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

Laporan Sementara
Praktikum Jaringan Komputer

Firewall And NAT

Muhammad Zidane Faiq Sidqi - 5024231040

2025

1 Pendahuluan

1.1 Latar Belakang

Dalam era digital yang semakin berkembang pesat, keamanan jaringan dan manajemen lalu lintas data menjadi aspek yang sangat penting dalam infrastruktur teknologi informasi. Setiap perangkat yang terhubung ke internet berpotensi menjadi sasaran serangan siber seperti peretasan, malware, dan akses tidak sah. Oleh karena itu, perlindungan terhadap jaringan komputer menjadi suatu keharusan, baik untuk individu, organisasi, maupun perusahaan. Salah satu teknologi utama yang digunakan untuk menjaga keamanan dan mengatur lalu lintas jaringan adalah Firewall dan Network Address Translation (NAT).

Urgensi dari pembelajaran topik ini terletak pada meningkatnya ketergantungan masyarakat dan organisasi terhadap layanan berbasis jaringan. Kesalahan dalam konfigurasi keamanan jaringan dapat berakibat fatal, mulai dari pencurian data hingga gangguan layanan yang signifikan. Oleh karena itu, penguasaan konsep dan praktik firewall dan NAT merupakan keterampilan fundamental bagi calon profesional di bidang jaringan komputer dan keamanan informasi.

Secara nyata, firewall dan NAT telah menjadi bagian dari teknologi sehari-hari mulai dari router rumah tangga, server perusahaan, hingga sistem keamanan data di pusat data skala besar. Pemahaman yang baik tentang topik ini akan mempersiapkan mahasiswa untuk menghadapi tantangan dunia kerja di bidang teknologi informasi, serta meningkatkan kesadaran akan pentingnya perlindungan jaringan dalam ekosistem digital yang kompleks.

Dengan dilaksanakannya praktikum ini, diharapkan mahasiswa tidak hanya memahami fungsi dan konfigurasi firewall dan NAT, tetapi juga mampu menerapkannya dalam konteks dunia nyata untuk menjaga keamanan dan efisiensi jaringan.

1.2 Dasar Teori

Firewall adalah sistem keamanan jaringan yang bertugas untuk memantau dan mengontrol lalu lintas jaringan berdasarkan aturan yang telah ditentukan. Firewall dapat berupa perangkat keras (hardware) maupun perangkat lunak (software). Tujuan utama firewall adalah mencegah akses tidak sah dan melindungi sistem dari serangan eksternal. Terdapat beberapa jenis firewall: Packet Filtering Firewall (Menganalisis setiap paket data dan mengizinkan atau menolak berdasarkan alamat IP, port, dan protokol). Stateful Inspection Firewall (Selain memeriksa header paket, jenis ini juga melacak status koneksi jaringan). Application-Level Firewall (Proxy Firewall) (Memfilter lalu lintas berdasarkan aplikasi atau protokol tertentu (HTTP, FTP, dll)). Next Generation Firewall (NGFW) (Firewall modern dengan fitur tambahan seperti deteksi intrusi dan kontrol aplikasi).

NAT adalah teknik yang digunakan untuk menerjemahkan alamat IP internal (privat) menjadi satu atau beberapa alamat IP eksternal (publik). NAT memungkinkan banyak perangkat di jaringan lokal untuk mengakses internet menggunakan satu alamat IP publik, yang sangat efisien dalam penggunaan sumber daya IP dan menambah lapisan keamanan. Jenis-jenis NAT: Static NAT (Setiap alamat IP privat dipetakan ke satu alamat IP publik secara tetap). Dynamic NAT (Alamat IP privat dipetakan ke alamat IP publik yang tersedia secara dinamis). Port Address Translation (PAT) / NAT Overload (Banyak alamat IP privat dipetakan ke satu alamat IP publik dengan membedakan berdasarkan nomor port).

2 Tugas Pendahuluan

1. Konfigurasi NAT yang diperlukan adalah Port Forwarding (Static NAT). Dalam hal ini, harus mengatur agar permintaan dari luar (internet) ke alamat IP publik pada port 80 diarahkan (forward) ke alamat IP lokal 192.168.1.10 port 80.

2. Firewall sebaiknya diterapkan terlebih dahulu sebelum NAT. Karena Firewall bertugas memfilter dan melindungi lalu lintas jaringan dari ancaman berbahaya, baik sebelum maupun sesudah NAT dilakukan. Tanpa filter firewall, seluruh lalu lintas yang sudah diterjemahkan oleh NAT bisa masuk tanpa kontrol, membuka peluang serangan (misalnya exploit port). Dengan menempatkan firewall lebih awal, administrator bisa mengontrol siapa saja dan apa saja yang boleh diteruskan atau diblokir, bahkan sebelum paket tersebut diproses oleh NAT.

3. Jika router tidak diberi filter firewall, maka seluruh trafik dari luar jaringan (internet) yang diarahkan ke IP publik router bisa masuk tanpa hambatan. Beberapa dampak negatifnya: Ancaman Keamanan Tinggi, Kompromi Sistem Lokal, Penggunaan Bandwidth Berlebihan, Tidak Ada Kendali Akses.