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

Laporan Sementara
Praktikum Jaringan Komputer

Firewall & NAT

Abraham Napitupulu - 5024231048

2025

1 Pendahuluan

1.1 Latar Belakang

Dalam era digital saat ini, konektivitas jaringan dan akses internet telah menjadi tulang punggung operasional bagi berbagai organisasi dan kebutuhan individu. Namun, seiring dengan meluasnya konektivitas ini, muncul pula berbagai tantangan keamanan siber yang semakin kompleks dan mengancam integritas serta kerahasiaan data. Untuk menghadapi ancaman tersebut, diperlukan mekanisme pertahanan yang kokoh di garda terdepan infrastruktur jaringan. Di sinilah peran vital Firewall sebagai sistem keamanan jaringan menjadi sangat krusial. Firewall bertindak sebagai filter selektif yang mengontrol lalu lintas data masuk dan keluar berdasarkan serangkaian aturan kebijakan yang telah ditentukan, secara efektif melindungi sumber daya jaringan internal dari akses tidak sah dan serangan berbahaya dari dunia luar.

Sejalan dengan kebutuhan akan keamanan, tantangan lain yang dihadapi dalam pengelolaan jaringan modern adalah keterbatasan alamat IP publik, khususnya IPv4, yang jumlahnya tidak sebanding dengan pesatnya pertumbuhan perangkat yang terhubung ke internet. Untuk mengatasi permasalahan ini, teknologi Network Address Translation (NAT) hadir sebagai solusi yang efisien. NAT memungkinkan sejumlah besar perangkat dalam jaringan lokal untuk berbagi satu alamat IP publik tunggal ketika mengakses internet, sehingga secara signifikan menghemat penggunaan alamat IP publik yang terbatas. Selain fungsi utamanya dalam konservasi alamat IP, NAT juga secara tidak langsung menambah lapisan keamanan dengan menyembunyikan struktur alamat IP internal dari jaringan eksternal. Pemahaman mendalam mengenai cara kerja, jenis, dan implementasi Firewall serta NAT menjadi esensial bagi para praktisi jaringan untuk membangun infrastruktur yang tidak hanya aman dan terkontrol, tetapi juga efisien dan mampu mengakomodasi kebutuhan konektivitas modern.

1.2 Dasar Teori

Firewall merupakan sebuah sistem keamanan jaringan, baik berupa perangkat keras maupun perangkat lunak, yang berfungsi sebagai penghalang atau filter antara jaringan internal yang aman dan jaringan eksternal yang tidak terpercaya, seperti internet. Prinsip dasar kerja firewall adalah melakukan inspeksi terhadap paket data yang masuk dan keluar dari jaringan. Berdasarkan serangkaian aturan kebijakan keamanan (security policies) yang telah dikonfigurasi sebelumnya, firewall akan memutuskan apakah suatu paket data diizinkan (accept), ditolak dengan notifikasi (reject), atau dibuang secara diam-diam (drop). Tujuan utama implementasi firewall adalah untuk mencegah akses tidak sah, melindungi sumber daya jaringan dari berbagai serangan siber seperti malware, virus, dan upaya peretasan, serta mengontrol aliran lalu lintas data sesuai dengan kebutuhan organisasi. Jenis-jenis firewall bervariasi berdasarkan metode operasinya, mulai dari packet filtering yang sederhana hingga Next-Generation Firewall (NGFW) yang mampu melakukan inspeksi mendalam terhadap konten paket dan status koneksi (stateful inspection).

Network Address Translation (NAT) adalah suatu mekanisme dalam jaringan komputer yang berfungsi untuk mentranslasikan (mengubah) alamat IP dari satu ruang alamat ke ruang alamat lainnya. Fungsi utama NAT adalah untuk mengatasi keterbatasan jumlah alamat IPv4 publik yang tersedia dengan memungkinkan banyak perangkat dalam jaringan lokal (yang menggunakan alamat IP privat) untuk berbagi satu atau beberapa alamat IP publik saat terhubung ke internet. Ketika perangkat di

jaringan lokal mengirimkan data ke internet, NAT pada router akan mengganti alamat IP privat asal dengan alamat IP publik router. Sebaliknya, ketika data balasan diterima, NAT akan mengembalikan alamat IP publik tujuan menjadi alamat IP privat perangkat yang sesuai di jaringan lokal, seringkali dengan memanfaatkan translasi nomor port (Port Address Translation/PAT) untuk membedakan antar koneksi dari perangkat yang berbeda. Selain konservasi alamat IP, NAT juga memberikan lapisan keamanan tambahan dengan menyembunyikan struktur topologi alamat IP jaringan internal dari pandangan luar.

