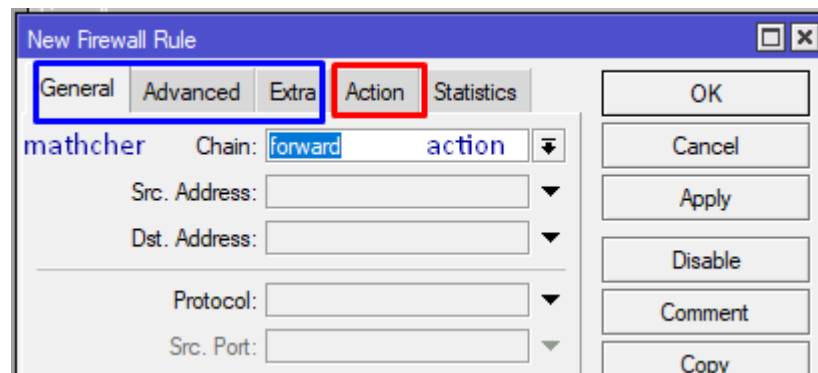


# BAGAIMANA FIREWALL BEKERJA

- Berdasarkan rule set yang dibuat oleh user dan dieksekusi secara berurutan sampai ada trafik yang cocok
- Rule set ini dipasangkan di “chain” dan tergantung pada flow trafiknya
- Chain ini dibagi 2 yaitu defulat dan custom atau bisa membuat sendiri

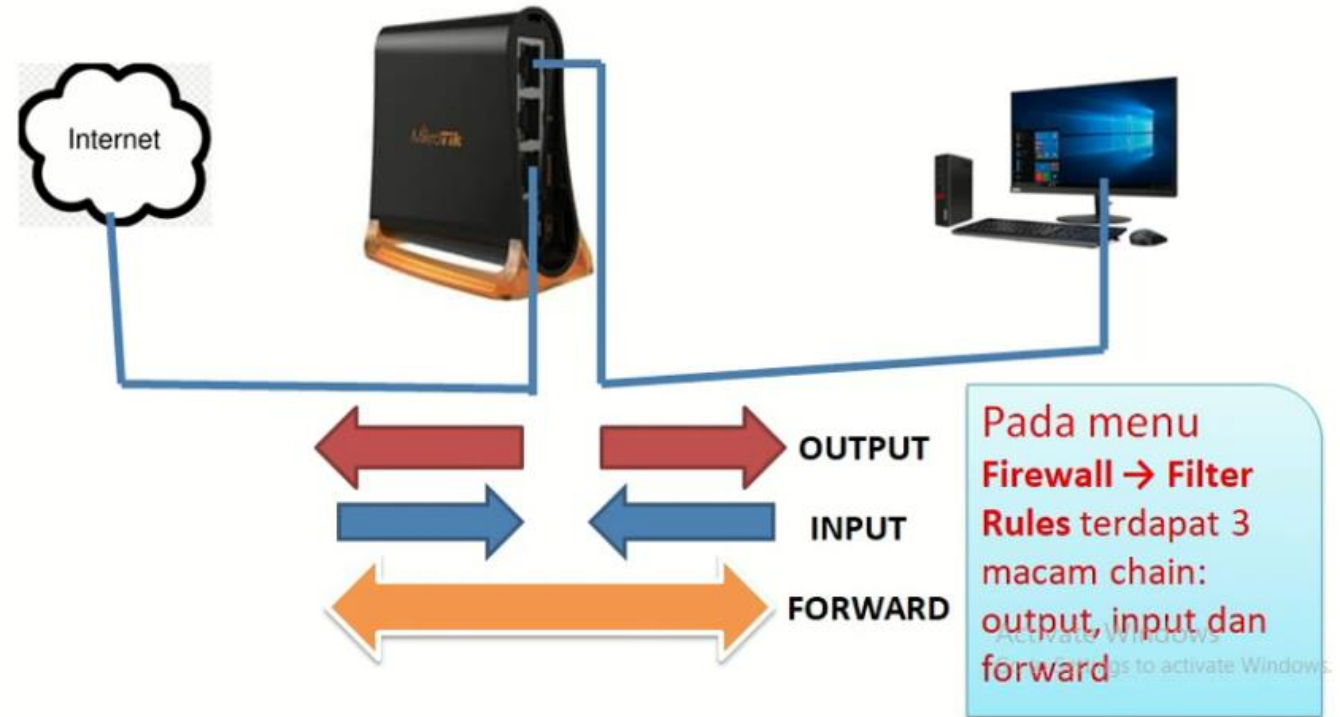
Setiap rule terdiri dari 2 bagian

1. Matcher : digunakan untuk menspesifikasikan pakaet yang akan diatur
2. Action: aksi/perlakuan jika paket data sesuai dengan mather



# Firewall Filter Chain

- Digunakan untuk melakukan kebijakan boleh atau tidaknya sebuah trafik ada dalam jaringan, identic dengan accept atau drop



# Output – input – forward

- Output : digunakan untuk memproses trafik paket data yang keluar dari router. Trafik yang berasal dari dengan tujuan jaringan public atau jaringan local.  
contoh: new terminal winbox, ping google
- Input : digunakan untuk memproses trafik paket data yang masuk ke dalam router melalui interface yang ada di router dan memiliki tujuan IP Address berupa ip yang terdapat pada router. Jenis trafik ini bisa berasal dari jaringan public atau jaringan local dengan tujuan router itu sendiri.  
contoh: akses router menggunakan winbox, webfix, telnet, ssh
- Forward : digunakan untuk memproses trafik paket data yang hanya melewati router. Misalnya trafik dari jaringan public ke local atau sebaliknya.  
contoh: saat melakukan browsing

