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

Laporan Sementara
Praktikum Jaringan Komputer

Firewall & NAT

Ria Angela Tanujaya - 5024231074

2025

1 Pendahuluan

1.1 Latar Belakang

Dalam perkembangan teknologi informasi saat ini, jaringan komputer memegang peranan penting dalam mendukung berbagai aktivitas, baik di sektor pendidikan, bisnis, pemerintahan, maupun kehidupan sehari-hari. Kebutuhan akan konektivitas yang cepat dan stabil membuat semakin banyak perangkat yang terhubung ke internet. Namun, kondisi ini juga memunculkan risiko yang semakin besar terhadap keamanan jaringan, seperti serangan dari pihak luar, penyebaran malware, hingga pencurian data.Permasalahan utama yang sering dihadapi adalah bagaimana mengatur lalu lintas jaringan agar tetap aman tanpa mengganggu kelancaran komunikasi data. Oleh karena itu, dibutuhkan mekanisme yang mampu mengelola dan mengamankan koneksi jaringan secara efektif. Salah satu solusi yang digunakan adalah firewall, yaitu sistem keamanan yang berfungsi untuk mengontrol lalu lintas data berdasarkan aturan tertentu. Firewall dapat mencegah akses tidak sah dan memblokir potensi ancaman sebelum masuk ke dalam sistem. Selain itu, keterbatasan alamat IP publik menjadi tantangan tersendiri dalam koneksi internet. Untuk mengatasi hal tersebut, digunakan teknologi Network Address Translation (NAT) yang memungkinkan banyak perangkat dalam satu jaringan lokal untuk mengakses internet menggunakan satu alamat IP publik. NAT tidak hanya membantu menghemat penggunaan IP publik, tetapi juga menambah lapisan keamanan dengan menyembunyikan struktur internal jaringan dari pihak luar. Topik firewall dan NAT sangat relevan untuk dipelajari karena kedua teknologi ini banyak digunakan dalam implementasi jaringan modern, baik pada skala kecil seperti rumah dan kantor, maupun skala besar seperti perusahaan dan pusat data. Pemahaman yang baik terhadap cara kerja dan jenis-jenis firewall serta NAT akan memberikan dasar yang kuat dalam merancang jaringan yang aman dan efisien. Melalui praktikum ini, praktikan akan diberikan gambaran tentang bagaimana teknologi tersebut diterapkan dalam situasi nyata, sehingga diharapkan praktikan mampu mengidentifikasi masalah jaringan dan menerapkan solusi yang tepat berbasis firewall dan NAT.

1.2 Dasar Teori

Firewall adalah sistem yang berfungsi sebagai pengatur dan penyaring lalu lintas data antara jaringan internal dan eksternal, berdasarkan aturan yang telah ditentukan. Fungsinya mirip dengan penjaga gerbang yang memutuskan apakah suatu data diizinkan masuk, ditolak, atau diabaikan. Berdasarkan cara kerjanya, firewall memiliki beberapa jenis, antara lain packet filtering, yang menyaring data berdasarkan IP, port, dan protokol; stateful inspection, yang mampu mengenali status koneksi; serta application layer firewall, yang dapat menganalisis data hingga ke tingkat aplikasi seperti HTTP dan FTP. Selain itu, ada Next Generation Firewall (NGFW) yang lebih canggih dengan kemampuan inspeksi data yang mendalam, serta cloud firewall yang dioperasikan melalui layanan berbasis cloud. Setiap jenis firewall ini memiliki keunggulan dan keterbatasan tergantung pada kebutuhan dan skala jaringan yang digunakan. Sementara itu, Network Address Translation (NAT) adalah metode yang digunakan untuk mengubah alamat IP pada paket data ketika melewati perangkat jaringan seperti router. NAT memungkinkan banyak perangkat dalam jaringan lokal dengan alamat IP privat untuk mengakses internet menggunakan satu alamat IP publik. Ini menjadi solusi atas keterbatasan jumlah alamat IPv4 yang tersedia. Terdapat beberapa jenis NAT, yaitu static NAT yang menetapkan satu IP lokal ke satu IP publik secara tetap, dynamic NAT yang menggunakan kumpulan IP publik secara

