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

Laporan Sementara
Praktikum Jaringan Komputer

Firewall & NAT

Mochamad Rafila Putra Firmansyah - 5024231066

2025

1 Pendahuluan

1.1 Latar Belakang

Dalam era digital yang semakin terhubung, keamanan dan efisiensi pengelolaan jaringan menjadi kebutuhan mendasar dalam pembangunan infrastruktur teknologi informasi. Salah satu tantangan terbesar adalah bagaimana melindungi jaringan internal dari akses tidak sah dan sekaligus memungkinkan konektivitas ke jaringan eksternal seperti internet. Untuk itu, dua konsep utama yang sering diterapkan adalah Firewall dan Network Address Translation (NAT). Firewall berperan sebagai pengendali akses dengan menyaring lalu lintas berdasarkan aturan tertentu, sehingga mampu mencegah berbagai ancaman seperti serangan siber atau malware. Di sisi lain, NAT memecahkan keterbatasan jumlah alamat IP publik dengan menerjemahkan alamat privat ke publik, serta membantu menyembunyikan struktur jaringan internal dari dunia luar. Keduanya bukan hanya solusi teknis, tetapi juga elemen penting dalam arsitektur jaringan modern yang aman, skalabel, dan efisien.

1.2 Dasar Teori

Firewall adalah sistem keamanan jaringan yang dirancang untuk memantau, menyaring, dan mengontrol lalu lintas data masuk dan keluar berdasarkan seperangkat aturan yang telah ditentukan. Tujuan utama firewall adalah melindungi jaringan internal dari ancaman eksternal seperti peretasan, malware, dan akses tidak sah. Firewall dapat berupa perangkat keras (hardware), perangkat lunak (software), atau gabungan keduanya, dan berfungsi sebagai titik kontrol utama antara jaringan terpercaya dan tidak terpercaya. Ada beberapa jenis firewall, seperti packet-filtering firewall, stateful inspection firewall, application-layer firewall, dan next-generation firewall (NGFW), masing-masing dengan pendekatan dan kemampuan filtering yang berbeda-beda tergantung pada kebutuhan keamanan jaringan.

Network Address Translation (NAT) adalah metode yang digunakan dalam jaringan komputer untuk mengubah alamat IP sumber atau tujuan pada paket data saat melewati perangkat jaringan seperti router. Tujuan utama NAT adalah memungkinkan banyak perangkat dalam jaringan lokal (private) untuk mengakses internet menggunakan satu alamat IP publik, serta menyembunyikan struktur internal jaringan dari dunia luar. NAT sangat berguna dalam mengatasi keterbatasan jumlah alamat IPv4 yang tersedia secara global. Terdapat beberapa jenis NAT, di antaranya adalah Static NAT, Dynamic NAT, dan Port Address Translation (PAT), yang masing-masing memiliki karakteristik berbeda dalam hal pemetaan dan fleksibilitas penggunaan alamat IP.

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 memungkinkan akses dari jaringan luar ke web server lokal dengan alamat IP `192.168.1.10` dan port `80`, konfigurasi NAT yang perlu diterapkan adalah **Static NAT dengan Port Forwarding**. Konfigurasi ini akan memetakan alamat IP publik ke alamat IP privat server di port tertentu. Contoh perintah konfigurasinya adalah:

   ```
   ip nat inside source static tcp 192.168.1.10 80 <IP_Publik> 80
   ```

Dengan konfigurasi tersebut, semua permintaan dari luar ke IP publik router pada port 80 akan diteruskan ke server lokal di `192.168.1.10:80`.

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

   Yang lebih penting diterapkan terlebih dahulu adalah **Firewall**, karena firewall berfungsi sebagai lapisan keamanan utama yang melindungi jaringan dari berbagai ancaman seperti akses tidak sah, malware, dan serangan dari luar. Firewall memungkinkan administrator untuk mengatur aturan lalu lintas yang diizinkan atau ditolak berdasarkan IP, port, dan protokol tertentu. Sementara NAT lebih berfokus pada penerjemahan alamat IP untuk keperluan konektivitas, bukan keamanan. Maka dari itu, firewall perlu diaktifkan terlebih dahulu sebelum mengatur koneksi keluar-masuk jaringan.

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

   Jika router tidak dilengkapi dengan firewall, semua lalu lintas data akan masuk dan keluar jaringan tanpa melalui penyaringan. Ini sangat berbahaya karena membuka peluang terjadinya serangan siber seperti *unauthorized access*, *DDoS attack*, dan *data breach*. Perangkat-perangkat dalam jaringan lokal seperti server, komputer, dan IoT device dapat menjadi sasaran serangan langsung dari internet. Ketiadaan firewall membuat jaringan sangat rentan terhadap gangguan keamanan dan kehilangan integritas data.

Referensi

- Kurose, J. F., & Ross, K. W. (2021). *Computer Networking: A Top-Down Approach* (7th ed.). Pearson.
- Cisco Networking Academy. *CCNA: Introduction to Networks v7*.