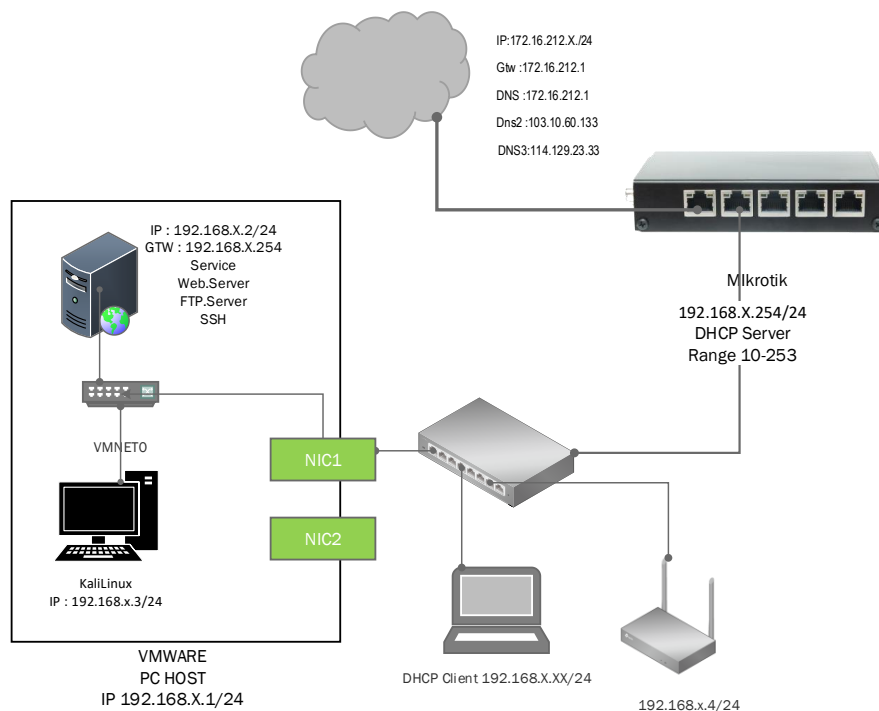


Proteksi Infrastruktur

Setelah dilakukan testing keamanan berdasarkan pengujian “macam-macam serangan jaringan komputer”, maka proteksi yang akan diterapkan meliputi , (1). upgrading topologi jaringan guna memisahkan jaringan berdasarkan kebutuhan pengguna yaitu : internet, server, client, wireless. (2). Proteksi menggunakan Firewall, untuk mencegah icmp , (3) DMZ Forwarding , meneruskan paket layanan dari router ke server.

