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

Laporan Akhir
Praktikum Jaringan Komputer

Firewall & NAT

Muhammad Rafli Satriani - 5024231033

31 Mei 2025

1 Langkah-Langkah Percobaan

1. Siapkan peralatan untuk praktikum
    - 3 kabel LAN
    - 2 router
    - 2 laptop
2. Sambungkan kabel LAN dari sumber internet ke port Ether 1 Router A dan kabel LAN dari port Ether 7 router A ke Laptop 1
3. Pada laptop 1 masuk ke winbox dan konfigurasi DHCP client pada router A dengan masuk ke menu IP -> DHCP client, klik "+" dan pilih interface Ether 1. Pastika status nya "Bound"
4. Masuk ke menu IP -> Address dan tambahkan alamat IP dengan klik "+" dan menambahkan IP 192.168.10.1/24 untuk Ether 7
5. Lakukan Konfigurasi DHCP pada server mikrotik dengan masuk ke menu IP -> DHCP Server dan klik opsi DHCP Setup
    - pilih interface Ether 7 lalu klik "Next"
    - verifikasi networka address yakni 192.168.10.0/24 lalu klik "Next"
    - verifikasi Gateway 192.168.10.1 lalu klik "Next"
    - pilih rentang alamat yang di distribusikan yakni dari 192.168.10.2 samapai 192.168.10.254 lalu klik "Next"
    - masukkan DNS Google yakni 8.8.8.8 dan 8.8.4.4 lalu klik "Next"
    - set waktu lease selama 10 menit lalu klik "Next"
    - akan muncul pesan "Setup has completed succesfully" lalu klik "Ok"
6. Konfigurasi NAT dengan masuk ke menu IP -> Firewall -> NAT. Klik ikon "+" lalu atur chain ke "src-nat" pada tab General dan atur action ke "masquerade" pada tab Action
7. Konfigurasi Firewall:
    - tambahkan aturan filter pada firewall dengan masuk ke menu IP -> Firewall -> Filter Rule dan klik ikon "+"
    - untuk pemblokiran ICMP, pada tab General atur chain ke "forward", atur protocol ke "icmp", atur In. interface ke "ether 7". Pada tab Action atur Action ke "drop"
    - untuk Pemblokiran Akses Situs Web Berdasarkan Konten, pada tab General atur chain ke "forward, atur Protocol ke "tcp", atur Dst.port ke "80,443", atur In. interface ke "ether 7", dan atur Out. Interface ke "ether 1". Pada tab Advanced atur content sesuai pada situs yang ingin diblokir akses internetnya dan pada tab Action atur ke Action ke "drop"
8. Lakukan konfigurasi bridge pada Router B menggunakan laptop 2 dan tambahkan 2 port dengan port pertama memilih interface yang tersabung ke laptop 1 dan port kedua memilih interface yang tersambung ke router A

