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

Laporan Sementara
Praktikum Jaringan Komputer

Firewall dan NAT

Farhan Abdurrahman Muthohhar - 5024221050

2025

1 Pendahuluan

1.1 Latar Belakang

Keamanan jaringan memiliki fungsi untuk menjaga kelancaran dan perlindungan sistem komunikasi data. Salah satu cara yang umum digunakan untuk mengatur lalu lintas jaringan adalah dengan menerapkan firewall. Firewall berfungsi sebagai penyaring data berdasarkan kebijakan atau aturan tertentu, sehingga hanya lalu lintas yang diizinkan yang dapat melewati jaringan. Dengan cara ini, firewall dapat mencegah akses yang tidak diotorisasi serta melindungi sistem dari berbagai risiko seperti virus, peretasan, atau aktivitas mencurigakan lainnya.

Selain firewall, teknologi Network Address Translation (NAT) juga berkontribusi besar dalam keamanan dan efisiensi jaringan. NAT bekerja dengan memodifikasi alamat IP pada paket data, memungkinkan perangkat di jaringan lokal untuk mengakses internet menggunakan satu alamat IP publik. Selain menghemat penggunaan alamat IP global, NAT juga memberikan lapisan keamanan tambahan dengan menyembunyikan alamat IP internal dari jaringan luar. Kombinasi antara NAT dan firewall sering digunakan sebagai strategi utama dalam membangun jaringan yang aman dan terstruktur dengan baik.

1.2 Dasar Teori

Firewall merupakan elemen krusial dalam sistem keamanan jaringan yang berperan dalam mengelola dan mengendalikan arus lalu lintas data sesuai dengan kebijakan yang telah ditetapkan. Dengan menyaring paket data berdasarkan kriteria tertentu, seperti alamat IP, port, dan jenis protokol, firewall mampu mencegah akses yang tidak sah serta melindungi jaringan dari berbagai serangan berbahaya seperti malware dan upaya peretasan. Firewall dapat diimplementasikan dalam bentuk perangkat lunak maupun perangkat keras, dan pengaplikasiannya mencakup berbagai jenis, seperti packet filtering, stateful inspection, serta application-layer firewall, yang masing-masing memiliki metode kerja dan tingkat perlindungan yang berbeda.

Network Address Translation (NAT) adalah mekanisme dalam jaringan komputer yang berfungsi untuk memodifikasi alamat IP sumber atau tujuan dalam paket data ketika melewati perangkat jaringan seperti router. NAT memungkinkan beberapa perangkat di jaringan lokal yang menggunakan alamat IP privat untuk mengakses jaringan publik menggunakan satu atau beberapa alamat IP publik. Selain membantu mengurangi kebutuhan alamat IP global, NAT juga berperan dalam meningkatkan keamanan dengan menyembunyikan struktur jaringan internal dari pihak luar. Beberapa jenis NAT yang umum diterapkan meliputi Static NAT, Dynamic NAT, dan Port Address Translation (PAT), yang masing-masing memiliki cara kerja tersendiri dalam mengelola 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 mengakses web server lokal dari jaringan luar memerlukan konfigurasi port forwarding. teknik port forwarding merupakan bagian dari teknik static NAT langkah langkah port forwarding yaitu atur NAT menjadi seperti ini: Public IP: 203.0.113.5 (alamat ip misal 203.0.113.5). eksternal port 80. internal ip 192.168.1.10. dan internal port 80. protocol yang digunakan tcp

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

   firewall sebaiknya diimplementasikan terlebih dahulu, karena firewell memberikan perlindungan proaktif, sedangkan NAT bisa menyusul ketika ada kebutuhan untuk akses internet atau translasi IP

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

   jika Router tanpa filter firewall maka jaringan menjadi terbuka dan tidak aman. Dampak utamanya adalah Jaringan mudah diretas, Data mudah dicuri, Sistem mudah diserang , dan Penggunaan jaringan tidak terkendali