



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

Laporan Sementara Praktikum Jaringan Komputer

Firewall & NAT

Muhammad Navis Azka Atqiya - 5024231035

2025

1 Pendahuluan

1.1 Latar Belakang

Dalam membangun dan mengelola jaringan komputer, terutama yang terhubung ke internet, diperlukan pemahaman mengenai cara kerja NAT (Network Address Translation) dan firewall. NAT memungkinkan banyak perangkat di jaringan lokal untuk mengakses internet menggunakan satu alamat IP publik, serta memungkinkan layanan seperti web server diakses dari luar jaringan. Sementara itu, firewall berfungsi sebagai sistem keamanan yang mengatur lalu lintas data dan melindungi jaringan dari akses yang tidak sah atau berbahaya. Melalui praktikum ini, mahasiswa akan mempelajari bagaimana mengkonfigurasi NAT dan firewall secara langsung, sehingga dapat memahami perannya dalam pengelolaan jaringan yang aman dan efisien.

1.2 Dasar Teori

NAT (Network Address Translation) adalah suatu metode yang digunakan pada perangkat jaringan, seperti router, untuk menerjemahkan alamat IP privat menjadi alamat IP publik dan sebaliknya. Teknik ini memungkinkan banyak perangkat dalam jaringan lokal dapat mengakses internet secara bersamaan hanya dengan satu alamat IP publik. Selain itu, NAT juga memungkinkan akses dari luar ke perangkat tertentu di jaringan lokal melalui teknik port forwarding, misalnya untuk mengakses server web lokal dari internet. NAT sangat penting dalam konservasi alamat IPv4 yang jumlahnya terbatas, serta berperan dalam menyembunyikan struktur internal jaringan dari dunia luar.

Firewall adalah sistem keamanan jaringan yang berfungsi untuk mengontrol dan menyaring lalu lintas data berdasarkan aturan yang telah ditentukan. Firewall dapat mencegah akses tidak sah dari luar ke dalam jaringan, serta membatasi lalu lintas keluar dari jaringan sesuai kebijakan yang diterapkan. Firewall dapat berupa perangkat keras (hardware) maupun perangkat lunak (software) yang bekerja pada level router, server, atau bahkan komputer pengguna. Dengan adanya firewall, administrator jaringan dapat mengamankan sistem dari ancaman seperti serangan malware, peretasan, atau trafik yang mencurigakan. Penerapan firewall yang baik menjadi salah satu kunci dalam menjaga keamanan dan kestabilan jaringan komputer.

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?

Menggunakan konfigurasi NAT berupa Destination NAT (DNAT) atau port forwarding pada router yang memiliki akses ke internet. Konfigurasi ini bertujuan agar setiap permintaan dari jaringan luar yang masuk ke IP publik router pada port tertentu, misalnya port 80 dapat diteruskan ke IP lokal 192.168.1.10 port 80.

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

Firewall sebaiknya diterapkan terlebih dahulu karena Firewall berperan sebagai pertahanan utama yang mengatur lalu lintas data berdasarkan aturan tertentu, sehingga dapat mencegah akses yang

tidak sah atau berbahaya dari luar. Sementara NAT hanya bertugas menerjemahkan alamat IP dan tidak memiliki kemampuan untuk menyaring atau memblokir koneksi yang berbahaya.

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

Jaringan menjadi sangat rentan terhadap serangan dari luar. Tanpa firewall, semua koneksi dari internet dapat langsung masuk ke perangkat lokal tanpa penyaringan, sehingga berisiko terkena serangan seperti malware, brute-force, atau akses ilegal.