Laboratorium
Multimedia dan Internet of Things
Departemen Teknik Komputer
Institut Teknologi Sepuluh Nopember

Laporan Akhir
Praktikum Jaringan Komputer

Firewall & NAT

Benice Didan Al Ghifari - 5024231045

2025

1 Langkah-Langkah Praktikum

1. **Mengembalikan Router ke Konfigurasi Awal**

   Langkah pertama adalah memastikan router tidak memiliki konfigurasi sebelumnya untuk mencegah konflik. Tahapan:

   - Buka aplikasi Winbox dan hubungkan ke router.
   - Arahkan ke `System > Reset Configuration`.
   - Aktifkan opsi `No Default Configuration`.
   - Klik `Reset Configuration` untuk memulai proses.

2. **Masuk ke Antarmuka Router**

   Gunakan Winbox untuk login ke router melalui MAC address atau IP default. Username default: `admin`, tanpa password.

3. **Konfigurasi DHCP Client pada** `ether1`

   Sambungkan kabel internet ke `ether1`, lalu:

   - Buka `IP > DHCP Client`, klik `+`.
   - Pilih `ether1` sebagai interface.
   - Klik `Apply` dan pastikan status menjadi `bound`.

4. **Menetapkan IP Statis pada Interface** `ether7`

   Digunakan untuk koneksi ke switch:

   - Akses `IP > Addresses`, klik `+`.
   - Isi `Address: 192.168.10.1/24`, Interface: `ether7`.

5. **Mengaktifkan DHCP Server di** `ether7`

   - Arahkan ke `IP > DHCP Server`, klik `DHCP Setup`.
   - Interface: `ether7`, jaringan: `192.168.10.0/24`.
   - Gateway: `192.168.10.1`, DNS: `8.8.8.8`, `8.8.4.4`.
   - Range IP: `192.168.10.2 - 192.168.10.254`, Lease Time: `00:10:00`.

6. **Penerapan NAT (Masquerade)**

   - Masuk ke `IP > Firewall > NAT`, klik `+`.
   - Tab General: Chain: `src-nat`.
   - Tab Action: pilih `masquerade`.
   - Untuk pengujian, lakukan `ping 8.8.8.8`.

7. **Menambahkan Filter Firewall**

   - **Blok ICMP:**

- Chain: `forward`, Protocol: `icmp`, In-Interface: `ether7`.
- Action: `drop`.

- **Konten Filtering:**
  - Chain: `forward`, Protocol: `tcp`, Dst Port: `80,443`.
  - In: `ether7`, Out: `ether1`, Content: `speedtest`.
  - Action: `drop`.

8. **Konfigurasi Bridge Router B**

   Untuk mengubah Router B menjadi hub:

   - Tambahkan Bridge melalui `Bridge > Add`, lalu `Apply`.
   - Masuk ke `Ports` dan tambahkan interface laptop dan interface ke Router A.

9. **Pengaturan IP Klien**

   Laptop dikonfigurasi otomatis (DHCP) dan dilakukan verifikasi IP dengan `ipconfig` di Command Prompt.

10. **Pengujian Konfigurasi**

    - **ICMP Test:** Ping ke `8.8.8.8`, saat rule aktif akan RTO. Setelah dinonaktifkan, ping berhasil.
    - **Web Filter Test:** Akses `speedtest.net` akan gagal saat rule konten aktif.

