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

Laporan Sementara
Praktikum Jaringan Komputer

Firewall dan NAT

Yudhi Nendra Kurniawan - 5024231012

2025

1 Pendahuluan

1.1 Latar Belakang

Dalam era digital yang semakin berkembang pesat, kebutuhan akan jaringan komputer yang aman dan efisien menjadi sangat penting, terutama dalam mendukung aktivitas komunikasi dan pertukaran data. Ketersediaan koneksi internet yang luas membuka peluang besar, namun di sisi lain juga menghadirkan berbagai ancaman keamanan yang dapat membahayakan sistem jaringan. Oleh karena itu, penggunaan teknologi seperti Firewall dan Network Address Translation (NAT) menjadi solusi utama dalam melindungi jaringan internal dari akses tidak sah sekaligus memungkinkan perangkat dalam jaringan lokal untuk terhubung ke internet secara efisien. Firewall bertindak sebagai pengawas lalu lintas jaringan yang menyaring data berdasarkan aturan keamanan, sementara NAT berfungsi untuk menerjemahkan alamat IP privat ke publik agar perangkat dapat mengakses internet dengan sumber daya IP yang terbatas. Praktikum ini disusun untuk memperkenalkan konsep dasar serta implementasi teknis dari firewall dan NAT menggunakan perangkat jaringan MikroTik, guna memberikan pemahaman praktis kepada peserta mengenai bagaimana keamanan dan konektivitas jaringan dapat dikonfigurasi secara langsung.

1.2 Dasar Teori

Dalam sistem jaringan komputer, aspek keamanan dan efisiensi komunikasi merupakan dua hal penting yang harus dikelola dengan baik. Untuk itu, penggunaan teknologi seperti Firewall dan Network Address Translation (NAT) telah menjadi komponen fundamental dalam desain jaringan modern, terutama dalam mengatur lalu lintas data serta menjaga sistem dari potensi ancaman eksternal. Firewall dan Network Address Translation (NAT) merupakan dua komponen krusial dalam sistem jaringan komputer yang berperan besar dalam menjaga keamanan dan efisiensi lalu lintas data. Firewall adalah sistem yang bertugas menyaring dan mengendalikan lalu lintas data berdasarkan aturan tertentu, sehingga hanya lalu lintas yang sah yang diizinkan masuk atau keluar dari jaringan. Jenis-jenis firewall sangat beragam, mulai dari packet filtering yang menyaring berdasarkan IP dan port, stateful inspection yang memantau status koneksi, hingga next-generation firewall (NGFW) yang mampu melakukan deep packet inspection dan pengenalan aplikasi. Di sisi lain, NAT adalah mekanisme yang memungkinkan banyak perangkat dalam jaringan lokal untuk mengakses internet melalui satu alamat IP publik, sehingga membantu mengatasi keterbatasan jumlah alamat IPv4. NAT memiliki beberapa jenis, seperti static NAT, dynamic NAT, dan yang paling umum digunakan yaitu Port Address Translation (PAT) yang memanfaatkan port untuk membedakan koneksi antar perangkat. Untuk mendukung kinerja firewall dan NAT, router modern dilengkapi dengan fitur connection tracking, yaitu kemampuan mencatat dan memantau semua koneksi yang melewati router. Fitur ini memungkinkan sistem mengenali koneksi yang sah, baru, atau tidak valid, sehingga dapat meningkatkan keamanan jaringan melalui penerapan stateful firewall serta membantu proses NAT secara lebih akurat. Dengan memadukan ketiga komponen ini—firewall, NAT, dan connection tracking—sistem jaringan dapat dikonfigurasi secara aman, efisien, dan dapat diandalkan untuk menunjang kebutuhan komunikasi data yang semakin kompleks di era digital saat ini.

2 Tugas Pendahuluan

1. Untuk dapat mengakses web server lokal dengan alamat IP 192.168.1.10 dan port 80 dari jaringan luar, diperlukan konfigurasi Static NAT atau lebih tepatnya Destination NAT (DNAT). Konfigurasi ini memungkinkan lalu lintas dari internet yang ditujukan ke IP publik router dialihkan ke alamat IP privat server yang ada di jaringan internal. Dengan kata lain, router akan menerjemahkan IP tujuan dari paket yang datang menjadi IP lokal server, sambil mempertahankan port-nya agar layanan web tetap dapat dijangkau. Contohnya, jika IP publik router adalah 203.0.113.5, maka router akan mengarahkan semua permintaan ke port 80 dari IP tersebut ke 192.168.1.10:80. Konsep ini umum digunakan dalam skenario hosting website di jaringan lokal tanpa harus memiliki banyak IP publik.

2. Dalam arsitektur keamanan jaringan, penerapan firewall sebaiknya dilakukan sebelum NAT. Firewall berfungsi sebagai lapisan pertahanan utama yang menyaring trafik berdasarkan kebijakan keamanan—baik dari luar maupun dalam jaringan. Setelah trafik yang aman terverifikasi, NAT barulah menerjemahkan alamat IP dan port untuk koneksi ke luar. Jika NAT diterapkan tanpa firewall terlebih dahulu, maka seluruh bawaannya akan terekspos ke internet, sehingga rentan terhadap serangan. Panduan dari teknologi keamanan seperti Palo Alto Networks dan Check Point menegaskan bahwa NAT dan routing dilakukan dulu untuk menentukan zona, namun rule firewall baru akan dievaluasi setelah itu

3. Router tanpa firewall berarti tidak ada screening atas lalu lintas yang masuk dan keluar, sehingga jaringan menjadi sangat rentan. Hal ini dapat menyebabkan berbagai risiko seperti downtime jaringan lengkap karena serangan DDoS, infeksi malware, eksploitasi port terbuka, serta pencurian atau kerusakan data bisnis . Sumber dari ITS ASAP dan Minerva bahkan menyebut tanpa firewall, "network downtime" bisa terjadi dan kerugian bisa membahayakan eksistensi bisnis . Diskusi di forum F5 dan DevCentral menambahkan bahwa membuka semua port sama artinya seperti mengundang kerusakan dan ekspos risiko serangan secara langsung

    - https://community.f5.com/discussions/technicalforum/if-there-is-no-firewall-the-risk-o 309784
    - https://live.paloaltonetworks.com/t5/next-generation-firewall/routing-and-nat-order-pr td-p/570455
    - https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Fireware/configuration_examples/snat_web_server_config_example.html