BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi jaringan komputer mendorong peningkatan kebutuhan akan konektivitas internet yang stabil dan aman. Jaringan komputer kini tidak hanya menjadi sarana pertukaran data, tetapi juga menjadi dasar bagi operasional berbagai sektor. Namun, kemajuan ini juga menimbulkan ancaman baru berupa akses tidak sah dari pihak luar yang berpotensi mengganggu sistem dan struktur jaringan dapat terlihat. Permasalahan ini menunjukkan pentingnya penerapan mekanisme keamanan jaringan yang mampu melindungi perangkat internal dari serangan eksternal tanpa mengganggu proses komunikasi antarperangkat [1].

Pada permasalahan diatas, dibutuhkan solusi yang mampu menjaga keamanan sekaligus mengatur lalu lintas data dengan baik. Pada penelitian ini, penerapan NAT difokuskan pada jaringan berbasis *Internet Protocol version 4* (IPv4) yang umum digunakan untuk mengatasi keterbatasan alamat IP serta meningkatkan keamanan jaringan. *Network Address Translation* (NAT) menjadi salah satu metode yang efektif untuk menyembunyikan alamat *Internet Protocol* (IP) internal sekaligus mengatur untuk proses translasi data antar jaringan lokal dan jaringan publik [2].

Selain membantu dalam efisiensi penggunaan IP, NAT juga berperan sebagai lapisan keamanan dengan mencegah akses langsung dari luar ke perangkat internal. Fungsi NAT sering kali belum dimanfaatkan secara maksimal, padahal mekanisme ini mampu meminimalkan risiko serangan langsung dengan menyembunyikan struktur jaringan internal [2]. Dengan demikian, fungsi NAT tidak hanya sebagai alat translasi alamat, tetapi juga penghalang awal terhadap ancaman eksternal. Implementasi NAT yang tepat dapat meningkatkan kontrol lalu lintas jaringan dan menjaga kestabilan sistem dari aktivitas mencurigakan.

Oleh karena itu, perlu adanya simulasi dalam implementasi NAT dengan menggunakan aplikasi *Cisco Packet Tracer* untuk membantu menggambarkan proses konfigurasi, translasi, serta pengujian konektivitas antarjaringan dengan konfigurasi *Static* NAT, *Dynamic* NAT, dan tanpa penerapan NAT. Simulasi ini memungkinkan analisis yang lebih terukur bagaimana setiap metode NAT memengaruhi performa

jaringan secara keseluruhan. Melalui simulasi ini, diharapkan dapat diperoleh pemahaman yang lebih mendalam mengenai perbandingan kinerja dan efektivitas masing-masing metode NAT dalam mengatur dan mengelola keamanan lalu lintas jaringan.

1.2 Rumusan Masalah

Berdasar uraian dari latar belakang, maka rumusan masalah dalam penelitian ini adalah :

1. Bagaimana fungsi NAT dalam melindungi akses jaringan internal dari ancaman eksternal?
2. Bagaimana hasil simulasi penerapan NAT terhadap stabilitas dan keamanan koneksi jaringan?

1.3 Batasan Masalah

Agar penelitian ini lebih terarah dan fokus, maka batasan masalah yang digunakan adalah sebagai berikut :

1. Penelitian dilakukan menggunakan simulasi jaringan pada aplikasi *Cisco Packet Tracer*.
2. Topologi jaringan dibatasi pada jaringan lokal yang terhubung ke jaringan publik melalui *Router* tunggal.
3. Jenis NAT yang akan digunakan sebagai pengujian adalah *Static* NAT dan *Dynamic* NAT.
4. Pengujian difokuskan pada aspek konektivitas dan perlindungan alamat IP internal tanpa membahas serangan siber kompleks atau enkripsi data.
5. Penelitian ini menggunakan skema alamat IP versi 4 (IPv4) sebagai dasar konfigurasi dan simulasi jaringan.

1.4 Tujuan Penelitian

Tujuan penelitian adalah sebagai berikut :

1. Untuk mengetahui proses konfigurasi dan penerapan NAT dalam simulasi jaringan komputer.
2. Menganalisis fungsi dan efektivitas NAT dalam meningkatkan keamanan jaringan terhadap akses eksternal.

3. Menunjukkan hasil simulasi yang menggambarkan perbedaan kondisi jaringan sebelum dan sesudah penerapan NAT.

1.5 Manfaat Penelitian

Hasil dari penelitian ini diharapkan dapat berdampak dan bermanfaat pada dua aspek berikut :

1. Secara teoritis, dapat memberikan manfaat dan pemahaman lebih mendalam tentang konsep dan fungsi dari NAT dalam konteks keamanan jaringan komputer.
2. Secara praktis, juga diharapkan menjadi referensi bagi mahasiswa, teknisi jaringan, maupun pengelola sistem dalam menerapkan NAT sebagai mekanisme perlindungan jaringan lokal agar lebih aman dari ancaman eksternal.

1.6 Sistematika Penulisan

BAB I PENDAHULUAN

berisi latar belakang masalah, rumusan masalah, batasan masalah, tujuan, manfaat, serta sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Pembahasan teori-teori dasar keamanan jaringan yang mendukung penelitian, jenis NAT dan konfigurasinya, serta hasil penelitian terdahulu yang relevan.

BAB III METODE PENELITIAN

Penjelasan metode serta langkah-langkah penelitian yang dilakukan, mulai dari identifikasi masalah, perancangan topologi jaringan, konfigurasi NAT, hingga pengujian simulasi.

BAB IV HASIL DAN PEMBAHASAN

Berisi hasil simulasi yang diperoleh dari penerapan NAT menggunakan *Cisco Packet Tracer*, meliputi konfigurasi, pengujian konektivitas, analisis hasil uji, dan membahas efektivitas NAT seta membandingkan kondisi jaringan sebelum dan sesudah penerapan NAT.

BAB V PENUTUP

Berisi kesimpulan dari hasil penelitian yang telah dilakukan serta saran yang dapat peneliti rangkum selama proses penelitian untuk kemudian dapat dijadikan bahan pertimbangan bagi pengembang atau peneliti selanjutnya.