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

Laporan Akhir
Praktikum Jaringan Komputer

Firewall dan NAT

Rendy Lexxy Kurniawan - 5024231007

2025

1 Langkah-Langkah Percobaan

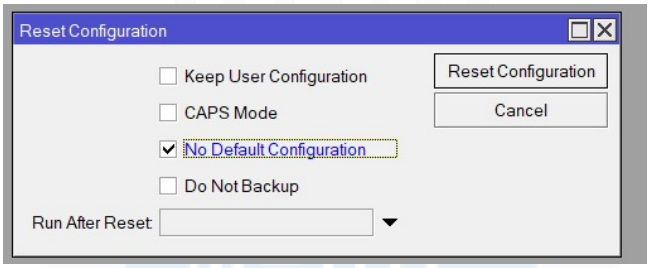
1.1 Alat dan Bahan

Alat dan bahan yang dipersiapkan untuk praktikum ini meliputi:

- Laptop
- Router MikroTik (2 unit)
- Adapter LAN ke USB (opsional, jika laptop tidak memiliki port LAN)
- Kabel LAN UTP

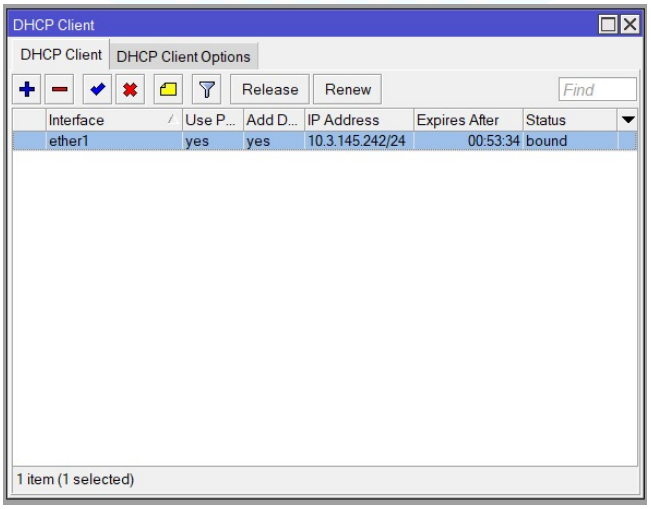
1.2 Konfigurasi Router

1. Hubungkan Laptop dengan Router melalui kabel lan dan login pada aplikasi WinBox
2. Reset Router sebelum memulai praktikum pada aplikasi WinBox dengan Reset Configuration



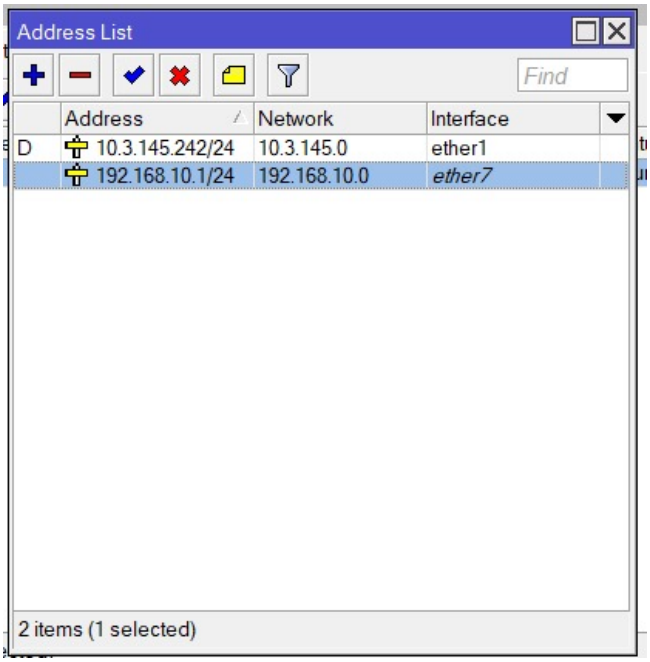
Gambar 1: Reset Configuration Router

3. Konfigurasi DHCP Client pada Router A, dengan memilih Ether 1 sebagai Interface, pastikan status koneksi "bound"



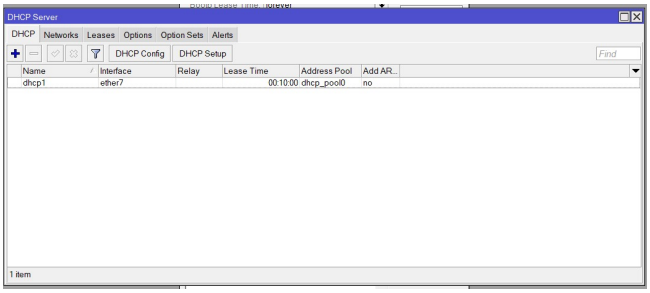
Gambar 2: DHCP Client dengan interface ether1

