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

Laporan Sementara
Praktikum Jaringan Komputer

Firewall & NAT

Muhammad Rafli Satriani - 5024231033

31 Mei 2025

1 Pendahuluan

1.1 Latar Belakang

Dalam era digital saat ini, keamanan jaringan menjadi salah satu aspek paling krusial dalam pengelolaan sistem informasi. Ancaman terhadap jaringan komputer seperti akses tidak sah, serangan siber, serta pencurian data terus berkembang seiring dengan pesatnya perkembangan teknologi. Oleh karena itu, diperlukan mekanisme perlindungan jaringan yang efektif, salah satunya melalui implementasi firewall dan Network Address Translation (NAT).

Firewall merupakan sistem yang digunakan untuk mengontrol lalu lintas jaringan berdasarkan aturan yang telah ditentukan. Firewall dapat berfungsi sebagai penghalang antara jaringan internal yang dipercaya dan jaringan eksternal yang tidak dipercaya, seperti internet. Dengan konfigurasi yang tepat, firewall mampu mencegah akses yang tidak sah, menyaring paket data, serta melindungi sistem dari berbagai jenis serangan.

Sementara itu, NAT adalah teknik yang digunakan untuk mengubah alamat IP dalam paket data yang melewati router atau firewall. NAT memungkinkan beberapa perangkat dalam jaringan lokal menggunakan satu alamat IP publik untuk terhubung ke internet, sehingga tidak hanya menghemat penggunaan IP, tetapi juga menambah lapisan keamanan terhadap jaringan internal.

1.2 Dasar Teori

Firewall dan Network Address Translation (NAT) merupakan dua konsep dalam pengamanan dan manajemen lalu lintas jaringan komputer. Firewall adalah sistem keamanan yang berfungsi untuk menyaring lalu lintas data berdasarkan aturan tertentu, baik berupa perangkat keras maupun perangkat lunak. Jenis firewall meliputi packet filtering, stateful inspection, dan application layer firewall, yang masing-masing bekerja pada level protokol yang berbeda dalam model OSI. Firewall menggunakan prinsip rule-based policy untuk menentukan apakah paket data diizinkan atau ditolak.

Sementara itu, NAT adalah teknik untuk mengubah alamat IP sumber atau tujuan dalam sebuah paket data. Tujuan utamanya adalah untuk menghemat penggunaan alamat IP publik dan menyembunyikan struktur jaringan internal. Tiga jenis utama NAT adalah static NAT, dynamic NAT, dan Port Address Translation (PAT). NAT bekerja pada layer jaringan (layer 3 OSI) dan sangat erat kaitannya dengan proses routing.

Konsep IP address dan port juga penting dalam praktik firewall dan NAT. Setiap perangkat jaringan memiliki alamat IP sebagai identitas, dan port digunakan untuk membedakan layanan dalam komunikasi data. Pengaturan firewall dan NAT sering digunakan bersama dengan konfigurasi routing untuk mengatur jalur lalu lintas antar jaringan. Secara umum, keduanya merupakan bagian dari strategi keamanan jaringan yang menerapkan prinsip seperti least privilege dan defense in depth, guna melindungi sistem dari akses tidak sah dan potensi ancaman eksternal.

2 Tugas Pendahuluan

Bagian ini berisi jawaban dari tugas pendahuluan yang telah anda kerjakan, beserta penjelasan dari jawaban tersebut

1. Untuk mengakses web server lokal dari jaringan luar, kamu perlu membuat Static NAT atau lebih spesifiknya Port Forwarding (DNAT). Konfigurasi ini mengarahkan permintaan dari alamat IP

publik router pada port 80 ke alamat IP privat 192.168.1.10 port 80. Dengan begitu, saat pengguna dari luar mengakses IP publik router melalui port 80, NAT akan meneruskan permintaan tersebut ke web server lokal.

2. Jika dilihat dari urutan kebutuhan fungsional, NAT lebih dahulu; tetapi jika dilihat dari prioritas keamanan, firewall sebaiknya diterapkan terlebih dahulu. Secara fungsi, NAT lebih dulu diperlukan secara teknis, terutama pada jaringan yang menggunakan IP privat dan ingin mengakses internet, karena NAT memungkinkan translasi alamat IP privat ke IP publik. Namun, dalam konteks keamanan, firewall lebih penting karena ia berfungsi sebagai pengontrol akses dan pelindung jaringan dari ancaman eksternal.

3. Jika router tidak diberi filter firewall sama sekali, maka semua lalu lintas jaringan baik masuk maupun keluar akan diteruskan tanpa pemeriksaan atau pembatasan. Hal ini bisa berbahaya karena:

    - Jaringan menjadi rentan terhadap serangan dari luar, seperti port scanning, malware, dan eksploitasi celah keamanan.
    - Tidak ada kontrol akses, sehingga perangkat dalam jaringan bisa diakses bebas oleh siapa saja dari luar.
    - Risiko kebocoran data meningkat karena tidak ada perlindungan terhadap lalu lintas keluar yang mencurigakan.