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

Laporan Sementara
Praktikum Jaringan Komputer

Firewall dan NAT

Zaky Ahmad Septyan Pradana - 5024231051

2025

1 Pendahuluan

1.1 Latar Belakang

Dalam era digital yang semakin berkembang pesat, kebutuhan akan jaringan komputer yang aman dan efisien menjadi sangat penting. Hampir seluruh aktivitas organisasi modern bergantung pada koneksi internet, mulai dari komunikasi internal, akses layanan cloud, hingga transaksi data sensitif. Namun, tingginya ketergantungan terhadap jaringan ini juga membawa tantangan besar, terutama dalam hal keamanan. Serangan siber seperti malware, peretasan, dan akses tidak sah menjadi ancaman nyata yang dapat menyebabkan kerugian besar bagi individu maupun institusi.

Permasalahan utama yang ingin diselesaikan dalam praktikum ini adalah bagaimana melindungi jaringan komputer dari akses yang tidak sah dan bagaimana mengatur alur lalu lintas data agar tetap efisien meskipun menggunakan sumber daya IP publik yang terbatas. Oleh karena itu, pembahasan mengenai Firewall, Network Address Translation (NAT), dan Connection Tracking menjadi sangat relevan. Firewall berfungsi sebagai lapisan perlindungan yang menyaring lalu lintas data berdasarkan aturan tertentu, sedangkan NAT memungkinkan banyak perangkat dalam jaringan lokal untuk mengakses internet dengan satu IP publik. Sementara itu, Connection Tracking berperan penting dalam memantau status koneksi dan membantu firewall bekerja lebih cerdas dengan memahami konteks komunikasi.

1.2 Dasar Teori

Dasar teori praktikum ini mencakup tiga komponen utama dalam keamanan dan manajemen jaringan, yaitu Firewall, Network Address Translation (NAT), dan Connection Tracking. Firewall berfungsi sebagai pengaman lalu lintas data dengan menyaring akses berdasarkan aturan tertentu, melindungi jaringan dari ancaman eksternal seperti malware atau peretas. Terdapat berbagai jenis firewall seperti packet filtering, stateful inspection, hingga next generation firewall (NGFW) yang mampu melakukan inspeksi mendalam terhadap data. NAT adalah mekanisme untuk menerjemahkan alamat IP privat menjadi IP publik agar banyak perangkat dalam jaringan lokal dapat mengakses internet secara bersamaan, dengan jenis-jenisnya seperti static NAT, dynamic NAT, dan PAT (Port Address Translation). NAT juga memperkenalkan istilah penting seperti inside local dan inside global address yang menggambarkan posisi dan peran alamat IP dalam proses translasi. Sementara itu, connection tracking adalah fitur yang mencatat dan memantau status koneksi antar perangkat, memungkinkan sistem mengenali lalu lintas sah dan menolak koneksi mencurigakan. Konsep ini sangat penting untuk efisiensi firewall dan NAT karena membantu menjaga keamanan, mengontrol lalu lintas, dan mengurangi beban pemrosesan pada perangkat jaringan. Ketiga komponen ini saling mendukung dan menjadi dasar penting dalam pengelolaan jaringan komputer yang aman dan efisien.

2 Tugas Pendahuluan

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

1. **Konfigurasi NAT apa yang perlu dibuat**
   Untuk mengakses web server lokal dari jaringan luar, perlu dilakukan konfigurasi *port forwarding*

menggunakan **Static NAT** atau **Destination NAT**. Konfigurasi ini memetakan IP publik milik router ke alamat IP lokal (192.168.1.10) pada port 80.

> *Contoh konfigurasi:* IP Publik (misalnya: 203.0.113.1) port 80 $\rightarrow$ IP Privat 192.168.1.10 port 80

Dengan konfigurasi ini, permintaan dari jaringan luar yang masuk ke IP publik pada port 80 akan diteruskan ke server web lokal.

2. **Lebih penting NAT atau Firewall?**
   Firewall lebih penting. karena, firewall berperan sebagai garis pertahanan pertama yang menentukan mana lalu lintas data yang aman dan mana yang berpotensi membahayakan. Tanpa firewall, semua jenis koneksi bisa masuk dan keluar tanpa pengawasan, membuka celah besar terhadap serangan. NAT juga penting untuk mengatur akses dan menghemat IP publik, tapi NAT tidak menjamin keamanan. Maka, firewall menjadi prioritas awal dalam desain jaringan untuk mengontrol akses sebelum koneksi diteruskan melalui NAT.

3. **Dampak negatif jika router tidak diberi filter firewall**
   Jika router tidak diberi filter firewall sama sekali, maka seluruh lalu lintas data dari luar akan diterima tanpa penyaringan. Hal ini membuka celah besar bagi berbagai serangan jaringan seperti *port scanning*, *brute force*, *malware*, dan *Distributed Denial of Service (DDoS)*. Tanpa adanya kontrol akses, perangkat-perangkat di dalam jaringan internal menjadi sangat rentan terhadap akses tidak sah yang dapat menyebabkan kebocoran data, gangguan layanan, hingga pengambilalihan sistem oleh pihak yang tidak bertanggung jawab. Firewall berfungsi sebagai penjaga gerbang jaringan, yang menyaring dan memblokir lalu lintas berbahaya sebelum mencapai sistem internal. Oleh karena itu, ketiadaan filter firewall akan membuat jaringan tidak aman dan berisiko tinggi terhadap berbagai ancaman cyber.