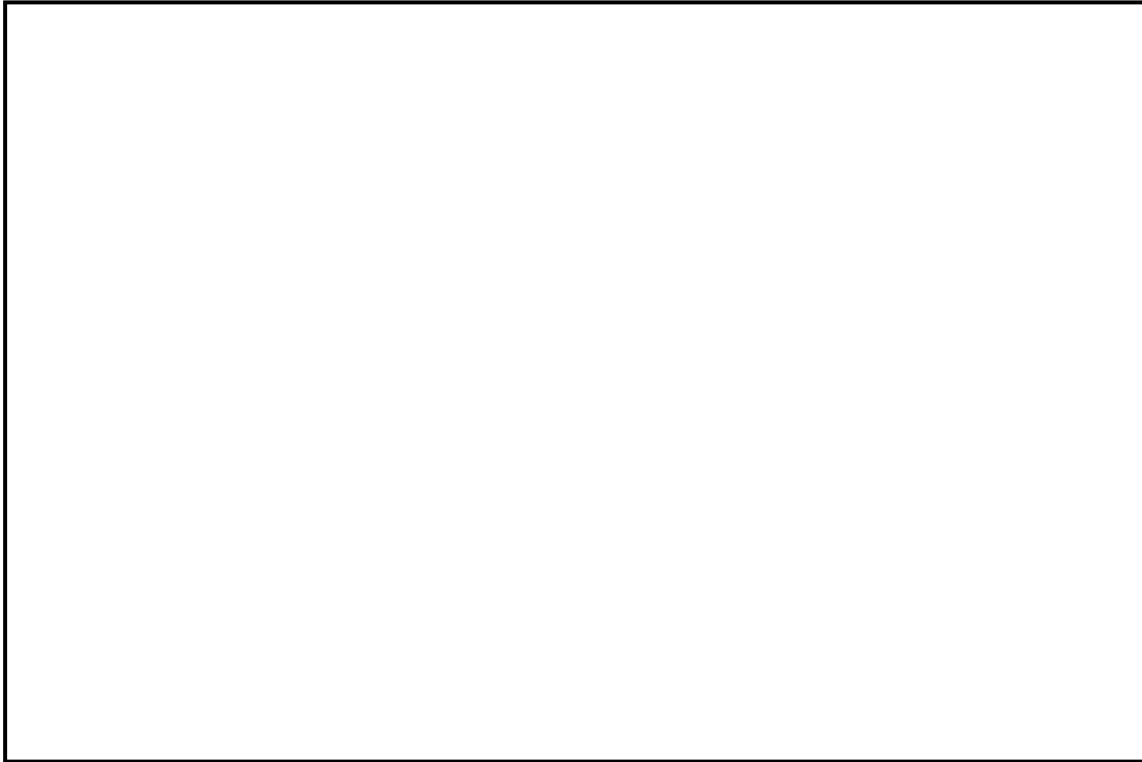
1. Upgrade topologi jaringan

Pada Topologi awal, jaringan sederhana yang dibangun hanya memiliki dua network saja meliputi jaringan internet dan jaringan lokal. Seperti skema topologi berikut berikut :



Desain , gambarkan rencana topologi jaringan yang lebih baik dan dapat memenuhi kebutuhan pengguna, meliputi adanya jaringan : (1). Internet, (2) server, (3) client,(4) Wireless dan (5) VPN. Desain dan gambarkan topologi tersebut pada tempat / area yang dibawah ini , rencanakan juga dan tuliskan pengalamatan ip address gateway untuk kebutuhan tiap jaringan. Untuk jaringan VPN tidak perlu diberikan alamat gateway

Desain jaringan beserta pengalamatan jaringan (vpn tidak perlu diber alamat gateway) :

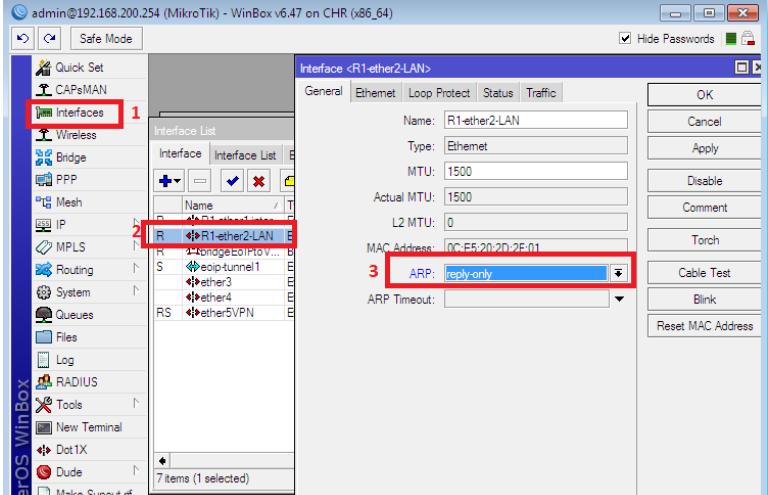
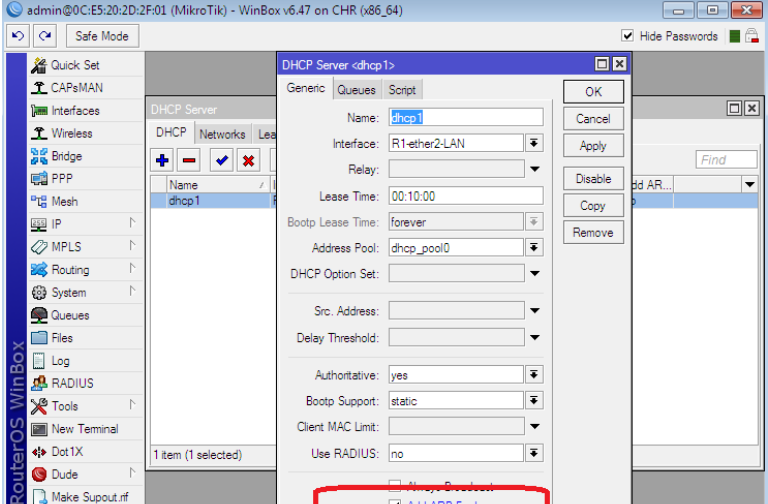


Implementasikan jaringan yang anda rancang pada router mikrotik, berikut perkabelan. Implementasi meliputi (1) Pemasangan Kabel (2) setting router : NAT, Routing, DNS , gateway (3), Setting IP Server, (4) setting Access Point (tambahkan keamanan wireless meliputi : hotspot, Wireless Scurity.

