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

# Laporan Sementara
# Praktikum Jaringan Komputer

## Modul Firewall dan NAT

Muhammad Panji Fathuroni - 5024231050

2025

# 1 Pendahuluan

## 1.1 Latar Belakang

Dalam pengelolaan jaringan komputer, keamanan menjadi aspek yang sangat penting untuk memastikan data dan sistem tetap terlindungi dari ancaman luar. Firewall dan Network Address Translation (NAT) adalah dua teknologi kunci yang sering digunakan untuk tujuan ini. Firewall bertugas menyaring lalu lintas jaringan berdasarkan aturan tertentu, sehingga hanya koneksi yang diizinkan saja yang dapat melewati jaringan. Sementara itu, NAT memungkinkan perangkat dalam jaringan lokal menggunakan satu alamat IP publik untuk berkomunikasi dengan jaringan luar, sekaligus menyembunyikan alamat IP internal guna menambah lapisan keamanan.

Melalui praktikum ini, akan mempelajari cara kerja serta implementasi firewall dan NAT dalam lingkungan jaringan komputer. Dengan mengkonfigurasi aturan-aturan dasar pada firewall dan menerapkan NAT, dapat memahami bagaimana kontrol akses dan keamanan jaringan dapat diatur secara efektif. Praktikum ini juga bertujuan untuk membekali keterampilan praktis dalam mengelola keamanan jaringan yang menjadi fondasi penting di dunia profesional teknologi informasi.

## 1.2 Dasar Teori

Dalam pengelolaan jaringan komputer, keamanan menjadi aspek yang sangat penting untuk memastikan data dan sistem tetap terlindungi dari ancaman luar. Firewall dan Network Address Translation (NAT) adalah dua teknologi kunci yang sering digunakan untuk tujuan ini. Firewall bertugas menyaring lalu lintas jaringan berdasarkan aturan tertentu, sehingga hanya koneksi yang diizinkan saja yang dapat melewati jaringan. Sementara itu, NAT memungkinkan perangkat dalam jaringan lokal menggunakan satu alamat IP publik untuk berkomunikasi dengan jaringan luar, sekaligus menyembunyikan alamat IP internal guna menambah lapisan keamanan.

Melalui praktikum ini, mahasiswa akan mempelajari cara kerja serta implementasi firewall dan NAT dalam lingkungan jaringan komputer. Dengan mengkonfigurasi aturan-aturan dasar pada firewall dan menerapkan NAT, mahasiswa dapat memahami bagaimana kontrol akses dan keamanan jaringan dapat diatur secara efektif. Praktikum ini juga bertujuan untuk membekali mahasiswa dengan keterampilan praktis dalam mengelola keamanan jaringan yang menjadi fondasi penting di dunia profesional teknologi informasi.

# 2 Tugas Pendahuluan

1. Jenis NAT yang digunakan dalam kasus ini adalah **Destination NAT (DNAT)** atau dikenal juga dengan istilah **port forwarding**. Dengan DNAT, koneksi dari luar yang menuju IP publik pada port tertentu akan diteruskan ke alamat IP dan port dalam jaringan lokal.

   ### Parameter yang Digunakan

   - **Public IP**: 203.0.113.5 (contoh alamat IP publik)
   - **Port Tujuan dari Luar**: 80 (HTTP)
   - **Private IP**: 192.168.1.10
   - **Port Tujuan di Lokal**: 80

### Logika NAT

Jika ada koneksi dari luar ke alamat IP publik `203.0.113.5` pada port 80, maka koneksi tersebut akan diarahkan ke IP lokal `192.168.1.10` pada port 80.

## Contoh Konfigurasi

### Menggunakan `iptables` (Linux)

```
iptables -t nat -A PREROUTING -p tcp --dport 80 \
  -j DNAT --to-destination 192.168.1.10:80

iptables -t nat -A POSTROUTING -p tcp -d 192.168.1.10 --dport 80 \
  -j MASQUERADE
```

### Menggunakan MikroTik (Command Line)

```
/ip firewall nat add chain=dstnat dst-address=203.0.113.5 \
protocol=tcp dst-port=80 action=dst-nat \
to-addresses=192.168.1.10 to-ports=80
```

## Catatan Penting

- Pastikan firewall tidak memblokir koneksi pada port 80.
- Pastikan web server berjalan dan mendengarkan pada port 80.
- Pastikan IP publik dapat diakses dari jaringan luar.

2. Dalam perancangan dan pengelolaan jaringan komputer, firewall sebaiknya diterapkan terlebih dahulu dibandingkan NAT. Firewall berperan sebagai sistem keamanan utama yang bertugas untuk menyaring lalu lintas jaringan berdasarkan aturan-aturan tertentu. Dengan firewall, administrator dapat mengontrol akses data masuk dan keluar, mencegah ancaman seperti serangan dari luar, port scanning, atau akses tidak sah ke jaringan internal. Sementara itu, NAT (Network Address Translation) lebih berfungsi untuk menerjemahkan alamat IP agar perangkat di jaringan lokal dapat terhubung ke internet menggunakan alamat IP publik. Walaupun NAT memberikan lapisan keamanan tambahan dengan menyembunyikan IP lokal, fungsi utamanya tetap bersifat fungsional, bukan protektif. Oleh karena itu, firewall lebih penting untuk diterapkan lebih dahulu karena memberikan kontrol langsung terhadap keamanan jaringan. NAT dapat diimplementasikan setelah firewall, sebagai bagian dari pengaturan konektivitas yang aman dan efisien.

3. Jika router tidak diberi filter firewall sama sekali, maka jaringan menjadi sangat rentan terhadap berbagai ancaman dari luar. Tanpa adanya penyaringan lalu lintas, semua data yang masuk dari internet akan diteruskan langsung ke perangkat di jaringan internal tanpa kontrol. Hal ini membuka peluang besar bagi serangan seperti port scanning, brute-force, serta eksploitasi terhadap celah keamanan pada sistem atau aplikasi yang berjalan di dalam jaringan. Selain itu,

perangkat-perangkat internal berisiko tinggi terinfeksi malware yang dapat menyebar dengan cepat dan bahkan menjadikan jaringan sebagai bagian dari botnet. Tanpa firewall, data sensitif yang seharusnya hanya diakses secara lokal juga dapat terekspos dan diakses oleh pihak luar tanpa otorisasi. Tidak adanya pembatasan lalu lintas juga dapat menyebabkan jaringan digunakan secara tidak semestinya, seperti untuk mengakses layanan ilegal atau menyedot bandwidth secara berlebihan. Lebih buruk lagi, tanpa firewall, administrator jaringan kehilangan kemampuan untuk mendeteksi, memantau, dan menanggulangi lalu lintas berbahaya secara dini. Oleh karena itu, penggunaan firewall sangat penting untuk menjaga keamanan, kestabilan, dan integritas jaringan secara keseluruhan.