



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

Laporan Akhir Praktikum Jaringan Komputer

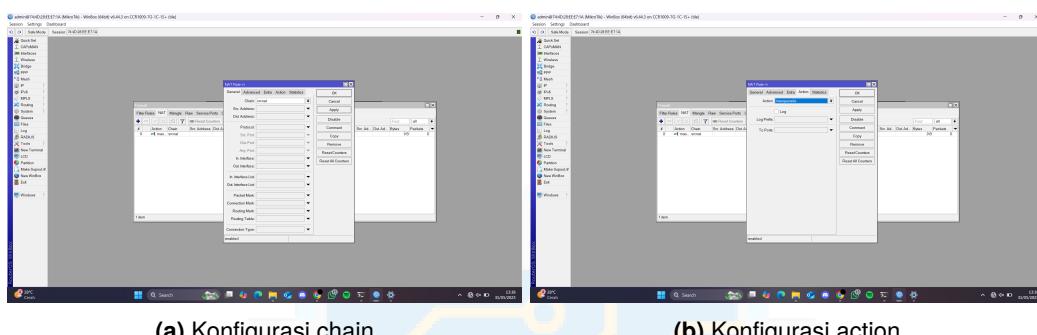
Firewall dan NAT

Muhammad Risang Radityatama - 5024231028

2025

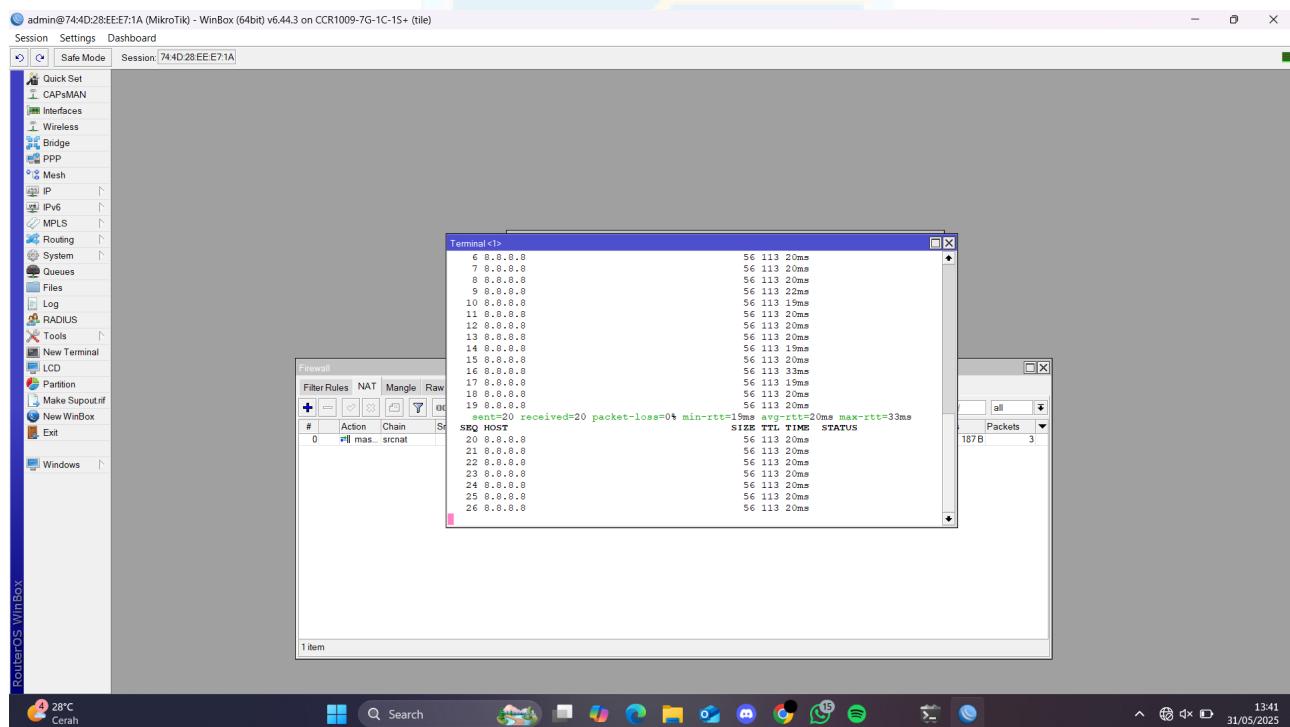
1 Langkah-Langkah Percobaan

1. Melakukan reset pada router bila diperlukan dan login ke router
 2. Melakukan setup client DHCP pada router A. DHCP client disetup pada interface ether1 yang akan menjadi penghubung router ke internet.
 3. Menambahkan alamat IP untuk interface ether7 dengan konfigurasi alamat IP 192.168.10.1/24.
 4. Melakukan setup DHCP server pada interface ether7.
 5. Melakukan konfigurasi NAT dengan menambahkan aturan baru dengan konfigurasi Chain: src-nat dan Action: masquerade.



