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

# Laporan Sementara
# Praktikum Jaringan Komputer

## Modul Firewall  NAT

Susilo Hendri Yudhoyono - 5024231016

2025

# 1 Pendahuluan

## 1.1 Latar Belakang

Perkembangan teknologi informasi dan komunikasi yang pesat telah menjadikan jaringan komputer sebagai bagian penting dalam kehidupan sehari-hari, baik dalam dunia pendidikan, bisnis, maupun pemerintahan. Seiring dengan meningkatnya kebutuhan akan konektivitas jaringan, aspek keamanan dan efisiensi jaringan menjadi hal yang sangat krusial untuk diperhatikan.

Firewall yaitu suatu kombinasi antara hardware (perangkat keras) dan software (perangkat lunak) yang fungsinya menjadi pemisah diantara jaringan komputer menjadi dua atau lebih untuk menjaga keamanan data. Pengertian lain dari firewall adalah suatu sistem kemanan pada jaringan komputer yang dipakai untuk melindungi komputer dari beberapa serangan dari komputer luar. Kenggunaan dari firewall adalah membatasi atau menjadi pengontrol kepada siapa saja yang memiliki akses ke jaringan pribadi dari jaringan luar. Firewall mengacu kepada sistem pengatur komunikasi antara dua jenis jaringan yang tidak sama. Dengan firewall dapat memastikan bahwa data pada komputer atau server yang tersambung tidak akan dapat dibuka oleh siapapun di Internet. Apabila ada pihak lain yang membuka atau mengakses informasi pribadi atau mengubah situs web maka akan di blokir oleh firewall.

NAT (Network Address Translation) adalah adalah sebuah proses pemetaan alamat IP dimana perangkat jaringan komputer akan memberikan alamat IP public ke perangkat jaringan local sehingga banyak IP private yang dapat mengakses IP public. Dengan kata lain NAT akan mentranslasikan alamat IP sehingga IP address pada jaringan local dapat mengakses IP public pada jaringan WAN. NAT mentranslasikan alamat IP private untuk dapat mengakses alamat host diinternat dengan menggunakan alamat IP public pada jaringan tersebut.

Melalui praktikum ini, mahasiswa diharapkan dapat memahami konsep dan implementasi firewall serta NAT dalam jaringan komputer. Praktikum ini memberikan kesempatan untuk mengonfigurasi aturan-aturan firewall, menerapkan teknik NAT, serta menganalisis dampak dan manfaatnya dalam pengelolaan jaringan yang aman dan efisien.

## 1.2 Dasar Teori

Network Address Translation (NAT) adalah proses pemetaan alamat IP yang memungkinkan perangkat dengan alamat IP privat pada jaringan lokal (LAN) untuk dapat terhubung ke jaringan publik seperti Internet melalui satu atau beberapa alamat IP publik. NAT sangat penting dalam lingkungan jaringan modern karena jumlah alamat IPv4 yang tersedia secara global semakin terbatas. Dengan menerjemahkan alamat IP privat menjadi IP publik, NAT memungkinkan banyak perangkat dalam jaringan lokal untuk berbagi satu alamat IP yang diberikan oleh ISP (Internet Service Provider).

Fungsi utama NAT adalah sebagai penghubung antara jaringan privat dan jaringan publik, serta sebagai penghemat penggunaan alamat IP global. Selain itu, NAT juga memberikan lapisan keamanan tambahan karena alamat IP privat tidak secara langsung terekspos ke jaringan luar. Hal ini membuat NAT umum digunakan dalam berbagai konfigurasi jaringan rumah maupun perusahaan.

Terdapat dua jenis utama dari NAT, yaitu Source NAT (SNAT) dan Destination NAT (DNAT). SNAT digunakan untuk mengubah alamat IP sumber dari paket data yang keluar dari jaringan internal ke jaringan eksternal. Biasanya SNAT diterapkan pada tahap postrouting. Sebaliknya, DNAT digunakan untuk mengubah alamat IP tujuan dari paket data yang masuk ke jaringan dari luar agar diarahkan

ke host tertentu dalam jaringan lokal. DNAT biasanya digunakan pada tahap prerouting, contohnya saat meneruskan permintaan ke server web lokal.

Cara kerja NAT melibatkan perubahan header pada paket data. Sebagai ilustrasi, ketika sebuah komputer dengan IP 192.168.1.2 mengirim permintaan ke www.google.com (misalnya IP 216.239.61.104), alamat sumber pada header akan diubah oleh router menjadi alamat IP publik, seperti 200.100.50.2. Ketika respons dari server kembali, NAT akan mengenali sesi tersebut dan mengubah alamat tujuan kembali menjadi alamat IP privat yang sesuai, sehingga paket sampai ke komputer pengirim.

