



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

Laporan Sementara

Praktikum Jaringan Komputer

Modul Firewall dan NAT

Athariq Qurani Fajri - 5024231031

2025

1 Pendahuluan

1.1 Latar Belakang

Dalam era digital yang serba terkoneksi, keamanan jaringan menjadi salah satu aspek penting yang harus diperhatikan oleh setiap individu maupun organisasi. Banyaknya ancaman seperti peretasan, virus, dan akses ilegal menuntut sistem jaringan memiliki perlindungan ekstra. Firewall hadir sebagai garda terdepan yang bertugas menyaring lalu lintas data, sehingga hanya data yang sah dan diizinkan saja yang bisa masuk ke atau keluar dari jaringan internal. Dengan meningkatnya ketergantungan pada internet, keberadaan firewall menjadi mutlak untuk menjaga kerahasiaan dan integritas informasi.

Selain firewall, teknologi Network Address Translation (NAT) juga menjadi komponen penting dalam arsitektur jaringan modern. Dengan terbatasnya jumlah IP publik yang tersedia, NAT memungkinkan banyak perangkat dalam jaringan lokal mengakses internet menggunakan satu IP publik saja. Ini bukan hanya efisien secara teknis dan finansial, tetapi juga memberikan lapisan keamanan tambahan karena menyembunyikan struktur internal jaringan dari dunia luar. Oleh karena itu, pemahaman mendalam tentang Firewall dan NAT sangat dibutuhkan untuk membangun dan menjaga sistem jaringan yang aman dan efisien.

1.2 Dasar Teori

Firewall adalah sistem yang berfungsi untuk mengontrol akses masuk dan keluar dari sebuah jaringan komputer berdasarkan aturan keamanan yang telah ditentukan. Firewall bekerja dengan cara menyaring paket data dan menentukan apakah paket tersebut boleh diteruskan, ditolak dengan pesan kesalahan, atau diabaikan begitu saja. Secara umum, firewall dibagi menjadi beberapa jenis seperti packet filtering, stateful inspection, application layer firewall, dan next generation firewall, yang masing-masing memiliki tingkat kemampuan analisis data yang berbeda.

NAT (Network Address Translation) adalah proses yang dilakukan router untuk mengubah alamat IP dalam paket data, sehingga perangkat dalam jaringan lokal dapat berkomunikasi dengan jaringan publik seperti internet. NAT terdiri dari beberapa jenis yaitu Static NAT, Dynamic NAT, dan PAT (Port Address Translation). Fungsi utama NAT adalah untuk menghemat penggunaan IP publik dan menyembunyikan struktur jaringan internal dari luar. NAT sangat erat kaitannya dengan firewall, karena keduanya saling bekerja sama untuk memastikan keamanan sekaligus efisiensi dalam pengelolaan lalu lintas jaringan.

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 dapat mengakses web server lokal dari jaringan luar, konfigurasi NAT yang perlu dibuat adalah *Port Forwarding* atau *Static NAT*. Konfigurasi ini memungkinkan router untuk meneruskan permintaan dari IP publik pada port tertentu ke alamat IP privat server lokal yang sesuai. Misalnya, jika IP publik router adalah 203.0.113.2 dan ingin mengakses web server di 192.168.1.10:80, maka perlu dilakukan port forwarding dari 203.0.113.2:80 ke 192.168.1.10:80.

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

Firewall lebih penting untuk diterapkan terlebih dahulu karena berfungsi sebagai sistem keamanan utama yang memfilter lalu lintas data berdasarkan aturan tertentu. Tanpa firewall, jaringan terbuka terhadap ancaman dari luar seperti serangan DDoS, malware, atau upaya peretasan. NAT memang memberikan keamanan pasif dengan menyembunyikan alamat IP privat, namun tidak memiliki kontrol selektif terhadap akses seperti yang dilakukan firewall.

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

Tanpa filter firewall, router tidak dapat membatasi jenis lalu lintas yang masuk atau keluar, sehingga berpotensi:

- Membuka seluruh port ke internet, yang memungkinkan akses tidak sah.
- Mempermudah penyebaran malware dan serangan terhadap perangkat di jaringan lokal.
- Menyebabkan kebocoran data karena tidak adanya pengawasan lalu lintas.
- Tidak adanya mekanisme log dan kontrol akses yang esensial untuk keamanan jaringan.

4. Referensi

- Cisco - NAT Configuration: <https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/13772-12.html>
- Cloudflare - What is a Firewall: <https://www.cloudflare.com/learning/ddos/what-is-a-firewall/>
- Hostinger - Pengertian Firewall dan Cara Kerjanya <https://www.hostinger.com/id/tutorial/apa-itu-firewall>
- Cyber Hub - Firewall: Pengertian, Fungsi, dan Cara Kerjanya: <https://cyberhub.id/pengetahuan-dasar/fungsi-manfaat-firewall>