4. Tambahkan alamat ip 192.168.10.1/24 dengan interface ether7 pada bagian addresses



Gambar 3: Penambahan IP pada ether7

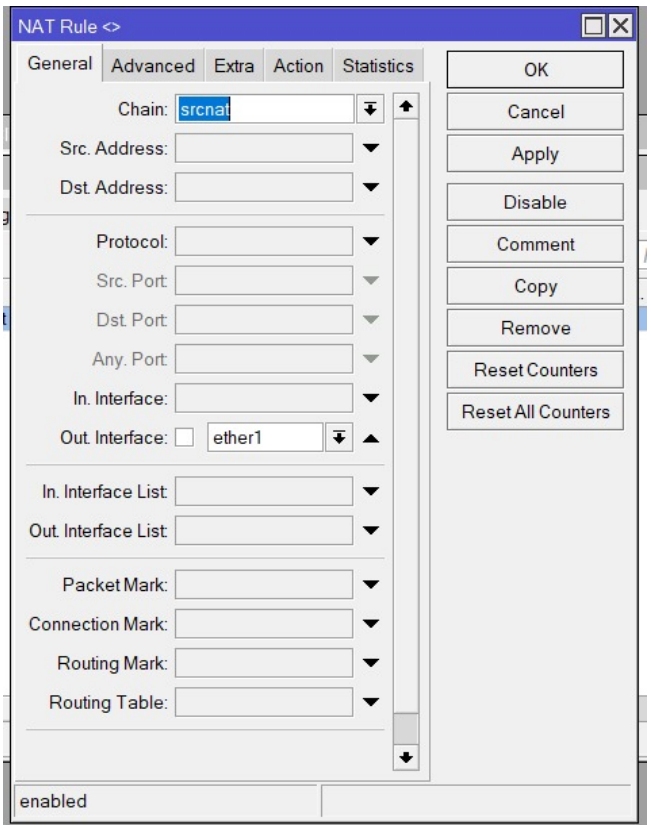
5. Konfigurasi DHCP Server dilakukan agar IP Address yang sudah diset dapat didistribusikan kepada perangkat klien yang terhubung melalui interface yang dipilih, hal ini dilakukan dengan set interface ether7



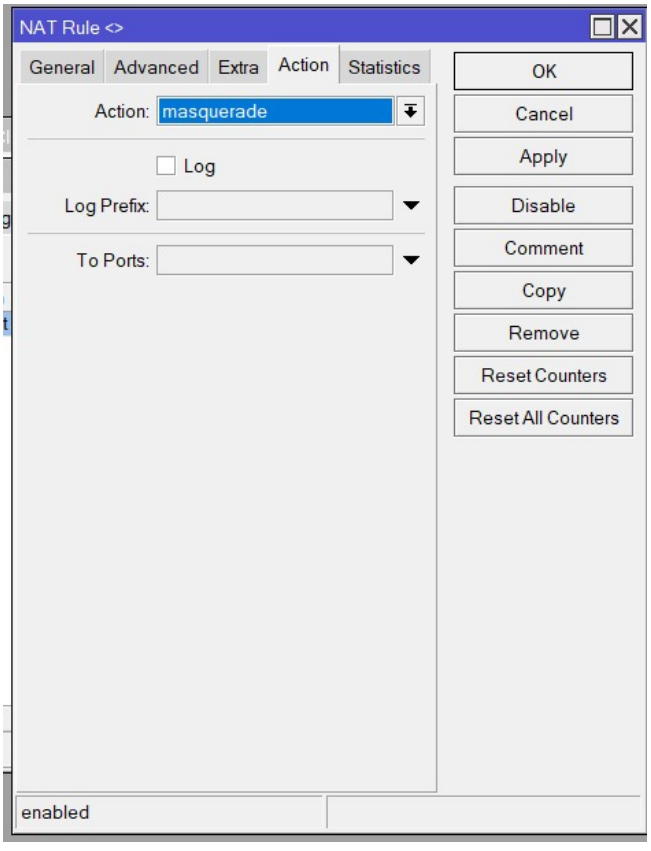
Gambar 4: DHCP Server pada interface ether7

1.3 Konfigurasi NAT

Pada bagian IP - Firewall, pilih bagian NAT dan membuat aturan NAT baru dengan chain: scr-nat dan action: masquerade. Kemudian, dicoba ping ke 8.8.8.8 sebagai Google DNS Server. Hal ini untuk membuktikan bahwa NAT berhasil mengganti local IP menjadi public IP dan mendapatkan echo reply yang mengindikasikan kesuksesan konfigurasi NAT.