Penggunaan NAT memiliki beberapa kelebihan, seperti menghindari konflik alamat IP di jaringan lokal, menghemat penggunaan IP legal, serta meningkatkan fleksibilitas pengelolaan jaringan. Namun, NAT juga memiliki kelemahan, antara lain dapat menambah latensi karena adanya proses translasi alamat, menyebabkan beberapa aplikasi tidak berjalan optimal (misalnya VoIP atau FTP aktif), serta menyulitkan proses pelacakan paket data karena informasi sumber atau tujuan telah dimodifikasi oleh NAT.

Firewall adalah sistem keamanan jaringan yang berfungsi untuk memfilter lalu lintas data antara dua atau lebih jaringan, serta melindungi jaringan internal dari akses yang tidak sah dari luar. Firewall dapat berupa kombinasi antara perangkat keras (hardware) dan perangkat lunak (software) yang bekerja dengan mengontrol data yang masuk dan keluar dari suatu jaringan berdasarkan seperangkat aturan keamanan yang telah ditentukan sebelumnya.

Fungsi utama dari firewall adalah sebagai pengontrol lalu lintas jaringan. Firewall memeriksa setiap paket data yang melewati jaringan dan menentukan apakah paket tersebut diizinkan atau ditolak berdasarkan kebijakan keamanan yang telah dikonfigurasi. Firewall juga dapat melakukan autentikasi terhadap permintaan akses data dan mendeteksi serta memblokir berbagai jenis ancaman, termasuk upaya peretasan atau pengaksesan informasi secara tidak sah. Selain itu, firewall dapat mencatat seluruh aktivitas jaringan yang mencurigakan, sehingga berguna sebagai alat monitoring dan analisis keamanan jaringan.

Secara umum, firewall terbagi menjadi dua jenis utama, yaitu *personal firewall* dan *network firewall*. Personal firewall dirancang untuk melindungi satu komputer dari akses tidak sah, dan sering kali dilengkapi dengan fitur tambahan seperti antivirus, antispyware, dan anti-spam. Sementara itu, network firewall dirancang untuk melindungi seluruh jaringan dan biasanya diimplementasikan pada tingkat gateway atau router. Network firewall dapat berupa perangkat khusus atau perangkat lunak yang berjalan di server dan dilengkapi fitur seperti packet filtering, stateful inspection, circuit-level gateway, application-level gateway, dan NAT firewall.

Firewall memiliki karakteristik khusus, seperti hanya mengizinkan lalu lintas jaringan yang dikenali dan melalui firewall, serta tahan terhadap berbagai bentuk serangan dari luar. Seluruh komunikasi yang terjadi dari dalam ke luar jaringan harus melalui firewall agar dapat diawasi dan dikendalikan.

Dalam cara kerjanya, firewall akan menganalisis setiap paket data berdasarkan aturan yang telah ditentukan. Jika sebuah paket tidak memenuhi kriteria yang telah ditetapkan, maka paket tersebut akan ditolak atau diblokir. Firewall juga dapat melakukan pencatatan terhadap seluruh aktivitas tersebut sebagai bagian dari fungsi pengawasan dan pelaporan.

Dengan penerapan firewall yang tepat, organisasi dapat memastikan bahwa data dan sistem jaringan mereka terlindungi dari berbagai jenis ancaman siber, menjaga kerahasiaan dan integritas informasi, serta menjaga ketersediaan layanan dalam jaringan.

## 2 Tugas Pendahuluan

1. Dilakukan dengan port forwarding. Konfigurasi akan meneruskan permintaan dari alamat IP publik (misalnya IP publik router) pada port tertentu (port 80) ke alamat IP privat 192.168.1.10 di dalam jaringan lokal.

2. Firewall jauh lebih penting, meskipun keduanya saling berhubungan. Alasannya adalah karena firewall berfungsi sebagai lapisan pertahanan utama terhadap serangan jaringan, seperti port scanning, akses tidak sah, malware, dan sebagainya. Tanpa firewall, jaringan lokal menjadi sangat rentan terhadap berbagai bentuk ancaman dari luar.

   https://www.cisco.com/site/us/en/learn/topics/security/what-is-a-firewall.html

3. Jika router tidak diberi filter firewall, maka jaringan menjadi sangat rentan terhadap akses tidak sah, serangan siber seperti malware dan port scanning, serta kebocoran data. Tanpa firewall, semua lalu lintas dari luar dapat langsung masuk ke jaringan internal tanpa penyaringan, sehingga meningkatkan risiko keamanan secara signifikan.

   https://www.techtarget.com/searchsecurity/definition/firewall