2 Analisis Hasil Praktikum

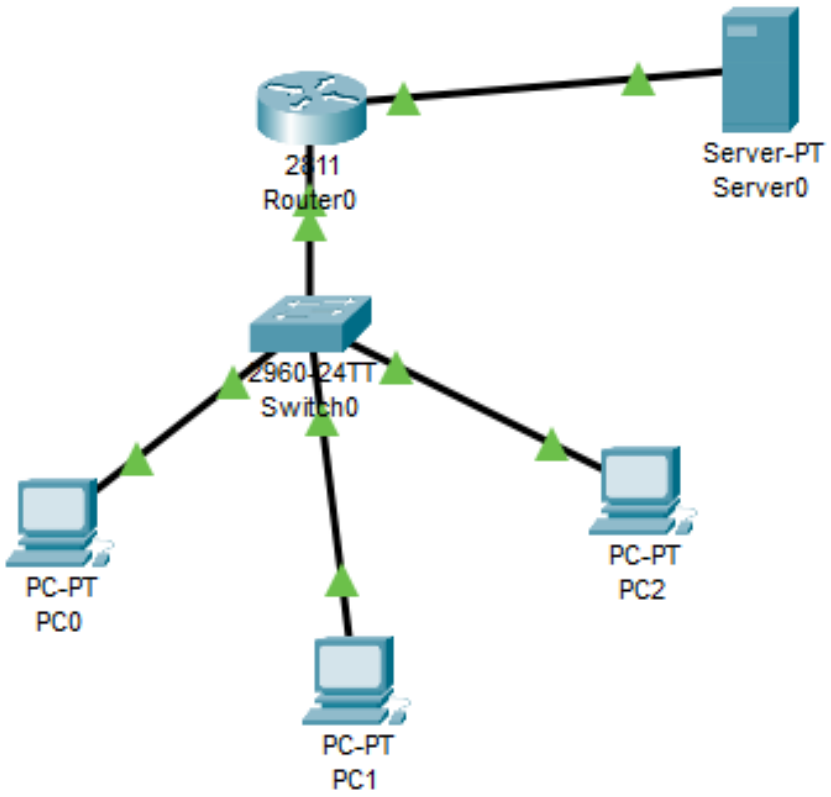
Seluruh konfigurasi berjalan sesuai dengan urutan dan tujuan percobaan. Reset konfigurasi memastikan router tidak memiliki konfigurasi lama yang dapat mengganggu pengaturan baru. DHCP Client memungkinkan router memperoleh IP dari ISP, sedangkan konfigurasi IP statis dan DHCP Server memungkinkan perangkat klien mendapatkan alamat IP secara otomatis.

Implementasi NAT dengan metode `masquerade` sukses menghubungkan klien ke internet. Pengujian `ping` ke DNS Google membuktikan konektivitas berjalan dengan baik. Fitur firewall juga bekerja sebagaimana mestinya. Aktivasi filter ICMP dan konten mampu memblokir koneksi ping dan akses web tertentu, sedangkan saat dinonaktifkan koneksi kembali normal.

Konfigurasi bridge pada Router B memungkinkan penggabungan dua interface agar klien tetap terhubung melalui router secara transparan. Seluruh pengujian validasi membuktikan bahwa router MikroTik mampu menangani fungsi dasar manajemen jaringan lokal secara efisien.

3 Hasil Tugas Modul

3.1 Topologi Jaringan NAT dan Firewall



Gambar 1: Desain topologi NAT dan Firewall ACL

3.2 Script Konfigurasi NAT pada Cisco

```
interface FastEthernet0/0
 ip nat inside
exit

interface FastEthernet0/1
 ip nat outside
exit

access-list 1 permit 192.168.10.0 0.0.0.255

ip nat inside source list 1 interface FastEthernet0/1 overload
```

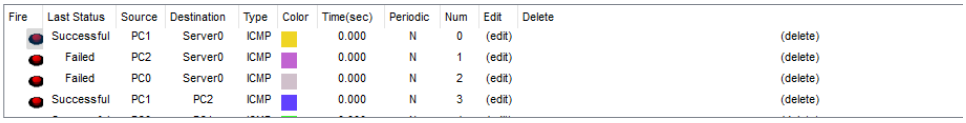
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC1	Server0	ICMP		0.000	N	6	(edit)	
	Successful	PC2	Server0	ICMP		0.000	N	7	(edit)	
	Successful	PC0	Server0	ICMP		0.000	N	8	(edit)	
	Successful	PC1	PC2	ICMP		0.000	N	9	(edit)	

Gambar 2: Implementasi NAT pada Cisco Router

3.3 Script Konfigurasi Firewall ACL pada Cisco

```
ip access-list extended FIREWALL_SERVER
 permit ip host 192.168.10.11 host 200.100.50.2
 deny ip host 192.168.10.10 host 200.100.50.2
 deny ip host 192.168.10.12 host 200.100.50.2
 permit ip 192.168.10.0 0.0.0.255 any

interface FastEthernet0/0
 ip access-group FIREWALL_SERVER in
exit
```



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC1	Server0	ICMP		0.000	N	0	(edit)	(delete)
	Failed	PC2	Server0	ICMP		0.000	N	1	(edit)	(delete)
	Failed	PC0	Server0	ICMP		0.000	N	2	(edit)	(delete)
	Successful	PC1	PC2	ICMP		0.000	N	3	(edit)	(delete)

Gambar 3: Penerapan Access Control List (ACL)