Gambar 5: Konfigurasi NAT - General

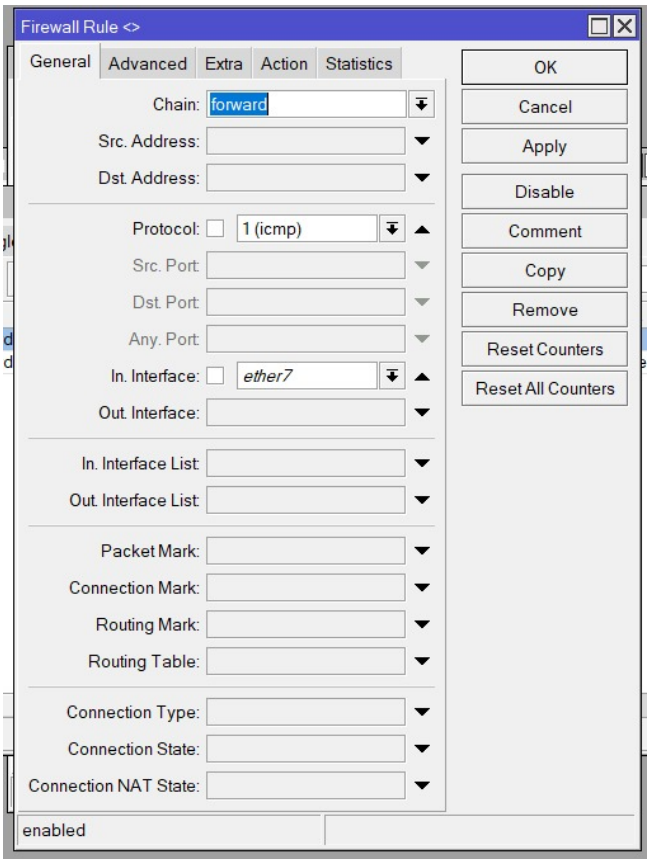


Gambar 6: Konfigurasi NAT - Action

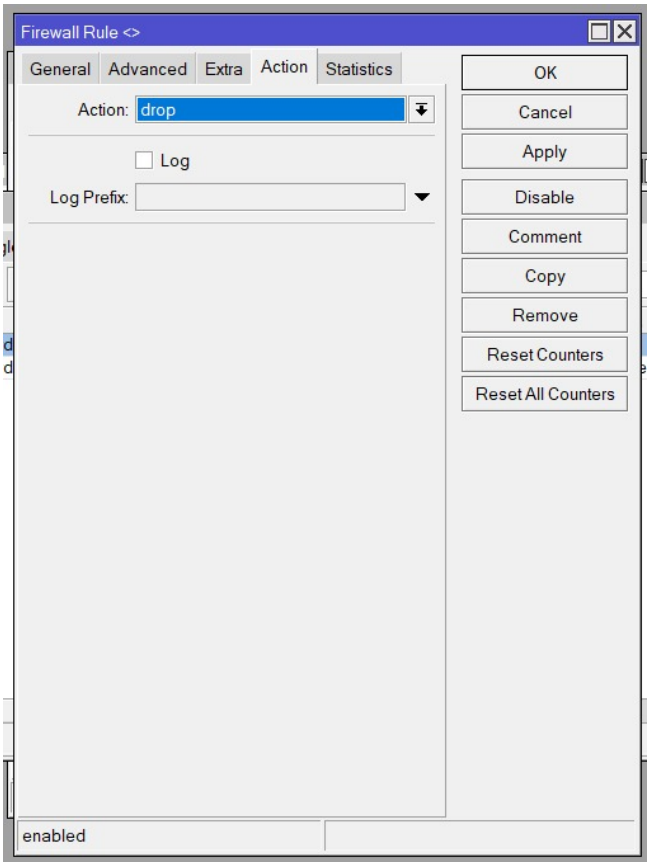
1.4 Konfigurasi Firewall

Pada bagian IP, pilih bagian Firewall untuk mengkonfigurasi beberapa hal, yaitu :

1. Membuat aturan filter pada firewall
2. Pemblokiran ICMP (Internet Control Message Protocol), dengan chain: forward, protocol: icmp, Input Interface: ether7, dan action: drop.

