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

Laporan Akhir
Praktikum Jaringan Komputer

Firewall dan NAT

Davi Ariq Nugroho - 5024231075

2025

1 Langkah-Langkah Percobaan

1.1 Percobaan 1: Firewall dan NAT

1. Siapkan alat dan bahan yang diperlukan. Lakukan reset pada perangkat Mikrotik melalui aplikasi Winbox dengan memilih opsi "Reset Configuration".

2. Pada Router A, buka menu IP kemudian pilih DHCP Client. Tambahkan konfigurasi pada interface ether1 dengan mencentang opsi "Use Peer DNS" dan "Use Peer NTP". Setelah diterapkan, pastikan status koneksi menunjukkan "Bound".

3. Tambahkan IP Address untuk interface ether7 yang terhubung ke switch. Caranya, masuk ke menu IP, pilih Addresses, lalu tambahkan alamat IP 192.168.10.1/24 pada interface ether7.

4. Konfigurasikan DHCP Server pada router dengan membuka menu IP, pilih DHCP Server, kemudian klik DHCP Setup dan pilih interface ether7. Klik "Next" hingga selesai tanpa mengubah konfigurasi default.

5. Lakukan konfigurasi NAT dengan membuka menu IP, pilih Firewall, kemudian NAT. Tambahkan aturan baru dengan memilih "src-nat" pada tab General dan memilih aksi "masquerade" pada tab Action.

6. Uji koneksi internet dengan membuka New Terminal dan menjalankan perintah ping ke alamat 8.8.8.8.

7. Konfigurasikan firewall untuk memblokir protokol ICMP. Buka menu IP, pilih Firewall lalu Filter Rules. Tambahkan aturan baru dengan Chain "forward", Protocol "icmp", dan In Interface "ether7". Pada tab Action, atur menjadi "drop".

8. Pada Router B, buat bridge baru melalui menu Bridge. Tambahkan dan terapkan pengaturannya.

9. Tambahkan interface yang terhubung ke laptop dan Router A ke dalam bridge melalui menu Bridge kemudian Port.

10. Pastikan pengaturan jaringan pada laptop menggunakan metode DHCP (otomatis), lalu lakukan ping ke situs google.com melalui command prompt.

11. Nonaktifkan aturan firewall ICMP yang telah dibuat sebelumnya dengan cara men-disable peraturan tersebut, kemudian lakukan ping ulang ke google.com untuk memastikan perubahan berhasil.

12. Tambahkan aturan firewall untuk pemblokiran akses situs berdasarkan konten (Content Filtering). Masuk ke menu IP lalu Firewall, kemudian Filter Rules. Tambahkan aturan baru dengan Chain "forward", Protocol "tcp", Destination Port "80,443", In Interface "ether7", dan Out Interface "ether1". Pada tab Advanced, isi Content dengan "speedtest". Pada tab Action, pilih "drop". Namun, pada percobaan ini, pemblokiran tidak berhasil karena laptop masih dapat mengakses konten speedtest.

2 Analisis Hasil Percobaan

Pada tahap awal, router Mikrotik dikembalikan ke kondisi default menggunakan fitur Reset Configuration. Setelah itu, dilakukan pengaturan DHCP Client pada interface `ether1` agar router dapat memperoleh alamat IP secara otomatis dari jaringan luar. Sementara itu, interface `ether7` dikonfigurasi dengan IP statis dan digunakan untuk mendistribusikan alamat IP kepada perangkat di jaringan lokal melalui layanan DHCP Server. Keberhasilan konfigurasi ini ditunjukkan oleh status "Bound" pada DHCP Client serta laptop yang berhasil menerima IP.

Konfigurasi NAT dengan metode masquerade juga berhasil diterapkan. Hal ini terlihat dari kemampuan perangkat dalam jaringan lokal untuk mengakses internet dan melakukan `ping` ke alamat publik seperti `8.8.8.8`, yang menandakan bahwa IP lokal telah berhasil diterjemahkan ke IP publik.

