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

Laporan Sementara
Praktikum Jaringan Komputer

Firewall dan NAT

Erdi Yanto - 5024231011

2025

1 Pendahuluan

1.1 Latar Belakang

Dalam era digital yang semakin berkembang, konektivitas jaringan menjadi kebutuhan utama dalam berbagai aktivitas, baik individu maupun organisasi. Namun, semakin terbukanya akses ke jaringan internet juga meningkatkan risiko terhadap ancaman dari luar seperti peretasan, malware, dan serangan lainnya. Oleh karena itu, keamanan jaringan menjadi aspek yang sangat penting untuk diperhatikan.

Firewall dan Network Address Translation (NAT) merupakan dua komponen utama dalam sistem keamanan jaringan. Firewall bertugas sebagai penjaga gerbang yang mengatur lalu lintas data masuk dan keluar berdasarkan aturan tertentu, sedangkan NAT memungkinkan banyak perangkat dalam jaringan lokal untuk mengakses internet menggunakan satu alamat IP publik. Pemahaman terhadap cara kerja, jenis, serta penerapan dari kedua teknologi ini sangat penting agar jaringan tetap aman dan efisien.

1.2 Dasar Teori

Firewall adalah sistem keamanan jaringan yang bertugas untuk mengatur dan memfilter lalu lintas jaringan berdasarkan aturan yang telah ditentukan. Ia dapat membatasi akses terhadap jaringan internal dari pihak luar serta mencegah akses tidak sah dari dalam ke luar. Firewall bekerja berdasarkan kebijakan akses seperti *accept*, *reject*, dan *drop* yang diterapkan pada setiap paket data yang masuk atau keluar. NAT adalah mekanisme yang digunakan untuk mengubah alamat IP lokal menjadi alamat IP publik sehingga memungkinkan banyak perangkat dalam jaringan lokal mengakses internet menggunakan satu IP publik. Connection Tracking adalah fitur pada firewall modern yang mencatat status dari setiap koneksi data yang terjadi. Informasi yang dicatat meliputi alamat IP sumber dan tujuan, nomor port, protokol, serta status koneksi. Dengan fitur ini, firewall dapat menerapkan filtering berdasarkan status koneksi dan mendukung NAT secara lebih efisien.

2 Tugas Pendahuluan

Bagian ini berisi jawaban dari tugas pendahuluan yang telah anda kerjakan, beserta penjelasan dari jawaban tersebut

1. Untuk mengakses web server lokal (IP: 192.168.1.10, port 80) dari jaringan luar, konfigurasi NAT yang perlu dibuat adalah **Port Forwarding** menggunakan **Static NAT** atau **Destination NAT (DNAT)**. Konfigurasi ini akan meneruskan permintaan dari IP publik router (misalnya: 203.0.113.5) ke IP lokal server. Berikut contoh aturan NAT:

```
1 iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT --to-destination
     192.168.1.10:80
2 iptables -t nat -A POSTROUTING -j MASQUERADE
3
```

2. Menurut saya, NAT lebih penting diterapkan terlebih dahulu sebelum firewall. Alasannya adalah karena NAT memungkinkan perangkat dengan IP privat dapat berkomunikasi ke/dari jaringan luar seperti internet.

3. Jika router tidak diberi filter firewall sama sekali, dampak negatif yang dapat terjadi antara lain:
    - Trafik berbahaya dari internet dapat langsung masuk ke jaringan lokal.
    - Server dan perangkat lain di jaringan internal menjadi rentan terhadap serangan seperti DDoS, pencurian data, dan akses ilegal.
    - Tidak ada kontrol terhadap layanan terbuka seperti HTTP, FTP, atau SSH, sehingga dapat dieksploitasi.
    - Malware atau program jahat dari jaringan lokal dapat menyebar ke luar tanpa deteksi.

2.1 Referensi

https://www.kaspersky.com/resource-center/definitions/firewall
https://www.noip.com/support/knowledgebase/general-port-forwarding-guide
https://www.itsasap.com/blog/3-top-risks-of-not-having-a-firewall