# FILTER ACTION

1. ACCEPT : paket diterima dan tidak melanjutkan membaca baris berikutnya
2. DROP : menolak paket secara diam-diam (tidak mengirimkan pesan penolakan ICMP)
3. REJECT: menolak paket dan mengirimkan pesan penolakan ICMP
4. TARPIT : menolak, tetapi tetap menjaga TCP Connection yang masuk
5. LOG : menambahkan informasi paket data ke log



# Latihan 1 Konfigurasi Dasar

1. Konfigurasi IP Seperti pada topologi di atas
2. Pastikan router sudah terkoneksi dengan internet
3. Pastikan computer client (LAN) terkoneksi dengan internet

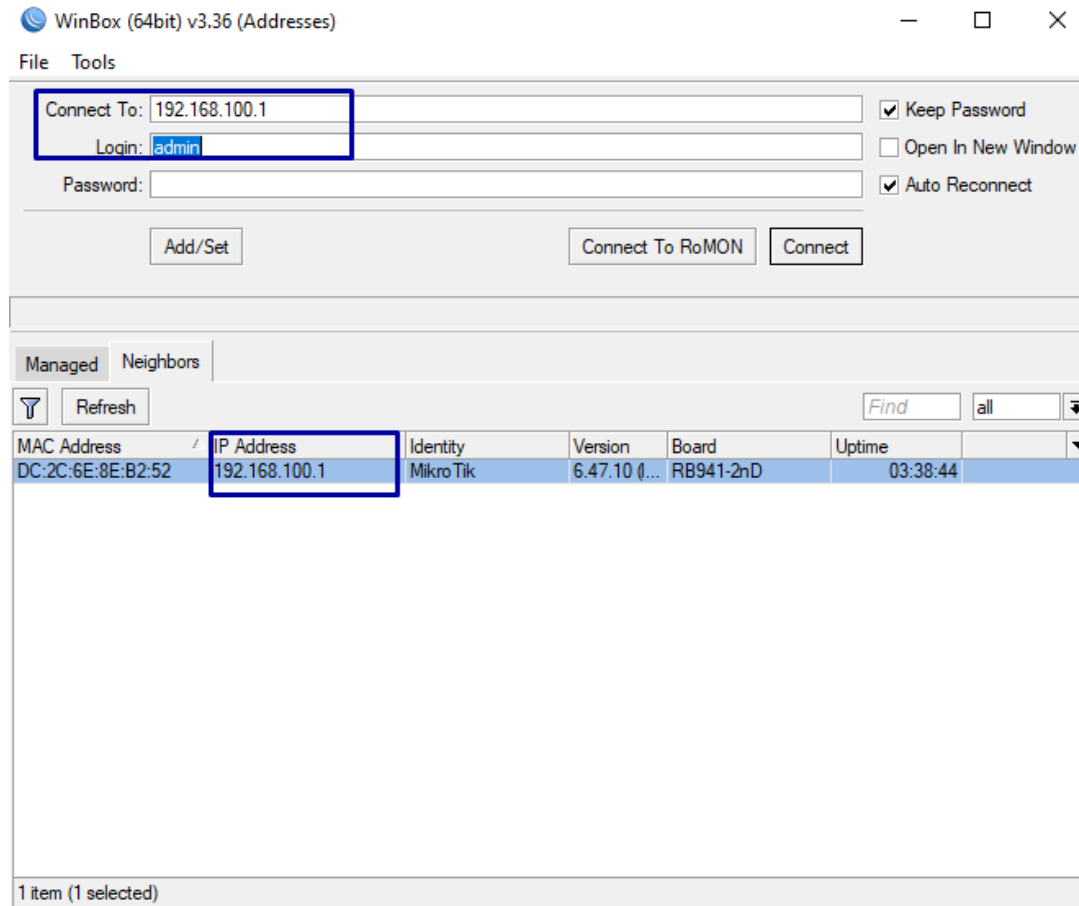
# Latihan 2 Chain Input Blokir akses router (winbox, wbfix, ssh, telnet)

1. Rule 1 :Dari ether 2 (LAN) HANYA IP 192.168.100.2 yang bisa akses router, lainnya diblokir
2. Login ke winbox menggunakan IP bukan menggunakan MAC Address
3. Rule matcher setting
  - Chain = input
  - Sc. Address = ip yang hanya boleh mengakses
  - Protokol = tcp
  - Dst port = port untuk ssh, telnet, winbox, webfig
  - Action = drop

