

# Praktikum Firewall Sederhana

## Alat dan Bahan:

- Mikrotik
- Laptop
- Kabel UTP (2 untuk 1 kelompok)

## Target

1. Mikrotik dapat terkoneksi ke mikrotik partner
2. Mikrotik dapat melakukan ping ke Laptop Partner
3. Antar laptop dapat saling melakukan ping melalui koneksi 2 mikrotik
4. Peserta dapat mem-blok koneksi ssh & telnet dari partner
5. Peserta dapat memblok ping dari partner

## Prequisitive

Peserta harus menyelesaikan **”Jobsheet 4 Wireless station-bridge .odt”** terlebih dahulu

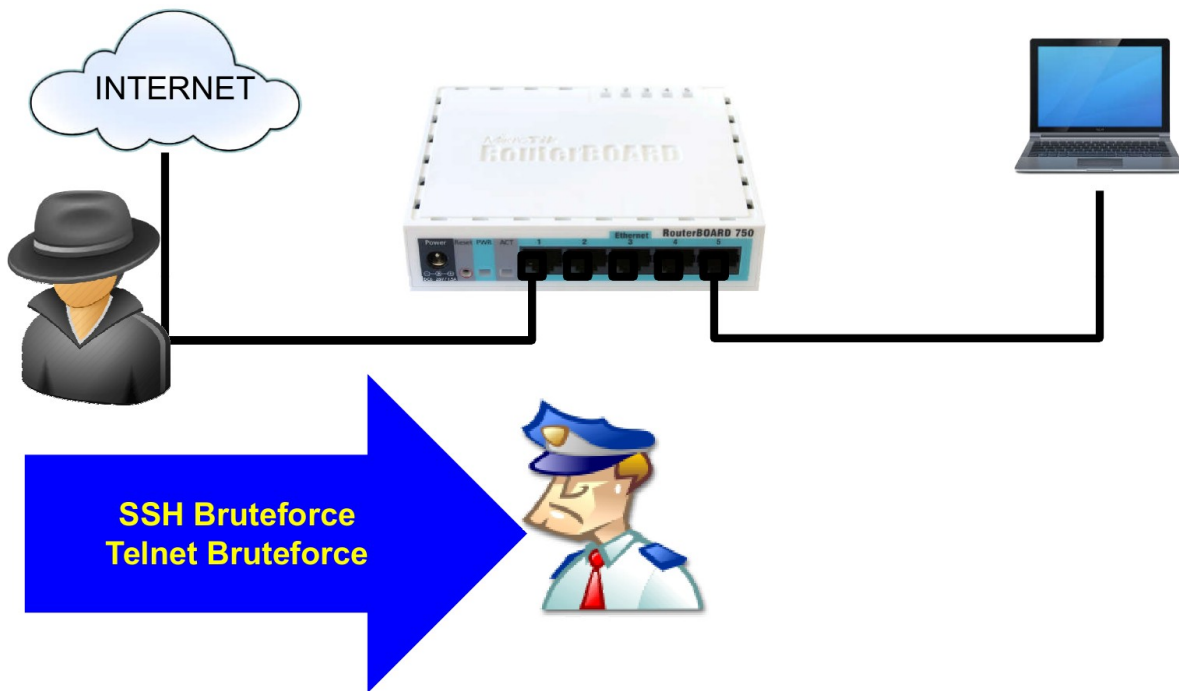
## Kelompok

Buatlah kelompok masing-masing 2 siswa kemudian tentukan salah satu dari kalian ada yang menjadi server dan ada yang jadi client!

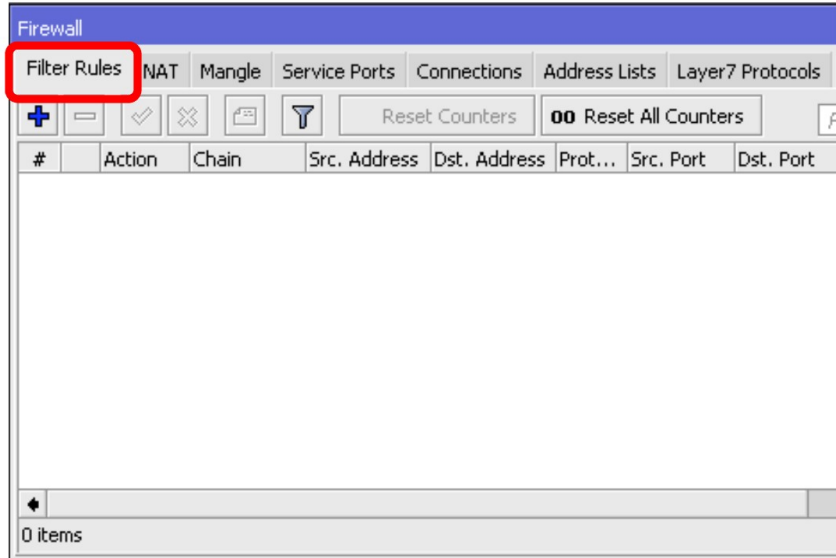
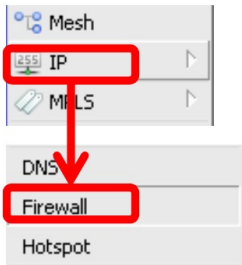
## Langkah:



