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

Laporan Sementara
Praktikum Jaringan Komputer

Firewall & NAT

Atria Caesariano Tinto - 5024231068

2025

1 Pendahuluan

1.1 Latar Belakang

Dalam era digital yang semakin maju, jaringan internet menjadi kebutuhan penting dalam berbagai aspek kehidupan, baik di bidang rumah tangga, bisnis, maupun pemerintahan. Namun, semakin luasnya akses terhadap jaringan global juga meningkatkan risiko keamanan jaringan, seperti penyusupan, serangan malware, hingga pencurian data. Oleh karena itu, dibutuhkan sistem pengamanan yang andal untuk menjaga integritas, kerahasiaan, dan ketersediaan data dalam jaringan komputer.

Firewall dan Network Address Translation (NAT) merupakan dua teknologi yang digunakan dalam infrastruktur jaringan untuk memastikan keamanan dan efisiensi data. Firewall berfungsi sebagai gerbang pengaman yang mengatur lalu lintas jaringan berdasarkan aturan tertentu, sementara NAT memungkinkan banyak perangkat lokal mengakses internet menggunakan satu alamat IP publik, sekaligus menyembunyikan struktur jaringan internal dari dunia luar.

Selain itu, fitur seperti Connection Tracking sangat membantu dalam mengenali status koneksi jaringan, memungkinkan pengambilan keputusan yang lebih cerdas dalam pengelolaan trafik dan implementasi kebijakan firewall maupun NAT.

1.2 Dasar Teori

Firewall merupakan komponen penting dalam sistem keamanan jaringan komputer yang berfungsi sebagai penjaga gerbang lalu lintas data. Firewall bekerja dengan menyaring paket data yang masuk dan keluar jaringan berdasarkan aturan tertentu yang telah ditetapkan oleh administrator. Dapat berupa alamat IP, nomor port, jenis protokol, serta status koneksi. Firewall dapat beroperasi mulai dari lapisan jaringan hingga aplikasi. Firewall dibagi menjadi beberapa jenis, di antaranya adalah Packet Filtering yang hanya memeriksa header paket, Stateful Inspection yang memantau status koneksi secara menyeluruh, Application Layer Firewall yang mampu membaca isi komunikasi pada tingkat aplikasi, hingga Next Generation Firewall yang mampu inspeksi paket lebih dalam dan deteksi ancaman yang lebih kompleks. Selain itu, firewall juga bisa berupa perangkat lunak yang terpasang di dalam sistem operasi, perangkat keras yang berdiri sebagai perantara fisik antara jaringan internal dan eksternal.

Network Address Translation (NAT) adalah metode yang digunakan untuk mengubah alamat IP dari paket data ketika paket tersebut melewati perangkat jaringan, seperti router. Tujuan utama dari NAT adalah memungkinkan beberapa perangkat dalam jaringan lokal yang menggunakan IP privat untuk mengakses internet menggunakan satu alamat IP publik. Terdapat beberapa jenis NAT, yaitu Static NAT yang menetapkan pemetaan tetap antara IP lokal dan IP publik, Dynamic NAT yang memanfaatkan pool IP publik secara dinamis, serta Port Address Translation (PAT) yang paling umum digunakan dan memungkinkan banyak perangkat menggunakan satu IP publik dengan membedakan koneksi berdasarkan nomor port. NAT bekerja dengan mencatat semua koneksi dalam sebuah tabel NAT agar perangkat jaringan tahu ke mana harus mengirimkan data balasan.

Untuk mendukung fungsi firewall dan NAT, digunakan fitur Connection Tracking atau pelacakan koneksi. Fitur ini mencatat informasi detail tentang setiap koneksi yang berlangsung, seperti alamat IP sumber dan tujuan, port, protokol, serta status koneksi (baru, aktif, terkait, atau tidak sah). Dengan adanya Connection Tracking, sistem jaringan dapat mengidentifikasi apakah suatu paket merupakan bagian dari koneksi yang sah atau bukan, sehingga dapat mempercepat proses pengambilan kepu-

tusan dalam filtering paket dan translasi alamat oleh NAT.

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?**

   Untuk dapat mengakses web server lokal dengan alamat IP 192.168.1.10 dan port 80 dari jaringan luar (internet), dibutuhkan konfigurasi Static NAT dengan Port Forwarding. Static NAT digunakan agar satu alamat IP publik dapat secara tetap merujuk ke satu IP privat di jaringan internal. Port forwarding mengarahkan dari port tertentu di IP publik ke port yang sama pada IP privat. Dengan kata lain, NAT akan menerjemahkan permintaan dari pengguna luar ke alamat IP publik router agar diteruskan ke server internal di 192.168.1.10:80. Konfigurasi ini penting agar layanan web di jaringan lokal dapat diakses dari luar jaringan tanpa harus memberikan IP publik langsung kepada web server.

   Referensi: Tanenbaum, A. S., & Wetherall, D. J. (2011). Computer Networks (5th ed.). Pearson.

2. **Menurutmu, mana yang lebih penting diterapkan terlebih dahulu di jaringan: NAT atau Firewall? Jelaskan alasanmu.**

   Firewall sebaiknya diterapkan terlebih dahulu dibandingkan NAT. Karena firewall merupakan pertahanan utama yang mengontrol jaringan masuk dan keluar berdasarkan aturan keamanan yang dibuat. Firewall dapat mencegah akses yang tidak valid, melindungi sistem dari serangan siber seperti malware yang mencoba masuk melalui port. NAT berperan penting dalam manajemen alamat IP dan konektivitas ke internet, tetapi tidak dirancang untuk menyaring ancaman atau memblokir akses berbahaya. Karena itu, firewall harus lebih dahulu dikonfigurasi agar semua jaringan baik dari dalam maupun luar dapat diawasi dan difilter sebelum diteruskan melalui mekanisme NAT.

   Referensi: Stallings, W. (2017). Network Security Essentials: Applications and Standards (6th ed.). Pearson.

3. **Apa dampak negatif jika router tidak diberi filter firewall sama sekali?**

   Jika sebuah router tidak dilengkapi dengan filter firewall sama sekali, maka jaringan akan sangat rentan terhadap berbagai ancaman. Semua paket data dari luar dapat masuk tanpa penyaringan, termasuk paket-paket yang membawa malware, serangan brute force, ataupun traffic yang mencoba masuk ke celah keamanan pada sistem. Tanpa firewall, pengguna jaringan internal juga dapat dengan bebas mengakses situs atau layanan berbahaya. Ini dapat menyebabkan pencurian data, pemanfaatan sumber daya jaringan untuk tujuan ilegal, serta membuat sistem jaringan menjadi target bagi penyerang.

   Referensi: Easttom, C. (2022). Computer Security Fundamentals (4th ed.). Pearson IT Cybersecurity.