Untuk melihat daftar port bisa dilihat melalui

IP → SERVICES

# 1. Login menggunakan IP



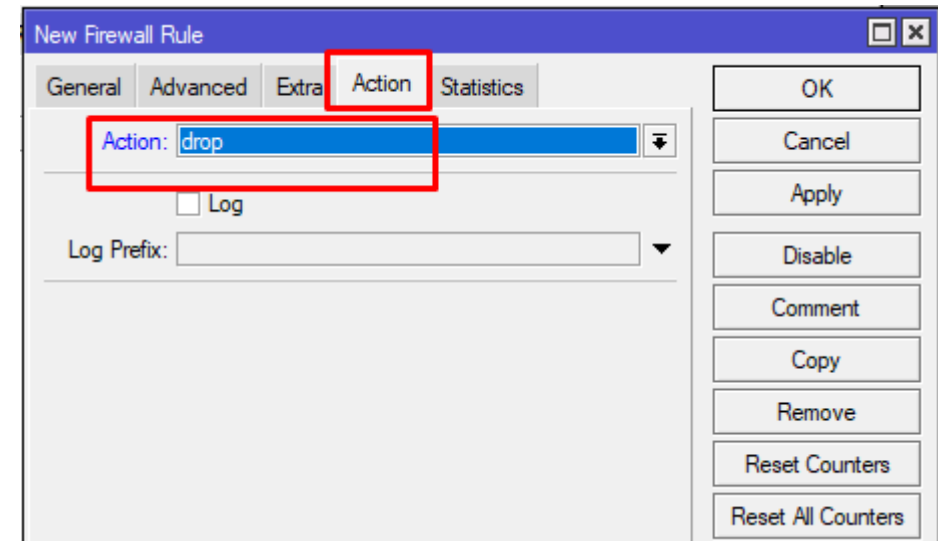
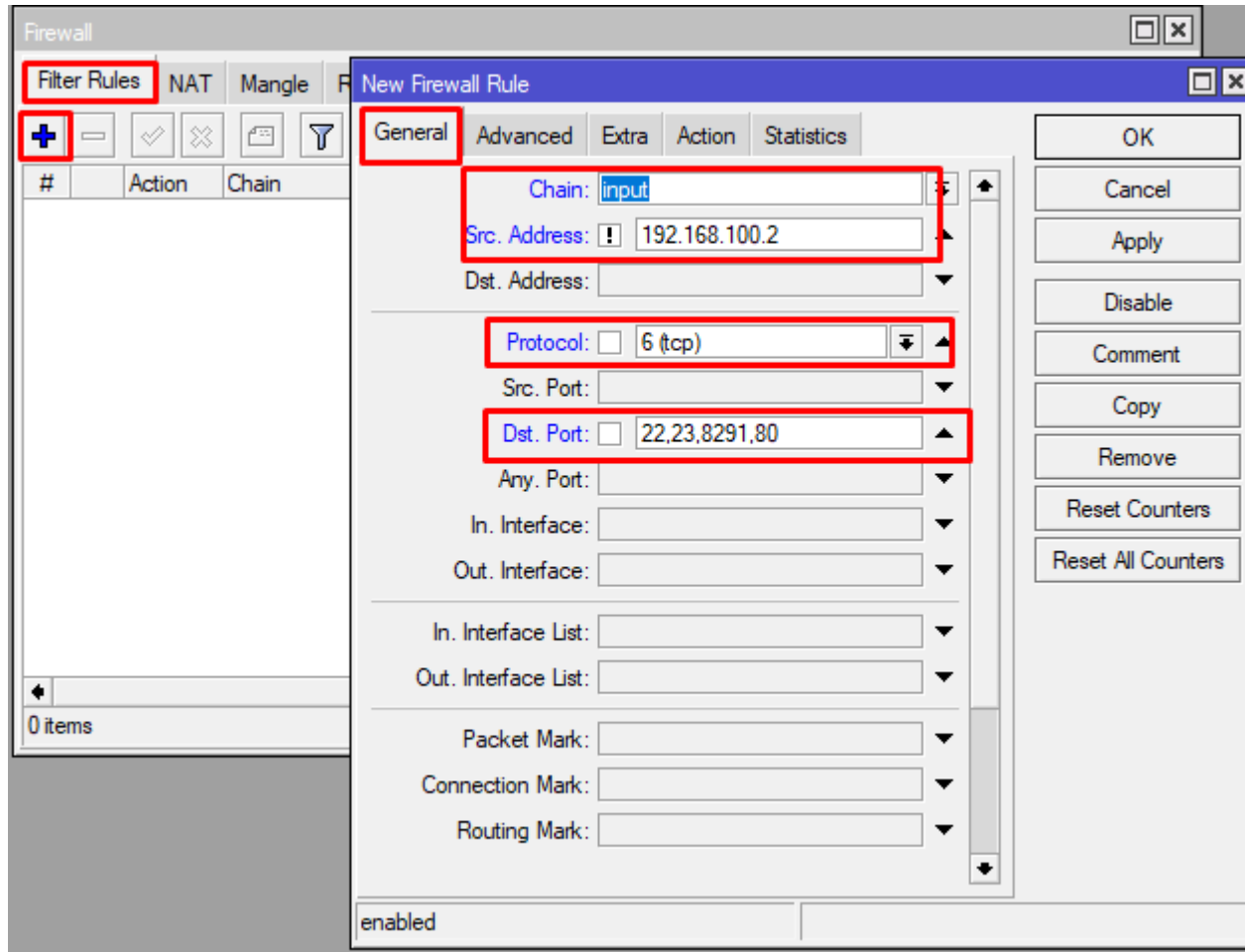
The screenshot shows the WinBox (64bit) v3.36 (Addresses) window. The 'Connect To' field is set to 192.168.100.1, and the 'Login' field is set to admin. The 'Keep Password' and 'Auto Reconnect' checkboxes are checked. Below the login fields are buttons for 'Add/Set', 'Connect To RoMON', and 'Connect'.

The 'Managed' tab is active, showing a table of managed devices. The table has columns for MAC Address, IP Address, Identity, Version, Board, and Uptime. One device is listed with MAC Address DC:2C:6E:8E:B2:52, IP Address 192.168.100.1, Identity MikroTik, Version 6.47.10 (...), Board RB941-2nD, and Uptime 03:38:44.