ARP Static

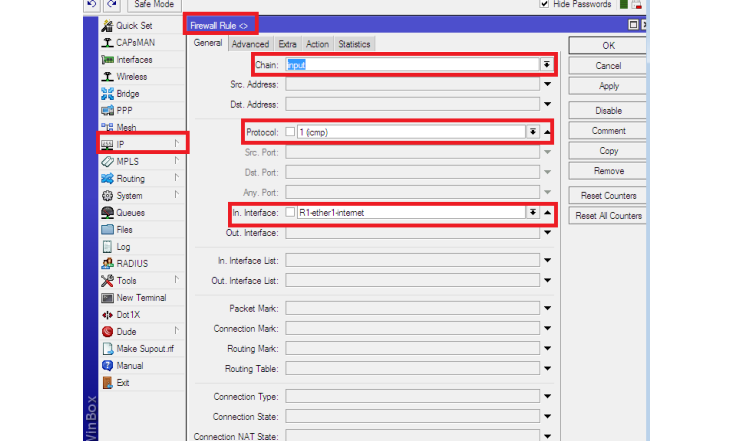
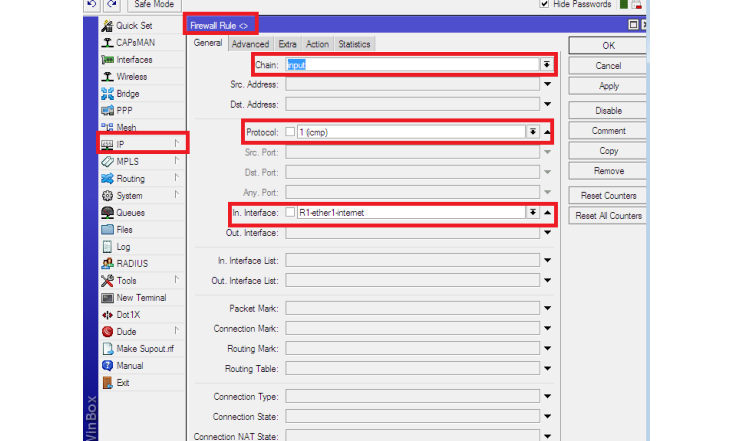
Berdasarkan hasil pengujian MIMA dan ARP poisoning maka , untuk peningkatan keamanan jaringan perlu melakukan perubahan ARP yang tadinya dyanmic menjadi ARP static. Dapat dilakukan dengan langkah berikut :

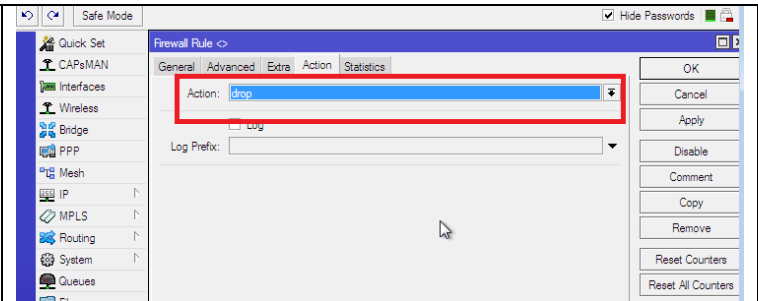
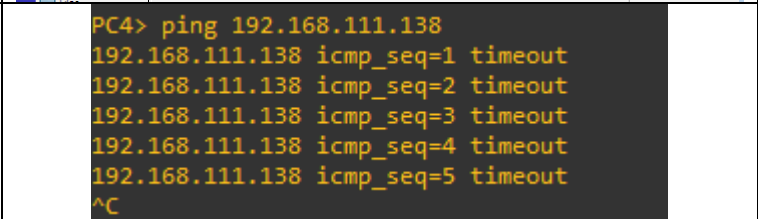
No	Steps	Information
ARP Static		
1.	Melalui winbox , pilih menu IP > ARP	<p>C=complete D=Dynamic</p>
2.	Pada ARP List tekan tanda "+"	
3.	Daftarkan Ip address yang , kemungkinan mendapat serangan ARP poisoning, Seperti Router Interface ether2LAN, Server.	

4.	Interface Ether2LAN, jadikan replay only	 <p>The screenshot shows the Mikrotik WinBox interface for configuring the R1-ether2-LAN interface. The 'General' tab is active, and the 'ARP' dropdown menu is set to 'reply-only'. Red boxes highlight the 'Interfaces' menu item, the 'R1-ether2-LAN' interface name, and the 'reply-only' ARP setting.</p>
5.	Untuk Membuat ARP Static pada DHCP server tambahkan ARP For Leases IP > DHCP Server	 <p>The screenshot shows the Mikrotik WinBox interface for configuring a DHCP server named 'dhcp1'. The 'Add ARP For Leases' checkbox is checked, which is highlighted with a red box. Other settings like 'Lease Time' and 'Bootp Lease Time' are also visible.</p>