bergantian, dan Port Address Translation (PAT) yang paling umum digunakan karena memungkinkan banyak perangkat berbagi satu IP publik dengan membedakan koneksi berdasarkan nomor port. NAT juga mengenal beberapa istilah penting seperti inside local address, inside global address, outside local address, dan outside global address, yang menggambarkan posisi dan peran alamat IP dalam proses translasi. Untuk mendukung proses firewall dan NAT, digunakan fitur connection tracking atau pelacakan koneksi. Connection tracking adalah mekanisme yang mencatat informasi penting dari setiap koneksi jaringan, seperti alamat IP sumber dan tujuan, port yang digunakan, protokol, dan status koneksi. Dengan informasi ini, sistem dapat mengenali apakah suatu paket merupakan bagian dari koneksi yang sah, baru, atau tidak valid. Connection tracking sangat penting dalam firewall jenis stateful, karena memungkinkan pengambilan keputusan berdasarkan konteks komunikasi yang sedang berlangsung, bukan hanya berdasarkan informasi paket secara individual.

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?**
   Jika ingin mengakses web server lokal dengan IP `192.168.1.10` melalui port `80` dari jaringan luar, maka konfigurasi NAT yang diperlukan adalah **Static NAT** atau **Destination NAT (DNAT)** dengan *port forwarding*. Konfigurasi ini mengarahkan permintaan dari IP publik router ke IP lokal web server.

   Contoh konfigurasi:

   `203.0.113.1:80` $\rightarrow$ `192.168.1.10:80`

   Dengan konfigurasi tersebut, permintaan dari luar ke alamat IP publik router pada port 80 akan diteruskan ke server lokal pada port yang sama.

2. **Menurutmu, mana yang lebih penting diterapkan terlebih dahulu di jaringan: NAT atau Firewall? Jelaskan alasanmu.**
   Secara teknis, Firewall lebih penting untuk diterapkan terlebih dahulu dibanding NAT. Firewall bertugas sebagai sistem penyaring lalu lintas data dan pelindung jaringan dari akses tidak sah. Meskipun NAT secara tidak langsung dapat membatasi akses dari luar, fungsinya lebih difokuskan pada penerjemahan alamat IP dan bukan sebagai mekanisme pertahanan utama.

   Tanpa firewall, sistem tidak dapat:

   - Menyaring lalu lintas berbahaya.
   - Mencegah akses tidak sah ke perangkat internal.
   - Mengontrol komunikasi antar segmen jaringan.

   Karena itu, firewall perlu diaktifkan terlebih dahulu sebagai garis pertahanan awal sebelum NAT digunakan untuk manajemen lalu lintas IP.

3. **Apa dampak negatif jika router tidak diberi filter firewall sama sekali?**
   Apabila router tidak dikonfigurasi dengan firewall, maka jaringan akan mengalami berbagai kerentanan, antara lain:

- **Tidak ada pembatasan akses dari luar:** Seluruh port dan layanan jaringan terbuka secara bebas tanpa filter.
- **Risiko serangan tinggi:** Rentan terhadap serangan seperti port scanning, DDoS, brute-force, dan eksploitasi layanan terbuka.
- **Penyebaran malware:** Tidak ada sistem untuk memblokir lalu lintas mencurigakan atau berbahaya.
- **Kebocoran data:** Data sensitif bisa diakses dari luar jaringan tanpa deteksi.

4. **Referensi**

- Cisco. (2020). *Cisco Networking Basics: Firewall and NAT*. `https://www.cisco.com`
- IETF. (2001). *RFC 3022: Traditional NAT*. `https://datatracker.ietf.org/doc/html/rfc3022`
- Stallings, W. (2017). *Network Security Essentials: Applications and Standards* (6th ed.). Pearson.
- MikroTik Wiki. *Firewall Configuration*. `https://wiki.mikrotik.com/wiki/Manual:IP/Firewall`