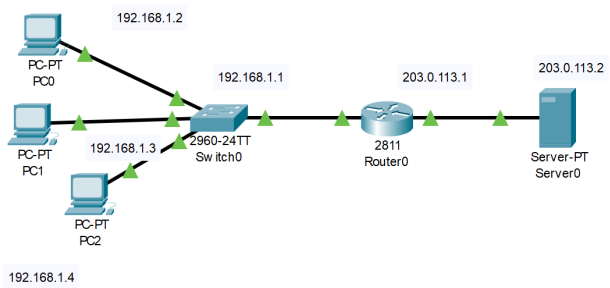
Pengujian firewall dilakukan dengan membuat aturan pemblokiran lalu lintas ICMP melalui *Filter Rule* menggunakan `chain "forward"` dan `protocol "icmp"`. Hasil pengujian menunjukkan bahwa saat aturan ini aktif, laptop gagal melakukan `ping` ke `google.com`, dan saat aturan dinonaktifkan, koneksi kembali normal. Hal ini membuktikan bahwa konfigurasi firewall berfungsi sebagaimana mestinya.

Kemudian dilakukan konfigurasi *bridge* pada Router B dengan menambahkan port yang terhubung ke laptop dan Router A. Pengaturan ini berhasil dilakukan karena koneksi jaringan tetap berjalan dan dapat diakses melalui perangkat laptop.

Pada tahap akhir, dilakukan upaya untuk memblokir konten berdasarkan kata kunci “speedtest” pada protokol TCP dengan port `80` dan `443` menggunakan fitur *content filtering*. Meskipun aturan firewall telah dibuat dengan benar secara teoritis, konten yang dimaksud masih dapat diakses melalui browser. Kemungkinan penyebab kegagalan ini adalah adanya keterbatasan pada sistem Mikrotik yang digunakan atau karena lalu lintas HTTPS (port `443`) bersifat terenkripsi, sehingga Mikrotik tidak dapat membaca isi konten untuk melakukan penyaringan berbasis kata kunci.

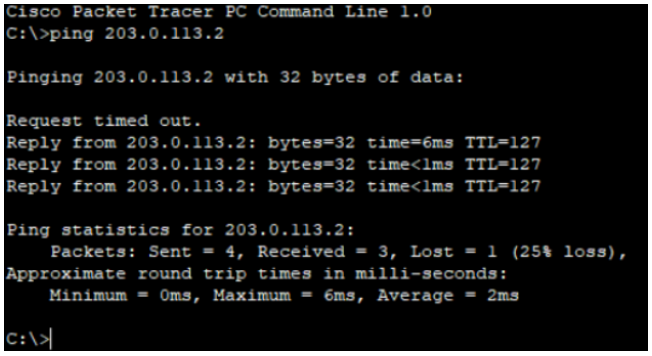
3 Hasil Tugas Modul

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

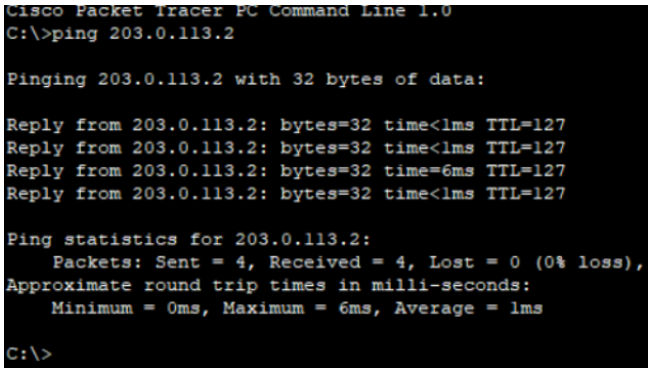


Gambar 1: Topologi

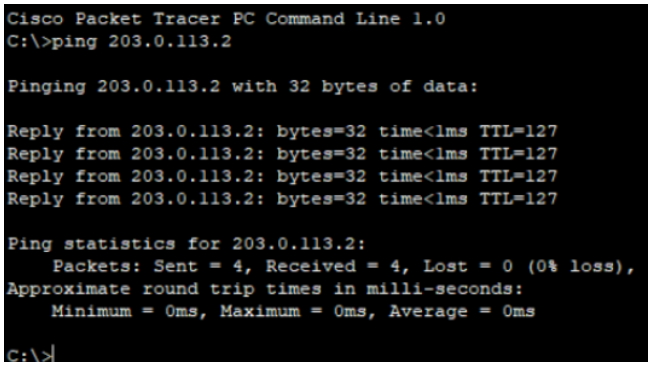
2. Konfigurasi NAT: Buat agar semua PC bisa mengakses Server menggunakan IP publik Router.



