COMPUTER ENGINEERING

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

Praktikum
Jaringan Komputer

Firewall NAT

Ahmad Arfian Syamsa - 5024231072

30 Mei 2025

1 Pendahuluan

1.1 Latar Belakang

Seiring berkembangnya teknologi dan meningkatnya ketergantungan terhadap jaringan komputer serta internet, ancaman terhadap keamanan data dan sistem juga ikut meningkat. Organisasi, institusi pendidikan, hingga pengguna individu kini tidak hanya membutuhkan koneksi internet yang cepat, tetapi juga sistem keamanan yang andal. Salah satu bentuk ancaman yang sering terjadi adalah upaya peretasan, penyebaran malware, serta akses tidak sah ke sistem internal. Untuk itu, dibutuhkan sebuah sistem pengaman yang mampu memfilter dan mengendalikan lalu lintas data yang keluar dan masuk ke dalam jaringan.

Sebelum adanya firewall, sistem keamanan jaringan masih mengandalkan Access Control List (ACL) yang hanya mampu membatasi akses berdasarkan alamat IP dan port tertentu. Namun, metode ini tidak cukup efektif karena tidak bisa menganalisis isi dari data yang dikirim, sehingga masih banyak celah keamanan yang bisa dimanfaatkan oleh pihak tidak bertanggung jawab. Oleh karena itu, teknologi firewall hadir sebagai solusi yang lebih canggih. Firewall dapat diibaratkan seperti satpam digital yang berjaga di gerbang jaringan—memeriksa, menyaring, dan mengatur data yang masuk atau keluar berdasarkan aturan yang telah ditentukan.

Firewall berperan penting dalam menjaga jaringan internal agar tetap aman dari serangan luar, terutama di era saat koneksi internet telah menjadi kebutuhan utama dalam kegiatan operasional. Dengan adanya firewall, sistem jaringan memiliki lapisan pertahanan yang kuat untuk mencegah gangguan dari pihak luar yang berpotensi membahayakan data atau sistem organisasi.

2 Dasar Teori

2.1 Pengertian Firewall

- Firewall adalah sistem keamanan jaringan yang berfungsi seperti penjaga gerbang digital—mengawasi dan mengatur lalu lintas data yang masuk dan keluar dari suatu jaringan atau perangkat. Firewall bekerja dengan cara menerapkan aturan tertentu untuk menentukan apakah data boleh diteruskan, diblokir, atau dicurigai sebagai ancaman.

2.2 Jenis jenis Firewall

2.2.1 Packet Filtering

- Berguna untuk memeriksa header paket data (seperti IP address, port, dan protocol).

2.2.2 Statefull Inspection Firewall

- Berfungsi untuk memantau status koneksi aktif dalam jaringan dan membuat keputusan berdasarkan konteks lalu lintas, bukan hanya berdasarkan satu paket data secara terpisah.

2.2.3 Application Layer Firewall

- Berfungsi untuk memeriksa header paket data (seperti IP atau port), tapi juga menganalisis isi sebenarnya dari data yang dikirim, seperti isi email, permintaan HTTP, atau data FTP.

2.2.4 Next Generation Firewall (NGFW)

- Berguna untuk menggabungkan fitur-fitur firewall tradisional (seperti packet filtering dan stateful inspection) dengan kemampuan keamanan tingkat lanjut

2.2.5 Circuit Level Gateway

- Menganalisis isi data (payload), tapi fokus pada apakah koneksi antar dua pihak sah dan sesuai aturan.

2.2.6 Software Firewall

- Bekerja di level sistem operasi dan biasanya digunakan untuk melindungi perangkat secara individual, bukan jaringan besar.

2.2.7 Hardware Firewall

- Seperti "gerbang pengaman" khusus yang berdiri sendiri dan bekerja tanpa harus diinstal di masing-masing komputer.

2.2.8 Cloud Firewall

- Firewall yang dijalankan di cloud. Cocok buat organisasi yang udah banyak pakai layanan cloud.

2.3 Cara kerja Firewa

Firewall itu seperti punya buku panduan aturan yang berisi siapa saja yang boleh atau tidak boleh mengakses jaringan. Setiap data yang ingin masuk atau keluar akan diperiksa dulu berdasarkan aturan ini. Contohnya, jika ada aturan yang melarang pegawai HRD mengakses server milik programmer, maka firewall akan otomatis memblokir akses tersebut. Aturan-aturan ini disesuaikan dengan kebutuhan dan kebijakan setiap organisasi.

2.4 Defini NAT (Network Addres Translation)

NAT ini semacam trik pintar yang memungkinkan banyak perangkat dalam satu jaringan — misalnya di rumah atau kantor kamu — bisa internetan hanya dengan satu IP publik saja. Jadi, walaupun cuma punya satu “alamat” di dunia maya, semua perangkat tetap bisa mengirim dan menerima data tanpa masalah.