# [LAB-1]Securing Router



# [LAB-1] Firewall Filter



# [LAB-1] Filter Input

The image shows the Mikrotik WinBox interface for configuring a new firewall rule. The main window is titled "New Firewall Rule" and has tabs for "General", "Advanced", "Extra", "Action", and "Statistics". The "General" tab is active, showing the following configuration:

- Chain:** input
- Src. Address:** (empty)
- Dst. Address:** (empty)
- Protocol:** 6 (tcp)
- Src. Port:** (empty)
- Dst. Port:** 22,23
- Any. Port:** (empty)
- P2P:** (empty)
- In. Interface:** wlan1
- Out. Interface:** (empty)

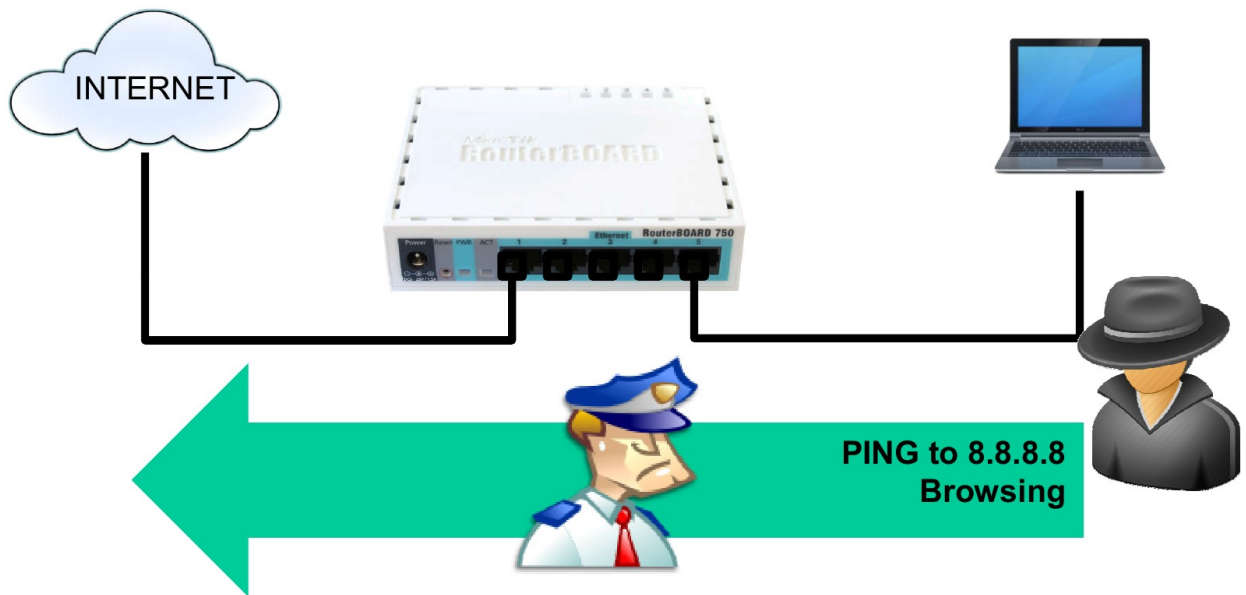
A secondary window, also titled "New Firewall Rule", is shown in the foreground, displaying the "Action" tab. The configuration in this window is:

- Action:** drop
- Log:** (unchecked)
- Log Prefix:** (empty)

Red boxes and arrows highlight the configuration steps: a red box around the "+" button in the "Filter Rules" list points to the "Chain" field; red boxes around "6 (tcp)", "22,23", and "wlan1" in the "General" tab have arrows pointing to the "Action" tab window; a red box around the "Action" tab in the secondary window has an arrow pointing to the "Log Prefix" field.