Gambar 2: Ping PC1 ke Server



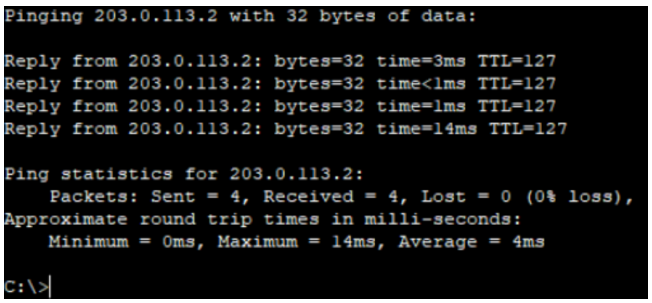
Gambar 3: Ping PC2 ke Server



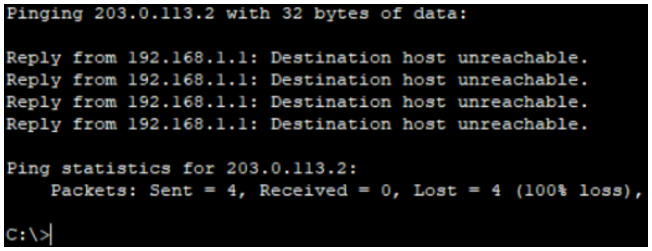
Gambar 4: Ping PC3 ke Server

3. Konfigurasi Firewall (ACL):

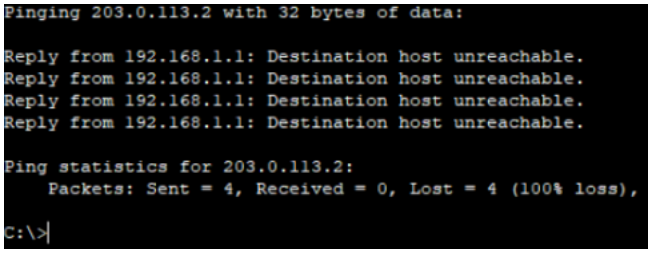
   - Izinkan hanya PC1 yang dapat mengakses Server.
   - Blokir PC1 dan PC3 dari mengakses Server.
   - Semua PC harus tetap bisa saling terhubung di LAN.