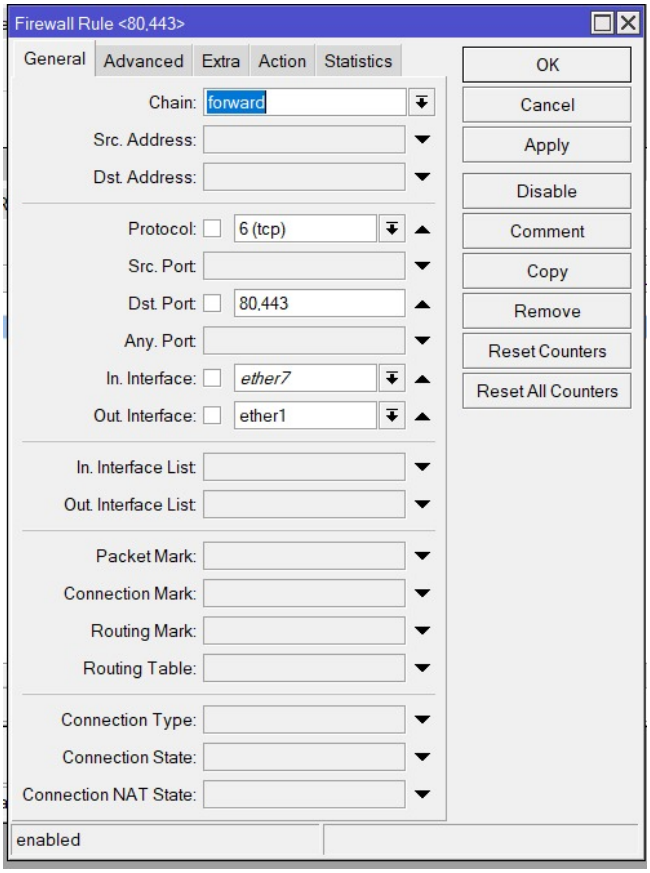


Gambar 7: Firewall Pemblokiran ICMP

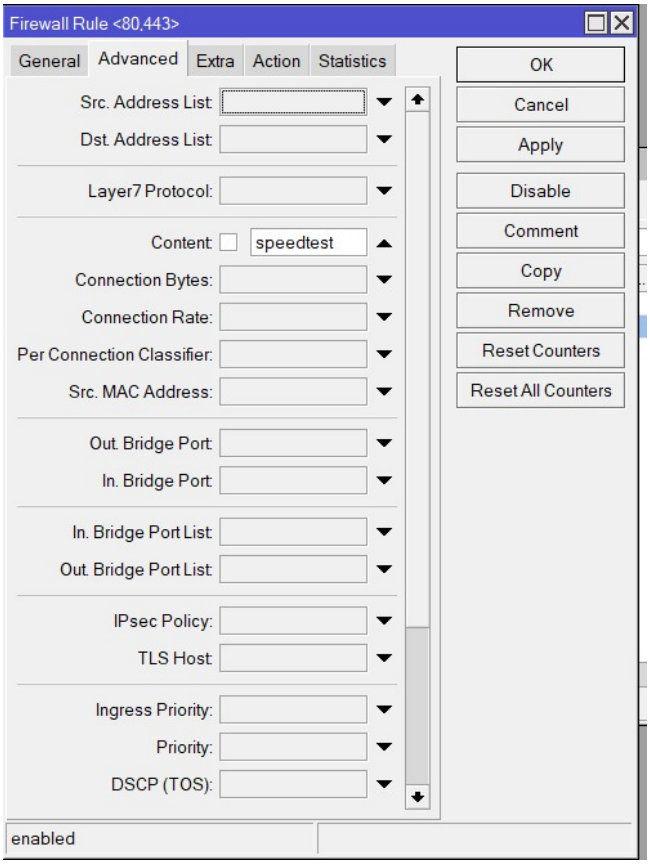


Gambar 8: Firewall Pemblokiran ICMP - Action Drop

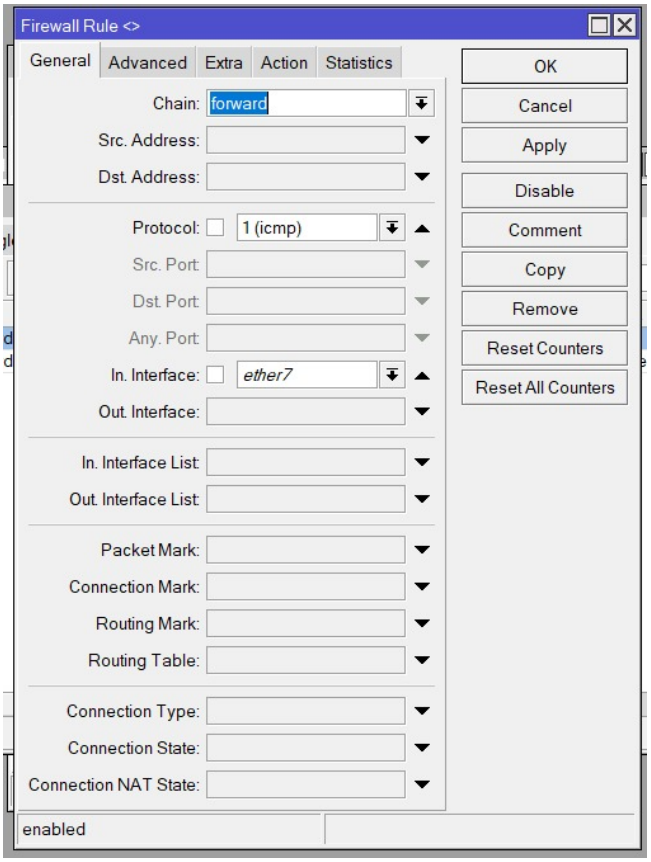
3. Pemblokiran akses situs web tertentu berdasarkan konten websitenya. Pada bagian ini, firewall akan membuat rule untuk block akses terhadap website tertentu. Dengan chain: forward, protocol : tcp, destination port: 80.443, input interface: ether7, dan output interface: ether1. Lalu, pada bagian advanced, pilih content: speedtest, serta pada bagian action: drop.