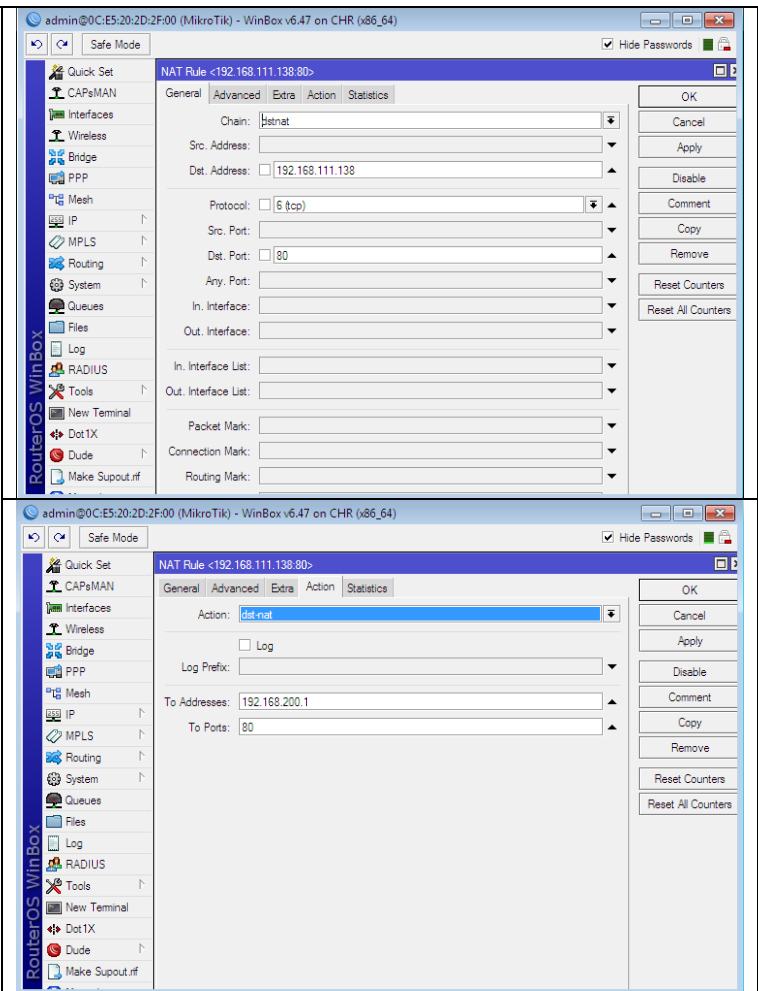
Firewall Proteksi

Mencegah Ping dari External jaringan

No	Steps	Information
1.	Menggunakan terminal dapat mengetikan : <pre>/ip firewall filter add chain=input action=drop protocol=icmp in-interface=R1Ether1Internet</pre>	 <p>The screenshot shows the Mikrotik WinBox interface for configuring a Firewall Rule. The 'Chain' is set to 'input' and the 'Protocol' is set to 'icmp'. The 'In-Interface' is set to 'R1-ether1-Internet'. Red boxes highlight these settings.</p>
2.	Atau menggunakan GUI winbox IP > Firewall Pada tab general Chain=Input Protocol = ICMP In-Interfaces=R1-Ether1Internet	 <p>This section is a textual description of the steps to configure the firewall rule using the GUI, corresponding to the screenshot in the previous row.</p>

3.	Pada tab Acction = Drop	
4.	Test Ping dari Luar jaringan	 <pre>PC4> ping 192.168.111.138 192.168.111.138 icmp_seq=1 timeout 192.168.111.138 icmp_seq=2 timeout 192.168.111.138 icmp_seq=3 timeout 192.168.111.138 icmp_seq=4 timeout 192.168.111.138 icmp_seq=5 timeout ^C</pre>

DMZ Port Forward

5.	<p>Dapat mengetikkan perintah apada terminal untuk dstnat:</p> <pre>ip firewall nat add chain=dstnat dst-address=192.168.111.138 protocol=tcp dst-port=80 action=dst-nat to-addresses=192.168.200.1 to-ports=80</pre> <p>Atau Menggunakan GUI pada winbox</p>	
----	---	---

6.

Dapat mengetikkan perintah apa saja di terminal untuk srcnat:

```
ip firewall nat add chain=srcnat src-address=192.168.200.1 out-interface=R1-ether1-internet action=src-nat to-addresses=192.168.111.138
```

Atau Menggunakan GUI pada WinBox

The image displays two screenshots of the Mikrotik WinBox GUI, showing the configuration of a NAT rule. The top screenshot shows the 'General' tab of the 'NAT Rule <192.168.200.1>' configuration window. The 'Chain' is set to 'srcnat', 'Src. Address' is '192.168.200.1', and 'Out. Interface' is 'R1-ether1-internet'. The bottom screenshot shows the 'Action' tab of the same NAT rule configuration window. The 'Action' is set to 'src-nat', and 'To Addresses' is '192.168.111.138'. Both screenshots show the 'RouterOS WinBox' sidebar on the left and the 'NAT Rule <192.168.200.1>' configuration window on the right.