Gambar 5: Ping PC1 ke Server dengan konfigurasi firewall ACL



Gambar 6: Ping PC2 ke Server dengan konfigurasi firewall ACL



Gambar 7: Ping PC3 ke Server dengan konfigurasi firewall ACL

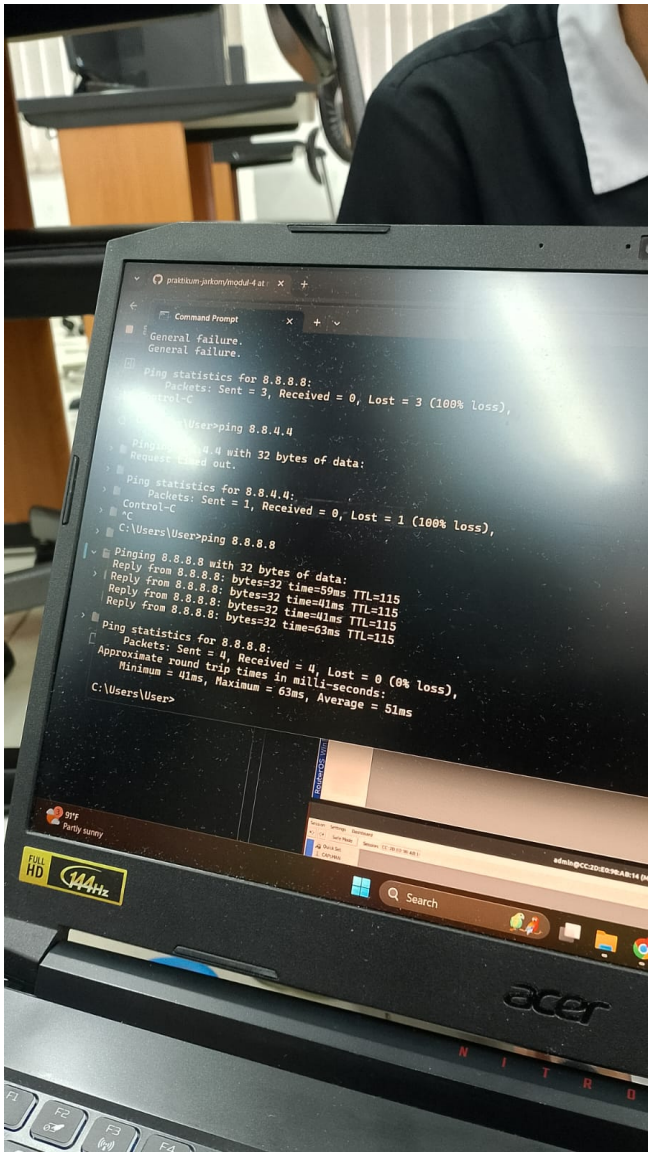
4 Kesimpulan

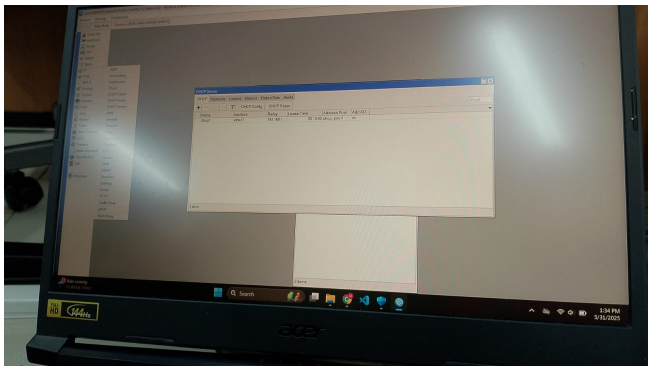
Berdasarkan hasil pengujian konfigurasi Firewall dan NAT pada perangkat Mikrotik, dapat disimpulkan bahwa beberapa pengaturan dasar seperti DHCP Client, penetapan IP statis, implementasi NAT dengan metode masquerade, serta konfigurasi DHCP Server telah berhasil dijalankan dan berfungsi dengan baik. Pengujian terhadap protokol ICMP juga membuktikan bahwa Mikrotik mampu menerapkan pemblokiran lalu lintas sesuai dengan aturan yang ditentukan. Selain itu, proses konfigurasi bridge pada Router B dapat dilakukan tanpa menyebabkan gangguan terhadap konektivitas perangkat pengguna.