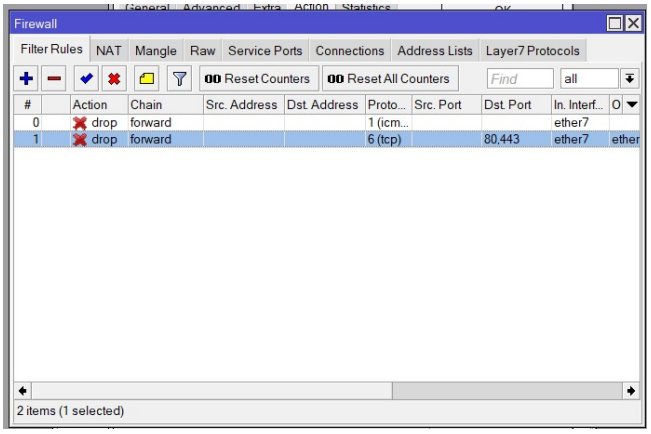
Gambar 9: Konfigurasi Firewall Pemblokiran Konten



Gambar 10: Firewall Pemblokiran Konten Speedtest



Gambar 11: Firewall Pemblokiran Konten - Action Drop

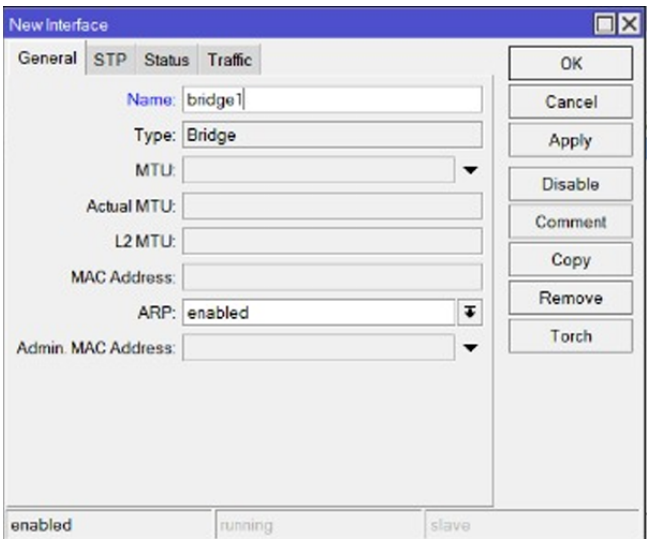


Gambar 12: List Rule Firewall Pemblokiran ICMP dan Pemblokiran Konten Speedtest

1.5 Konfigurasi Bridge

1. Router B pada modul ini akan digunakan sebagai Hub/Bridge, ini bisa dilakukan dengan mengakses menu Bridge dan menambahkan Bridge Baru.

