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

Laporan Sementara
Praktikum Jaringan Komputer

Firewall & NAT

Muhammad Tamim Nugraha - 5024231060

2025

1 Pendahuluan

1.1 Latar Belakang

Perkembangan pesat teknologi jaringan komputer menimbulkan kebutuhan yang semakin besar akan keamanan dan efisiensi dalam pengelolaan jaringan. Jaringan komputer tidak hanya menghubungkan perangkat dalam lingkup terbatas, tetapi juga memungkinkan akses ke sumber daya global seperti internet. Namun, dengan konektivitas yang luas ini, risiko terhadap ancaman keamanan seperti akses tanpa izin, serangan malware, dan penyalahgunaan data juga meningkat.

Untuk melindungi jaringan, diperlukan perangkat dan teknik yang mampu mengatur aliran data yang masuk dan keluar. Salah satu komponen penting adalah firewall, yang berfungsi sebagai pertahanan pertama dengan cara menyaring dan memblokir trafik yang mencurigakan atau berbahaya sesuai aturan keamanan yang diterapkan. Dengan firewall, administrator jaringan dapat mengontrol akses dan menjaga jaringan dari berbagai risiko keamanan.

Selain itu, keterbatasan jumlah alamat IP publik yang tersedia menjadi tantangan dalam mengelola jaringan, terutama bagi organisasi dengan banyak perangkat. Network Address Translation (NAT) menjadi solusi dengan memungkinkan banyak perangkat di jaringan lokal memakai alamat IP privat untuk terhubung ke internet melalui satu atau beberapa alamat IP publik. Selain menghemat penggunaan alamat IP, NAT juga menambah lapisan keamanan dengan menyembunyikan alamat IP internal dari jaringan luar.

Praktikum ini bertujuan memberikan pemahaman langsung tentang konfigurasi firewall dan NAT, sehingga mahasiswa dapat menerapkan konsep keamanan dan pengelolaan alamat IP dalam jaringan komputer. Melalui pengalaman praktis ini, diharapkan mahasiswa dapat merancang jaringan yang tidak hanya terhubung dengan baik tetapi juga aman dan efisien.

1.2 Dasar Teori

1.3 Firewall

Firewall adalah sistem keamanan jaringan yang bertugas mengatur dan mengawasi aliran data yang masuk dan keluar dari suatu jaringan sesuai dengan aturan yang telah ditetapkan. Fungsi utama firewall adalah melindungi jaringan dari akses ilegal serta serangan yang dapat merusak sistem. Firewall bisa berupa perangkat keras maupun perangkat lunak, dan biasanya digunakan untuk membatasi akses berdasarkan alamat IP, port, serta tipe protokol yang dipakai.

Jenis firewall yang umum digunakan antara lain:

- **Packet Filtering Firewall**, yang bekerja dengan menyaring paket berdasarkan header paket seperti alamat IP dan port.

- **Stateful Inspection Firewall**, yang selain memeriksa header paket juga memantau status koneksi sehingga lebih aman.
- **Application Layer Firewall**, yang mampu menginspeksi data pada tingkat aplikasi untuk deteksi ancaman lebih spesifik.

1.4 Network Address Translation (NAT)

NNetwork Address Translation (NAT) adalah metode yang digunakan untuk memodifikasi alamat IP pada header paket data saat melewati router atau firewall. Tujuan utama NAT adalah menghubungkan jaringan lokal yang memakai alamat IP privat dengan jaringan publik seperti internet melalui satu atau lebih alamat IP publik.

Ada beberapa jenis NAT, yaitu:

- **Static NAT**, yang memetakan alamat IP privat ke alamat IP publik secara tetap.
- **Dynamic NAT**, yang memetakan alamat IP privat ke alamat IP publik dari sebuah pool secara dinamis.
- **Port Address Translation (PAT)** atau NAT Overload, yang memungkinkan banyak perangkat menggunakan satu alamat IP publik dengan membedakan berdasarkan nomor port.

