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

Laporan Sementara
Praktikum Jaringan Komputer

Firewall dan NAT

Rendy Lexxy Kurniawan - 5024231007

2025

1 Pendahuluan

1.1 Latar Belakang

Dalam perkembangan teknologi jaringan komputer saat ini, kebutuhan akan komunikasi jaringan yang terbuka dan cepat harus diimbangi dengan sistem perlindungan yang handal (*robust*) untuk menjaga keamanan data dan stabilitas koneksi. Setiap sistem jaringan, baik berskala kecil maupun besar, rentan terhadap ancaman eksternal seperti akses tidak sah, peretasan, dan penyalahgunaan layanan jaringan. Oleh karena itu, dibutuhkan mekanisme pengendalian lalu lintas data dan perlindungan terhadap sumber daya internal yang efektif, salah satunya melalui penggunaan firewall dan NAT (Network Address Translation). Keduanya merupakan komponen penting dalam pengamanan dan manajemen jaringan yang bekerja pada lapisan yang berbeda namun saling melengkapi. Modul praktikum ini dirancang untuk memperkenalkan dan mengasah pemahaman mahasiswa dalam mengimplementasikan konfigurasi firewall dan NAT, baik secara konseptual maupun praktis, guna menciptakan jaringan yang aman dan efisien.

Firewall berperan sebagai sistem penyaring lalu lintas data yang masuk maupun keluar dari jaringan, berdasarkan seperangkat aturan yang ditentukan. Sementara itu, NAT memungkinkan perangkat dalam jaringan privat untuk mengakses jaringan publik (seperti internet) menggunakan satu atau beberapa alamat IP publik. Dengan menggabungkan fungsi perlindungan dan manajemen pengalamatan, firewall dan NAT menjadi fondasi penting dalam desain jaringan komputer modern. Praktikum ini bertujuan tidak hanya untuk memahami fungsi teknis dari masing-masing komponen, tetapi juga untuk melatih keterampilan konfigurasi dalam skenario nyata, termasuk pengaturan connection tracking dan penerapan kebijakan akses yang adaptif.

1.2 Dasar Teori

Firewall adalah sistem keamanan jaringan yang berfungsi untuk mengontrol dan memfilter lalu lintas data berdasarkan aturan yang telah ditentukan oleh administrator. Firewall dapat berupa perangkat keras (hardware) maupun perangkat lunak (software), dan biasanya ditempatkan di antara jaringan internal dan eksternal. Berdasarkan metode kerjanya, terdapat beberapa jenis firewall, antara lain: packet filtering firewall yang bekerja dengan menyaring paket berdasarkan header (IP, port, dan protokol), stateful inspection firewall yang dapat melacak status koneksi, application layer firewall yang bekerja pada lapisan aplikasi dan mampu memfilter konten, serta next-generation firewall (NGFW) yang menggabungkan kemampuan inspeksi mendalam dan deteksi ancaman berbasis konteks. Firewall bekerja dengan menerapkan kebijakan akses (access control policies), yang bisa bersifat allow, deny, atau drop, tergantung pada parameter yang dipantau.

Network Address Translation (NAT) adalah proses yang digunakan untuk mengubah alamat IP sumber atau tujuan dalam header paket IP saat melewati perangkat jaringan, seperti router. Tujuan utama NAT adalah untuk menghemat penggunaan alamat IP publik, memungkinkan banyak perangkat di jaringan privat untuk berbagi satu atau beberapa alamat IP publik saat mengakses internet. Terdapat beberapa jenis NAT, antara lain Static NAT (pemetaan satu-ke-satu antara IP privat dan publik), Dynamic NAT (pemetaan dari IP privat ke IP publik dari sebuah pool secara acak), dan Port Address Translation (PAT) atau NAT Overload, yang merupakan bentuk paling umum digunakan—menggunakan satu IP publik dengan identifikasi unik melalui nomor port. NAT tidak hanya meningkatkan efisiensi pengalamatan, tetapi juga memberi efek keamanan dengan menyembunyikan

struktur jaringan internal dari jaringan eksternal.