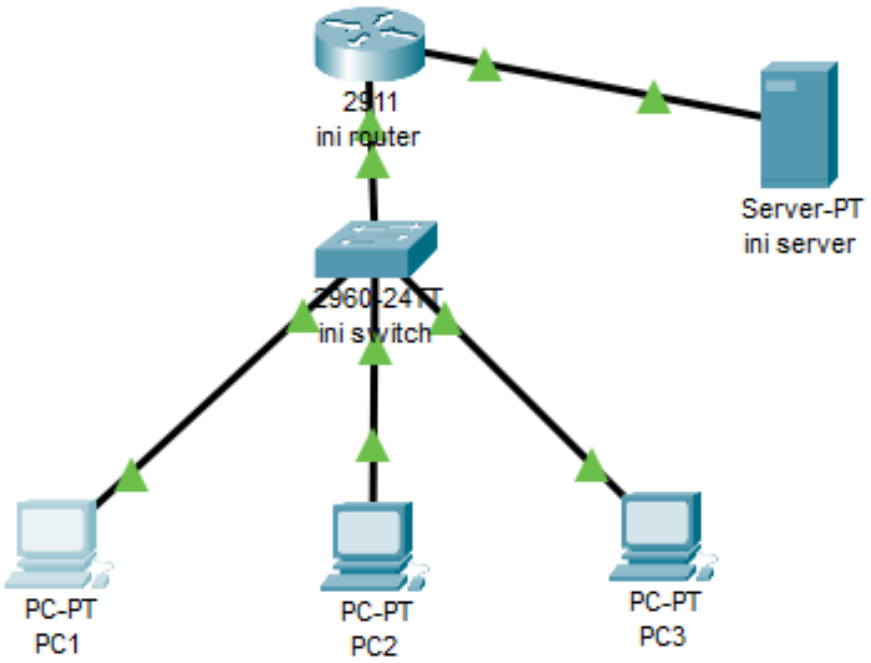
9. Atur IP Address laptop ke otomatis DHCP dan konfirmasi alamat IP melalui CMD menggunakan ipconfig
10. uji coba dengan melakukan ping DNS 8.8.8.8 pada terminal dan lakukan uji coba dengan mengkases situs sesuai yang ditambahkan pada pemblokiran di firewall

2 Analisis Hasil Percobaan

Hasil percobaan menandakan berhasil. Hal ini dibuktikan pada ping DNS 8.8.8.8 dimana respon feedback menampilkan request timed out menandakan DNS berhasil diblokir oleh firewall dan saat mengakases situs speedtest, situs yang di tambahkan di firewall, situs memberikan response timed out yang artinya firewall berhasil memblokir situs.

3 Hasil Tugas Modul

1. Buatlah topologi sederhana di Cisco Packet Tracer dengan:
    - 1 Router
    - 1 Switch
    - 3 PC (LAN)
    - 1 Server (Internet/Public)
2. Konfigurasi NAT: Buat agar semua PC bisa mengakses Server menggunakan IP publik Router.
3. Konfigurasi Firewall (ACL):
    - Izinkan hanya PC1 yang dapat mengakses Server.
    - Blokir PC1 dan PC3 dari mengakses Server.
    - Semua PC harus tetap bisa saling terhubung di LAN.