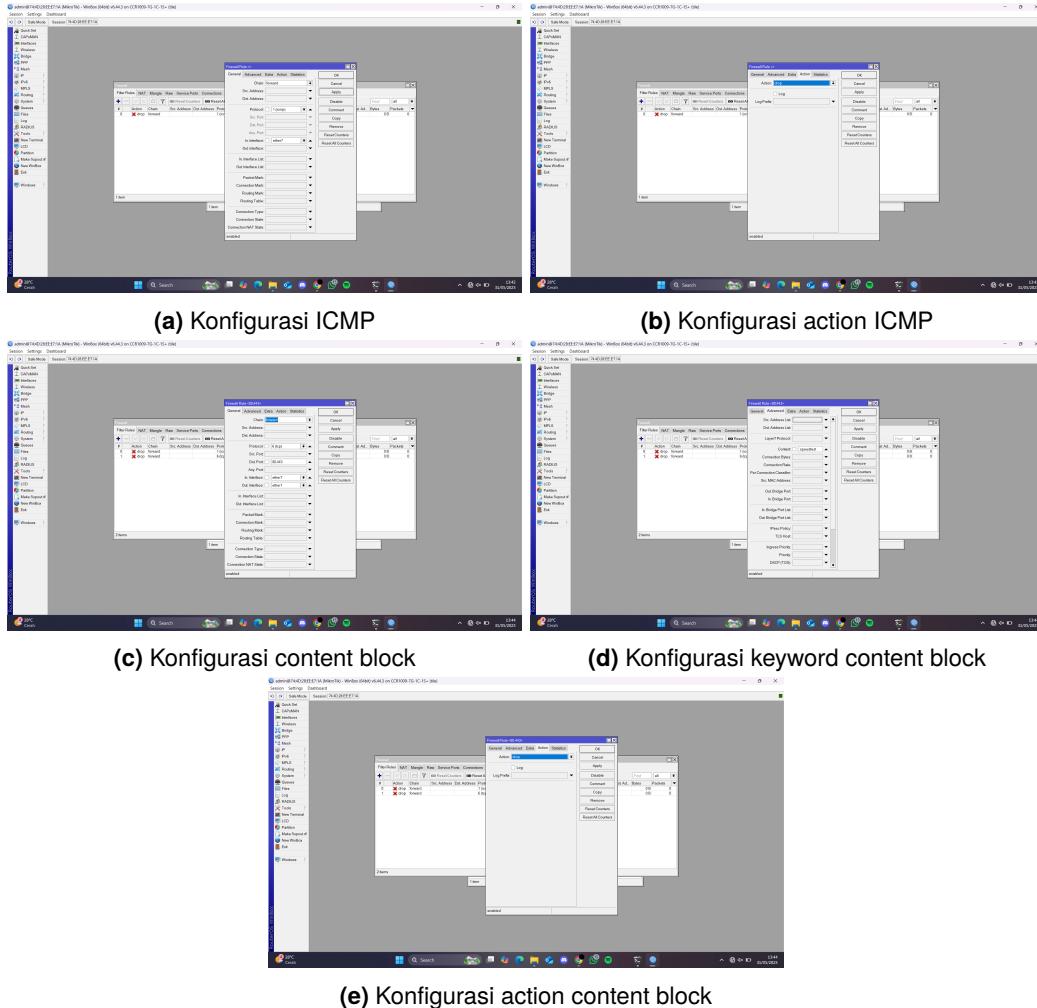
Gambar 1: Konfigurasi NAT

6. Menguji NAT dengan melakukan ping ke 8.8.8.8 dari router melalui interface winbox.



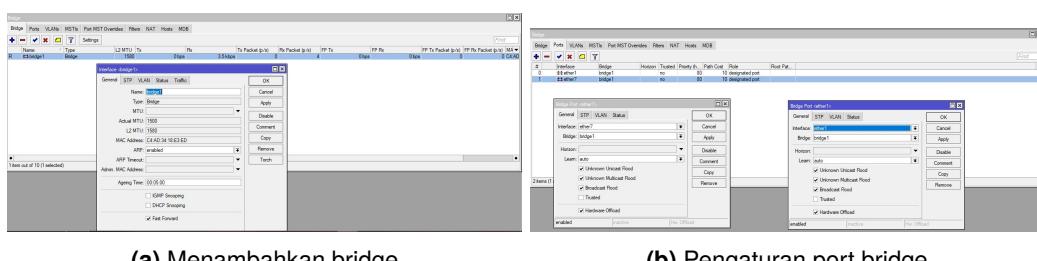
Gambar 2: Tes ping 8.8.8.8

7. Melakukan konfigurasi firewall dengan menambahkan aturan baru untuk pemblokiran ICMP dan content blocking. Untuk aturan pemblokiran ICMP menggunakan konfigurasi Chain: forward, Protocol icmp, In.Interface: ether7, Action: drop. Untuk aturan pemblokiran konten menggunakan konfigurasi Chain: forward, Protocol: tcp, Dsr. Port: 80,443, In. Interface: ether7, Out. Interface: ether1, Content: speedtest, Action: drop.



Gambar 3: Konfigurasi Firewall

8. Melakukan konfigurasi bridge pada router B dengan menambahkan bridge baru dengan konfigurasi port yang digunakan adalah interface yang terhubung pada laptop dan interface yang terhubung dengan router A.



Gambar 4: Konfigurasi bridge router B

9. Melakukan konfigurasi IP pada laptop. Karena IP diberikan secara otomatis oleh server DHCP, maka hanya perlu memeriksa IP yang diberikan oleh server melalui command ipconfig pada cmd atau powershell.
10. Menguji aturan ICMP dengan melakukan ping ke 8.8.8.8 dengan keadaan firewall aktif dan nonaktif.
11. Menguji aturan content blocking dengan mengakses speedtest.net dengan keadaan firewall aktif dan nonaktif.

