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

Laporan Sementara
Praktikum Jaringan Komputer

Firewall & NAT

Aminah Nur'aini Muchayati - 5024231034

2025

1 Pendahuluan

1.1 Latar Belakang

Dalam perkembangan teknologi informasi dan komunikasi yang semakin pesat, jaringan komputer memiliki peran yang sangat penting dalam menunjang berbagai aktivitas, baik dalam bidang pendidikan, bisnis, pemerintahan, maupun kehidupan sehari-hari. Namun, seiring dengan tingginya ketergantungan terhadap jaringan, muncul pula berbagai ancaman terhadap keamanan data dan sistem yang dapat mengganggu integritas, kerahasiaan, dan ketersediaan informasi. Salah satu upaya yang dilakukan untuk melindungi jaringan dari berbagai potensi ancaman tersebut adalah dengan menerapkan sistem keamanan jaringan berupa firewall, yang berfungsi sebagai pengatur lalu lintas data berdasarkan aturan tertentu untuk mencegah akses yang tidak sah, baik dari dalam maupun luar jaringan. Di sisi lain, penggunaan alamat IP publik yang terbatas menuntut adanya solusi yang dapat mengakomodasi banyak perangkat dalam satu jaringan lokal untuk dapat terhubung ke jaringan global (internet), dan di sinilah peran Network Address Translation (NAT) menjadi sangat penting, karena memungkinkan pengubahan alamat IP privat menjadi IP publik, serta memungkinkan pemetaan lalu lintas jaringan secara fleksibel. Melalui praktikum ini, mahasiswa diharapkan tidak hanya memahami konsep dasar firewall dan NAT secara teoritis, tetapi juga mampu mengimplementasikan dan mengkonfigurasikannya secara langsung dalam skenario jaringan, sehingga dapat meningkatkan pemahaman terhadap pengelolaan dan pengamanan jaringan komputer secara menyeluruh dan aplikatif.

1.2 Dasar Teori

1.2.1 Firewall

Firewall merupakan salah satu komponen penting dalam sistem keamanan jaringan komputer. Secara umum, firewall berfungsi sebagai penghalang antara jaringan internal yang terpercaya dan jaringan eksternal yang tidak terpercaya seperti internet. Firewall dapat berupa perangkat keras khusus, perangkat lunak, atau gabungan keduanya yang dirancang untuk memantau, menyaring, serta mengatur lalu lintas data yang masuk maupun keluar dari jaringan berdasarkan aturan keamanan yang telah ditentukan. Firewall bekerja dengan prinsip "allow" dan "deny", di mana setiap paket data diperiksa dan dibandingkan dengan kebijakan yang telah dikonfigurasikan sebelumnya. Dengan firewall, administrator dapat mencegah akses tidak sah, serangan siber, serta kebocoran data sensitif yang berasal dari atau menuju luar jaringan (Stallings, 2007). Penerapan firewall sangat krusial, khususnya pada jaringan organisasi dan perusahaan yang menyimpan data penting dan memiliki banyak titik akses.

1.2.2 Jenis-Jenis Firewall

Terdapat beberapa jenis firewall berdasarkan cara kerja dan tingkat perlindungan yang diberikan, antara lain:

1. Packet Filtering Firewall
   Memeriksa header paket (IP, port, protokol) dan mengizinkan atau memblokir berdasarkan aturan sederhana. Cepat tapi hanya melihat data permukaan.
2. Stateful Inspection Firewall
   Melacak status koneksi dan konteks lalu lintas untuk keputusan lebih cerdas dan aman.

3. Application Layer Firewall
   Memantau isi data pada lapisan aplikasi dan memfilter berdasarkan jenis aplikasi atau konten.
4. Next Generation Firewall (NGFW)
   Menggabungkan fitur inspeksi mendalam, deteksi intrusi, dan kontrol aplikasi untuk perlindungan lebih lengkap.

1.2.3 Network Address Translation (NAT)

NAT adalah teknik yang digunakan pada router untuk menerjemahkan alamat IP dari satu jaringan ke jaringan lainnya. Biasanya NAT digunakan untuk menghubungkan jaringan lokal (yang menggunakan alamat IP privat) ke jaringan internet publik. NAT memungkinkan banyak perangkat dalam jaringan lokal berbagi satu alamat IP publik, sehingga membantu mengurangi kebutuhan alamat IP publik dan memberikan lapisan keamanan tambahan karena perangkat di jaringan privat tidak dapat langsung diakses dari luar. Dalam NAT, router mencatat koneksi yang keluar dan melakukan pemetaan ulang terhadap paket data yang masuk agar sampai ke tujuan yang benar (Kurose & Ross, 2021). Penggunaan NAT sangat umum dalam perangkat seperti router rumah tangga, jaringan perkantoran, dan sistem firewall berbasis perangkat lunak seperti pfSense dan MikroTik.

