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

Laporan Sementara
Praktikum Jaringan Komputer

Firewall & NAT

Nur Anisa Hidayatul Masruroh

2025

1 Pendahuluan

1.1 Latar Belakang

Dalam era digital yang semakin berkembang pesat, jaringan komputer menjadi tulang punggung utama bagi berbagai aktivitas komunikasi dan operasional, baik dalam lingkup personal, organisasi, hingga skala global. Namun, seiring dengan meningkatnya ketergantungan terhadap jaringan, ancaman terhadap keamanan jaringan pun kian kompleks dan beragam. Serangan siber seperti Distributed Denial of Service (DDoS), port scanning, data exfiltration, hingga akses tidak sah terhadap sistem internal telah menjadi peristiwa umum yang dapat menyebabkan gangguan layanan, pencurian data, dan kerugian finansial maupun reputasi yang besar. Dalam konteks ini, pengamanan jaringan menjadi hal yang tidak bisa diabaikan, dan dua komponen penting yang sering menjadi garda depan dalam perlindungan jaringan adalah Network Address Translation (NAT) dan firewall. NAT berperan dalam menyembunyikan struktur internal jaringan dengan menerjemahkan alamat IP privat menjadi IP publik, sehingga mempersulit pelaku ancaman dari luar untuk mengidentifikasi perangkat dalam jaringan internal secara langsung. Di sisi lain, firewall bertugas menyaring lalu lintas jaringan berdasarkan aturan keamanan tertentu, sehingga hanya lalu lintas yang sah dan diperlukan saja yang diizinkan masuk atau keluar dari sistem. Firewall juga menerapkan prinsip keamanan seperti "least privilege", yakni memberikan akses seminimal mungkin hanya kepada entitas yang berhak, guna meminimalkan potensi eksploitasi. Praktikum ini bertujuan untuk memperkenalkan serta memberikan pemahaman praktis mengenai cara kerja dan konfigurasi NAT serta firewall dalam menghadapi ancaman nyata di jaringan, sekaligus menunjukkan kontribusi nyata dari kedua mekanisme tersebut dalam menjaga integritas, kerahasiaan, dan ketersediaan informasi dalam sebuah sistem jaringan modern. Dengan memahami penerapan NAT dan firewall, diharapkan peserta praktikum mampu merancang solusi dasar pertahanan jaringan dan mengidentifikasi potensi celah keamanan yang bisa dimitigasi melalui konfigurasi yang tepat.

1.2 Dasar Teori

Keamanan jaringan merupakan aspek fundamental dalam sistem informasi yang bertujuan untuk menjaga integritas, kerahasiaan, dan ketersediaan data dari berbagai ancaman, baik dari dalam maupun luar jaringan. Seiring berkembangnya teknologi dan keterhubungan sistem ke internet, serangan jaringan seperti peretasan, malware, sniffing, dan Distributed Denial of Service (DDoS) menjadi semakin umum terjadi, sehingga dibutuhkan mekanisme proteksi yang handal. Dua komponen penting dalam membangun pertahanan jaringan adalah firewall dan Network Address Translation (NAT). Firewall adalah sistem penyaring lalu lintas jaringan yang bekerja berdasarkan aturan-aturan tertentu untuk menentukan apakah suatu paket data diizinkan atau ditolak masuk/keluar dari jaringan, serta berperan besar dalam penerapan prinsip "least privilege" dengan hanya mengizinkan akses seminimal mungkin sesuai kebutuhan. Jenis-jenis firewall meliputi packet filtering firewall yang menyaring paket berdasarkan alamat IP, port, dan protokol; stateful inspection firewall yang memperhatikan status koneksi; application-layer firewall (proxy firewall) yang menyaring data berdasarkan konten aplikasi seperti HTTP dan FTP; serta Next-Generation Firewall (NGFW) yang memiliki fitur canggih seperti inspeksi mendalam dan deteksi ancaman. Implementasi firewall bisa dilakukan pada berbagai titik jaringan seperti router, gateway, atau dedicated firewall device. Sementara itu, NAT adalah teknik yang digunakan untuk menerjemahkan alamat IP privat dalam jaringan lokal ke alamat IP pu-

blik untuk berkomunikasi dengan jaringan luar, dan sebaliknya. Dengan menggunakan NAT, struktur internal jaringan dapat disembunyikan, sekaligus menghemat penggunaan IP publik yang terbatas. Jenis-jenis NAT mencakup static NAT yang memetakan satu IP privat ke satu IP publik, dynamic NAT yang memetakan IP privat ke kumpulan IP publik yang tersedia, serta Port Address Translation (PAT) atau NAT overload yang memungkinkan banyak alamat IP privat menggunakan satu alamat IP publik dengan membedakan koneksi berdasarkan port. Implementasi NAT umumnya dilakukan pada router atau gateway yang menghubungkan jaringan lokal ke internet. Penggunaan NAT dan firewall secara bersamaan menjadi sangat krusial dalam menjaga keamanan jaringan, karena NAT membantu menyamarkan identitas perangkat internal dan mengendalikan aliran lalu lintas ke luar jaringan, sedangkan firewall menyaring semua lalu lintas berdasarkan kebijakan keamanan yang ditentukan. Oleh karena itu, pemahaman terhadap dasar-dasar keamanan jaringan, termasuk fungsi, jenis, dan implementasi NAT dan firewall sangat penting untuk membekali peserta praktikum dalam merancang serta menerapkan solusi keamanan dasar yang dapat mencegah potensi ancaman dan memastikan kestabilan serta keamanan sistem jaringan secara menyeluruh.

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 mengubungkan jaringan luar ke jaringan internal, yang bisa digunakan adalah port forwading atau destination NAT. Pada konfigurasi, selain jenis NAT yang perlu dispesifikasikan, yaitu dnat. Kita juga perlu mensepesifikasikan destinasi alamat lokal yang akan digunakan (192.168.1.10) dan alamat port nya (80).
   Link : `https://help.mikrotik.com/docs/spaces/RKB/pages/154042388/Port+forwarding`

2. Menurutmu, mana yang lebih penting diterapkan terlebih dahulu di jaringan: NAT atau Firewall? Jelaskan alasanmu.
   Sebaiknya terapkan Firewall dulu baru NAT. Dalam networking ada prinsip "Pinciple of Last Privilage", yaitu setiap entitas diberikan akses paling minimum dengan tujuan untuk memastikan tidak sembarang entitas bisa mengakses data atau resource penting. Firewall berfungsi sebagai pertahanan pertama agar tidak ada jaringan nakal yang mengakses resource. Dengan pertimbangan ini, Firewall sudah seharusnya diterapkan lebih dahulu daripada NAT yang fungsinya memungkinkan jaringan dari dalam atau luar untuk terhubung atau mengakses resource.
   Link : `apakahdiwebsiteiniadpenjelasankalaufirewallharusditerapkandulusebelumnat`

3. Apa dampak negatif jika router tidak diberi filter firewall sama sekali?
   Banyak dampak negatif yang bisa muncul. Yang paling berbahaya adalah jaringan tidak terpercaya dapat mengakses resource atau network internal kita. Hal ini, bisa mengakibatkan kehilangan data dan kerusakan data yang fatal.
   Link : `https://www.geeksforgeeks.org/the-importance-of-using-a-firewall/`