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

Laporan Sementara
Praktikum Jaringan Komputer

Firewall dan NAT

Danendra Galang Yugastama - 5024231049

31 Mei 2025

1 Pendahuluan

1.1 Latar Belakang

Keamanan jaringan merupakan aspek penting dalam menjaga kestabilan dan perlindungan sistem komunikasi data. Salah satu mekanisme yang digunakan untuk mengontrol akses ke dalam jaringan adalah firewall. Firewall bertugas menyaring lalu lintas data berdasarkan aturan yang telah ditentukan, sehingga hanya data yang diizinkan saja yang dapat masuk atau keluar dari jaringan. Dengan fungsinya tersebut, firewall dapat mencegah akses tidak sah, serta melindungi jaringan dari berbagai potensi serangan seperti malware, peretasan, dan upaya penyusupan lainnya.

Selain firewall, Network Address Translation (NAT) juga memiliki peran penting dalam pengelolaan dan pengamanan jaringan. NAT bekerja dengan cara mengubah alamat IP pada paket data, sehingga perangkat dalam jaringan lokal dapat berbagi satu alamat IP publik saat berkomunikasi dengan internet. Teknik ini tidak hanya membantu menghemat penggunaan alamat IP publik, tetapi juga menyembunyikan struktur internal jaringan dari pihak luar. Penggunaan NAT dan firewall secara bersamaan menjadi strategi efektif dalam membangun jaringan yang efisien sekaligus aman dari berbagai ancaman eksternal.

1.2 Dasar Teori

Firewall merupakan salah satu komponen penting dalam sistem keamanan jaringan yang berfungsi untuk mengatur dan mengontrol lalu lintas data berdasarkan aturan yang telah ditentukan. Dengan menerapkan kebijakan tertentu, firewall dapat memfilter paket data yang masuk dan keluar dari suatu jaringan guna mencegah akses yang tidak sah dan melindungi sistem dari berbagai ancaman, seperti serangan malware atau peretasan. Firewall dapat berupa perangkat keras maupun perangkat lunak, dan bekerja berdasarkan parameter seperti alamat IP, nomor port, serta jenis protokol. Jenis-jenis firewall yang umum digunakan antara lain adalah packet filtering, stateful inspection, dan application-layer firewall.

Sementara itu, Network Address Translation (NAT) adalah teknik yang digunakan untuk mengubah alamat IP sumber atau tujuan dari paket data saat melewati perangkat jaringan seperti router. NAT memungkinkan beberapa perangkat dalam jaringan lokal yang menggunakan alamat IP privat untuk berkomunikasi ke jaringan publik (misalnya internet) dengan menggunakan satu atau beberapa alamat IP publik. Selain menghemat penggunaan IP publik, NAT juga meningkatkan keamanan jaringan karena menyembunyikan alamat IP internal dari jaringan luar. Beberapa bentuk NAT yang umum digunakan antara lain Static NAT, Dynamic NAT, dan Port Address Translation (PAT).

2 Tugas Pendahuluan

1. Jika kamu ingin mengakses web server lokal (IP: 192.168.1.10, port 80) dari jaringan luar, konfigurasi NAT apa yang perlu kamu buat?

   Jawaban:
   Konfigurasi NAT yang perlu dibuat adalah *Port Forwarding* (juga dikenal sebagai *Static NAT* atau *Destination NAT*). Dengan port forwarding, permintaan dari IP publik router diarahkan ke alamat IP privat web server.

Contoh konfigurasi:

- **Public IP**: 123.123.123.1 (IP publik router)
- **Port**: 80
- **Internal IP**: 192.168.1.10
- **Internal Port**: 80

Artinya, setiap kali ada permintaan dari luar ke 123.123.123.1:80, router akan meneruskannya ke 192.168.1.10:80.

2. Menurutmu, mana yang lebih penting diterapkan terlebih dahulu di jaringan: NAT atau Firewall? Jelaskan alasanmu.

   Jawaban:
   Secara fungsional, **NAT perlu diterapkan lebih dulu** agar perangkat di jaringan lokal bisa terhubung ke internet, terutama jika menggunakan alamat IP privat. Namun, dari sisi keamanan, **firewall lebih penting** karena berfungsi sebagai pelindung utama dari ancaman luar.

3. Apa dampak negatif jika router tidak diberi filter firewall sama sekali?

   Jawaban:
   Tanpa filter firewall, router akan **membuka semua akses masuk dan keluar**, yang sangat berbahaya. Dampaknya antara lain:

   - Jaringan rentan disusupi oleh hacker, malware, dan bot.
   - Layanan internal (seperti web server atau file server) bisa diakses bebas dari luar.
   - Tidak ada kontrol terhadap lalu lintas mencurigakan atau berbahaya.
   - Privasi dan data pengguna bisa terekspos.