2 Analisis Hasil Percobaan

Pada praktikum ini dilakukan percobaan pengaturan firewall dan NAT pada router mikrotik. Secara teori, bila konfigurasi NAT berhasil maka router dapat melakukan ping ke 8.8.8.8 dan mendapat balasan. Bila konfigurasi firewall berhasil, maka bila aturan pemblokiran ICMP diaktifkan maka laptop bisa melakukan ping ke 8.8.8.8 tapi tidak akan mendapat jawaban (time out) dan bila aturan pemblokiran konten diaktifkan maka laptop tidak akan bisa membuka konten dari situs web yang mengandung kata kunci "speedtest" dan akan diberi message time out oleh browser. Setelah percobaan dilakukan, didapatkan hasil bahwa router A dapat melakukan ping 8.8.8.8, yang artinya pengaturan NAT sudah berhasil. Saat firewall aturan pemblokiran ICMP diaktifkan, laptop tidak bisa mendapatkan respon time out ketika melakukan ping ke 8.8.8.8 dan baru bisa mendapat balasan apabila aturan firewall untuk pemblokiran ICMP dimatikan. Hal ini menunjukkan bahwa pemblokiran ICMP ke alamat 8.8.8.8 dengan action drop telah berhasil karena laptop dapat melakukan ping namun tidak mendapat balasan (drop) saat aturan firewall aktif.

```

Command Prompt
General failure.

Ping statistics for 8.8.8.8:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\Hp>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\Hp>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=20ms TTL=112
Reply from 8.8.8.8: bytes=32 time=24ms TTL=112
Reply from 8.8.8.8: bytes=32 time=20ms TTL=112
Reply from 8.8.8.8: bytes=32 time=20ms TTL=112

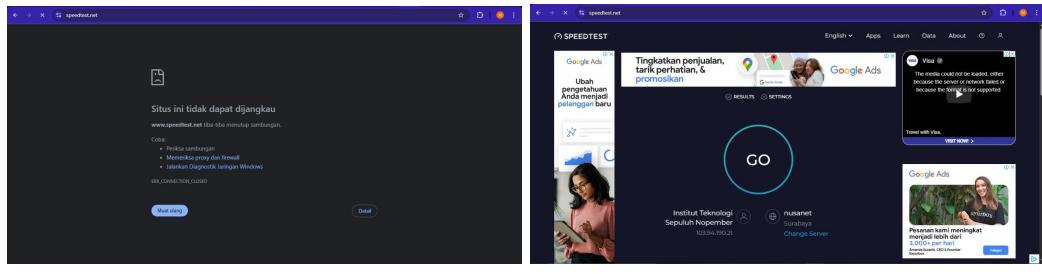
Ping statistics for 8.8.8.8:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 20ms, Maximum = 24ms, Average = 21ms
C:\Users\Hp>

```

Gambar 5: Hasil ping 8.8.8.8 dari laptop. Bagian atas adalah saat firewall dinyalakan dan bagian bawah adalah saat firewall dimatikan

Saat firewall aturan pemblokiran konten diaktifkan, laptop tidak bisa membuka situs speedtest.net melalui browser dan muncul peringatan connection timed out dan baru bisa mengakses kembali situs

speedtest.net ketika aturan firewall dimatikan. Hal ini menunjukkan bahwa firewall aturan pemblokiran konten telah berhasil memblokir akses laptop ke situs yang memiliki kata kunci "speedtest".