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?**

   Agar dapat mengakses web server lokal (IP: `192.168.1.10`, port 80) dari jaringan luar, maka perlu membuat konfigurasi Port Forwarding (DNAT) pada router yang digunakan. Parameter yang umumnya diperlukan adalah sebagai berikut:

   - *Rule Objective (Tujuan Aturan)*: Meneruskan lalu lintas yang datang dari jaringan luar (internet/WAN) pada port tertentu di alamat IP publik router ke alamat IP dan port spesifik dari web server lokal di jaringan internal (LAN).
   - *External Port (Port Publik)*: Adalah nomor port yang akan "didengarkan" oleh router dari jaringan luar untuk permintaan ke web server. Bisa menggunakan port 80 jika port tersebut tidak digunakan untuk layanan lain di router dan diizinkan oleh ISP. Alternatifnya, bisa menggunakan port lain (misalnya, 8080, 8888, dll.) jika port 80 sudah terpakai atau diblokir. Pengguna dari luar akan mengakses `http://<Alamat_IP_Publik_Router>:<External_Port>`.
   - *Internal IP Address (Alamat IP Internal)*: Adalah alamat IP dari web server lokal, yaitu `192.168.1.10`.
   - *Internal Port (Port Internal)*: Adalah port tempat web server berjalan di jaringan lokal, yaitu port 80.
   - *Protocol (Protokol)*: Untuk layanan web HTTP, protokol yang digunakan adalah TCP.
   - *Source IP (IP Sumber) (Opsional)*: Dapat digunakan untuk membatasi akses hanya dari alamat IP publik tertentu jika diperlukan, tetapi untuk akses umum biasanya dikosongkan (any/semua).
   - *WAN interface (Antarmuka WAN)*: Digunakan untuk menentukan antarmuka jaringan router yang terhubung ke internet.

   Berikut merupakan contoh penggunaannya:

   Jika kita memilih External Port adalah 8080, maka pengguna dari luar akan mengakses web server kita dengan mengetikkan `http://<Alamat_IP_Publik>:8080` di browser mereka. Router kemudian akan meneruskan permintaan ini ke `192.168.1.10:80`.

2. **Menurutmu, mana yang lebih penting diterapkan terlebih dahulu di jaringan: NAT atau Firewall? Jelaskan alasanmu.**

   Menurut pendapat saya, Firewall lebih penting untuk diterapkan terlebih dahulu. Berikut adalah alasannya:

- *Keamanan Sebagai Fondasi Utama*: Fungsi utama Firewall adalah untuk keamanan. Ia bertindak sebagai benteng pertahanan pertama yang melindungi jaringan internal dari berbagai ancaman eksternal seperti peretas, malware, dan akses tidak sah. Tanpa firewall, setiap perangkat di jaringan kita akan terekspos langsung ke internet, membuatnya sangat rentan.
- *NAT Bukan Alat Keamanan Utama*: Fungsi utama NAT (khususnya Port Address Translation/PAT) adalah untuk konservasi alamat IP publik dan memungkinkan banyak perangkat berbagi satu koneksi internet. Meskipun NAT secara tidak langsung memberikan lapisan keamanan dengan menyembunyikan alamat IP internal (disebut *security through obscurity*), ini bukanlah fitur keamanan yang dirancang secara eksplisit dan tidak bisa diandalkan sebagai satu-satunya mekanisme pertahanan.
- *Firewall Mengontrol Akses Bahkan dengan NAT*: Jika menerapkan NAT terlebih dahulu, misalnya untuk melakukan port forwarding agar server internal bisa diakses dari luar, sebenarnya membuka "pintu" ke jaringan internal. Tanpa firewall yang mengontrol lalu lintas yang melewati pintu tersebut, server dan jaringan menjadi target empuk.
- *Urutan Logis dalam Membangun Pertahanan*: Secara logis, membangun "tembok" (Firewall) terlebih dahulu sebelum mengatur "pintu dan jendela" (aturan NAT dan port forwarding). Firewall menetapkan kebijakan keamanan dasar tentang apa yang boleh dan tidak boleh melintasi batas jaringan. Setelah dasar keamanan ini ada, barulah bisa mengkonfigurasi NAT dengan lebih aman untuk kebutuhan konektivitas.

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

   Jika sebuah router tidak dilengkapi dengan filter firewall sama sekali, maka dampak negatifnya terhadap keamanan jaringan akan sangat signifikan dan berpotensi merusak. Tanpa firewall, seluruh jaringan internal beserta semua perangkat yang terhubung di dalamnya akan terekspos secara langsung ke internet publik. Ini seperti membiarkan pintu rumah terbuka lebar tanpa penjagaan, mengundang siapa saja untuk masuk. Akibatnya, jaringan menjadi sasaran empuk bagi berbagai jenis serangan siber. Peretas dapat dengan mudah melakukan pemindaian port untuk menemukan celah keamanan, mencoba akses tidak sah ke perangkat seperti komputer, server, atau bahkan perangkat IoT di dalam jaringan. Serangan malware seperti virus, worm, dan ransomware dapat menyebar dengan lebih leluasa, menginfeksi sistem dan berpotensi menyebabkan kehilangan data atau kerusakan sistem.

   Lebih lanjut, ketiadaan firewall membuat router dan perangkat di belakangnya rentan terhadap serangan Denial of Service (DoS) atau Distributed Denial of Service (DDoS) yang dapat melumpuhkan koneksi internet dan layanan jaringan. Informasi sensitif yang tersimpan di perangkat internal juga berisiko tinggi untuk dicuri atau disadap. Router itu sendiri bisa diambil alih (dikompromikan), diubah konfigurasinya untuk tujuan jahat, digunakan sebagai bagian dari botnet untuk menyerang target lain, atau bahkan lalu lintas data yang melewatinya dapat dimata-matai.