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

Laporan Sementara
Praktikum Jaringan Komputer

Firewall & NAT

Devanka Raditanti Citasevi - 5024231053

2025

1 Pendahuluan

1.1 Latar Belakang

Dalam era digital saat ini, pertukaran data antarperangkat dan akses terhadap layanan internet menjadi kebutuhan utama bagi individu maupun organisasi. Namun, seiring meningkatnya ketergantungan terhadap jaringan, risiko terhadap keamanan juga semakin besar. Ancaman seperti serangan siber, akses ilegal, serta penyalahgunaan data menjadi tantangan nyata yang harus dihadapi dalam pengelolaan jaringan komputer.

Untuk mengatasi permasalahan tersebut, diterapkan berbagai teknologi pengaman jaringan, di antaranya adalah Firewall dan Network Address Translation (NAT). Firewall berperan sebagai pengendali akses data yang masuk dan keluar dari jaringan, layaknya penjaga gerbang yang menyaring lalu lintas berdasarkan aturan tertentu. Sementara itu, NAT memungkinkan banyak perangkat dalam jaringan lokal untuk berbagi satu alamat IP publik saat mengakses internet, sehingga menghemat penggunaan IP serta memberi lapisan keamanan tambahan.

Modul Firewall & NAT dalam praktikum jaringan komputer ini dirancang untuk memperkenalkan konsep dan mekanisme kerja kedua teknologi tersebut. Melalui pemahaman dan implementasi langsung, mahasiswa diharapkan dapat memahami pentingnya keamanan jaringan, serta mampu mengonfigurasi sistem jaringan yang aman dan efisien.

1.2 Dasar Teori

1. Firewall
   Firewall adalah sistem pengamanan jaringan yang berfungsi untuk mengontrol lalu lintas data berdasarkan kebijakan akses yang telah ditentukan. Firewall dapat diterapkan dalam bentuk perangkat lunak (software firewall) maupun perangkat keras (hardware firewall), dan bertugas menyaring paket data berdasarkan berbagai parameter seperti alamat IP, port, serta protokol yang digunakan.
   Jenis-jenis Firewall:
   - Packet Filtering: Menyaring data berdasarkan IP, port, dan protokol, namun tidak melihat konteks koneksi.
   - Stateful Inspection: Memeriksa status koneksi data, sehingga hanya koneksi sah yang diizinkan.
   - Application Layer Firewall: Menyaring lalu lintas berdasarkan konten aplikasi (misalnya HTTP atau FTP).
   - Next Generation Firewall (NGFW): Memiliki fitur lanjutan seperti deep packet inspection dan deteksi malware.
   - Circuit Level Gateway: Mengatur koneksi pada level session tanpa memeriksa isi data.
   - Software Firewall: Diinstal pada host untuk perlindungan individu, lebih fleksibel tapi membutuhkan konfigurasi.
   - Hardware Firewall: Berbentuk perangkat terpisah yang menyaring lalu lintas sebelum masuk ke jaringan internal.
   - Cloud Firewall: Diimplementasikan melalui layanan cloud untuk melindungi infrastruktur virtual.

Kebijakan Akses Firewall:

- Accept: Mengizinkan lalu lintas.
- Reject: Menolak lalu lintas dan memberi respon error.
- Drop: Menolak tanpa memberi respon.

2. Network Address Translation (NAT)
   NAT adalah metode untuk menerjemahkan alamat IP privat ke alamat IP publik dan sebaliknya. NAT memungkinkan beberapa perangkat dalam jaringan lokal mengakses internet menggunakan satu alamat IP publik, sehingga menghemat alokasi IP dan meningkatkan keamanan.
   Jenis-jenis NAT:

   - Static NAT: Pemetaan satu-ke-satu antara IP privat dan publik.
   - Dynamic NAT: IP privat diubah menjadi IP publik dari pool yang tersedia.
   - Port Address Translation (PAT): Banyak IP privat berbagi satu IP publik dengan membedakan koneksi melalui nomor port.