## [LAB-2]Securing User



# [LAB-2] Filter Forward

The screenshot displays the Mikrotik WinBox Firewall configuration interface. The main window is titled "Firewall Rule <8.8.8.8>" and has tabs for "General", "Advanced", "Extra", "Action", and "Statistics". The "General" tab is selected, showing the following configuration:

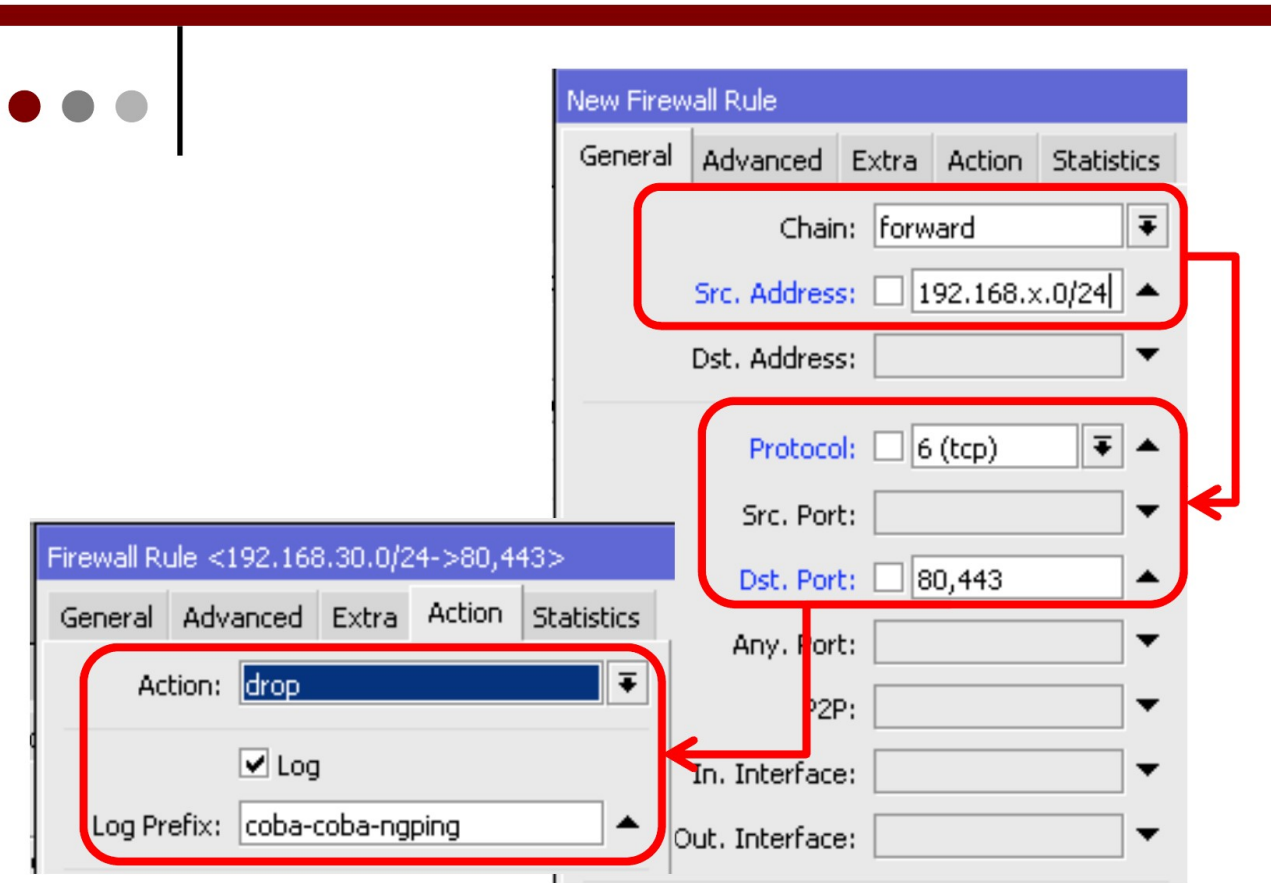
- Chain: forward
- Src. Address: [empty]
- Dst. Address: 192.168.y.0/24
- Protocol: 1 (icmp)
- Src. Port: [empty]
- Dst. Port: [empty]
- Any. Port: [empty]
- P2P: [empty]
- In. Interface: ether1
- Out. Interface: [empty]

A secondary window titled "Firewall Rule <>" is open over the "Action" tab, showing the following configuration:

- Action: reject
- Log: [unchecked]
- Log Prefix: [empty]
- Reject With: icmp admin prohibited

Red boxes and arrows highlight the configuration elements: the "+" button in the Filter Rules list, the "Chain" dropdown, the "Dst. Address" field, the "Protocol" dropdown, the "In. Interface" dropdown, and the "Action" tab and "Action" dropdown in the secondary window.

\* Y adalah nomor teman kalian



### Pengecekan

1. Silahkan minta teman semeja untuk mencoba telnet / ssh ke router kita
2. Test ping ke 192.168.y.1 dan 192.168.y.2 dari laptop
3. Test ping ke 192.168.y.1 dan 192.168.y.2 dari terminal winbox