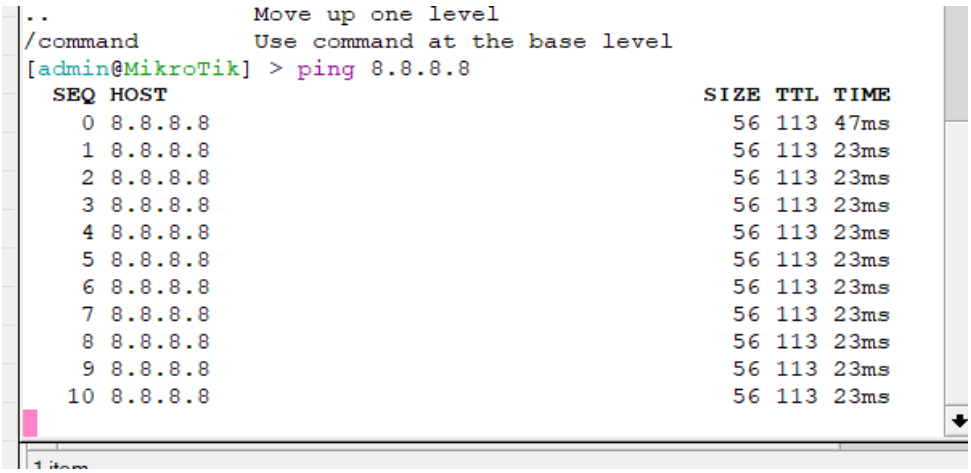
4 Kesimpulan

Percobaan ini membuktikan bahwa router MikroTik memiliki kapabilitas tinggi dalam menangani distribusi alamat IP, penyediaan koneksi internet via NAT, serta pengaturan akses melalui firewall. Seluruh konfigurasi yang dilakukan — mulai dari DHCP, NAT, hingga content filtering — dapat berjalan sebagaimana mestinya dan terverifikasi melalui uji konektivitas.

Selain itu, implementasi ACL pada perangkat Cisco juga memperlihatkan bagaimana kontrol lalu lintas data dapat dibatasi sesuai dengan kebijakan jaringan. Percobaan ini memperluas wawasan praktikan terhadap kombinasi konfigurasi manual dan keamanan jaringan berbasis firewall.