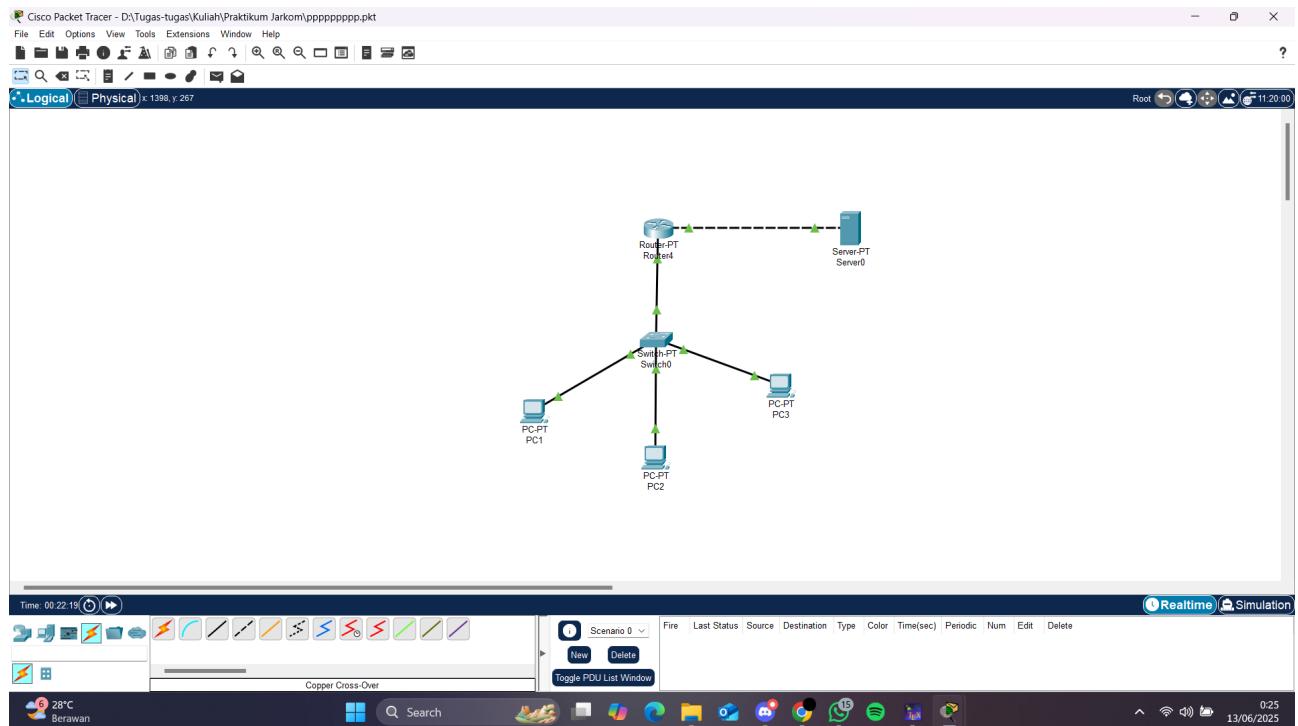
(a) Akses speedtest.net saat firewall aktif

(b) Akses speedtest.net saat firewall mati

Gambar 6: Hasil akses speedtest.net

3 Hasil Tugas Modul

Pada tugas modul ini, digunakan 1 server dengan IP lokal 192.168.105.1 dan IP publik 10.10.10.1, 1 router, 1 switch, dan 3 PC dengan IP address lokal masing masing 192.168.10.2, 192.168.10.3, 192.168.10.4. Interface fa0/0 router terhubung pada sercer