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

Laporan Sementara
Praktikum Jaringan Komputer

Firewall & NAT

Moh. Wildan Risqi Maulidi - 5024231056

2025

1 Pendahuluan

1.1 Latar Belakang

Penggunaan NAT sangat penting pada jaringan komputer modern, dikarenakan sekarang internet menjadi hal pokok dalm kehidupan sehari-hari manusia, tanpa Penggunaan NAT jaringan komputer dapat dibobol oleh orang jahat seperti hacker, yang dapat mengakses data pribadi kita. NAT juga dapat menghemat penggunaan IP Address, karena satu IP Address dapat digunakan untuk banyak komputer dalam satu jaringan lokal. NAT juga dapat digunakan untuk menghubungkan jaringan lokal dengan internet, sehingga komputer dalam jaringan lokal dapat mengakses internet.
dalam praktikum yang akan dilakukan adalah bagaimana cara mneggunakan NAT pada jaringan komputer, dengan menggunakan perangkat router. Praktikum ini bertujuan untuk memberikan pemahaman tentang cara kerja NAT, serta bagaimana cara mengkonfigurasi NAT pada router. Dengan memahami konsep NAT, dapat diimplementasikan dalam dunia jaringan komputer.

1.2 Dasar Teori

1.2.1 Network Address Translation (NAT)

NAT (Network Address Translation) adalah suatu teknologi yang digunakan untuk menerjemahkan alamat IP privat (internal) di jaringan lokal ke alamat IP publik (eksternal) sebelum data dikirim ke internet. Ini memungkinkan beberapa perangkat di jaringan lokal untuk berbagi satu alamat IP publik dan terhubung ke internet.

1.2.2 Jenis-jenis NAT

- **Static NAT**
  Static NAT adalah jenis yang mengalokasikan alamat IP publik secara manual ke alamat IP private dari komputer dalam jaringan. Umumnya, jenis ini digunakan oleh bisnis untuk menghubungkan server Web ke Internet.
  Artinya, pengguna dapat mengkonfigurasi NAT secara manual untuk setiap mesin pada jaringan sehingga setiap mesin memiliki alamat IP publik yang unik.
  Dalam static NAT, alamat IP publik dialokasikan secara **permanen** untuk mesin tertentu dan tidak berubah, kecuali jika diubah secara manual oleh pengguna.

- **Dynamic NAT**
  Dynamic NAT adalah jenis yang mengalokasikan alamat IP publik secara otomatis kepada mesin di dalam jaringan. Bisnis yang lebih besar menggunakan jenis ini karena dapat beroperasi dengan kumpulan alamat publik.
  Pada jenis ini, mesin di dalam jaringan akan diberi alamat IP publik secara dinamis apabila mesin tersebut memerlukan koneksi ke jaringan luar.
  Pada dynamic NAT, mesin di dalam jaringan menggunakan alamat IP private, sehingga tidak terlihat oleh jaringan luar.
  Ketika mesin tersebut memerlukan koneksi ke jaringan luar, NAT akan mengalokasikan alamat IP publik yang tersedia dan dialokasikan secara dinamis ke mesin tersebut.

- **Port Address Translation (PAT)**
  Sebagian besar jaringan rumah yang menggunakan Digital Subscriber Line (DSL) atau modem kabel menggunakan jenis NAT ini.
  Port Address Translation (PAT) adalah teknik Network Address Translation yang mengubah alamat port sumber dan tujuan dari paket data yang dikirimkan dari mesin di dalam jaringan.
  Tujuan utama dari penggunaan PAT adalah untuk memperluas jumlah mesin yang dapat terhubung ke internet melalui satu alamat IP publik.
  Dalam PAT, alamat IP private mesin di dalam jaringan diganti dengan alamat IP publik dari router atau gateway jaringan.
  Selain itu, nomor port sumber dan tujuan pada paket data yang dikirimkan juga diubah untuk memastikan bahwa paket tersebut dapat diterima oleh mesin yang tepat di dalam jaringan.
  PAT sangat berguna dalam jaringan dengan banyak mesin dan terbatasnya jumlah alamat IP publik yang tersedia.

1.2.3 Fungsi NAT

- Menerjemahkan Alamat IP
- Meningkatkan Keamanan
- Menghemat Alamat IP
- Meningkatkan Kinerja Jaringan
- Memungkinkan Akses Internet

1.2.4 Cara Kerja NAT

1. NAT memilih gateway yang ditempatkan antara dua jaringan lokal, jaringan internal, dan jaringan luar.
2. Sistem pada jaringan internal biasanya diberi alamat IP yang tidak dapat di rute ke jaringan eksternal (misalnya jaringan pada blok 10.0.0.0/8).
3. Beberapa alamat IP yang valid secara eksternal diberikan kepada gateway.
4. Gateway membuat lalu lintas keluar dari sistem di jaringan internal muncul berasal dari salah satu alamat eksternal yang valid.
5. Gateway menerima lalu lintas masuk yang ditujukan ke alamat eksternal yang valid dan mengirimkannya ke sistem internal yang tepat.
6. Hal ini membantu memastikan keamanan karena setiap permintaan keluar atau masuk harus melalui proses terjemahan yang menawarkan kesempatan untuk memverifikasi arus masuk dan mencocokkannya dengan permintaan keluar.
7. NAT menghemat jumlah alamat IP global yang dibutuhkan oleh perusahaan dalam kombinasi dengan Classless Inter-Domain Routing (CIDR) – telah banyak berkontribusi untuk memperpanjang umur IPv4 yang berguna.

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?
   Jawab:
   Untuk bisa mengakses web server lokal dari luar jaringan, kita perlu menggunakan port forwarding atau yang dikenal juga sebagai Static NAT.
   Konfigurasinya, Semua koneksi dari internet ke IP publik router (misalnya 123.123.123.123) dengan port 80 akan diteruskan ke IP lokal 192.168.1.10 di port 80.
   Jadi, ketika ada orang dari luar yang mengakses http://123.123.123.123, router akan langsung meneruskan permintaan itu ke server lokal yang IP-nya 192.168.1.10.

2. Menurutmu, mana yang lebih penting diterapkan terlebih dahulu di jaringan: NAT atau Firewall? Jelaskan alasanmu. Jawab:
   firewall lebih penting, karena firewall berfungsi sebagai pelindung utama jaringan dari akses yang tidak sah atau ancaman dari luar. Tanpa firewall, jaringan kita terbuka lebar dan sangat rentan terhadap serangan seperti malware, DDoS, atau penyusupan dari hacker.
   jadi sederhananya pengaman dahulu (firewall) baru daripada konektivitas (NAT).

3. Apa dampak negatif jika router tidak diberi filter firewall sama sekali? jawab:

   - Perangkat dalam jaringan jadi rentan disusupi virus atau malware
   - Serangan dari luar seperti DDoS bisa langsung menghantam sistem
   - Data sensitif bisa bocor karena tidak ada penyaringan akses
   - Router bisa overload karena menerima terlalu banyak trafik liar dari luar