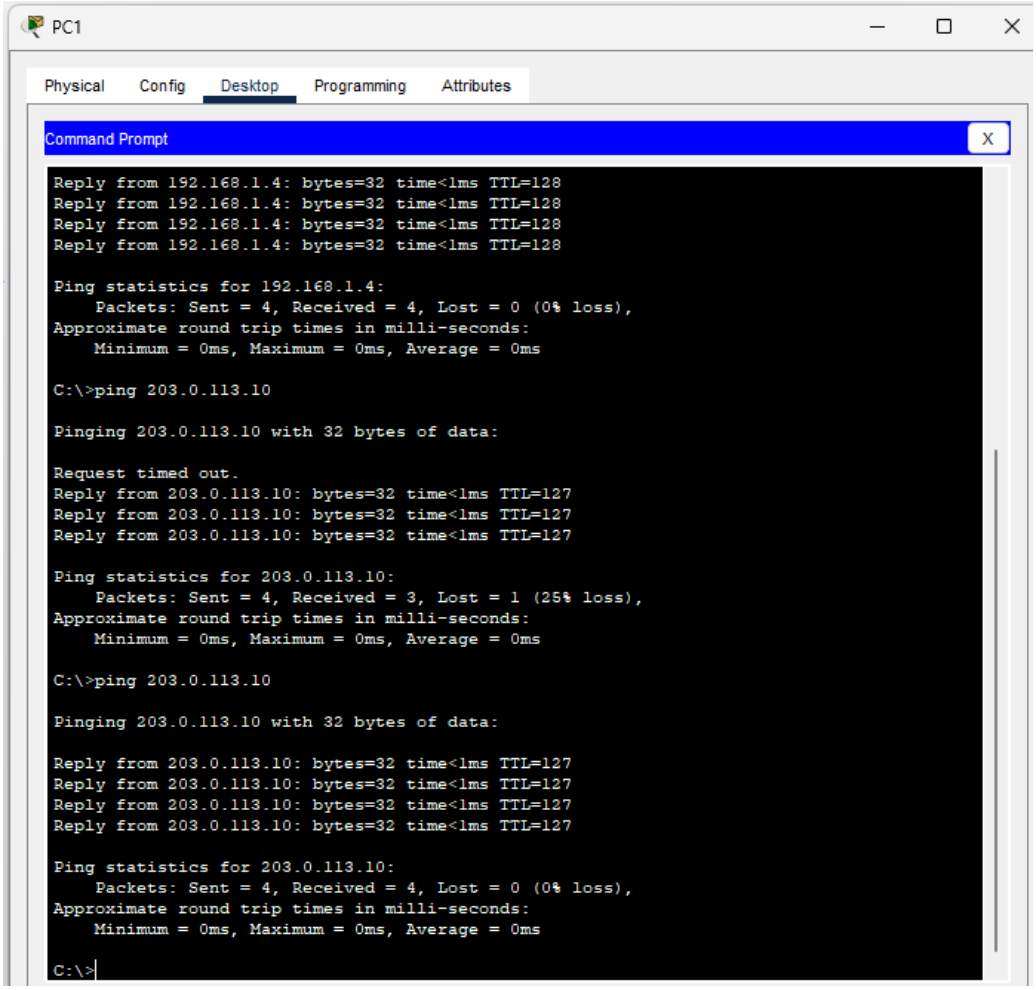
Topologi Tugas Modul

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

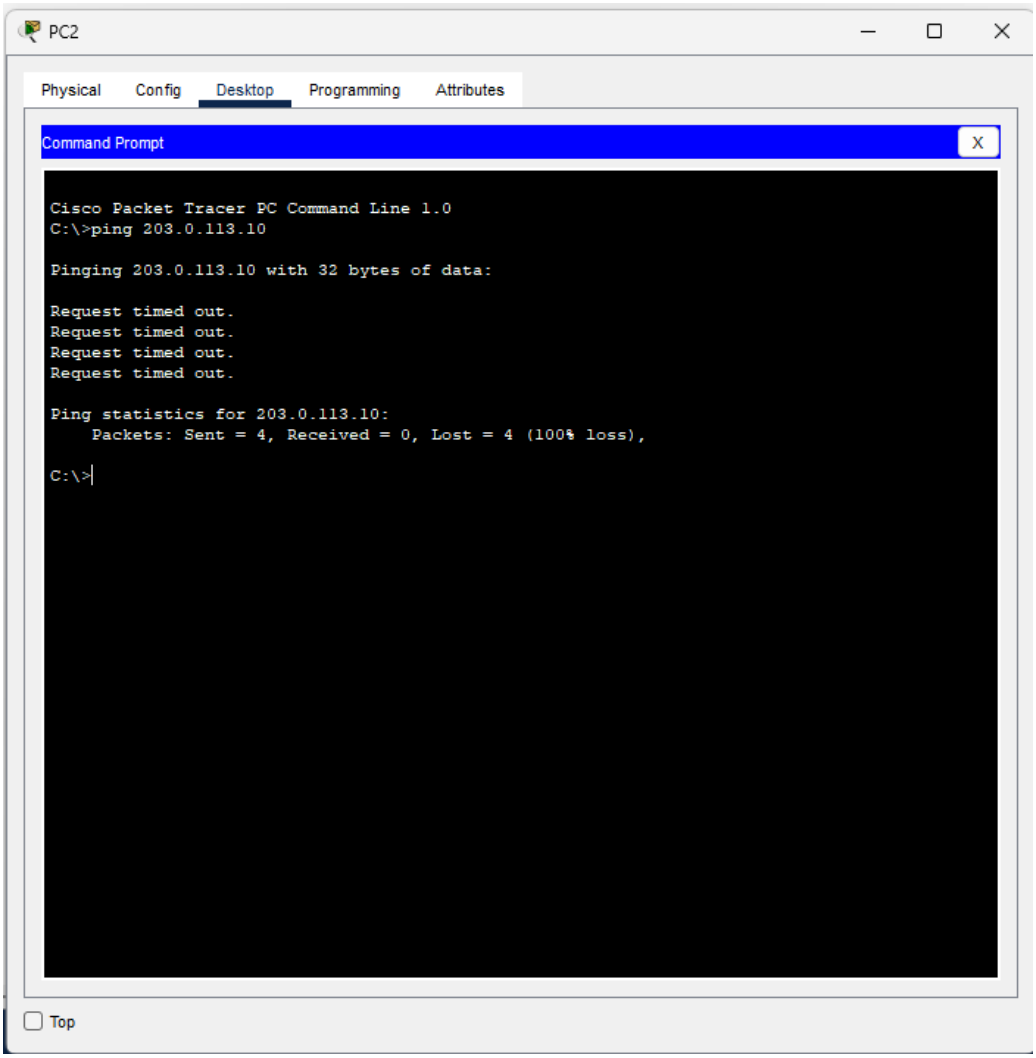
PC1 berhasil PING PC2

```
C:\>ping 192.168.1.4

Pinging 192.168.1.4 with 32 bytes of data:

Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

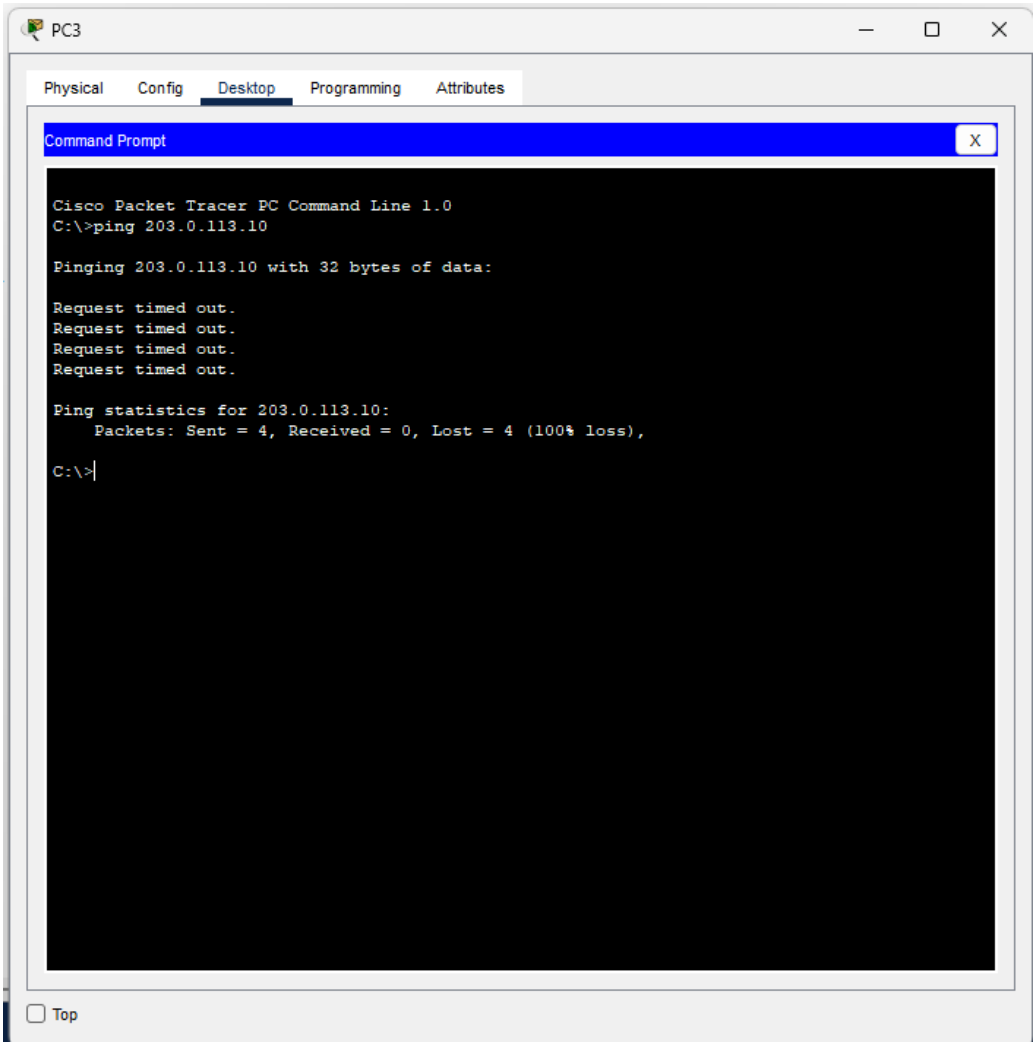
PC1 berhasil PING PC3



PC1 berhasil PING Server



PC2 tidak bisa PING Server



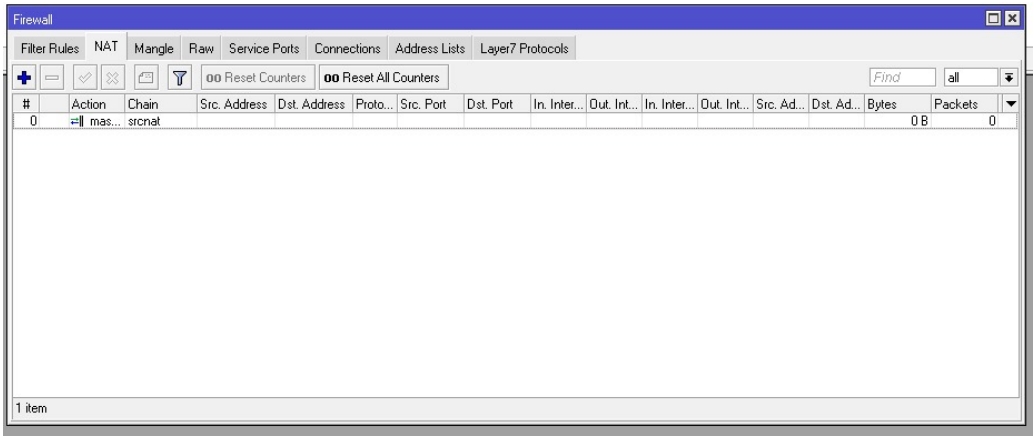
PC3 tidak bisa PING Server

4 Kesimpulan