MAC Address	IP Address	Identity	Version	Board	Uptime
DC:2C:6E:8E:B2:52	192.168.100.1	MikroTik	6.47.10 (...)	RB941-2nD	03:38:44

1 item (1 selected)

## 2. FIREWALL RULE



# CEK HASIL KONFIGURASI

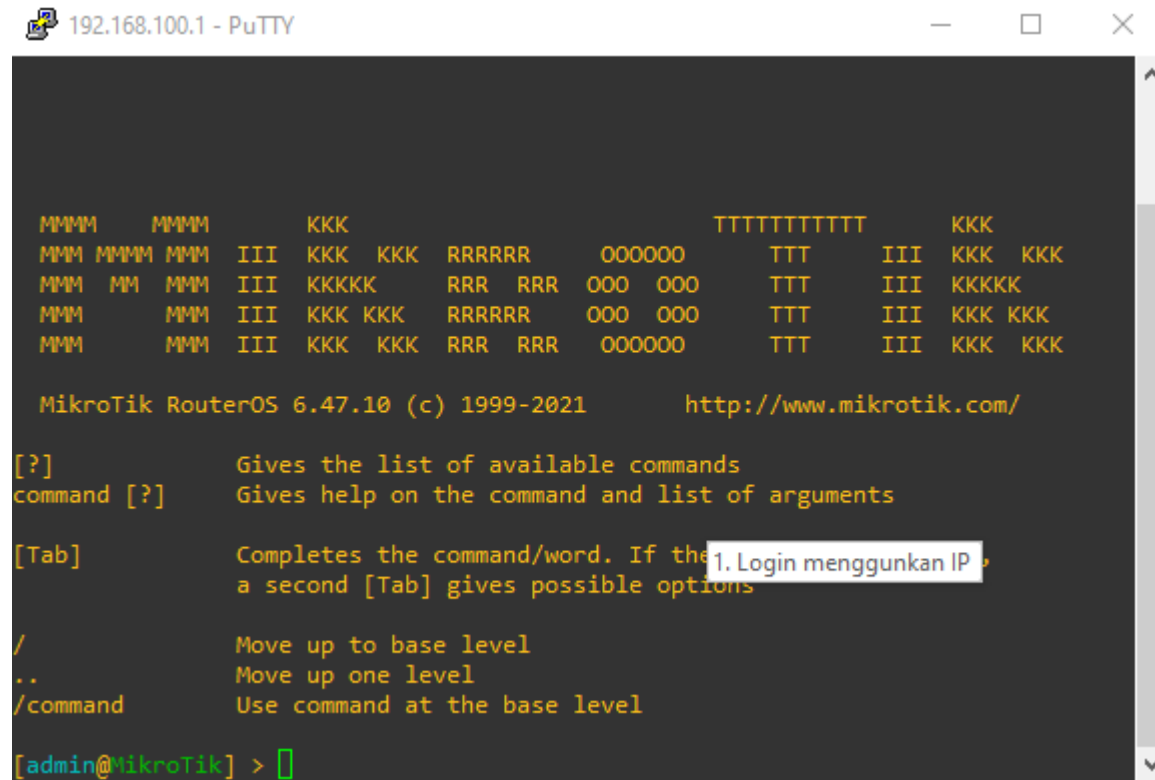
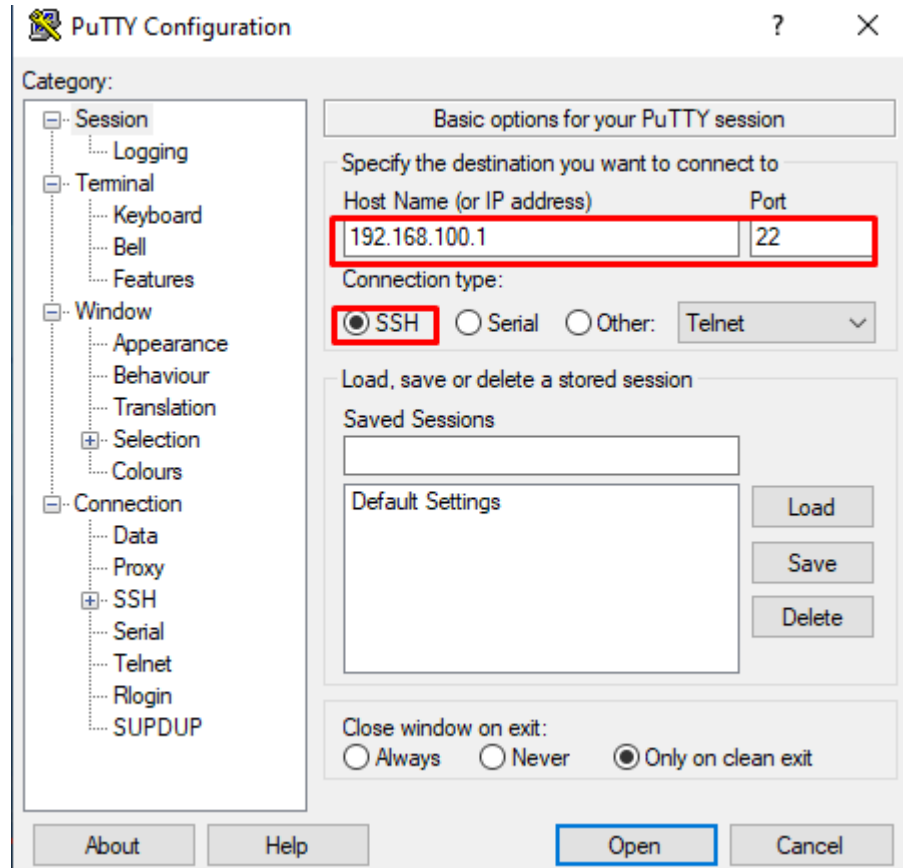
1. Gunakan IP 192.168.100.2 untuk client
  - Akses router menggunakan webfig → masuk ke browser
  - Akses router menggunakan SSH
  - Akses router menggunakan telnet
2. Gunakan IP 192.168.100.3 -254 untuk client
  - lakukan akses router menggunakan webfig, ssh, telnet