Dalam implementasi NAT, terdapat beberapa istilah penting yang perlu dipahami, seperti inside local address (alamat IP privat dari host dalam jaringan internal), inside global address (alamat publik yang digunakan untuk merepresentasikan host internal di internet), outside local address (alamat IP dari host luar yang terlihat oleh jaringan internal), dan outside global address (alamat IP asli dari host eksternal di internet). Pemahaman terhadap istilah-istilah ini penting untuk dapat membaca dan menganalisis tabel NAT serta log koneksi dengan benar.

Salah satu komponen penting dalam sistem firewall dan NAT modern adalah Connection Tracking. Connection tracking adalah mekanisme yang memungkinkan sistem untuk memantau status koneksi jaringan secara real-time, sehingga perangkat seperti router atau firewall dapat mengetahui apakah sebuah paket merupakan bagian dari koneksi baru, koneksi yang sudah ada, atau koneksi yang tidak sah. Dalam praktiknya, connection tracking digunakan untuk mendukung firewall berbasis status (stateful firewall), memungkinkan penerapan aturan yang lebih dinamis dan adaptif. Misalnya, aturan firewall dapat mengizinkan paket hanya jika termasuk dalam koneksi yang sudah diinisiasi dari dalam jaringan, dan menolak koneksi masuk yang tidak diminta dari luar. Connection tracking juga menjadi dasar dalam pembuatan log keamanan dan diagnosis lalu lintas jaringan.

2 Tugas Pendahuluan

Berikut adalah jawaban dari tugas pendahuluan yang telah dikerjakan, beserta penjelasan dari jawaban tersebut!

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?
   Ketika ingin mengakses web server lokal dari jaringan luar (akses masuk), konfigurasi NAT yang cocok dipakai adalah Destination NAT (DNAT) atau lebih dikenal sebagai Port Forwarding. Dalam hal ini, NAT akan mengalihkan permintaan dari IP publik router (misalnya IP: 203.0.113.2 pada port 80) ke alamat IP internal 192.168.1.10 pada port yang sama. Pada MikroTik, hal ini bisa dikonfigurasi dengan fitur Firewall → NAT, menggunakan *chain=dstnat, protocol=tcp, dst-port=80*, dan *action=dst-nat* ke IP lokal dan port 80.

2. Menurutmu, mana yang lebih penting diterapkan terlebih dahulu di jaringan: NAT atau Firewall? Jelaskan alasanmu!
   Secara teknis, firewall lebih penting untuk diterapkan terlebih dahulu, karena fungsinya bersifat preventif dan protektif terhadap akses yang tidak sah, serangan dari luar, serta lalu lintas yang tidak diinginkan. Firewall menentukan siapa yang boleh masuk dan keluar dari jaringan serta mengatur jenis data apa yang diizinkan. Tanpa firewall, semua lalu lintas akan diterima begitu saja tanpa adanya filtering data, sehingga berpotensi masuknya ancaman seperti port scanning, brute force login, dan malware.

   Meskipun NAT juga penting, terutama untuk menghubungkan jaringan privat ke internet dan menghemat IP publik, fungsinya lebih bersifat pengelolaan alamat daripada perlindungan. Dengan kata lain, NAT mengatur “jalur keluar-masuk” alamat IP, sedangkan firewall menentukan apakah lalu lintas tersebut diizinkan atau diblokir. Dalam praktik terbaik, NAT dan firewall memang saling melengkapi, namun keamanan harus selalu menjadi prioritas utama, sehingga firewall idealnya dikonfigurasi terlebih dahulu.

3. Apa dampak negatif jika router tidak diberi filter firewall sama sekali?
   Jika router tidak memiliki filter firewall, maka seluruh lalu lintas, baik masuk maupun keluar akan diterima tanpa batasan. Hal ini akan menimbulkan risiko yang serius, di antaranya:

   - **Terbukanya akses langsung ke layanan internal**, seperti SSH, Telnet, Web Server, atau database, yang seharusnya dibatasi hanya untuk jaringan internal.
   - **Router menjadi target serangan langsung**, seperti brute-force login, port scanning, atau eksploitasi layanan terbuka.
   - **Potensi penyebaran malware atau serangan DDoS** melalui jaringan yang tidak terlindungi (tidak ada firewall), baik sebagai korban maupun sebagai titik penyebar.
   - **Tidak ada kontrol terhadap lalu lintas keluar**, sehingga host dalam jaringan bisa mengakses situs berbahaya atau mengirim data ke luar tanpa terdeteksi.