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

Laporan Sementara
Praktikum Jaringan Komputer

Firewall & NAT

I Gusti Ngurah Eka Febrian Suantara Putra - 5024231078

2025

1 Pendahuluan

1.1 Latar Belakang

Seiring dengan pesatnya kemajuan teknologi jaringan komputer, kebutuhan akan sistem yang aman dan efisien dalam pengelolaan jaringan menjadi semakin penting. Jaringan komputer saat ini tidak hanya terbatas pada komunikasi lokal antar perangkat, tetapi juga membuka akses ke berbagai layanan dan informasi global melalui internet. Namun, kemudahan ini disertai dengan tantangan besar terkait keamanan, seperti risiko akses ilegal, serangan siber, hingga kebocoran data sensitif.

Untuk mengatasi berbagai risiko tersebut, perlu diterapkan mekanisme yang mampu mengatur dan memfilter lalu lintas data yang keluar dan masuk ke dalam jaringan. Salah satu alat utama dalam sistem keamanan jaringan adalah *firewall*, yang berfungsi sebagai penjaga gerbang digital dengan menyaring paket data berdasarkan kebijakan tertentu. Dengan penggunaan firewall yang tepat, administrator dapat menentukan siapa yang boleh mengakses apa, serta mencegah lalu lintas yang mencurigakan masuk ke dalam jaringan.

Selain masalah keamanan, keterbatasan alamat IP publik juga menjadi tantangan tersendiri, terutama dalam jaringan berskala besar. Teknologi *Network Address Translation* (NAT) hadir sebagai solusi dengan memungkinkan banyak perangkat lokal berbagi akses ke internet melalui satu atau beberapa alamat IP publik. Selain membantu menghemat penggunaan IP, NAT juga berkontribusi pada aspek keamanan dengan menyembunyikan struktur internal jaringan dari dunia luar.

Melalui praktikum ini, mahasiswa diajak untuk memahami secara langsung cara kerja dan konfigurasi firewall serta NAT. Tujuannya tidak hanya agar mahasiswa mampu menerapkan konsep dasar keamanan jaringan, tetapi juga dapat merancang sistem jaringan yang efisien, terlindungi, dan sesuai dengan kebutuhan nyata di lapangan.

1.2 Dasar Teori

1.2.1 Firewall

Firewall merupakan sistem pengaman jaringan yang dirancang untuk memantau dan mengatur lalu lintas data berdasarkan aturan yang telah ditentukan. Tujuan utamanya adalah mencegah akses yang tidak sah ke dalam jaringan serta melindungi sistem dari berbagai potensi serangan. Firewall dapat berbentuk perangkat lunak atau perangkat keras, dan umumnya dikonfigurasi untuk membatasi lalu lintas berdasarkan alamat IP, nomor port, atau jenis protokol.

Jenis-jenis firewall yang sering digunakan antara lain:

- **Packet Filtering Firewall**: Menyaring paket berdasarkan informasi header, seperti alamat IP dan port.
- **Stateful Inspection Firewall**: Menganalisis lalu lintas berdasarkan status koneksi dan tidak hanya dari header paket.

- **Application Layer Firewall**: Melakukan pemeriksaan pada tingkat aplikasi, sehingga mampu mendeteksi ancaman secara lebih spesifik.

1.2.2 Network Address Translation (NAT)

Network Address Translation (NAT) adalah mekanisme yang digunakan untuk mengubah alamat IP pada header paket data yang melewati perangkat jaringan seperti router. Fungsinya adalah menjembatani komunikasi antara perangkat dengan alamat IP privat dan jaringan publik seperti internet.

Beberapa tipe NAT yang umum digunakan adalah:

- **Static NAT**: Memetakan satu alamat IP privat ke satu alamat IP publik secara permanen.
- **Dynamic NAT**: Memetakan alamat IP privat ke IP publik yang tersedia secara acak dari sebuah pool.
- **Port Address Translation (PAT)** atau NAT Overload: Menggunakan satu alamat IP publik untuk banyak perangkat dengan membedakan berdasarkan nomor port.

Selain memungkinkan koneksi ke internet, NAT juga membantu menjaga keamanan jaringan dengan menyembunyikan alamat IP internal dari pihak luar.

1.2.3 Hubungan antara Firewall dan NAT

Dalam praktiknya, firewall dan NAT sering digunakan secara bersamaan untuk membangun jaringan yang aman sekaligus efisien. NAT memungkinkan perangkat lokal terhubung ke internet dengan keterbatasan IP publik, sementara firewall bertugas menyaring lalu lintas dan mencegah aktivitas berbahaya. Keduanya saling melengkapi untuk mendukung konektivitas tanpa mengorbankan keamanan.

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 server web lokal dengan IP 192.168.1.10 melalui port 80 dari luar jaringan, dibutuhkan konfigurasi berupa *Destination NAT* (DNAT), atau yang lebih dikenal sebagai *port forwarding*. Dengan konfigurasi ini, router akan meneruskan permintaan dari jaringan eksternal yang masuk ke alamat IP publik pada port 80 ke alamat IP privat 192.168.1.10 di port yang sama. Hal ini memungkinkan pengguna dari luar untuk mengakses layanan web seolah-olah server berada di jaringan publik. Konfigurasi ini biasanya diterapkan melalui aturan NAT di router yang memetakan IP publik dan port tertentu ke alamat dan port internal server.

2. Menurutmu, mana yang lebih penting diterapkan terlebih dahulu di jaringan: NAT atau Firewall? Jelaskan alasanmu.
   Menurut saya, penerapan NAT sebaiknya dilakukan terlebih dahulu. NAT berfungsi sebagai jembatan awal agar perangkat dengan IP privat dalam jaringan lokal dapat terkoneksi dengan jaringan publik. Tanpa NAT, konektivitas ke luar jaringan seperti internet tidak bisa dilakukan karena IP privat tidak bisa dirutekan di internet. Setelah konektivitas terbangun, barulah firewall berperan penting dalam mengamankan lalu lintas data yang mengalir, baik keluar maupun masuk. Dengan demikian, NAT menjadi langkah awal yang esensial sebelum mengimplementasikan mekanisme perlindungan tambahan seperti firewall.

3. Apa dampak negatif jika router tidak diberi filter firewall sama sekali?
   Tanpa adanya filter firewall, jaringan akan sangat terbuka terhadap berbagai bentuk ancaman keamanan. Semua jenis lalu lintas data akan diterima dan diteruskan tanpa penyaringan, memungkinkan pihak tidak bertanggung jawab untuk mengakses sistem internal dengan mudah. Hal ini dapat menyebabkan penyebaran malware, serangan dari luar seperti DDoS, pencurian data, dan gangguan performa jaringan. Tidak adanya firewall juga membuat jaringan sulit dikendalikan secara lalu lintas, yang berisiko menurunkan stabilitas dan keandalan sistem secara keseluruhan. Dalam jangka panjang, kondisi ini dapat menyebabkan kerusakan sistem dan kerugian operasional yang signifikan.