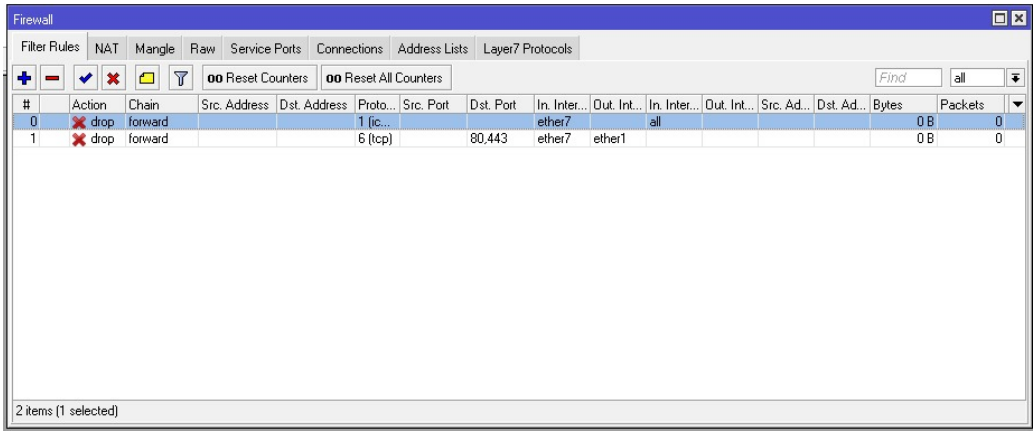
Dalam praktikum ini dapat disimpulkan konfigurasi NAT untuk memungkinkan perangkat di jaringan lokal mengakses jaringan publik menggunakan satu IP publik, serta Firewall (ACL) untuk membatasi akses ke server. Hasilnya, setelah konfigurasi