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

Laporan Sementara
Praktikum Jaringan Komputer

Firewall & NAT

Davi Ariq Nugroho - 5024231075

2025

1 Pendahuluan

1.1 Latar Belakang

Perkembangan teknologi jaringan komputer yang semakin pesat menuntut adanya sistem yang aman dan efisien dalam pengelolaan jaringan. Saat ini, jaringan komputer tidak hanya digunakan dalam skala lokal, tetapi juga memungkinkan koneksi ke sumber daya global seperti internet. Namun, perluasan konektivitas ini juga meningkatkan risiko terhadap ancaman keamanan, seperti akses tidak sah, serangan malware, dan penyalahgunaan data.

Untuk menjaga keamanan jaringan, diperlukan alat dan metode yang mampu mengatur aliran data yang masuk dan keluar dari jaringan. Salah satu komponen penting yang digunakan adalah *firewall*. *Firewall* berfungsi sebagai garis pertahanan pertama dengan cara menyaring dan memblokir lalu lintas yang mencurigakan berdasarkan kebijakan keamanan yang telah ditentukan. Dengan *firewall*, administrator jaringan dapat mengatur hak akses serta melindungi jaringan dari potensi ancaman.

Di sisi lain, keterbatasan jumlah alamat IP publik juga menjadi tantangan dalam pengelolaan jaringan, terutama bagi organisasi yang memiliki banyak perangkat. *Network Address Translation* (NAT) merupakan solusi yang memungkinkan banyak perangkat dalam jaringan lokal menggunakan alamat IP privat untuk terhubung ke internet melalui satu atau beberapa alamat IP publik. Selain menghemat penggunaan alamat IP, NAT juga menambah lapisan keamanan dengan menyembunyikan alamat IP internal dari jaringan eksternal.

Praktikum ini bertujuan untuk memberikan pemahaman praktis mengenai konfigurasi *firewall* dan NAT, sehingga mahasiswa dapat menerapkan konsep keamanan dan manajemen alamat IP dalam jaringan komputer. Melalui pengalaman ini, diharapkan mahasiswa mampu merancang jaringan yang terhubung dengan baik, sekaligus aman dan efisien.

1.2 Dasar Teori

1.2.1 Firewall

Firewall adalah sistem keamanan jaringan yang berfungsi untuk mengatur dan memantau lalu lintas data yang masuk maupun keluar dari suatu jaringan berdasarkan aturan tertentu. Fungsi utama *firewall* adalah melindungi jaringan dari akses tidak sah dan potensi serangan berbahaya. *Firewall* dapat berupa perangkat keras maupun perangkat lunak, dan umumnya digunakan untuk membatasi akses berdasarkan alamat IP, port, serta jenis protokol yang digunakan.

Jenis-jenis *firewall* yang umum digunakan antara lain:

- **Packet Filtering Firewall**, menyaring paket berdasarkan informasi dalam header paket seperti alamat IP dan port.

- **Stateful Inspection Firewall**, selain memeriksa header paket juga memantau status koneksi, sehingga lebih aman.
- **Application Layer Firewall**, melakukan inspeksi pada lapisan aplikasi untuk mendeteksi ancaman secara lebih spesifik.

1.2.2 Network Address Translation (NAT)

Network Address Translation (NAT) adalah teknik yang digunakan untuk mengubah alamat IP pada header paket data yang melewati sebuah router atau *firewall*. Fungsi utama NAT adalah menghubungkan jaringan lokal yang menggunakan alamat IP privat dengan jaringan publik seperti internet, melalui satu atau beberapa alamat IP publik.

Jenis-jenis NAT yang umum digunakan:

- **Static NAT**, memetakan alamat IP privat ke alamat IP publik secara tetap.
- **Dynamic NAT**, memetakan alamat IP privat ke alamat IP publik dari kumpulan alamat yang tersedia secara dinamis.
- **Port Address Translation (PAT)** atau NAT Overload, memungkinkan banyak perangkat menggunakan satu alamat IP publik dengan membedakan berdasarkan nomor port.