NAT juga berfungsi sebagai lapisan keamanan tambahan karena menyembunyikan alamat IP asli perangkat dalam jaringan lokal dari dunia luar.

1.5 Hubungan Firewall dan NAT

Firewall dan NAT biasanya digunakan bersamaan untuk menjaga keamanan serta mengelola alamat IP dalam sebuah jaringan. NAT memungkinkan perangkat di jaringan lokal yang menggunakan alamat IP privat untuk terhubung ke internet. Sementara itu, firewall berfungsi mengatur dan membatasi akses sekaligus melindungi jaringan dari berbagai ancaman, baik yang berasal dari luar maupun dari dalam. Gabungan kedua teknologi ini sangat penting dalam pengelolaan jaringan modern agar konektivitas tetap terjaga sekaligus keamanan jaringan dapat dipertahankan.

2 Tugas Pendahuluan

1. 1. Konfigurasi NAT untuk akses web server lokal dari jaringan luar

   Untuk mengakses web server lokal dengan alamat IP 192.168.1.10 pada port 80 dari luar jaringan, perlu dilakukan konfigurasi NAT tipe Destination NAT (DNAT) atau port forwarding. Konfigurasi ini membuat router meneruskan permintaan yang masuk ke alamat IP publik router pada port 80 ke alamat IP lokal server tersebut di jaringan

privat. Dengan demikian, pengguna dari luar dapat mengakses server lokal seolah-olah server tersebut berada di jaringan publik. Pengaturan ini biasanya dilakukan dengan menambahkan aturan NAT pada router yang memetakan alamat IP publik dan port tertentu ke alamat IP privat dan port server.

2. Mana yang lebih penting diterapkan terlebih dahulu: NAT atau Firewall?

Menurut saya, NAT (Network Address Translation) harus diterapkan terlebih dahulu karena berperan sebagai dasar yang memungkinkan perangkat dengan alamat IP privat dalam jaringan lokal dapat terhubung ke jaringan luar seperti internet menggunakan satu atau beberapa alamat IP publik. Tanpa NAT, perangkat dengan IP privat tidak bisa berkomunikasi langsung dengan jaringan eksternal karena alamat privat tidak dapat dirutekan di internet. Setelah koneksi jaringan terbentuk melalui NAT, firewall dapat dipasang untuk mengontrol dan mengamankan lalu lintas data yang masuk dan keluar. Firewall berfungsi membatasi akses, menyaring paket, dan mencegah ancaman, sehingga fungsinya akan optimal jika koneksi jaringan sudah tersedia lewat NAT. Oleh sebab itu, NAT harus diterapkan terlebih dahulu agar jaringan dapat terkoneksi, kemudian firewall diterapkan untuk meningkatkan keamanan.

3. Dampak negatif jika router tidak memiliki filter firewall

Jika router tidak dilengkapi filter firewall, maka jaringan akan sangat rentan terhadap berbagai ancaman dari luar maupun dalam. Tanpa firewall, semua lalu lintas data yang masuk dan keluar tidak disaring atau dibatasi, sehingga semua jenis koneksi akan diterima tanpa pengecekan. Kondisi ini memudahkan pihak tidak berwenang seperti peretas atau malware untuk mengakses perangkat di jaringan internal tanpa hambatan. Akibatnya, jaringan bisa mengalami kebocoran data, penyebaran virus, serta serangan serius seperti hacking, brute force, atau Distributed Denial of Service (DDoS). Selain itu, tanpa firewall tidak ada mekanisme untuk mengendalikan atau memblokir trafik yang mencurigakan, yang bisa menurunkan performa dan mengancam stabilitas sistem. Singkatnya, tanpa firewall jaringan menjadi terbuka sepenuhnya dan tidak terlindungi, sehingga berisiko mengalami kerugian besar secara teknis maupun operasional.