firewall pada alamat tertentu, perangkat tidak dapat mengakses alamat tersebut meski sudah terhubung dengan jaringan.

5 Lampiran

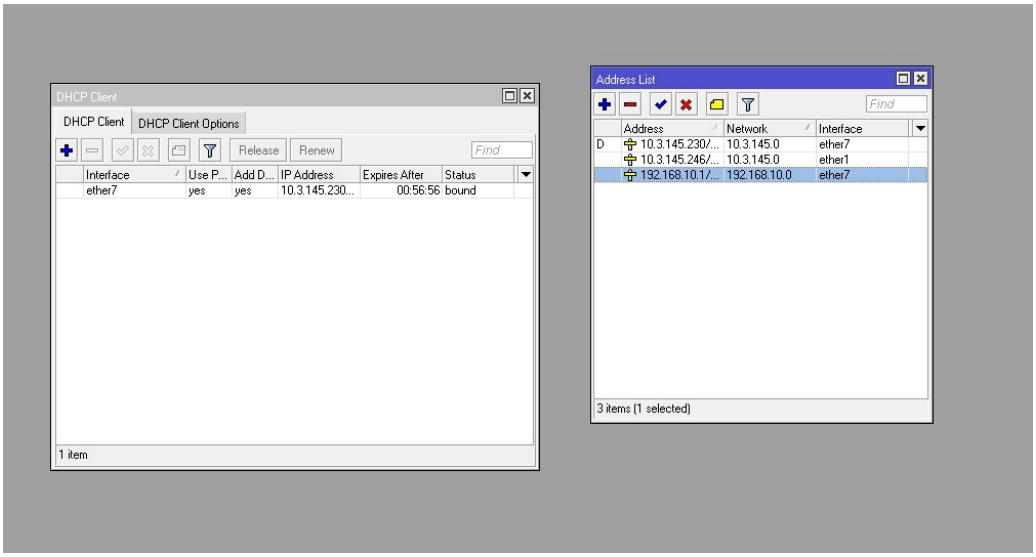
5.1 Dokumentasi saat praktikum



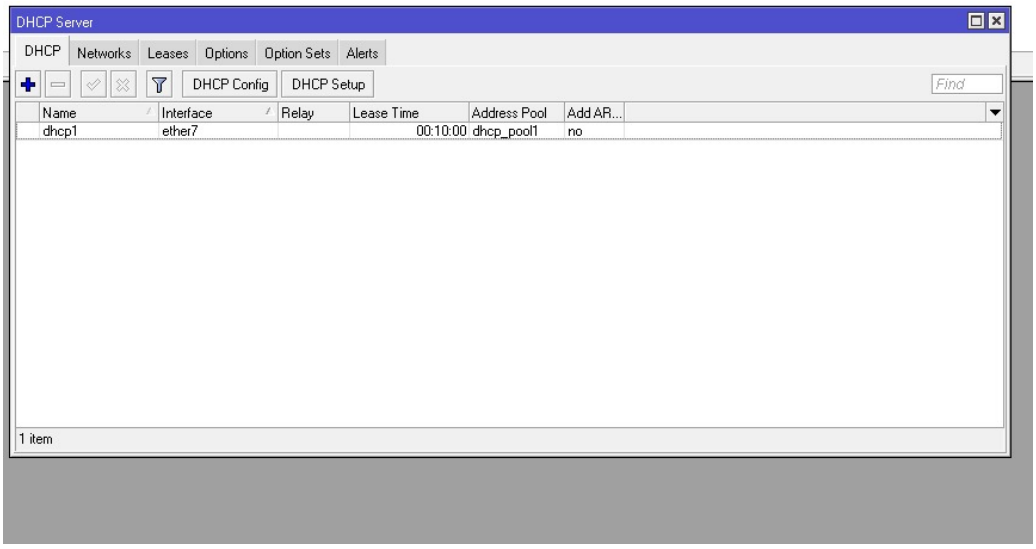
Konfigurasi NAT