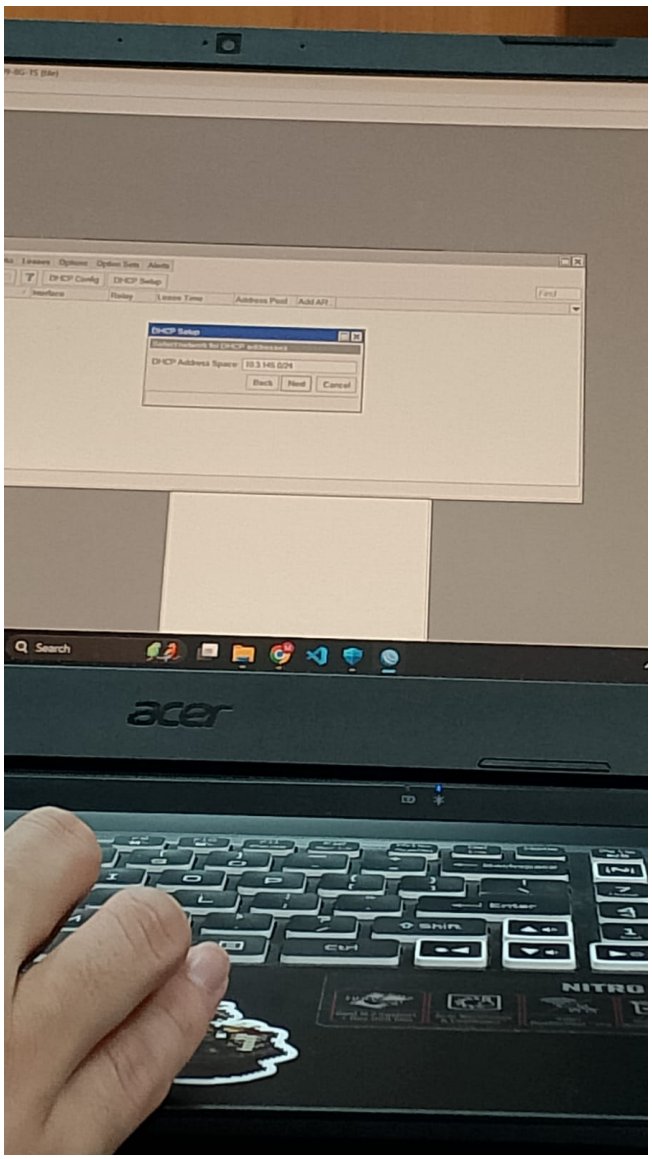
Namun demikian, percobaan penyaringan konten berbasis kata kunci tidak memberikan hasil yang diharapkan. Kegagalan ini menunjukkan bahwa fitur content filtering pada Mikrotik kurang efektif, khususnya dalam memproses lalu lintas HTTPS yang terenkripsi. Selain enkripsi sebagai kendala utama, tidak menutup kemungkinan bahwa terdapat gangguan atau keterbatasan pada sistem Mikrotik yang turut memengaruhi tidak berfungsinya fitur penyaringan secara optimal.

