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

Laporan Sementara
Praktikum Jaringan Komputer

Firewall & NAT

Theo Kawalisa Pinem - 5024231008

2025

1 Pendahuluan

1.1 Latar Belakang

Dalam era digital yang semakin terhubung seperti sekarang, keamanan jaringan menjadi aspek yang sangat krusial. Organisasi maupun individu kini semakin bergantung pada jaringan internet untuk berbagai aktivitas, mulai dari komunikasi hingga penyimpanan data penting. Namun, koneksi ke jaringan publik juga membuka banyak celah yang bisa dimanfaatkan oleh pihak tidak bertanggung jawab seperti peretas atau malware. Oleh karena itu, dibutuhkan mekanisme perlindungan yang mampu menyaring lalu lintas jaringan dan memastikan hanya data yang sah saja yang dapat masuk atau keluar dari jaringan. Salah satu solusi utama yang digunakan adalah firewall dan Network Address Translation (NAT). Praktikum ini bertujuan untuk memberikan pemahaman praktis kepada praktikan mengenai bagaimana firewall dan NAT bekerja dalam menjaga keamanan serta efisiensi jaringan komputer, termasuk pengelolaan koneksi dan penghematan penggunaan IP publik.

1.2 Dasar Teori

Firewall adalah sistem keamanan jaringan yang bertugas untuk mengatur dan memfilter lalu lintas data berdasarkan aturan tertentu. Secara sederhana, firewall dapat diibaratkan seperti satpam digital yang menentukan apakah suatu paket data boleh melewati jaringan atau tidak. Terdapat berbagai jenis firewall, seperti packet filtering, stateful inspection, application layer firewall, hingga next generation firewall (NGFW), yang masing-masing memiliki metode dan tingkat kecanggihan berbeda dalam memeriksa data. Firewall bekerja berdasarkan kebijakan akses seperti accept (menerima), reject (menolak dengan pesan), dan drop (menolak tanpa balasan), yang dapat disesuaikan dengan kebutuhan jaringan.

Sementara itu, Network Address Translation (NAT) adalah metode yang digunakan untuk mengubah alamat IP dari paket data agar memungkinkan banyak perangkat dalam satu jaringan lokal mengakses internet menggunakan satu IP publik. NAT sangat penting karena keterbatasan jumlah alamat IPv4 yang tersedia secara global. Dengan menggunakan teknik seperti static NAT, dynamic NAT, dan terutama Port Address Translation (PAT), NAT dapat mengelola lalu lintas data secara efisien dan mencegah konflik alamat. NAT biasanya diterapkan pada router dan bekerja dengan mencatat serta menerjemahkan alamat IP dan port untuk setiap koneksi yang terjadi.

Selain itu, praktikum ini juga membahas connection tracking, yaitu proses pelacakan status koneksi jaringan. Fitur ini memungkinkan sistem mengenali apakah suatu paket merupakan bagian dari koneksi yang sah atau bukan. Dengan adanya connection tracking, firewall dapat bekerja secara stateful, yaitu mempertimbangkan konteks dan status koneksi dalam proses filtering, bukan hanya berdasarkan atribut statis seperti IP dan port. Hal ini membuat sistem jaringan menjadi lebih aman dan efisien, karena dapat mendeteksi serta memblokir lalu lintas yang mencurigakan atau tidak diizinkan. Kombinasi dari firewall, NAT, dan connection tracking memberikan landasan yang kuat dalam membangun sistem jaringan yang aman dan stabil.

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 di port 80 dari jaringan luar, diperlukan konfigurasi Static NAT atau port forwarding. Konfigurasi ini akan memetakan satu IP publik ke IP lokal tersebut pada port tertentu, sehingga permintaan dari luar yang masuk ke IP publik pada port 80 akan diteruskan ke IP 192.168.1.10 port 80 di dalam jaringan lokal.

2. Menurutmu, mana yang lebih penting diterapkan terlebih dahulu di jaringan: NAT atau Firewall? Jelaskan alasanmu.
   Jawaban : Menurut saya, Firewall lebih penting diterapkan terlebih dahulu dibandingkan NAT karena firewall berfungsi sebagai sistem keamanan utama yang menyaring lalu lintas data masuk dan keluar. NAT memang penting untuk menghubungkan jaringan lokal ke internet, tapi tanpa firewall, seluruh lalu lintas bisa masuk tanpa kontrol sehingga rentan terhadap serangan. Firewall memastikan hanya lalu lintas yang aman yang diizinkan sebelum data diteruskan melalui NAT.

3. Apa dampak negatif jika router tidak diberi filter firewall sama sekali?
   Jawaban : Jika router tidak diberi filter firewall sama sekali, maka semua lalu lintas dari luar bisa langsung masuk ke jaringan internal tanpa penyaringan. Hal ini sangat berbahaya karena membuka peluang besar bagi serangan dari luar seperti DDoS, peretasan, dan penyebaran malware. Akibatnya, data bisa bocor, sistem bisa rusak, dan jaringan menjadi tidak aman sama sekali.