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

Laporan Sementara
Praktikum Jaringan Komputer

Firewall & NAT

Rafli J.S.P.T. - 5024231061

2025

1 Pendahuluan

1.1 Latar Belakang

Dalam era digital saat ini, pertumbuhan jumlah perangkat yang terhubung ke internet semakin pesat, mulai dari komputer, ponsel pintar, hingga perangkat IoT (Internet of Things). Pertumbuhan ini membawa tantangan besar dalam hal pengelolaan alamat IP dan keamanan jaringan. Salah satu kendala utama adalah keterbatasan jumlah alamat IPv4 yang tersedia secara global. Untuk mengatasi masalah ini, teknologi Network Address Translation (NAT) dikembangkan. NAT memungkinkan satu alamat IP publik digunakan oleh banyak perangkat di jaringan lokal melalui proses translasi alamat, sehingga menghemat penggunaan alamat IP global dan memungkinkan lebih banyak perangkat terhubung ke internet. Selain efisiensi penggunaan IP, NAT juga memberikan manfaat tambahan berupa perlindungan dasar terhadap akses langsung dari luar ke jaringan lokal karena alamat IP privat tidak terlihat dari luar.Di sisi lain, pertumbuhan konektivitas ini juga membawa risiko keamanan yang tinggi. Setiap perangkat yang terhubung ke internet berpotensi menjadi target serangan siber seperti penyusupan, pencurian data, malware, atau bahkan serangan denial-of-service (DoS). Oleh karena itu, diperlukan sistem keamanan yang mampu memantau, menyaring, dan mengendalikan lalu lintas data yang masuk maupun keluar dari jaringan. Firewall menjadi salah satu komponen vital dalam sistem pertahanan jaringan. Dengan menerapkan kebijakan keamanan berbasis aturan, firewall dapat menentukan jenis trafik apa yang diizinkan atau ditolak, berdasarkan alamat IP, port, protokol, maupun pola perilaku tertentu. Dalam praktiknya, NAT dan firewall sering digunakan secara bersamaan untuk membentuk lapisan perlindungan ganda: NAT menyembunyikan struktur jaringan internal, sementara firewall secara aktif memblokir atau mengizinkan lalu lintas sesuai kebijakan keamanan yang ditetapkan. Kombinasi keduanya menjadi fondasi penting dalam arsitektur jaringan modern untuk menjaga stabilitas, efisiensi, dan keamanan komunikasi data

1.2 Dasar Teori

NAT adalah proses menerjemahkan alamat IP privat menjadi alamat IP publik (dan sebaliknya) saat paket data melewati router. Ada beberapa jenis NAT, seperti Static NAT, Dynamic NAT, dan Port Address Translation (PAT). Teknik ini memungkinkan komunikasi antara jaringan lokal dan eksternal tanpa mengungkapkan alamat internal secara langsung.Sementara itu, firewall adalah sistem pengaman jaringan yang bekerja berdasarkan aturan tertentu untuk mengizinkan atau menolak lalu lintas data. Firewall bisa berupa perangkat keras atau perangkat lunak, dan berfungsi sebagai penghalang antara jaringan internal yang dipercaya dan jaringan eksternal yang tidak dipercaya (seperti internet). Firewall dapat memfilter lalu lintas berdasarkan alamat IP, port, protokol, dan bahkan konten data, sehingga menjadi elemen penting dalam menjaga keamanan jaringan dari akses tidak sah dan serangan siber.

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 ,saya akan membuat port forwarding pada router menggunakan NAT. Konfigurasinya adalah dengan memetakan trafik dari IP publik router pada port 80 ke IP lokal 192.168.1.10 port 80.

2. Menurutmu, mana yang lebih penting diterapkan terlebih dahulu di jaringan: NAT atau Firewall? Jelaskan alasanmu.
   Jawaban : Menurut saya, Antara NAT dan firewall, yang lebih penting diterapkan terlebih dahulu adalah firewall.Dikarenakan firewall memberikan kontrol yang lebih spesifik dan ketat terhadap trafik yang boleh masuk atau keluar dari jaringan, termasuk jenis protokol, port, dan alamat IP. Firewall bertindak sebagai garis pertahanan utama terhadap ancaman seperti serangan DDoS, eksploitasi port, dan akses ilegal,Sementara NAT hanya menyembunyikan IP Internal dan membatasi akses dari luar

3. Apa dampak negatif jika router tidak diberi filter firewall sama sekali?
   Jawaban :.maka tidak ada penyaringan atau filtering untuk semua trafik yang diarahkan ke IP public,hal ini tentunya sangat berbahaya karena bias terjadi kebocoran data dan yang paling parah bisa saja terjadi infeksi malware dari trafik yang kita akses tanpa adanya penyaringan.