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

Laporan Sementara
Praktikum Jaringan Komputer

Modul Firewall dan NAT

Muhammad Fawaaz Dhawi - 5024231052

2025

1 Pendahuluan

1.1 Latar Belakang

Di era digital yang terus maju, jaringan komputer menjadi fondasi utama untuk komunikasi dan pertukaran data. Namun, seiring meningkatnya ketergantungan pada jaringan, ancaman keamanan seperti peretasan, malware, dan akses tanpa izin juga semakin rumit. Untuk mengatasinya, diperlukan sistem keamanan jaringan yang handal, salah satunya firewall. Firewall bertindak sebagai filter lalu lintas data yang masuk dan keluar jaringan berdasarkan aturan yang ditentukan administrator, sehingga mampu mencegah akses ilegal dan melindungi aset jaringan dari ancaman eksternal. Selain itu, teknologi Network Address Translation (NAT) juga memainkan peran kunci dalam pengelolaan jaringan. NAT memungkinkan perangkat di jaringan lokal dengan alamat IP privat untuk terhubung ke internet menggunakan satu alamat IP publik. Ini tidak hanya menghemat penggunaan alamat IP, tetapi juga meningkatkan keamanan dengan menyamarkan struktur jaringan internal dari dunia luar. Kombinasi firewall dan NAT tidak hanya meningkatkan efisiensi jaringan, tetapi juga memperkuat perlindungan terhadap ancaman eksternal. Oleh karena itu, memahami cara kerja dan implementasi kedua teknologi ini sangat penting untuk menjaga jaringan yang aman dan efisien.

1.2 Dasar Teori

1.2.1 Firewall

Firewall adalah sistem yang mengatur lalu lintas data masuk dan keluar dalam jaringan komputer. Sistem ini bertugas menyaring dan mengontrol akses berdasarkan aturan keamanan yang telah ditetapkan. Firewall bisa berbentuk perangkat lunak (software) yang beroperasi pada sistem operasi atau perangkat keras (hardware) yang berdiri sendiri. Secara umum, firewall memeriksa header paket data, seperti alamat IP asal dan tujuan, port, serta protokol, untuk menentukan apakah paket tersebut diizinkan melintasi jaringan. Berdasarkan mekanisme kerjanya, firewall terbagi menjadi beberapa jenis seperti Packet Filtering Firewall, Stateful Inspection Firewall,Application Layer Firewall, dll

1.3 NAT

Network Address Translation (NAT) adalah teknik dalam jaringan komputer untuk mengubah alamat IP pada paket data saat melintasi perangkat seperti router. NAT memungkinkan beberapa perangkat di jaringan lokal dengan alamat IP privat (misalnya, 192.168.x.x) untuk menggunakan satu alamat IP publik saat terhubung ke internet. Tujuan utama NAT adalah mengatasi keterbatasan jumlah alamat IP publik sekaligus meningkatkan keamanan jaringan dengan menyembunyikan struktur jaringan internal dari pihak eksternal. Dalam praktiknya, NAT sering dipadukan dengan firewall untuk mengelola dan mengamankan lalu lintas jaringan. NAT menutupi perangkat internal dari internet, sementara firewall menyaring paket data masuk dan keluar berdasarkan aturan keamanan yang ditetapkan.

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?

Jawaban:

Untuk mengakses web server lokal dengan IP 192.168.1.10 pada port 80 dari jaringan luar, diperlukan konfigurasi Port Forwarding (bagian dari NAT) pada router. Dengan konfigurasi sebagai berikut

- Tentukan IP publik router yang menerima permintaan dari internet. Atur aturan NAT untuk meneruskan lalu lintas dari IP publik pada port 80 ke 192.168.1.10 port 80
- Pastikan IP lokal server (192.168.1.10) bersifat statis atau dikonfigurasi melalui DHCP reservation agar tidak berubah.
- Jika router memiliki firewall, buat aturan untuk mengizinkan lalu lintas ke port 80 dan pastikan web server di 192.168.1.10 dikonfigurasi dengan benar untuk menerima koneksi, dan ISP tidak memblokir port 80.

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

   Firewall lebih penting diterapkan terlebih dahulu karena keamanan adalah prioritas utama. Firewall mengontrol lalu lintas jaringan dan melindungi dari ancaman seperti akses tidak sah, serangan DDoS, atau eksploitasi dan NAT hanya memetakan alamat dan port tanpa memberikan perlindungan keamanan. Jika NAT diterapkan tanpa firewall, perangkat internal seperti web server dapat terekspos ke internet tanpa filter.

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

   Jawaban:

   Serangan eksploitasi yang Port terbuka dapat dieksploitasi untuk mendapatkan akses atau menyebarkan malware, dapat mengalami kebocoran data, penyerang dari internet dapat mengakses semua perangkat di jaringan lokal