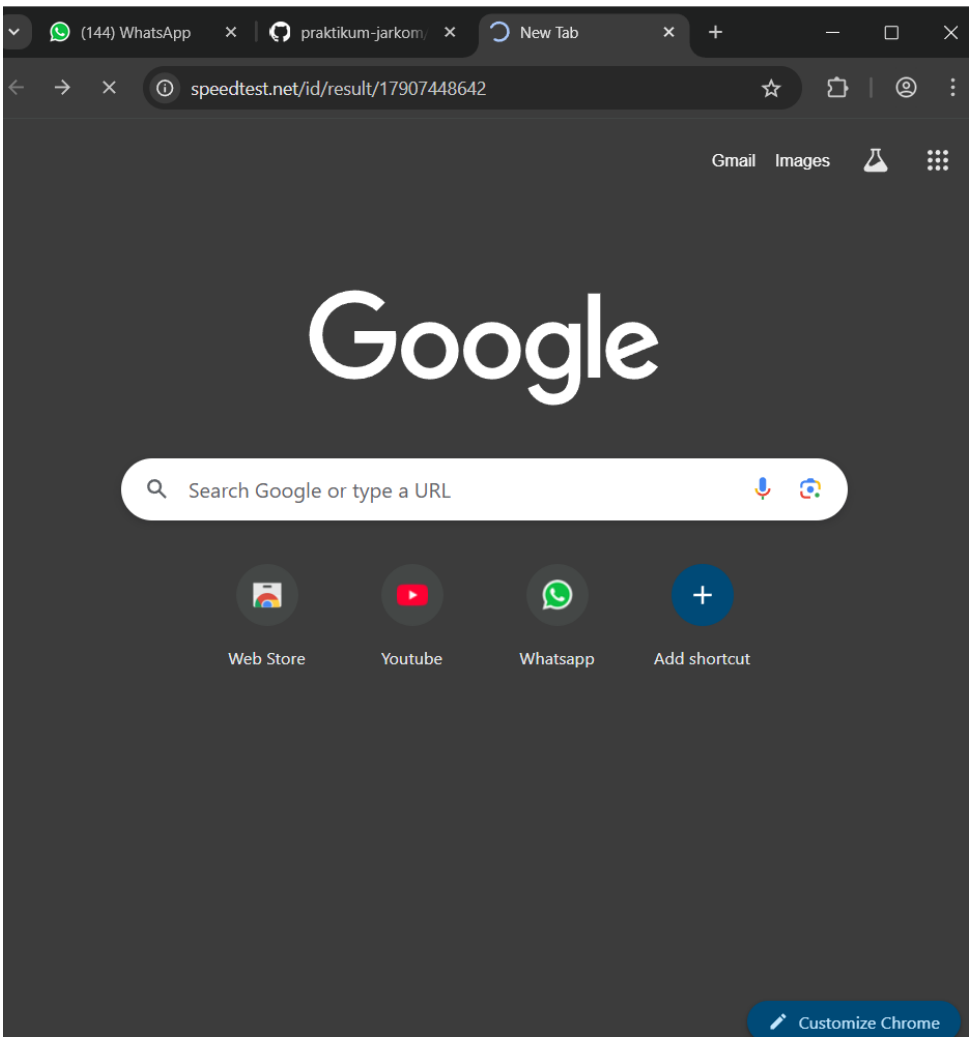
5 Lampiran

5.1 Dokumentasi Praktikum di Laboratorium

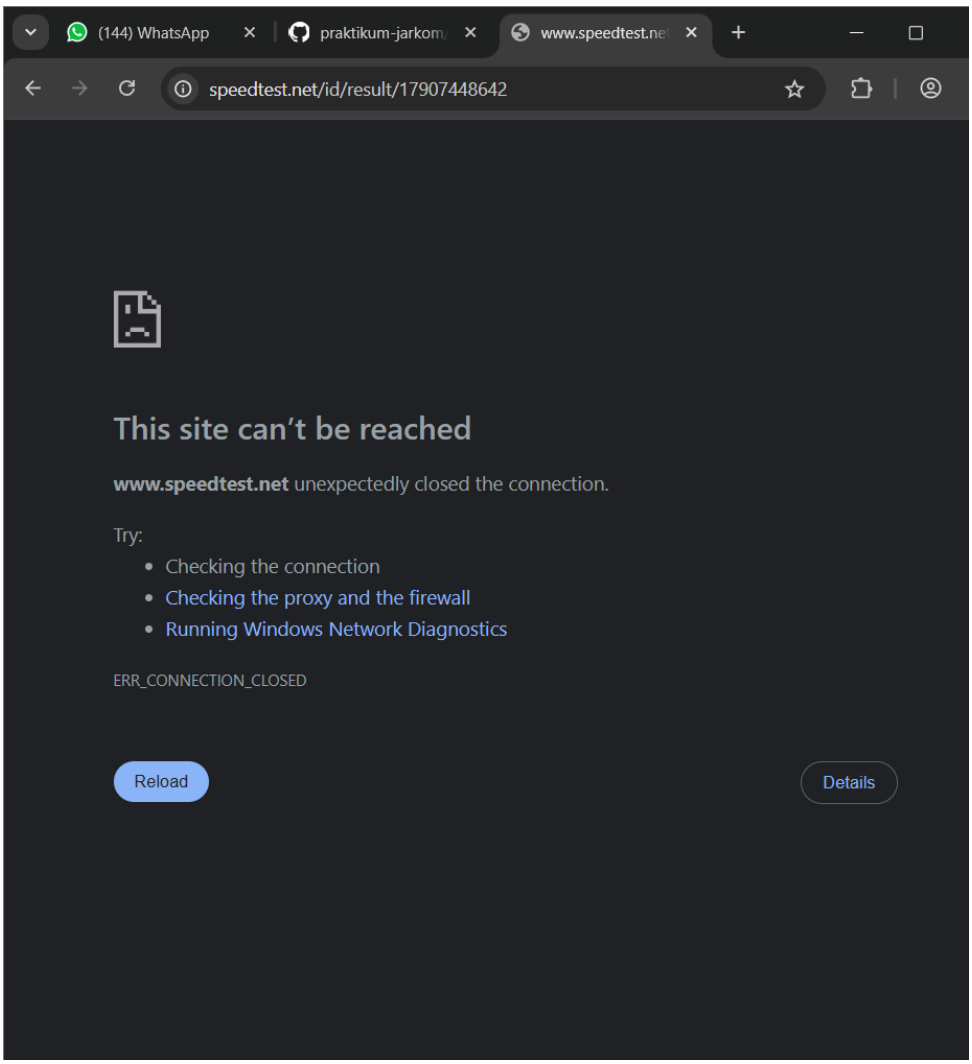


```
..              Move up one level
/command        Use command at the base level
[admin@MikroTik] > ping 8.8.8.8
  SEQ HOST                                     SIZE TTL TIME
    0 8.8.8.8                                    56 113 47ms
    1 8.8.8.8                                    56 113 23ms
    2 8.8.8.8                                    56 113 23ms
    3 8.8.8.8                                    56 113 23ms
    4 8.8.8.8                                    56 113 23ms
    5 8.8.8.8                                    56 113 23ms
    6 8.8.8.8                                    56 113 23ms
    7 8.8.8.8                                    56 113 23ms
    8 8.8.8.8                                    56 113 23ms
    9 8.8.8.8                                    56 113 23ms
   10 8.8.8.8                                    56 113 23ms
```

