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

Laporan Sementara
Praktikum Jaringan Komputer

Firewall and NAT

Alfito Ichsan Galaksi - 5024231071

2025

1 Pendahuluan

1.1 Latar Belakang

Seiring berkembangnya teknologi informasi dan komunikasi, kebutuhan akan jaringan komputer yang aman dan efisien menjadi sangat penting, khususnya dalam lingkungan organisasi maupun rumah tangga yang terhubung ke internet. Akses ke berbagai layanan seperti web server, email, dan layanan cloud tidak terlepas dari risiko ancaman keamanan seperti peretasan, pencurian data, dan penyebaran malware. Oleh karena itu, penerapan sistem keamanan jaringan seperti Firewall dan Network Address Translation (NAT) sangat diperlukan. Firewall bertugas sebagai pengawas lalu lintas data yang masuk dan keluar dari jaringan dengan menerapkan kebijakan tertentu, sedangkan NAT berfungsi untuk menghubungkan jaringan privat ke internet menggunakan IP publik secara efisien. Selain itu, fitur Connection Tracking juga berperan penting dalam mengelola status koneksi dan mempermudah proses filtering dan NAT. Praktikum ini bertujuan untuk memahami dan mengimplementasikan konsep dasar firewall dan NAT dalam jaringan komputer, serta mengenali pentingnya mekanisme keamanan tersebut dalam mencegah ancaman siber.

1.2 Dasar Teori

Firewall adalah sistem keamanan jaringan yang berfungsi untuk mengatur dan mengendalikan lalu lintas data berdasarkan aturan yang telah ditentukan. Firewall dapat berupa perangkat keras (hardware) atau perangkat lunak (software) yang bertindak sebagai penyaring lalu lintas data antara dua jaringan, umumnya antara jaringan internal dan internet. Berdasarkan jenisnya, firewall dapat berupa packet filtering, stateful inspection, hingga next-generation firewall (NGFW) yang mendukung pemeriksaan mendalam terhadap data (deep packet inspection).

Network Address Translation (NAT) adalah metode yang digunakan untuk mengubah alamat IP dalam paket data agar dapat melintasi jaringan yang menggunakan skema alamat berbeda, biasanya dari jaringan lokal ke jaringan publik (internet). Jenis NAT yang umum digunakan meliputi Static NAT, Dynamic NAT, dan Port Address Translation (PAT). NAT memungkinkan banyak perangkat dalam satu jaringan lokal mengakses internet menggunakan satu alamat IP publik, sehingga menghemat penggunaan IP dan menambah lapisan keamanan.

Connection Tracking adalah fitur yang mencatat dan memantau status dari setiap koneksi yang melewati perangkat jaringan. Dengan informasi seperti alamat IP, nomor port, protokol, dan status koneksi, connection tracking memungkinkan sistem mengenali koneksi yang sah dan membedakannya dari koneksi yang mencurigakan atau tidak valid. Fitur ini sangat penting dalam implementasi firewall berbasis stateful dan dalam mendukung proses NAT secara efisien.

2 Tugas Pendahuluan

Bagian ini berisi jawaban dari tugas pendahuluan yang telah anda kerjakan, beserta penjelasan dari jawaban tersebut

1. **Konfigurasi NAT yang diperlukan untuk mengakses web server lokal (IP: 192.168.1.10, port 80) dari jaringan luar** adalah *Port Forwarding* atau *Destination NAT*. Teknik ini memungkinkan lalu lintas dari IP publik pada port 80 diteruskan ke alamat IP privat internal (192.168.1.10:80).

Konfigurasi ini umum digunakan pada router atau firewall yang mendukung NAT, seperti MikroTik atau iptables.
Referensi: Universitas Brawijaya. 2020. *Modul Praktikum Jaringan Komputer: Firewall dan NAT*. Malang: Jurusan Teknik Informatika, Fakultas Ilmu Komputer, Universitas Brawijaya.

2. **Firewall lebih penting untuk diterapkan terlebih dahulu daripada NAT.** Hal ini karena firewall bertugas menyaring dan mengendalikan lalu lintas jaringan berdasarkan kebijakan keamanan yang telah ditentukan. Tanpa firewall, semua lalu lintas—baik yang sah maupun berbahaya—dapat masuk tanpa kontrol. Sementara itu, NAT hanya bertugas menerjemahkan alamat IP dan port, tanpa memiliki kecerdasan dalam menilai ancaman atau kontrol lalu lintas secara menyeluruh. Oleh sebab itu, firewall harus diterapkan lebih dulu sebagai lini pertama pertahanan jaringan.
   Referensi: Politeknik Elektronika Negeri Surabaya. 2021. *Dasar Keamanan Jaringan Komputer*. Surabaya: Departemen Teknologi Informasi, PENS.

3. **Dampak negatif jika router tidak diberi filter firewall sama sekali** adalah meningkatnya risiko serangan terhadap jaringan internal. Tanpa firewall, tidak ada mekanisme untuk memblokir lalu lintas berbahaya seperti malware, scanning port, atau upaya peretasan. Hal ini dapat menyebabkan pencurian data, gangguan layanan, atau bahkan pengambilalihan sistem. Firewall penting untuk membatasi lalu lintas berdasarkan IP, port, dan protokol, serta membantu mendeteksi koneksi yang mencurigakan.
   Referensi: Universitas Gadjah Mada. 2019. *Keamanan Jaringan Komputer*. Yogyakarta: Fakultas Teknik, Universitas Gadjah Mada.