   Istilah Penting dalam NAT:

   - Inside Local Address: IP lokal dalam jaringan privat.
   - Inside Global Address: IP publik yang mewakili perangkat lokal ke luar.
   - Outside Local Address: Alamat IP tujuan dari sudut pandang jaringan internal.
   - Outside Global Address: Alamat IP sebenarnya dari tujuan di luar jaringan.

3. Connection Tracking
   Connection Tracking adalah mekanisme untuk mencatat dan memantau status koneksi data yang terjadi dalam jaringan. Fitur ini membantu firewall dan NAT dalam mengenali apakah suatu paket merupakan bagian dari koneksi yang sah atau tidak.
   Connection Tracking mencatat informasi seperti:

   - Alamat sumber dan tujuan
   - Port sumber dan tujuan
   - Protokol yang digunakan
   - Status koneksi (baru, aktif, selesai, invalid)

   Dengan adanya Connection Tracking, sistem dapat melakukan inspeksi status koneksi dengan lebih cerdas (stateful inspection), serta meningkatkan efisiensi dan keamanan lalu lintas jaringan.

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?
   Jawaban:
   Konfigurasi NAT yang perlu dibuat adalah Port Forwarding menggunakan Static NAT atau Destination NAT (DNAT).

Penjelasan:
Karena web server berada di jaringan lokal dengan IP privat (192.168.1.10), sedangkan yang mengakses berasal dari jaringan luar (internet), maka router harus meneruskan permintaan dari IP publik ke IP privat tersebut. Ini dilakukan dengan mengatur agar:

- Semua permintaan dari IP publik router ke port 80 diteruskan ke IP 192.168.1.10:80

Contoh Konfigurasi (secara umum):

```
1 iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT --to-destination
    192.168.1.10:80
2 iptables -A FORWARD -p tcp -d 192.168.1.10 --dport 80 -j ACCEPT
```

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

   - Keamanan adalah prioritas utama. Firewall bertugas menyaring lalu lintas yang boleh atau tidak boleh masuk/keluar dari jaringan, mencegah akses tidak sah, malware, dan serangan dari luar.
   - Firewall bekerja sebelum NAT dalam memfilter paket, terutama di banyak implementasi modern. Jadi, tanpa firewall, paket berbahaya bisa langsung masuk ke jaringan internal, bahkan sebelum proses NAT terjadi.
   - NAT hanya mengatur alur IP dan port, bukan menyaring konten. Jadi, meskipun NAT bisa menyembunyikan IP lokal, itu tidak cukup untuk mencegah serangan seperti DDoS, spoofing, atau akses ilegal.

   Kesimpulannya, firewall adalah garis pertahanan pertama. NAT bisa ditambahkan setelah itu sesuai kebutuhan komunikasi ke/dari internet.

3. Apa dampak negatif jika router tidak diberi filter firewall sama sekali?
   Jawaban:
   Beberapa dampak negatif yang mungkin terjadi adalah:

   (a) Jaringan jadi terbuka untuk semua akses eksternal.
      - Hacker bisa memindai dan menyerang perangkat internal karena tidak ada penyaring lalu lintas.

   (b) Potensi serangan malware meningkat.
      - Tanpa filter, malware bisa masuk dengan mudah dan menyebar ke seluruh jaringan lokal.

   (c) Penggunaan bandwidth tidak terkendali.
      - Akses ilegal dari luar bisa membebani jaringan, menurunkan performa.

   (d) Kebocoran data.
      - Tanpa firewall, tidak ada pengawasan lalu lintas keluar, sehingga data sensitif bisa bocor ke luar tanpa disadari.

(e) Tidak bisa menerapkan kebijakan akses internal.

- Misalnya pembatasan antar divisi atau blokir akses ke situs tertentu tidak bisa dilakukan.

Kesimpulan: Router tanpa firewall sama seperti rumah tanpa pintu: semua orang bisa masuk dan keluar seenaknya tanpa pengawasan, sangat berisiko.