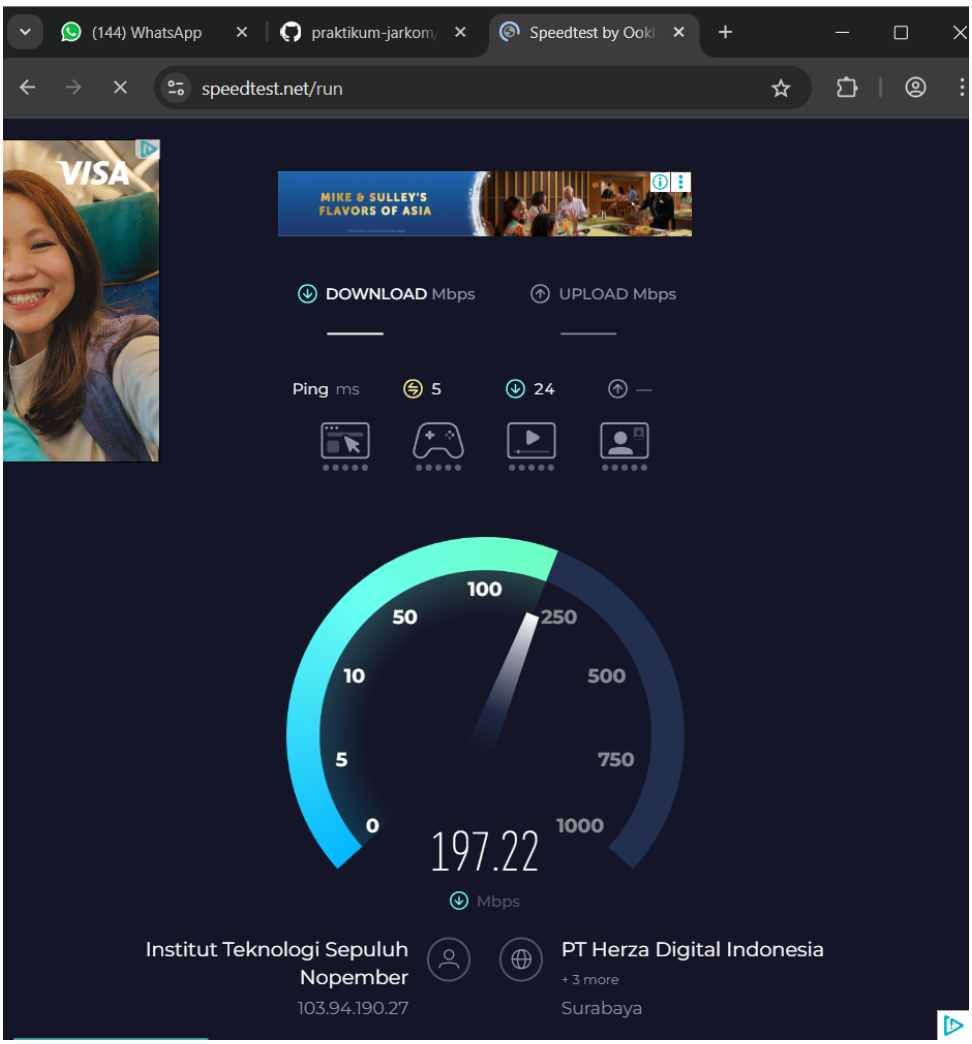
Gambar 4: Tampilan antarmuka Winbox saat konfigurasi NAT



Gambar 5: Konfigurasi DHCP Server berhasil dijalankan



Gambar 6: Hasil pengujian pemblokiran ICMP



Gambar 7: Tes konektivitas setelah firewall dinonaktifkan