2. Kemudian, tambahkan port pada menu bridge dengan memilih interface yang terhubung dengan router A dan port yang terhubung dengan laptop



Name: bridge1

Type: Bridge

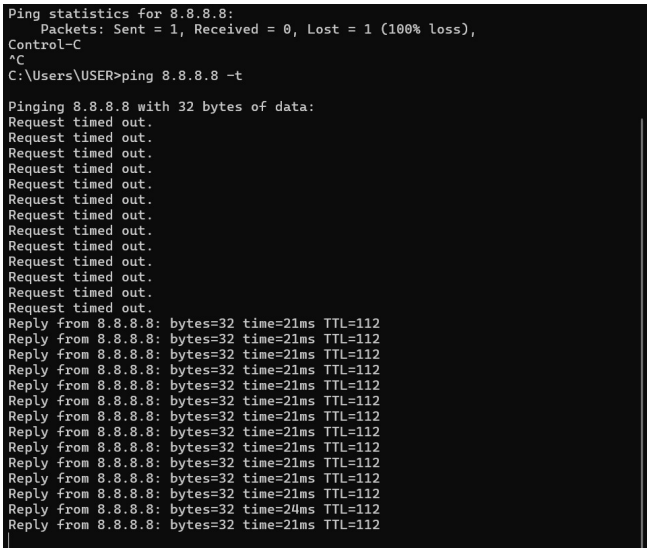
ARP: enabled

enabled

Gambar 13: Konfigurasi Bridge Baru

1.6 Konfigurasi Alamat IP dan PING

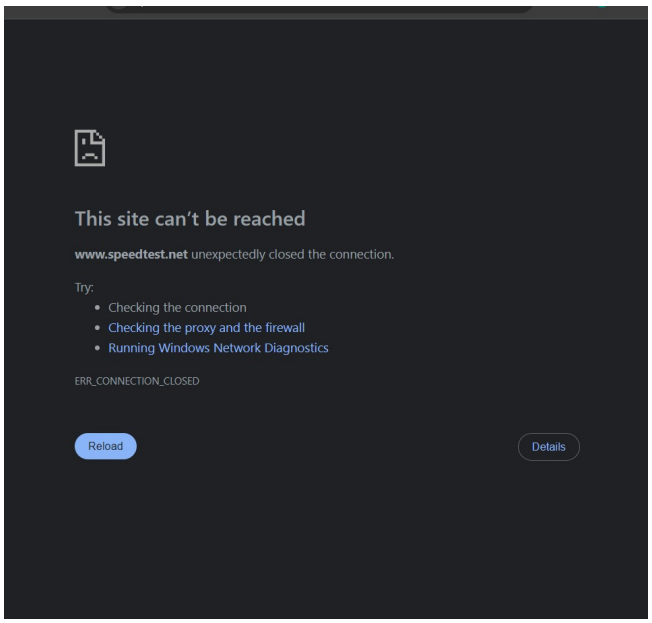
1. Konfigurasi alamat IP pada laptop sesuai dan mengikuti DHCP, lalu verifikasi alamat IP laptop dengan command "ipconfig" pada cmd.
2. Terakhir, Uji Coba konfigurasi Firewall dan pemblokiran konten yang sudah di set
   - Pengujian Pemblokiran ICMP dilakukan dengan menggunakan terminal/cmd dan melakukan ping ke 8.8.8.8, firewall sukses apabila hasil ping adalah Request Timed Out (RTO)



```
Ping statistics for 8.8.8.8:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),
Control-C
^C
C:\Users\USER>ping 8.8.8.8 -t

Pinging 8.8.8.8 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 8.8.8.8: bytes=32 time=21ms TTL=112
Reply from 8.8.8.8: bytes=32 time=21ms TTL=112
Reply from 8.8.8.8: bytes=32 time=21ms TTL=112
Reply from 8.8.8.8: bytes=32 time=21ms TTL=112
Reply from 8.8.8.8: bytes=32 time=21ms TTL=112
Reply from 8.8.8.8: bytes=32 time=21ms TTL=112
Reply from 8.8.8.8: bytes=32 time=21ms TTL=112
Reply from 8.8.8.8: bytes=32 time=21ms TTL=112
Reply from 8.8.8.8: bytes=32 time=21ms TTL=112
Reply from 8.8.8.8: bytes=32 time=21ms TTL=112
Reply from 8.8.8.8: bytes=32 time=21ms TTL=112
Reply from 8.8.8.8: bytes=32 time=21ms TTL=112
Reply from 8.8.8.8: bytes=32 time=24ms TTL=112
Reply from 8.8.8.8: bytes=32 time=21ms TTL=112
```

Gambar 14: Pengujian Firewall Pemblokiran ICMP

   - Pengujian Pemblokiran Konten pada situs web yang memiliki kata kunci "speedtest", pengujian dilakukan dengan membuka website: www.speedtest.net. Apabila firewall aktif dan konfigurasi sukses, maka website tidak dapat diakses.