NAT juga memberikan perlindungan tambahan karena alamat IP internal tidak secara langsung terlihat oleh jaringan luar.

1.2.3 Hubungan Firewall dan NAT

Firewall dan NAT umumnya digunakan secara bersamaan untuk mengamankan jaringan sekaligus mengelola penggunaan alamat IP. NAT memungkinkan perangkat dengan IP privat di dalam jaringan lokal mengakses internet melalui IP publik, sedangkan *firewall* berperan dalam membatasi dan melindungi lalu lintas data dari dan menuju jaringan. Kombinasi kedua teknologi ini sangat penting dalam pengelolaan jaringan modern agar tetap aman, efisien, dan terkoneksi dengan baik.

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?**
   Untuk mengakses web server lokal dengan alamat IP 192.168.1.10 pada port 80 dari jaringan luar, konfigurasi NAT yang diperlukan adalah *Destination NAT* (DNAT) atau yang biasa disebut *port forwarding*. Konfigurasi ini memungkinkan router untuk meneruskan permintaan dari jaringan luar ke alamat IP publik router pada port 80, lalu mengarahkan lalu lintas tersebut ke alamat IP privat server, yaitu 192.168.1.10 pada

port yang sama. Dengan demikian, pengguna dari luar jaringan dapat mengakses web server seolah-olah server tersebut berada di jaringan publik. Konfigurasi ini biasanya diterapkan pada router dengan menambahkan aturan NAT yang memetakan IP publik dan port tertentu ke IP dan port milik server internal.

2. **Menurutmu, mana yang lebih penting diterapkan terlebih dahulu di jaringan: NAT atau Firewall? Jelaskan alasanmu.**
   Menurut saya, NAT (Network Address Translation) sebaiknya diterapkan terlebih dahulu dalam jaringan. Hal ini karena NAT berperan sebagai dasar agar perangkat-perangkat dalam jaringan lokal yang menggunakan IP privat dapat terhubung ke jaringan luar seperti internet. Tanpa NAT, perangkat dengan IP privat tidak dapat melakukan komunikasi langsung ke jaringan publik karena alamat tersebut tidak dapat dirutekan di internet. Setelah konektivitas jaringan terbangun melalui NAT, barulah *firewall* diterapkan untuk mengatur serta mengamankan lalu lintas data yang keluar dan masuk jaringan. Dengan demikian, *firewall* berfungsi sebagai pelindung tambahan setelah konektivitas berhasil dibangun. Oleh karena itu, dari segi urutan penerapan, NAT lebih mendasar dan perlu diterapkan lebih dahulu sebelum *firewall*.

3. **Apa dampak negatif jika router tidak diberi filter firewall sama sekali?**
   Jika router tidak dilengkapi dengan *firewall* atau filter sama sekali, maka jaringan akan sangat rentan terhadap berbagai jenis ancaman keamanan, baik dari luar maupun dari dalam jaringan. Tanpa *firewall*, seluruh lalu lintas data akan diizinkan masuk dan keluar tanpa adanya penyaringan atau pembatasan. Hal ini membuka peluang bagi pihak tidak bertanggung jawab, seperti peretas, malware, atau program jahat lainnya untuk mengakses sistem di dalam jaringan. Akibatnya, jaringan dapat mengalami kebocoran data, serangan virus, hingga gangguan serius seperti serangan DDoS atau peretasan. Selain itu, tidak adanya *firewall* juga menyebabkan tidak adanya kontrol terhadap trafik mencurigakan, yang dapat mengganggu performa dan kestabilan jaringan. Dengan kata lain, jaringan tanpa *firewall* sangat terbuka dan tidak terlindungi, sehingga berisiko tinggi menimbulkan kerugian secara teknis maupun operasional.