BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan mengenai penerapan NAT untuk perlindungan akses jaringan menggunakan *Cisco Packet Tracer*, dari pengujian konektivitas serta pengujian keamanan maka didapatkan kesimpulan adalah sebagai berikut :

1. Hasil analisis kinerja jaringan menunjukkan bahwa skenario dengan tingkat stabilitas tertinggi adalah *Static* NAT dengan kategori "Sangat Stabil", ditunjukkan oleh nilai rata-rata *delay* 1.23 ms, *max delay* 10 ms, dan *jitter* 0.47 ms. Hal ini dipengaruhi oleh pemetaan IP secara tetap (*one-to-one*) sehingga proses translasi berlangsung lebih konsisten.
2. Hasil analisis keamanan jaringan menunjukkan bahwa *Static* NAT dan *Dynamic* NAT memiliki tingkat keamanan "Relatif Aman" karena mampu menyembunyikan alamat IP privat dan mencegah akses langsung dari luar jaringan. *Dynamic* NAT dinilai lebih fleksibel karena menggunakan mekanisme *address pool* (*many-to-many*), sehingga alamat IP publik yang digunakan dapat berubah-ubah.
3. Tanpa NAT tidak memberikan perlindungan terhadap jaringan internal karena alamat IP privat terekspos dan dapat diakses langsung. Meskipun secara teori kinerjanya lebih sederhana, hasil pengujian menunjukkan perbedaan *delay* dan *jitter* yang tidak signifikan dibandingkan skenario yang menggunakan NAT.
4. Secara keseluruhan, penggunaan NAT direkomendasikan karena efektif meningkatkan keamanan dengan menyembunyikan alamat IP privat dan membatasi akses dari luar, tanpa mengorbankan kinerja jaringan secara signifikan.

5.2 Saran

Berdasarkan hasil penelitian yang telah dilakukan, terdapat beberapa saran yang dapat diberikan untuk pengembangan penelitian selanjutnya :

1. Penelitian selanjutnya dapat menguji performa NAT pada skala jaringan yang lebih besar dengan jumlah *host* dan trafik yang lebih bervariasi agar diperoleh hasil yang lebih representatif.
2. Dapat dilakukan perbandingan dengan mekanisme keamanan lain seperti IDS / IPS, VPN, VLAN, atau *proxy server* untuk melihat efektivitas NAT dalam konteks keamanan jaringan secara lebih luas.
3. Pengujian dapat dikembangkan menggunakan perangkat nyata (*real device*) selain simulator untuk mengetahui performa NAT pada kondisi jaringan yang lebih realistis.
4. Penelitian selanjutnya dapat mengkaji pengaruh konfigurasi NAT yang berbeda (seperti NAT *Overload*) terhadap kinerja dan keamanan jaringan untuk memperoleh perbandingan yang lebih lengkap.