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

# Laporan Sementara
# Praktikum Jaringan Komputer

## Firewall & NAT

Edward Natasaputra - 5024231023

2025

# 1 Pendahuluan

## 1.1 Latar Belakang

Perkembangan teknologi informasi yang pesat, terutama penggunaan internet dalam berbagai aktivitas organisasi dan individu, membawa tantangan baru dalam menjaga keamanan jaringan komputer. Koneksi internet yang terbuka memungkinkan akses yang luas, namun juga membuka celah bagi ancaman keamanan seperti serangan hacker, malware, dan akses tidak sah yang dapat merusak sistem atau mencuri data penting.

Sebelum adanya teknologi firewall, pengamanan jaringan masih menggunakan metode sederhana seperti Access Control List (ACL) yang hanya mampu membatasi akses berdasarkan alamat IP atau port tanpa kemampuan menganalisis isi data yang lewat. Hal ini menyebabkan banyak celah keamanan yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab.

Firewall hadir sebagai solusi keamanan yang lebih canggih dengan kemampuan memeriksa dan memfilter lalu lintas jaringan berdasarkan aturan yang lebih rinci dan kontekstual, mulai dari pemeriksaan paket sederhana hingga inspeksi pada lapisan aplikasi. Berbagai jenis firewall seperti Stateful Inspection dan Next Generation Firewall (NGFW) terus dikembangkan untuk menghadapi ancaman yang semakin kompleks.

Selain itu, keterbatasan alamat IP publik dalam protokol IPv4 menimbulkan kebutuhan akan mekanisme yang efisien dalam penggunaan alamat IP, sehingga lahirlah Network Address Translation (NAT). NAT memungkinkan banyak perangkat dalam jaringan lokal menggunakan satu alamat IP publik yang sama untuk mengakses internet, sekaligus berperan dalam menjaga keamanan jaringan dengan menyembunyikan alamat IP asli perangkat internal.

Untuk mendukung fungsi firewall dan NAT secara optimal, fitur Connection Tracking diperlukan agar router atau firewall dapat mengenali status koneksi dan mengizinkan paket data yang merupakan bagian dari koneksi yang sah, sekaligus memblokir koneksi yang tidak valid atau mencurigakan.

# 2 Dasar Teori

## 1. Firewall

Firewall adalah perangkat atau sistem keamanan jaringan yang bertindak sebagai satpam digital untuk memonitor dan mengendalikan lalu lintas data yang masuk dan keluar dari jaringan komputer. Firewall berfungsi untuk melindungi jaringan internal dari akses tidak sah, serangan, atau ancaman lain seperti virus dan malware.

Sebelum firewall, keamanan jaringan hanya mengandalkan Access Control List (ACL) yang kurang mampu mengontrol isi data secara mendetail. Dengan perkembangan teknologi dan kebutuhan koneksi internet, firewall hadir sebagai solusi yang lebih efektif untuk menjaga keamanan jaringan.

### Jenis-Jenis Firewall

**Tabel 1:** Jenis-Jenis Firewall

| Jenis Firewall | Keterangan |
|---|---|
| Packet Filtering | Memeriksa paket data satu per satu berdasarkan IP, port, dan protokol, namun tidak mengerti konteks komunikasi sehingga lebih kaku. |
| Stateful Inspection | Mampu mengenali status koneksi dan memeriksa apakah paket data bagian dari koneksi yang sah. |
| Application Layer Firewall | Memeriksa isi paket pada level aplikasi (misal HTTP, FTP) dan dapat memblokir konten tertentu. Biasanya menggunakan proxy. |
| Next Generation Firewall (NGFW) | Firewall modern dengan kemampuan inspeksi paket secara mendalam (deep packet inspection), termasuk data terenkripsi SSL. |
| Circuit Level Gateway | Beroperasi pada level koneksi (session) dan hanya memverifikasi validitas koneksi tanpa memeriksa isi data. |
| Software Firewall | Firewall yang terpasang pada komputer atau server, memberikan fleksibilitas pengaturan. |
| Hardware Firewall | Perangkat fisik yang dipasang di antara jaringan internet dan internal, untuk menahan serangan lebih awal. |
| Cloud Firewall | Firewall yang berjalan di layanan cloud, cocok untuk organisasi yang menggunakan layanan cloud. |

### Cara Kerja Firewall

Firewall menggunakan aturan (policy) yang telah ditentukan untuk memutuskan apakah suatu paket data boleh diteruskan (accept), ditolak dengan pesan error (reject), atau dibuang tanpa balasan (drop).

## 2. Network Address Translation (NAT)

NAT adalah teknik untuk menerjemahkan alamat IP lokal (private) ke alamat IP publik, sehingga banyak perangkat dalam jaringan lokal dapat menggunakan satu alamat IP publik yang sama untuk mengakses internet. Hal ini mengatasi keterbatasan jumlah alamat IPv4 yang terbatas.

### Jenis-Jenis NAT

### Cara Kerja NAT

Router yang menerapkan NAT mengubah alamat IP sumber paket data dari alamat lokal menjadi alamat publik saat data keluar, dan mengubah kembali alamat tujuan paket data dari publik ke lokal saat data masuk. Selain itu, NAT juga mengubah nomor port untuk membedakan koneksi yang terjadi secara bersamaan dari beberapa perangkat.

**Tabel 2:** Jenis-Jenis NAT

| Jenis NAT | Keterangan |
|---|---|
| Static NAT | Menghubungkan satu alamat IP lokal ke satu alamat IP publik secara permanen (one-to-one). Biasanya digunakan untuk server yang membutuhkan alamat tetap. |
| Dynamic NAT | Menggunakan kumpulan alamat IP publik yang tersedia dan menerjemahkan alamat lokal secara dinamis. Jika IP publik habis, koneksi ditolak. |
| Port Address Translation (PAT) | Banyak alamat IP lokal menggunakan satu alamat IP publik dengan membedakan setiap koneksi berdasarkan nomor port. Paling umum dan efisien. |

## 3. Connection Tracking

Connection Tracking adalah fitur yang melacak status koneksi jaringan dengan mencatat informasi seperti alamat sumber dan tujuan, port, protokol, serta status koneksi (baru, sudah ada, atau tidak valid). Fitur ini penting dalam mendukung firewall stateful dan NAT yang efisien, karena memungkinkan pengenalan paket balasan dan pencegahan koneksi tidak sah.

# 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?**

   Untuk mengakses web server lokal dari jaringan luar, konfigurasi NAT yang diperlukan adalah *Static NAT* atau *Port Forwarding*. Dengan konfigurasi ini, alamat IP publik diarahkan ke IP lokal 192.168.1.10 pada port 80 sehingga permintaan dari luar dapat diteruskan ke server lokal.

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

   Firewall sebaiknya diterapkan terlebih dahulu karena berfungsi sebagai pengaman utama yang memfilter lalu lintas data masuk dan keluar jaringan berdasarkan kebijakan keamanan. Firewall dapat memblokir akses yang tidak diinginkan sebelum data mencapai NAT dan jaringan internal. NAT berfokus pada penerjemahan alamat IP, sedangkan firewall berfokus pada pengamanan jaringan.

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

   Jika router tidak memiliki filter firewall, jaringan menjadi rentan terhadap serangan dari luar seperti akses tidak sah, penyebaran malware, dan eksploitasi celah keamanan. Tanpa firewall, tidak ada mekanisme kontrol lalu lintas data yang masuk dan keluar, sehingga potensi terjadinya pencurian data, gangguan layanan, atau kerusakan sistem meningkat secara signifikan.