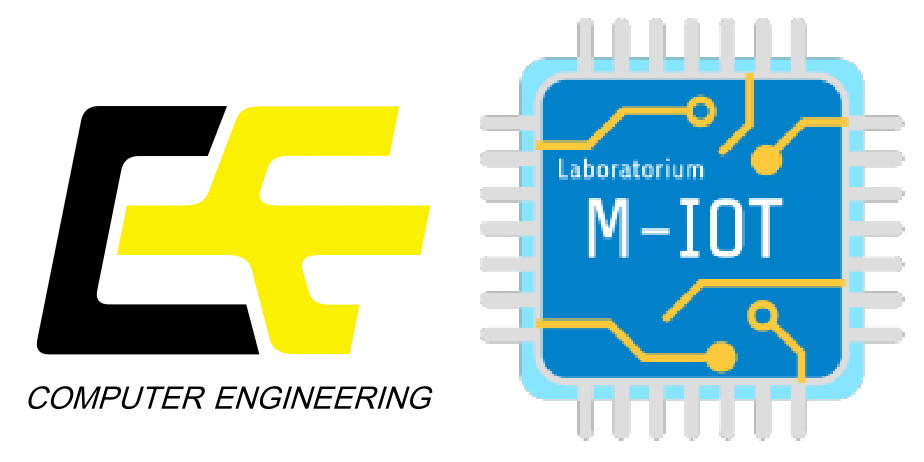
**Laboratorium Multimedia dan Internet of Things Departemen Teknik Komputer**

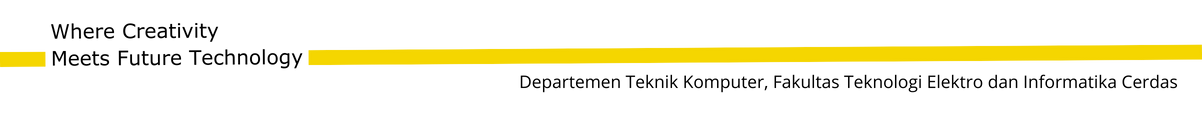
***Institut Teknologi Sepuluh Nopember***

Laporan Sementara Praktikum Jaringan Komputer

**Modul Firewall dan NAT**

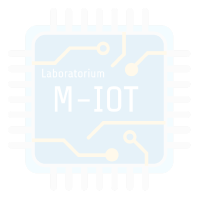
Benice Didan Al Ghifari- 5024231045

2025



# Pendahuluan

## Latar Belakang

 Di zaman digital yang semakin terhubung, aspek keamanan jaringan menjadi hal krusial yang harus diperhatikan baik oleh individu maupun organisasi. Berbagai ancaman seperti peretasan, malware, hingga akses tanpa izin menuntut adanya sistem perlindungan yang handal. Dalam konteks ini, firewall berperan sebagai lapisan pertahanan utama yang menyaring lalu lintas data, memastikan hanya data yang valid dan diotorisasi yang dapat masuk atau keluar dari jaringan internal. Seiring dengan meningkatnya penggunaan internet dalam berbagai aktivitas, keberadaan firewall menjadi kebutuhan penting untuk menjaga kerahasiaan serta keutuhan informasi.

Selain itu, Network Address Translation (NAT) juga memegang peran sentral dalam struktur jaringan masa kini. Dengan jumlah IP publik yang terbatas, NAT memungkinkan banyak perangkat di dalam jaringan lokal untuk mengakses internet hanya dengan satu alamat IP publik. Hal ini tidak hanya efisien dari sisi teknis dan biaya, tetapi juga menambah tingkat keamanan karena struktur internal jaringan tidak langsung terlihat oleh pihak luar.  
Oleh karena itu, pemahaman yang kuat mengenai konsep dan fungsi firewall serta NAT sangat diperlukan guna merancang sistem jaringan yang aman, efisien, dan tahan terhadap ancaman dari luar.