# Menggunakan webfig

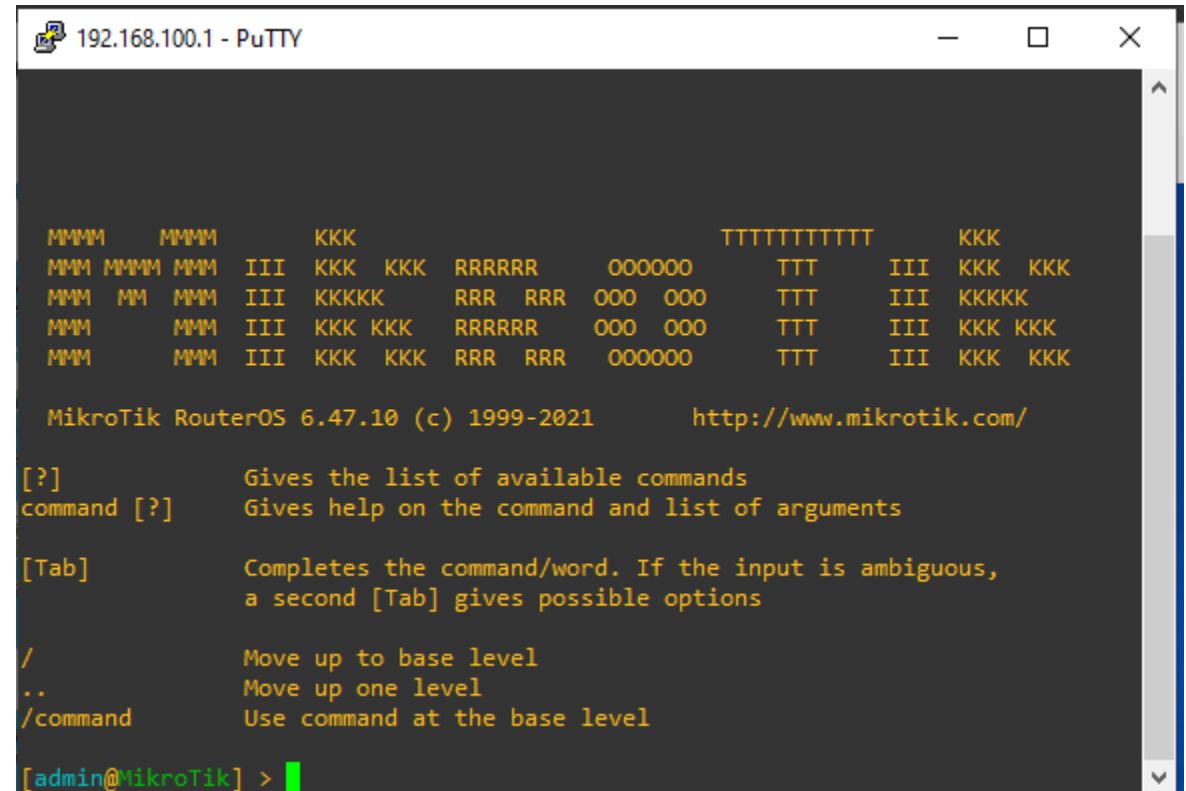
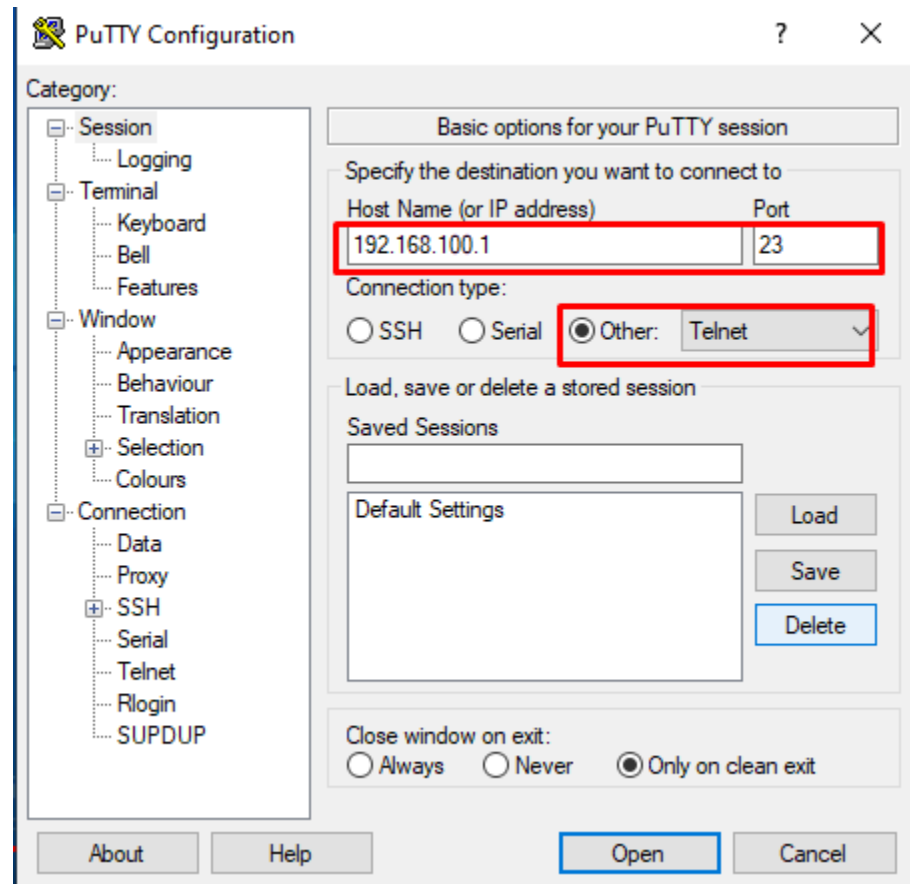
The screenshot displays the MikroTik RouterOS v6.47.10 webfig interface. The browser address bar shows the URL `192.168.100.1/webfig/#Interfaces`. The interface list is shown under the 'Interface List' tab, with a sub-tab for 'LTE'. The list contains 6 items:

		Name	Type	Actual MTU	L2 MTU	Tx	Rx
<input type="checkbox"/>	R	ether1 internet	Ethernet	1500	1598	0 bps	0 bps
<input type="checkbox"/>	R	ether2 local	Ethernet	1500	1598	119.7 kbps	44.6 kbps
<input type="checkbox"/>		ether3 server	Ethernet	1500	1598	0 bps	0 bps
<input type="checkbox"/>		ether4	Ethernet	1500	1598	0 bps	0 bps
<input type="checkbox"/>		pwr-line1	PWR	1500	1598	0 bps	0 bps
<input type="checkbox"/>	R	wlan1	Wireless (Atheros AR9130)	1500	1600	0 bps	0 bps

# Menggunakan SSH

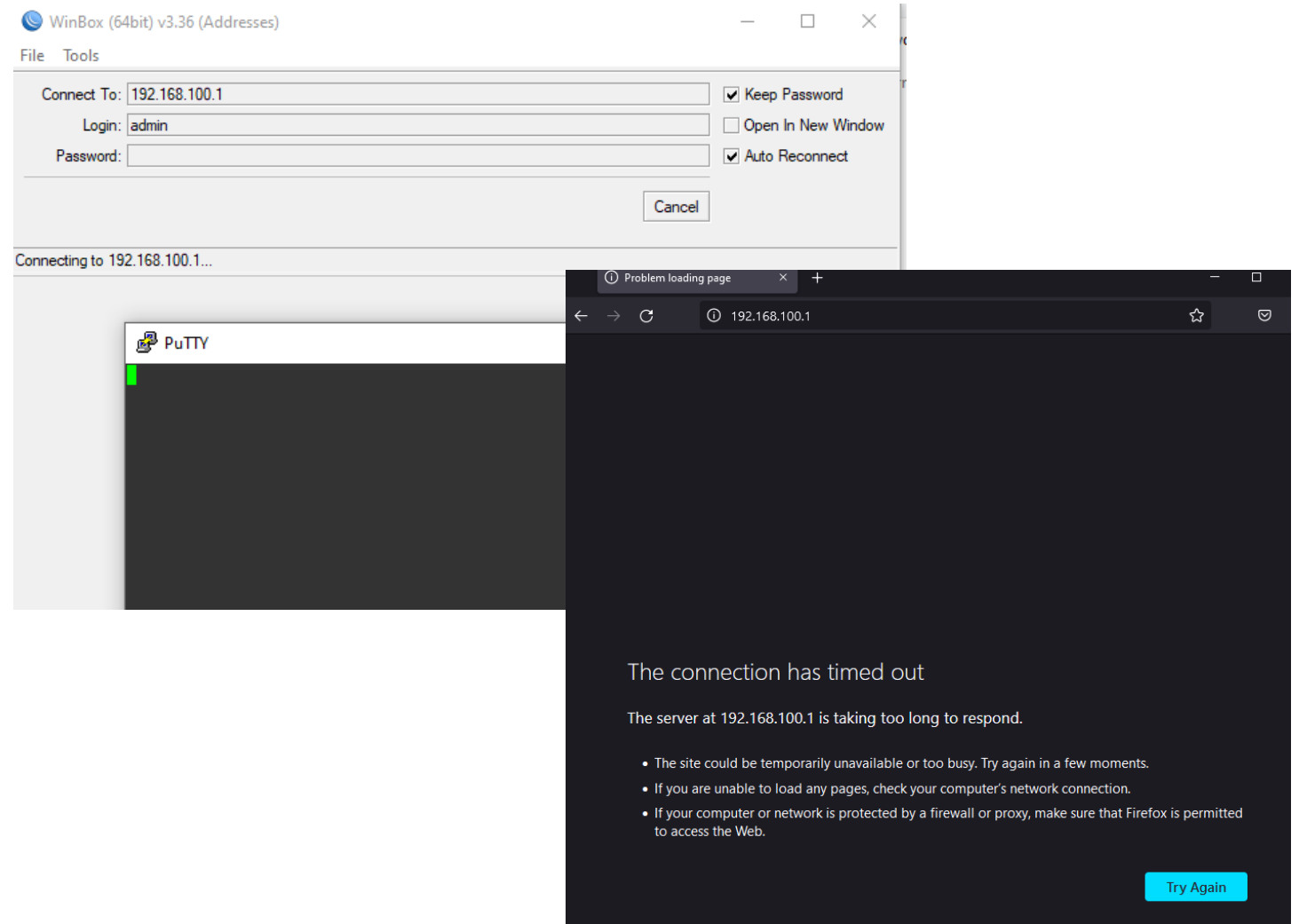
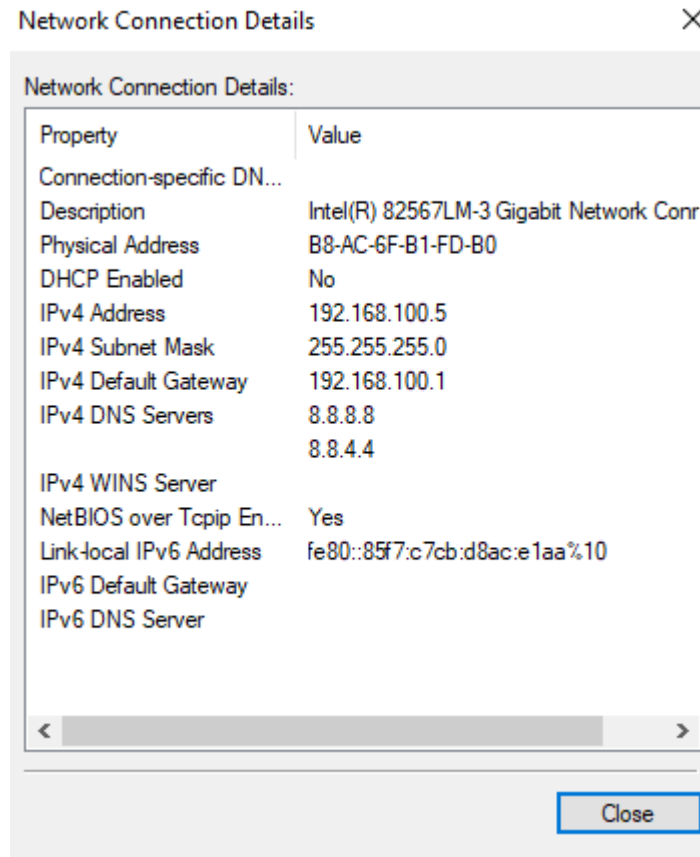