Gambar 15: Firewall Pemblokiran ICMP

2 Analisis Hasil Percobaan

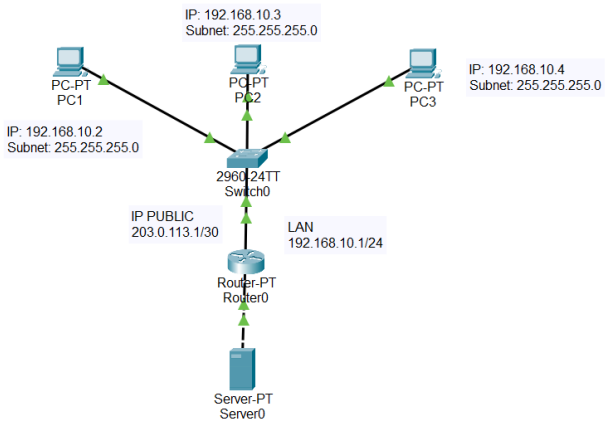
Hasil percobaan menunjukkan dengan jelas bahwa konfigurasi firewall berjalan sesuai ekspektasi. Saat aturan untuk memblokir akses diterapkan, misalnya untuk memblokir ping (protokol ICMP) atau memblokir konten dengan kata kunci tertentu untuk situs web (port 80.443), laptop (client) terbukti tidak dapat terhubung. Sebaliknya, laptop (client) yang diizinkan (tidak diaktifkan firewallnya) dapat berkomunikasi tanpa masalah. Fakta ini membuktikan efektivitas firewall dalam menyaring lalu lintas data sesuai aturan yang telah dibuat. Sebuah aspek menarik lainnya adalah kemampuan stateful inspection firewall. Ketika sebuah koneksi sudah diizinkan, paket balasan dari koneksi tersebut dapat masuk secara otomatis tanpa perlu aturan tambahan, menjadikan firewall tidak hanya aman tetapi juga lebih cerdas dan efisien.

Pengujian Network Address Translation (NAT) menunjukkan fitur masquerading berhasil menyediakan koneksi internet untuk semua komputer di jaringan lokal. Berdasarkan pemeriksaan, alamat IP privat dari setiap komputer (misalnya, 192.168.1.10) terbukti telah ditranslasikan menjadi satu alamat IP publik milik router saat paket dikirim ke internet. Mekanisme ini secara efektif menyembunyikan seluruh perangkat di belakang satu alamat IP, sehingga dari luar terlihat seolah-olah hanya ada satu perangkat yang terhubung. Proses sebaliknya juga berjalan lancar; router dapat dengan tepat meneruskan paket balasan dari internet ke komputer lokal yang sesuai. Hal ini mengindikasikan bahwa mekanisme pelacakan koneksi pada router berfungsi dengan baik.

3 Tugas Modul

1. Buatlah topologi sederhana di Cisco Packet Tracer dengan:
    - 1 Router
    - 1 Switch
    - 3 PC (LAN)

- 1 Server (Internet/Public)