## Dasar Teori

**Firewall** adalah mekanisme keamanan jaringan yang digunakan untuk mengatur lalu lintas data yang masuk dan keluar dari sebuah sistem jaringan berdasarkan aturan tertentu. Fungsinya adalah menyaring paket data dan menentukan apakah data tersebut diizinkan untuk diteruskan, ditolak dengan pemberitahuan kesalahan, atau diabaikan tanpa tanggapan.  
Secara umum, terdapat beberapa jenis firewall yang dibedakan berdasarkan metode analisis datanya, seperti **packet filtering**, **stateful inspection**, **application layer firewall**, dan **next generation firewall**, yang memiliki tingkat kemampuan dan kecanggihan berbeda-beda dalam mendeteksi serta menangani lalu lintas jaringan.

Sementara itu, **NAT (Network Address Translation)** merupakan teknik yang digunakan oleh router untuk mengubah alamat IP dalam paket data. Dengan NAT, perangkat-perangkat di jaringan lokal bisa berkomunikasi dengan jaringan publik seperti internet.  
Terdapat beberapa varian NAT, yaitu **Static NAT**, **Dynamic NAT**, dan **PAT (Port Address Translation)**. Fungsi utama dari NAT adalah untuk menghemat penggunaan alamat IP publik dan melindungi struktur jaringan internal agar tidak terlihat dari luar. Dalam praktiknya, NAT sering kali bekerja berdampingan dengan firewall untuk menjaga keamanan jaringan sekaligus mengoptimalkan pengelolaan trafik data.

# Tugas Pendahuluan

### 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 dapat mengakses web server lokal dari jaringan luar, konfigurasi NAT yang perlu dibu- at adalah *Port Forwarding* atau *Static NAT*. Konfigurasi ini memungkinkan router untuk mene- ruskan permintaan dari IP publik pada port tertentu ke alamat IP privat server lokal yang se- suai. Misalnya, jika IP publik router adalah 203.0.113.2 dan ingin mengakses web server di

192.168.1.10:80, maka perlu dilakukan port forwarding dari 203.0.113.2:80 ke 192.168.1.10:80.

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

Firewall lebih penting untuk diterapkan terlebih dahulu karena berfungsi sebagai sistem keaman- an utama yang memfilter lalu lintas data berdasarkan aturan tertentu. Tanpa firewall, jaringan terbuka terhadap ancaman dari luar seperti serangan DDoS, malware, atau upaya peretasan. NAT memang memberikan keamanan pasif dengan menyembunyikan alamat IP privat, namun tidak memiliki kontrol selektif terhadap akses seperti yang dilakukan firewall.

### Apa dampak negatif jika router tidak diberi filter firewall sama sekali?

Tanpa filter firewall, router tidak dapat membatasi jenis lalu lintas yang masuk atau keluar, se- hingga berpotensi:

* + Membuka seluruh port ke internet, yang memungkinkan akses tidak sah.
  + Mempermudah penyebaran malware dan serangan terhadap perangkat di jaringan lokal.
  + Menyebabkan kebocoran data karena tidak adanya pengawasan lalu lintas.
  + Tidak adanya mekanisme log dan kontrol akses yang esensial untuk keamanan jaringan.

### Referensi

* + [Cisco - NAT Configuration: https://www.cisco.com/c/en/us/support/docs/ip/network-addr](https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/13772-12.html)ess- [translation-nat/13772-12.html](https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/13772-12.html)
  + [Cloudflare - What is a Firewall: https://www.cloudflare.com/learning/ddos/what-is-a-firewall/](https://www.cloudflare.com/learning/ddos/what-is-a-firewall/)
  + [Hostinger - Pengertian Firewall dan Cara Kerjanya https://www.hostinger.com/id/tutorial/apa-](https://www.hostinger.com/id/tutorial/apa-itu-firewall) [itu-firewall](https://www.hostinger.com/id/tutorial/apa-itu-firewall)
  + [Cyber Hub - Firewall: Pengertian, Fungsi, dan Cara Kerjanya: https://cyberhub.id/penge](https://cyberhub.id/pengetahuan-dasar/fungsi-manfaat-firewall)tahuan- [dasar/fungsi-manfaat-firewall](https://cyberhub.id/pengetahuan-dasar/fungsi-manfaat-firewall)