1.2.4 Jenis-Jenis NAT

NAT memiliki beberapa jenis utama berdasarkan cara pemetaan alamat IP-nya:

1. Static NAT: Jenis NAT ini menerjemahkan satu alamat IP privat ke satu alamat IP publik secara permanen. Digunakan jika suatu perangkat internal harus dapat diakses dari luar, seperti server web atau FTP.
2. Dynamic NAT: Pemetaan antara IP privat dan IP publik dilakukan secara dinamis dari sebuah kumpulan (pool) alamat IP publik. Cocok untuk jaringan dengan jumlah IP publik terbatas dan trafik yang tidak tetap.
3. Port Address Translation (PAT): Juga dikenal sebagai NAT Overload, jenis ini memungkinkan banyak perangkat dengan IP privat menggunakan satu IP publik dengan membedakan sesi komunikasi berdasarkan port sumber. PAT sangat efisien dan merupakan jenis NAT yang paling banyak digunakan, terutama dalam lingkungan rumah dan kantor kecil.

1.2.5 Peran Firewall dan NAT dalam Keamanan dan Efisiensi Jaringan

Firewall dan NAT merupakan komponen integral dalam sistem pengamanan dan pengelolaan jaringan modern. Firewall bertindak sebagai lapisan pertahanan utama terhadap akses yang tidak sah dan serangan dari luar, sementara NAT memberikan fleksibilitas dalam pengalokasian alamat IP serta menyembunyikan struktur internal jaringan. Keduanya sering diimplementasikan bersamaan dalam satu perangkat atau sistem terintegrasi, seperti pada router Mikrotik, pfSense firewall, dan perangkat UTM (Unified Threat Management). Dengan menggabungkan penggunaan firewall dan NAT, jaringan tidak hanya menjadi lebih aman dari ancaman eksternal, tetapi juga lebih efisien dan ekonomis dalam pemanfaatan sumber daya alamat IP.

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 : Untuk memungkinkan akses dari jaringan luar ke web server lokal yang berada di jaringan privat dengan alamat IP 192.168.1.10 dan port 80, diperlukan konfigurasi Network Address Translation (NAT) jenis Port Forwarding atau Destination NAT (DNAT). Konfigurasi ini memungkinkan router meneruskan permintaan dari IP publik pada port tertentu (dalam hal ini port 80) ke alamat IP privat server di dalam jaringan lokal. Dengan kata lain, ketika pengguna dari luar mengakses IP publik router melalui port 80, router akan mengalihkan permintaan tersebut ke 192.168.1.10:80. Teknik ini umum digunakan untuk mempublikasikan layanan lokal ke internet secara terbatas dan terkendali

2. **Menurutmu, mana yang lebih penting diterapkan terlebih dahulu di jaringan: NAT atau Firewall? Jelaskan alasanmu**
   jawaban : Menurut saya, firewall lebih penting untuk diterapkan terlebih dahulu, meskipun secara teknis NAT biasanya dikonfigurasikan lebih dulu. NAT memang dibutuhkan agar perangkat lokal bisa terkoneksi ke internet (Kurose and Ross, 2021), tetapi firewalllah yang memastikan keamanan jaringan saat koneksi itu terjadi. Firewall menyaring lalu lintas, mencegah akses tidak sah, dan mendeteksi ancaman. Tanpa firewall, NAT justru membuka jalan bagi potensi serangan dari luar. Jadi, firewall adalah fondasi utama dalam membangun jaringan yang aman.

3. **Apa dampak negatif jika router tidak diberi filter firewall sama sekali?**
   jawaban : Jika router tidak diberi filter firewall sama sekali, jaringan akan sangat terbuka terhadap berbagai ancaman eksternal. Lalu lintas data masuk akan diterima tanpa adanya proses verifikasi atau penyaringan, yang memungkinkan terjadinya eksploitasi sistem melalui port scanning, serangan brute force, maupun penyebaran malware. Bahkan, perangkat internal dapat digunakan secara tidak sah sebagai bagian dari serangan siber skala besar seperti distributed denial-of-service (DDoS). Tanpa firewall, kontrol terhadap lalu lintas masuk dan keluar tidak tersedia, sehingga data penting pun berpotensi bocor atau disalahgunakan (Stallings, 2007). Firewall menyediakan perlindungan berlapis yang dapat mengidentifikasi pola serangan, membatasi akses berdasarkan IP atau port, serta mencatat log untuk audit keamanan jaringan.