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

Laporan Sementara
Praktikum Jaringan Komputer

Firewall & NAT

Muhammad Rifqi Abdillah - 5024231082

2025

1 Pendahuluan

1.1 Latar Belakang

Dalam era digital saat ini, jaringan komputer telah menjadi tulang punggung berbagai aktivitas, mulai dari komunikasi pribadi hingga operasional bisnis skala besar. Seiring meningkatnya penggunaan internet, ancaman terhadap keamanan jaringan juga ikut meningkat. Untuk itu, perlu adanya mekanisme perlindungan seperti Firewall dan Network Address Translation (NAT) guna memastikan koneksi jaringan tetap aman dan efisien.

Firewall berperan sebagai penjaga gerbang jaringan yang mengatur lalu lintas data berdasarkan aturan tertentu, sehingga dapat mencegah akses yang tidak sah atau berbahaya. Sementara itu, NAT memungkinkan banyak perangkat dalam jaringan lokal untuk terhubung ke internet dengan hanya satu IP publik, yang sangat penting mengingat keterbatasan jumlah IP publik yang tersedia.

Pemahaman terhadap konsep dasar firewall, NAT, dan connection tracking sangat penting sebagai bekal dalam pengelolaan serta pengamanan jaringan. Oleh karena itu, praktikum ini dirancang untuk memperkenalkan dan memperdalam pemahaman mahasiswa mengenai konsep dan implementasi dari teknologi-teknologi tersebut.

1.2 Dasar Teori

Firewall merupakan sistem keamanan jaringan yang bertugas untuk memantau dan mengontrol lalu lintas data yang masuk maupun keluar berdasarkan aturan tertentu. Firewall dapat berbentuk perangkat keras, perangkat lunak, atau gabungan dari keduanya. Tujuan utamanya adalah melindungi jaringan dari akses yang tidak sah atau berbahaya. Terdapat berbagai jenis firewall, mulai dari packet filtering yang hanya memeriksa header paket berdasarkan alamat IP dan port, hingga next generation firewall (NGFW) yang mampu melakukan inspeksi mendalam terhadap isi paket data, bahkan data yang terenkripsi. Firewall lain seperti stateful inspection dapat mengenali apakah suatu paket merupakan bagian dari koneksi yang sah. Selain itu, terdapat juga application layer firewall yang mampu menyaring data hingga ke tingkat aplikasi seperti HTTP atau FTP, serta circuit level gateway yang hanya memverifikasi validitas koneksi tanpa melihat isi data. Firewall berbasis perangkat lunak biasanya terpasang pada sistem operasi dan lebih fleksibel dalam pengaturan, sedangkan hardware firewall adalah perangkat fisik yang ditempatkan di antara jaringan internal dan internet. Di sisi lain, cloud firewall hadir sebagai solusi berbasis layanan awan yang sesuai dengan kebutuhan organisasi modern yang banyak menggunakan cloud computing. Dalam operasionalnya, firewall dapat menerapkan kebijakan akses seperti accept (mengizinkan lalu lintas), reject (menolak dengan memberi balasan error), dan drop (menolak tanpa respon).

Network Address Translation (NAT) adalah teknik yang digunakan untuk menghemat penggunaan alamat IP publik dengan cara menerjemahkan alamat IP lokal ke alamat IP publik. Dengan adanya NAT, satu alamat IP publik dapat digunakan oleh banyak perangkat dalam jaringan lokal untuk mengakses internet secara bersamaan. NAT sangat penting mengingat jumlah alamat IPv4 yang tersedia sangat terbatas. Terdapat tiga jenis NAT, yaitu static NAT yang menghubungkan satu alamat IP lokal ke satu alamat IP publik, dynamic NAT yang menerjemahkan IP lokal dari kumpulan IP publik yang tersedia, dan port address translation (PAT) yang paling umum digunakan karena memungkinkan banyak perangkat menggunakan satu IP publik dengan membedakan koneksi berdasarkan nomor port. NAT biasanya diimplementasikan pada router, dan router akan mencatat semua koneksi dalam se-

buah tabel NAT untuk memastikan paket balasan dari internet dapat dikirimkan kembali ke perangkat yang tepat.

Connection Tracking atau pelacakan koneksi adalah fitur penting yang memungkinkan sistem jaringan mencatat semua koneksi aktif. Fitur ini mencatat alamat sumber, alamat tujuan, nomor port, protokol, dan status koneksi. Dengan adanya connection tracking, firewall dapat mengenali status suatu paket data, apakah merupakan koneksi baru, sah, atau mencurigakan. Misalnya, saat sebuah komputer mengakses situs web, connection tracking akan mencatat koneksi tersebut sehingga ketika server mengirimkan balasan, sistem langsung mengizinkan paket masuk tanpa perlu proses verifikasi ulang. Fitur ini mendukung keamanan jaringan yang lebih baik karena mampu memfilter koneksi berdasarkan statusnya, membantu efisiensi NAT, mengurangi beban pemrosesan pada router, dan memberikan kontrol yang lebih detail terhadap lalu lintas jaringan.

2 Tugas Pendahuluan

1. **Jika ingin mengakses web server lokal (IP: 192.168.1.10, port 80) dari jaringan luar, konfigurasi NAT apa yang perlu dibuat?**
   Untuk mengakses web server lokal dari jaringan luar, kita perlu membuat konfigurasi *Port Forwarding* menggunakan *Static NAT*. Konfigurasi ini akan mengarahkan permintaan dari IP publik (misalnya 203.0.113.1:80) ke IP lokal 192.168.1.10:80.

   Contoh aturan NAT menggunakan `iptables`:

   ```
   iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT --to-destination 192.168.1.10:80
   iptables -t nat -A POSTROUTING -p tcp -d 192.168.1.10 --dport 80 -j MASQUERADE
   ```

2. **Menurutmu, mana yang lebih penting diterapkan terlebih dahulu di jaringan: NAT atau Firewall? Jelaskan alasanmu.**
   Firewall lebih penting diterapkan terlebih dahulu. Alasannya, firewall bertindak sebagai pelindung utama yang menyaring lalu lintas jaringan berdasarkan aturan keamanan. Meskipun NAT penting untuk konektivitas, NAT sendiri tidak memberikan perlindungan dari serangan. Firewall dapat mencegah akses berbahaya dari luar bahkan sebelum NAT bekerja.

3. **Apa dampak negatif jika router tidak diberi filter firewall sama sekali?**
   Jika router tidak diberi filter firewall sama sekali, maka semua lalu lintas masuk akan diterima tanpa pengecekan, sehingga meningkatkan risiko serangan seperti DDoS dan malware. Selain itu, tidak adanya kontrol atas akses jaringan bisa menyebabkan kebocoran data sensitif. Tanpa firewall, router tidak mampu membedakan antara koneksi sah dan tidak sah, yang membuat jaringan menjadi rentan terhadap serangan.