# MENGGUNAKAN TELNET

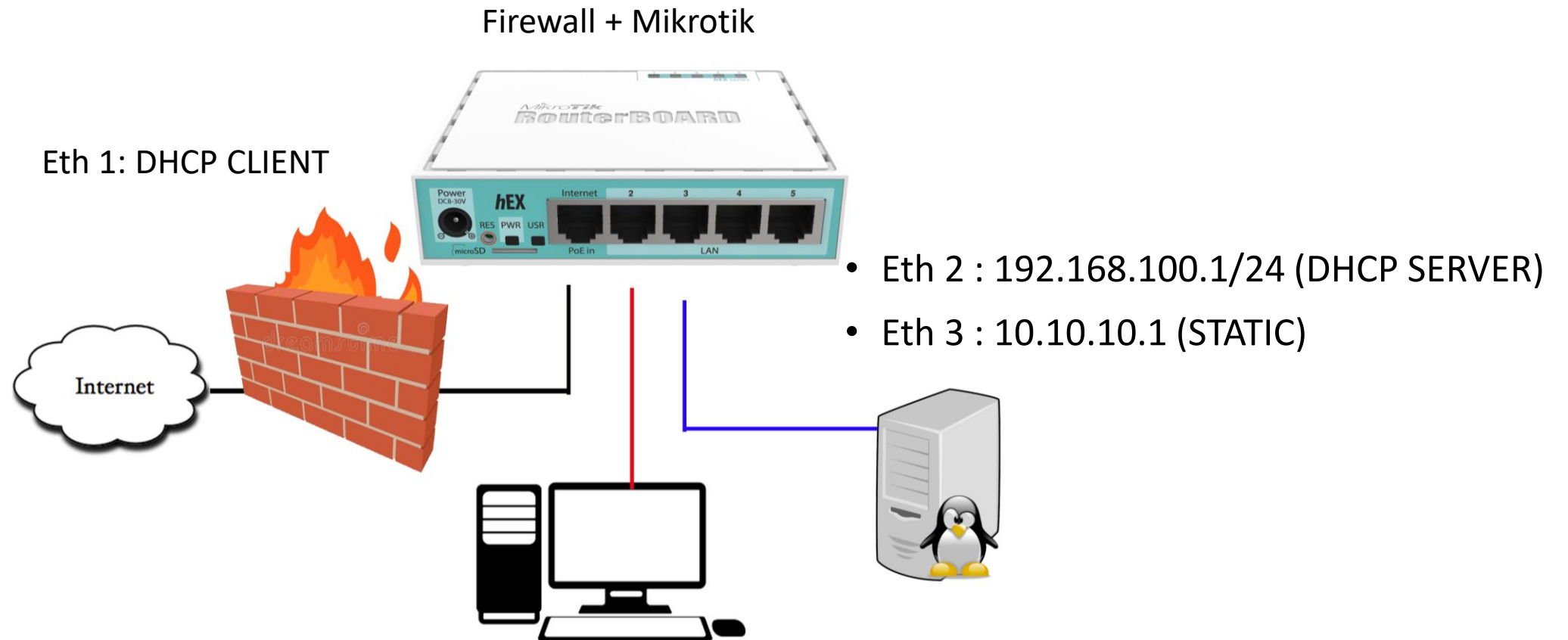


# Client dengan IP selain 192.168.100.2

hasilnya adalah, client tidak bisa terhubung dengan mikrotik/terblokir



# LATIHAN CHAIN FORWARD



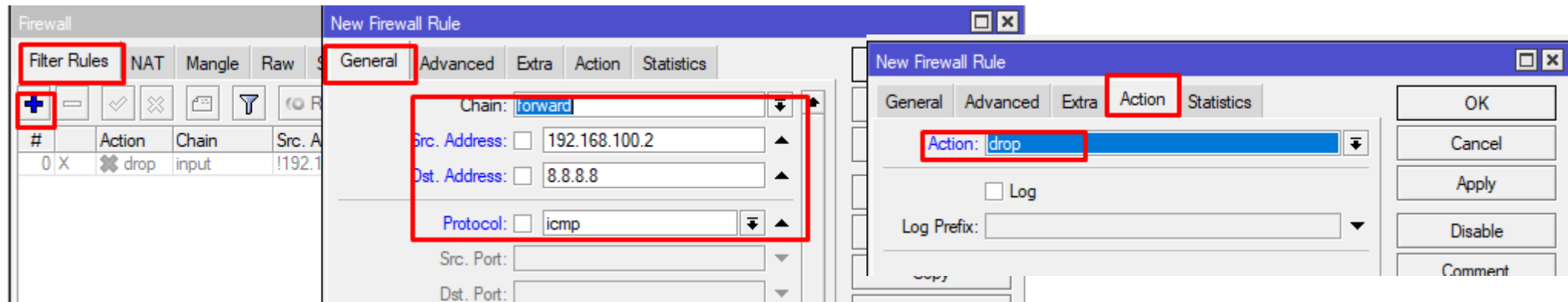
**FORWARD** digunakan untuk memproses trafik paket data yang hanya melewati router

