



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

Laporan Sementara

Praktikum Jaringan Komputer

Modul Firewall dan NAT

Ahmad Dafa Salam - 5024231024

30 MEI 2025

1 Pendahuluan

1.1 Latar Belakang

Praktikum ini bertujuan untuk mempelajari cara kerja firewall, NAT, dan connection tracking dalam pengelolaan dan pengamanan jaringan. Ketiga teknologi ini penting untuk melindungi jaringan dari akses tidak sah, mengatur lalu lintas data, dan memungkinkan banyak perangkat berbagi satu IP publik secara efisien.

1.2 Dasar Teori

Firewall adalah sistem keamanan jaringan yang mengontrol lalu lintas data masuk dan keluar berdasarkan aturan tertentu. Firewall dapat diimplementasikan dalam bentuk perangkat keras (hardware) maupun perangkat lunak (software), dan terbagi menjadi beberapa jenis, seperti packet filtering, stateful inspection, application layer firewall, hingga next generation firewall. Setiap jenis memiliki cara kerja dan tingkat pengamanan yang berbeda, mulai dari menyaring berdasarkan alamat IP hingga melakukan inspeksi terhadap isi data secara mendalam (deep packet inspection).

Network Address Translation (NAT) adalah metode untuk mengubah alamat IP sumber dalam paket data ketika melewati router. NAT biasanya digunakan untuk mengatasi keterbatasan jumlah IP publik dengan memungkinkan beberapa perangkat dalam jaringan lokal berbagi satu alamat IP publik. Ada beberapa jenis NAT, antara lain Static NAT, Dynamic NAT, dan Port Address Translation (PAT), yang masing-masing memiliki kegunaan tersendiri tergantung kebutuhan jaringan.

Connection Tracking atau pelacakan koneksi adalah fitur yang mencatat dan memantau status koneksi jaringan. Dengan mencatat informasi seperti alamat IP sumber dan tujuan, port, protokol, serta status koneksi, sistem dapat mengenali apakah suatu paket merupakan bagian dari koneksi yang sah. Connection tracking sangat berguna untuk firewall berbasis status (stateful firewall) dan dalam penerapan NAT, karena membantu mengidentifikasi dan mengelola lalu lintas data dengan lebih akurat.

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?**

Konfigurasi NAT yang perlu dibuat adalah *Static NAT* atau *Port Address Translation (PAT)*. Static NAT digunakan jika satu IP publik dipetakan langsung ke satu IP privat, cocok untuk server seperti web server. Dalam hal ini, IP publik akan memetakan port 80 langsung ke IP lokal 192.168.1.10 port 80, sehingga server lokal dapat diakses dari luar jaringan.

Referensi: Pada bagian 1.2.1 *Jenis-Jenis NAT*.

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

Firewall lebih penting diterapkan terlebih dahulu karena bertugas sebagai pengawas dan penjaga akses lalu lintas jaringan. Firewall akan memeriksa apakah paket data yang masuk atau

keluar diperbolehkan sesuai dengan aturan. Sementara itu, NAT hanya mengatur penerjemahan alamat IP tanpa fitur keamanan. Oleh karena itu, firewall menjadi komponen utama dalam menjaga keamanan jaringan.

Referensi: Pada bagian *1.1 Apa itu Firewall?* dan *1.1.2 Cara Kerja Firewall*.

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

Jika router tidak memiliki filter firewall, maka semua lalu lintas akan diizinkan masuk dan keluar tanpa kontrol. Hal ini berbahaya karena:

- Router tidak bisa membedakan antara lalu lintas sah dan berbahaya.
- Potensi serangan dari luar seperti malware dan hacker meningkat.
- Tidak ada mekanisme pemblokiran otomatis untuk koneksi tidak sah.

Ini membuat jaringan menjadi sangat rentan terhadap gangguan keamanan.

Referensi: Pada bagian *1.1 Apa itu Firewall?* dan *1.1.2 Cara Kerja Firewall*.