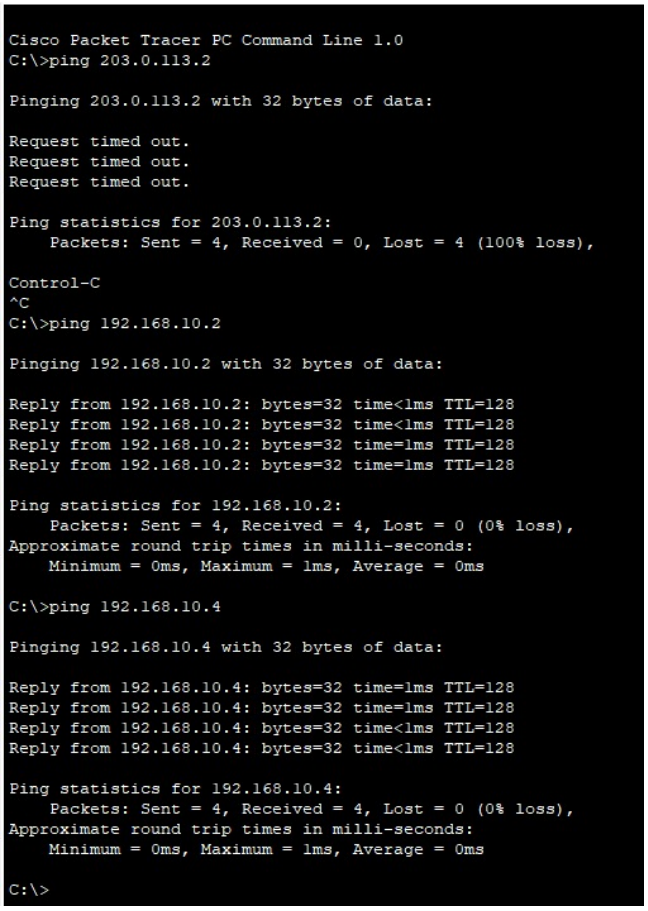


Gambar 16: Topologi

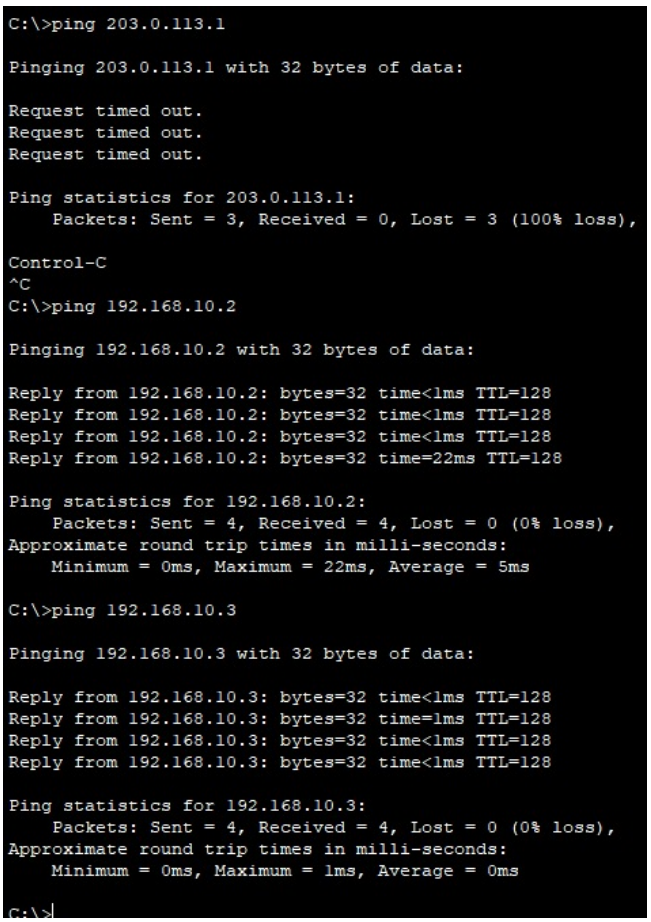
2. Konfigurasi NAT: Buat agar semua PC bisa mengakses Server menggunakan IP publik Router.
3. Konfigurasi Firewall (ACL):
    - Izinkan hanya PC1 yang dapat mengakses Server.
    - Blokir PC1 dan PC3 dari mengakses Server.
    - Semua PC harus tetap bisa saling terhubung di LAN.

```
C:\>ping 203.0.113.2

Pinging 203.0.113.2 with 32 bytes of data:

Reply from 203.0.113.2: bytes=32 time<1ms TTL=255
Reply from 203.0.113.2: bytes=32 time<1ms TTL=255
Reply from 203.0.113.2: bytes=32 time<1ms TTL=255
Reply from 203.0.113.2: bytes=32 time<1ms TTL=255

Ping statistics for 203.0.113.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.10.3

Pinging 192.168.10.3 with 32 bytes of data:

Reply from 192.168.10.3: bytes=32 time<1ms TTL=128
Reply from 192.168.10.3: bytes=32 time<1ms TTL=128
Reply from 192.168.10.3: bytes=32 time<1ms TTL=128
Reply from 192.168.10.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.10.4

Pinging 192.168.10.4 with 32 bytes of data:

Reply from 192.168.10.4: bytes=32 time=1ms TTL=128
Reply from 192.168.10.4: bytes=32 time<1ms TTL=128
Reply from 192.168.10.4: bytes=32 time=11ms TTL=128
Reply from 192.168.10.4: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 11ms, Average = 3ms

C:\>
```

Gambar 17: PC1



Gambar 18: PC2



Gambar 19: PC3

4 Kesimpulan

Jadi, dari semua pengujian ini bisa disimpulkan bahwa firewall dan NAT memiliki peran yang berbeda namun saling melengkapi. Firewall bertindak seperti seorang satpam yang dengan ketat mengatur lalu lintas mana yang boleh masuk dan keluar jaringan berdasarkan serangkaian aturan keamanan yang detail. Sementara itu, NAT berfungsi seperti resepsionis yang membuat semua perangkat di jaringan lokal bisa mengakses internet menggunakan satu identitas publik, sekaligus menyembunyikan struktur asli jaringan internal kita. Ketika kedua teknologi ini digabungkan, kita mendapatkan sebuah jaringan yang tidak hanya aman dari ancaman luar, tetapi juga terstruktur dengan efisien di bagian dalamnya.