Jika, alamat IPv4 yang tersedia cuma sekitar 4,3 miliar, tapi perangkat yang pakai internet jauh lebih banyak. Kalau tiap perangkat harus punya IP publik sendiri, alamatnya pasti cepat habis. Makanya NAT ini penting banget, karena dia bikin satu IP publik bisa dipakai bareng-bareng oleh semua perangkat di jaringan lokal. Jadi, internet tetap lancar tanpa perlu IP tambahan untuk tiap perangkat.

2.4.1 Jenis - jenis NAT

1. Static NAT Satu IP lokal dihubungkan ke satu IP publik (one-to-one). Jarang dipakai karena mahal dan boros IP publik. Cocok buat server yang butuh alamat tetap, misalnya buat hosting website.
2. Dynamic NAT IP lokal diubah ke IP publik dari kumpulan (pool) IP yang tersedia. Kalau IP di pool habis, permintaan koneksi ditolak. Tetap butuh banyak IP publik.
3. Port Address Translation (PAT) Ini yang paling sering dipakai. Banyak IP lokal bisa pakai satu IP publik dengan membedakan tiap koneksi berdasarkan port. Hemat dan efisien!

2.4.2 Cara Kerja NAT

1. **Alamat Privat dan Publik**
    - Setiap perangkat di jaringan lokal punya alamat IP privat (contoh: 192.168.x.x) yang cuma bisa dipakai di dalam jaringan itu saja. Tapi untuk akses ke internet, dibutuhkan alamat IP publik yang dikenali secara global.
2. **Translasi Alamat**
    - Saat perangkat di jaringan lokal ingin mengirim data ke internet, NAT akan mengganti alamat IP privat perangkat itu dengan alamat IP publik milik jaringan (misalnya alamat IP publik modem/router kamu).
3. **Mencatat Koneksi**
    - NAT juga mencatat port dan alamat asal setiap koneksi keluar. Jadi, ketika data balasan dari internet masuk, NAT tahu ke perangkat mana data itu harus diteruskan.
4. **Pengembalian Data**
    - Saat data dari internet datang kembali ke alamat IP publik, NAT mengubahnya lagi menjadi alamat IP privat yang sesuai dan meneruskannya ke perangkat yang benar di jaringan lokal.

2.4.3 Istilah Penting di NAT

- Inside Local Address: IP lokal perangkat di jaringan dalam (biasanya IP privat seperti 192.168.x.x)
- Inside Global Address: IP publik yang mewakili perangkat dari dalam jaringan ke dunia luar
- Outside Local Address: IP tujuan dari sisi luar yang udah diterjemahin di dalam jaringan
- Outside Global Address: IP asli dari tujuan di luar jaringan

3 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?**

Port Forwarding itu mengarahkan permintaan dari alamat IP publik dan port tertentu ke alamat IP privat dan port di dalam jaringan lokal. Jadi, ketika ada request ke IP publik (misal IP router/modem kamu) pada port 80, NAT akan meneruskan request itu ke server lokal di IP 192.168.1.10 port 80.

Dengan konfigurasi, seperti ;

- IP publik: [alamat IP publik kita sendiri]
- Port publik: 80 (HTTP)
- IP privat tujuan: 192.168.1.10
- Port privat tujuan: 80

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

   Menurutku, firewall lebih penting diterapkan terlebih dahulu di jaringan sebelum NAT, karena Firewall berfungsi sebagai penjaga utama jaringan yang mengontrol dan memfilter lalu lintas data masuk dan keluar berdasarkan aturan keamanan. Kemudian, Firewall bisa dipasang baik sebelum atau setelah NAT, bahkan di perangkat yang sama (seperti router modern). Tapi fungsi firewall sebagai filter utama harus aktif dulu untuk melindungi jaringan dari ancaman.

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

   - Tanpa firewall, router akan membuka semua jalur komunikasi ke dan dari internet. Ini berarti siapa pun dari luar bisa mencoba mengakses jaringan lokal, termasuk server, printer, atau perangkat pribadi.
   - Firewall biasanya memblokir lalu lintas mencurigakan atau berbahaya. Tanpanya, file atau paket data berisi malware, spyware, atau ransomware bisa langsung masuk ke jaringan tanpa hambatan.
   - Router yang terbuka bisa jadi target serangan DDoS atau lalu lintas ilegal, yang membuat jaringan lemot bahkan lumpuh. Firewall bisa membatasi koneksi yang tidak perlu dan menjaga bandwidth tetap optimal.
   - Firewall juga bisa digunakan untuk mengatur siapa bisa akses apa, misalnya blokir situs tertentu, batasi jam akses internet, atau cegah pegawai akses server yang bukan bagiannya. Tanpa itu, semua bebas mengakses apa saja.