dan fa1/0 terhubung pada switch. Berikut merupakan topologi jaringan:



Gambar 7: Topolofi Tugas Modul

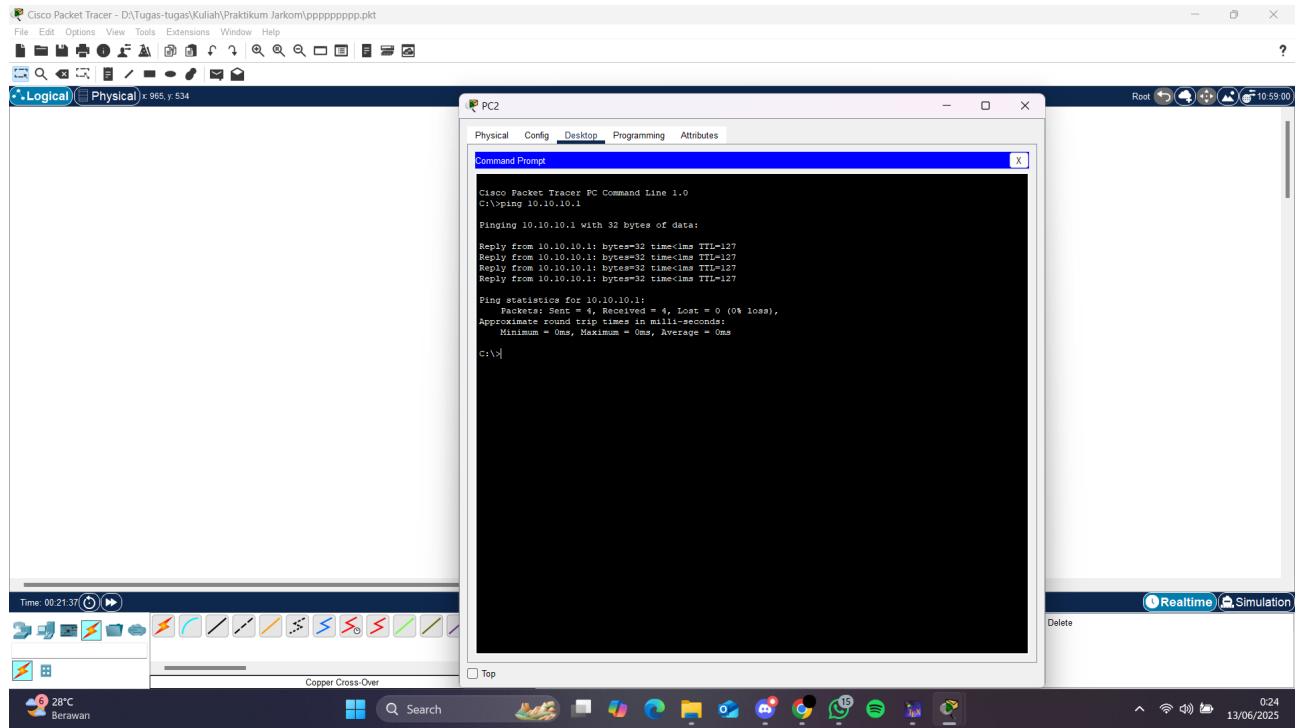
untuk melakukan konfigurasi NAT, digunakan command sebagai berikut pada router:

```

1 Router(config)#ip nat inside source static 192.168.105.1 10.10.10.1
2 Router(config)#interface fa0/0
3 Router(config-if)#ip nat inside
4 Router(config)#interface fa1/0
5 Router(config-if)#ip nat outside