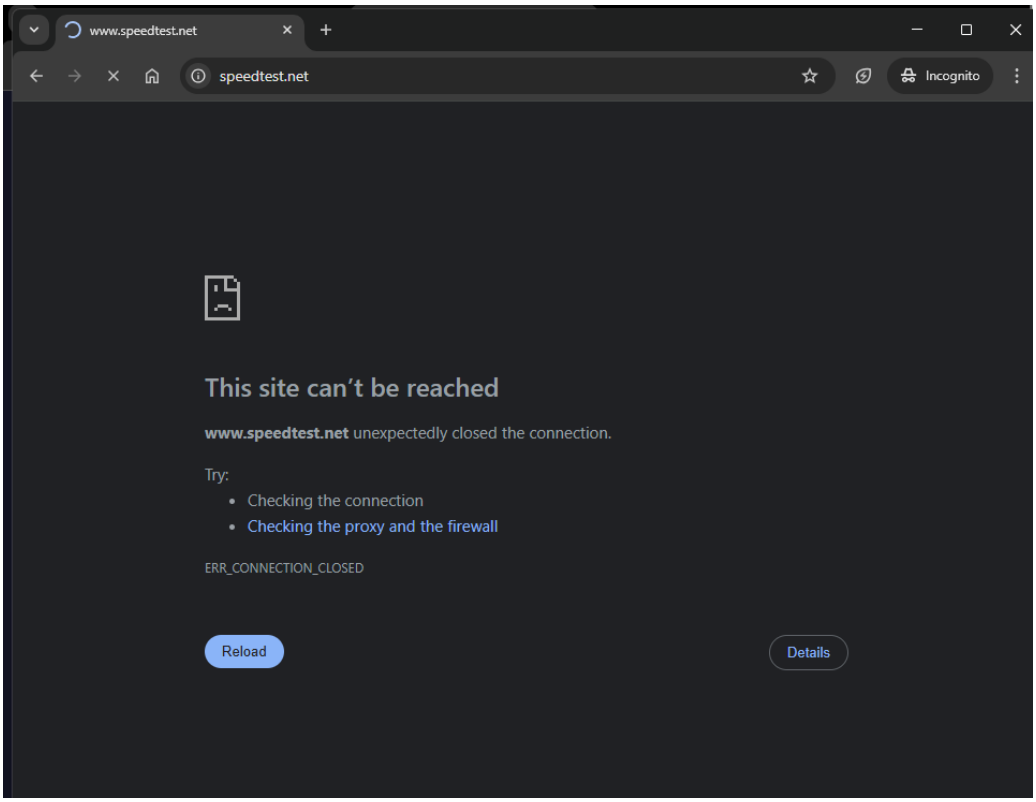
Konfigurasi Firewall dan pemblokiran akses



Konfigurasi DHCP client dan alamat IP



Konfigurasi DHCP server pada Ether7



Berhasil memblokir situs speedtest melalui firewall

Berhasil memblokir ICMP melalui firewall