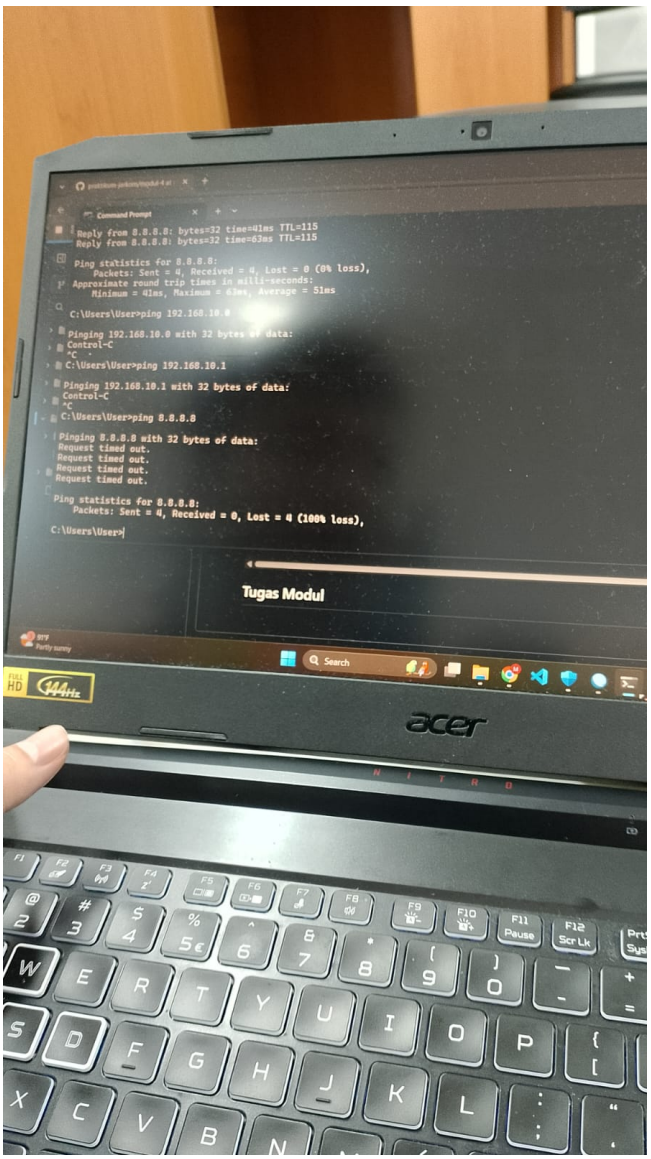
5 Lampiran

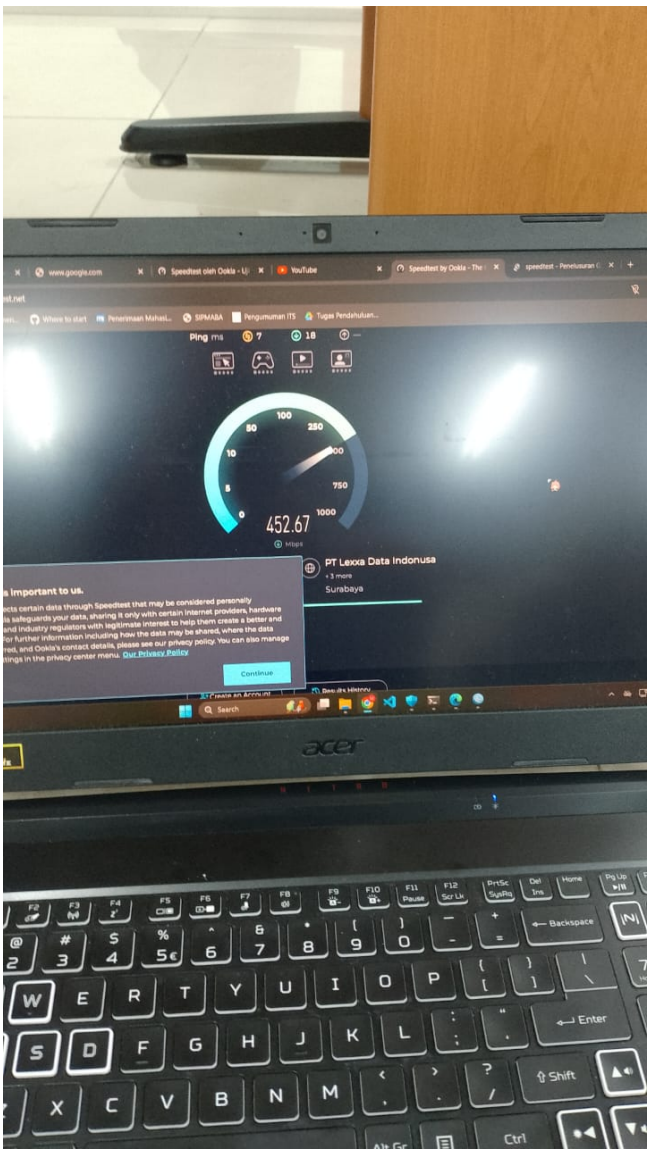
5.1 Dokumentasi saat praktikum






DHCP Setup
DHCP Address Space:
Back
Next
Cancel
Search
acer
NITRO


Command Prompt
Reply from 8.8.8.8: bytes=32 time=41ms TTL=115
Reply from 8.8.8.8: bytes=32 time=63ms TTL=115
Ping statistics for 8.8.8.8:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 41ms, Maximum = 63ms, Average = 51ms
C:\Users\User>ping 192.168.10.0
Pinging 192.168.10.0 with 32 bytes of data:
Control-C
^C
C:\Users\User>ping 192.168.10.1
Pinging 192.168.10.1 with 32 bytes of data:
Control-C
^C
C:\Users\User>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\User>
Tugas Modul
Search
acer



Gambar 8: Dokumentasi saat praktikum