**Address list**, adalah salah satu fitur **mikrotik** yang fungsinya untuk memudahkan kita dalam menandai suatu konfigurasi **address**. Sehingga dengan **address list**, kita bisa membuat **list address** yang ingin ditandai tanpa harus mengganggu konfigurasi penting di fitur lainnya

**Layer 7** – Protokol adalah metode pencarian pola terhadap paket data yang melewati jalur ICMP, TCP, dan UDP

# Konfigurasi

1. Pastikan router dan client jaringan local sudah terhubung ke internet
2. Rule firewall
  - Chain = forward
  - Src.address = 192.168.100.2
  - Dst. Address = 8.8.8.8
  - Action = drop



# CEK HASIL KONFIGURASI PADA CLIENT dengan IP 192.168.100.2

```
C:\Users\Rifa>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

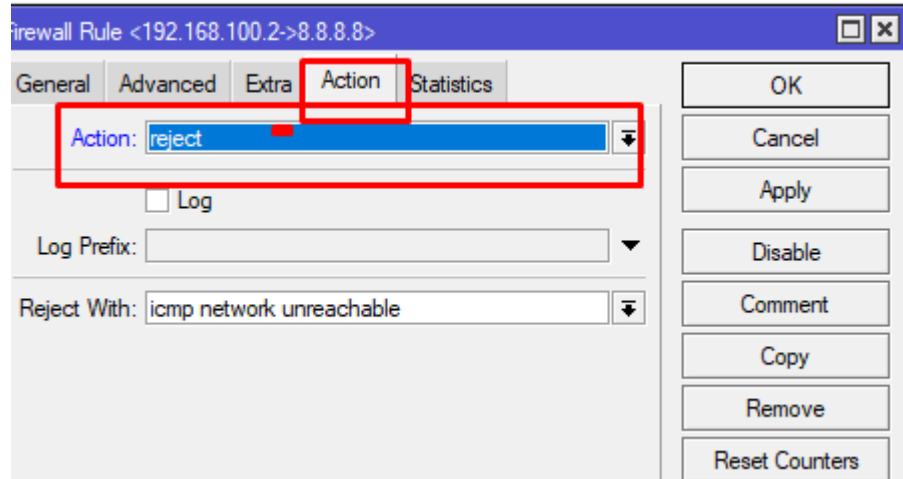
Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Rifa>ping google.com

Pinging google.com [74.125.130.100] with 32 bytes of data:
Reply from 74.125.130.100: bytes=32 time=31ms TTL=55
Reply from 74.125.130.100: bytes=32 time=56ms TTL=55
Request timed out.
Reply from 74.125.130.100: bytes=32 time=134ms TTL=55

Ping statistics for 74.125.130.100:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 31ms, Maximum = 134ms, Average = 73ms
```

# Selanjutnya ganti action menjadi reject dan lakukan ping kembali

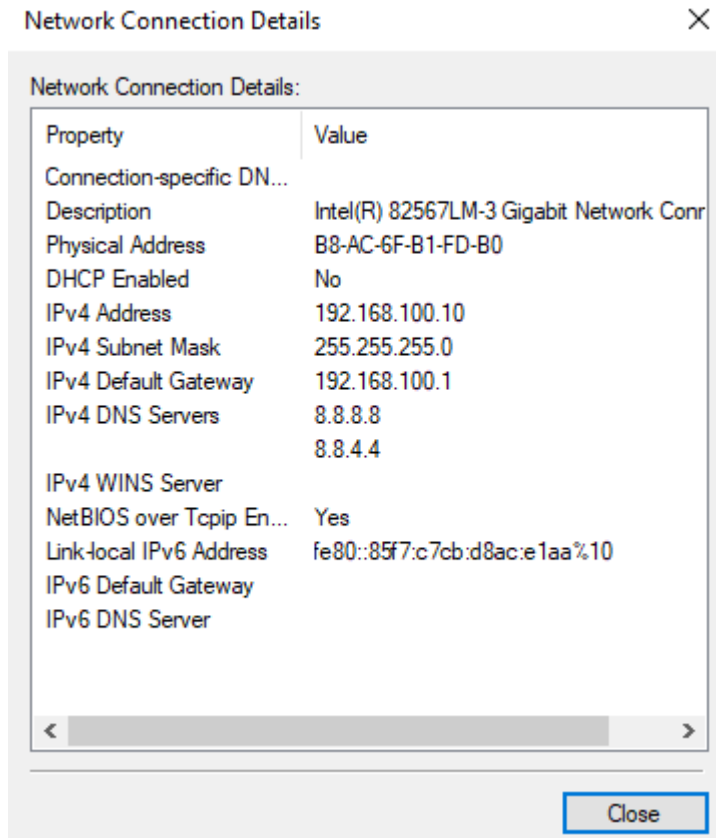


```
C:\Users\Rifa>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 192.168.100.1: Destination net unreachable.
Reply from 192.168.100.1: Destination net unreachable.
Reply from 192.168.100.1: Destination net unreachable.
Reply from 192.168.100.1: Destination net unreachable.

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

# Ganti ip client menjadi selain dari 192.168.100.2 kemudian lakukan ping kembali



```
C:\Users\Rifa>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=55ms TTL=113
Reply from 8.8.8.8: bytes=32 time=54ms TTL=113
Reply from 8.8.8.8: bytes=32 time=29ms TTL=113
Reply from 8.8.8.8: bytes=32 time=30ms TTL=113

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 29ms, Maximum = 55ms, Average = 42ms
```

# TUGAS

- Bagaimana cara memblokir semua client tidak bisa terhubung/masuk ke dalam winbox baik menggunakan webfig, ssh, dan telnet
- Bagaimana cara memblokir semua client agar tidak bisa mengirim paket icmp (ping 8.8.8.8)