```

Dengan konfigurasi seperti di atas, maka ketiga PC dapat mengakses server menggunakan alamat IP publiknya yaitu 10.10.10.1.



Gambar 8: Hasil ping server menggunakan IP publik dari PC2

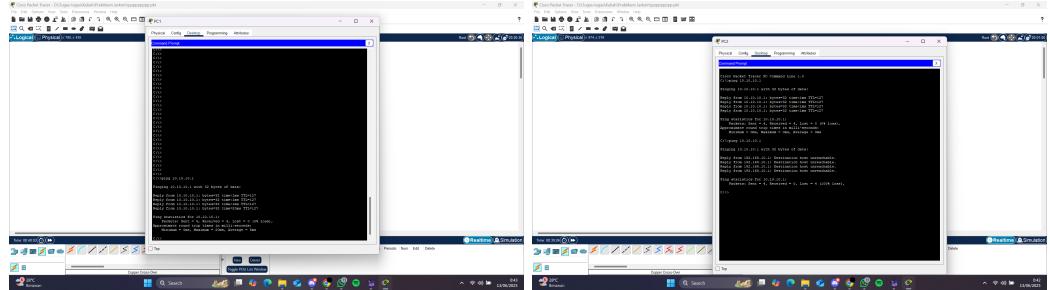
Penerapan firewall untuk memblokir masing-masing PC dapat diterapkan menggunakan command berikut:

```
1 Router(config)#access-list 100 deny icmp 192.168.10.3 0.0.0.0 192.168.105.0 0.0.0.0
2 Router(config)#access-list 101 deny icmp 192.168.10.4 0.0.0.0 192.168.105.0 0.0.0.0
3 Router(config)#access-list 102 deny icmp 192.168.10.2 0.0.0.0 192.168.105.0 0.0.0.0
```

Access list 100 digunakan untuk memblokir PC2, 101 digunakan untuk memblokir PC3, dan 102 digunakan untuk memblokir PC1. Untuk kasus pertama yaitu hanya PC1 yang bisa mengakses server maka PC2 dan PC3 harus diblokir. Pemblokiran diterapkan atau dinyalakan dengan command berikut:

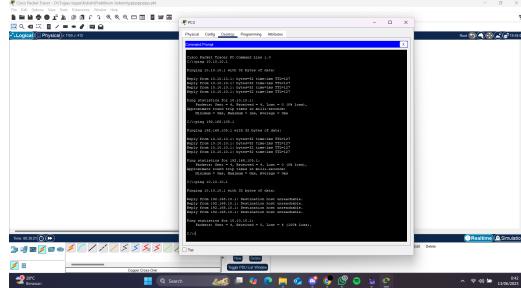
```
1 Router(config)#interface fa1/0
2 Router(config-if)#ip access-list 100 in
3 Router(config-if)#ip access-list 101 in
4 Router(config-if)#no ip access-list 102 in
```

Command di atas akan memblokir PC2 dan PC3 lalu mengangkat pemblokiran PC1, sehingga hanya PC1 yang bisa mengakses server.



(a) Hasil ping ke server dari PC1

(b) Hasil ping ke server dari PC2



(c) Hasil ping ke server dari PC3

Gambar 9: Hasil ping ke server dari PC

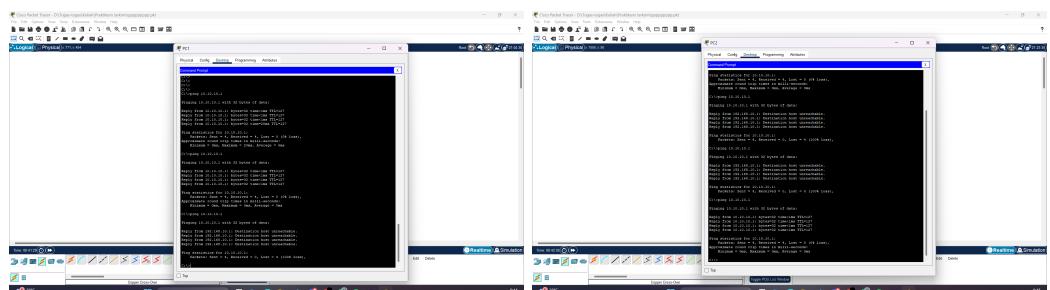
Untuk kasus kedua yaitu PC1 dan PC3 dilarang mengakses server dapat diterapkan dengan command sebagai berikut:

```

1 Router(config)#interface fa1/0
2 Router(config-if)#ip access-list 100 in
3 Router(config-if)#no ip access-list 101 in
4 Router(config-if)#ip access-list 102 in

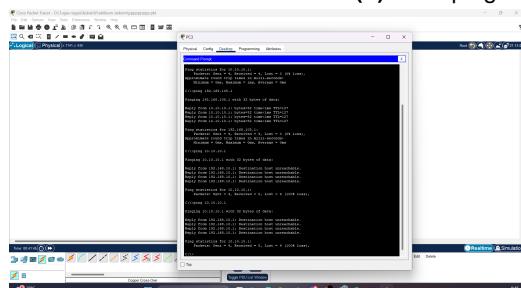
```

Command di atas akan memblokir PC1 dan PC3 saja lalu mengangkat pemblokiran PC2 (karena sebelumnya PC2 diblokir aksesnya).



(a) Hasil ping ke server dari PC1

(b) Hasil ping ke server dari PC2



(c) Hasil ping ke server dari PC3

Gambar 10: Hasil ping ke server dari PC

Dengan menerapkan access list, maka akses dari PC ke server dapat dibatasi namun tidak akan mempengaruhi komunikasi LAN antar PC sama sekali.

4 Kesimpulan

Adannya NAT dan firewall memungkinkan perancangan jaringan yang lebih murah (berkat kemampuan NAT untuk mentraslasikan banyak IP lokal menjadi IP publik yang lebih sedikit jumlahnya) dan lebih aman (berkat firewall yang dapat membatasi akses terhadap komunikasi dan konten). Berdasarkan hasil percobaan, baik NAT dan firewall sudah bekerja sesuai dengan teori dan hasil yang didapatkan sesuai dengan hasil yang diharapkan.

5 Lampiran

5.1 Dokumentasi saat praktikum



Gambar 11: Dokumentasi praktikum