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

Laporan Sementara
Praktikum Jaringan Komputer

Firewall dan NAT

Bintang Narindra Putra Pratama - 5024231038

2025

1 Pendahuluan

1.1 Latar Belakang

Jaringan komputer sudah menjadi bagian kehidupan kita sehari-hari di era modern ini. Contoh paling utamanya adalah internet yang dapat diakses hampir oleh semua orang di berbagai belahan dunia. Dengan adanya internet kita dapat mencari, bertukar, dan mengakses informasi dari negara lain dengan mudah. Namun, karena jaringan dari internet ini sangat luas, bukan tidak mungkin terdapat orang-orang yang memiliki niat jahat untuk menggunakan internet dengan tujuan mencuri data pribadi kita, melakukan penipuan, dan sebagainya. Untuk itu diperlukan persiapan pencegahan untuk menjaga keamanan kita saat menggunakan internet. Contoh dari langkah persiapan ini adalah NAT (Network Address Translation) dan Firewall. Pada praktikum ini, dibahas tentang bagaimana cara menyiapkan firewall dan NAT tersebut.

1.2 Dasar Teori

Firewall adalah sebuah perangkat baik berupa hardware maupun software yang berguna untuk memfilter traffic data yang masuk dan keluar berdasarkan sebuah aturan yang telah ditentukan. Firewall memiliki tiga kebijakan akses yaitu Accept, yaitu firewall memberikan akses dan membiarkan traffic untuk berjalan. Kemudian Reject, yaitu firewall memblokir akses traffic dan memberikan reply "unreachable error". Kebijakan akses terakhir adalah Drop, yaitu memblokir akses traffic namun tidak memberikan balasan sama sekali. Firewall sendiri memiliki beberapa jenis, pertama adalah Packet Filtering Firewall, dimana data yang lewat berdasarkan IP, protocols, dan ports sumber dan tujuan dari paket data. Firewall jenis ini tidak dapat mengetahui apakah sebuah paket adalah bagian dari sebuah arus atau traffic yang sudah ada dan hanya dapat memberikan akses berdasarkan header dari paket tersebut. Kedua adalah Stateful Inspection Firewall merupakan pengembangan dari paket Filtering yang mana dapat membedakan paket apakah bagian dari paket atau traffic yang sudah diberikan akses. Selanjutnya, adalah Application Layer Firewall dimana firewall dapat memfilter hingga tingkat aplikasi, dimana firewall ini dapat memblokir konten yang spesifik dan mengenali ketika aplikasi atau protokol sedang disalah gunakan. Kemudian adalah Next Generation Firewall (NGFW) yaitu firewall yang dapat melakukan Deep Packet Inspection, Application Inspection, SSL/SSH inspection dan berbagai fitur lainnya untuk melindungi data. Kemudian adalah Circuit Level Gateway Firewall, adalah firewall yang hanya bekerja pada level koneksi, sehingga ini firewall jenis ini kurang efektif karena malware dapat diluluskan apabila berada dalam suatu paket yang telah terkoneksi sebelumnya. Selanjutnya adalah Software Firewall yaitu firewall yang paling baik dalam mengontrol traffic dari paket data dan membatasi jumlah koneksi yang terhubung ke suatu perangkat, namun cukup rumit dalam pemasangannya. Selanjutnya adalah Hardware Firewall, yaitu sebuah perangkat fisik yang memiliki fungsi umum dari firewall. Terakhir adalah Cloud Firewall yang dipasang pada cloud service untuk mencegah adanya akses data yang tidak diinginkan.

Metode pengamanan selanjutnya adalah Network Address Translation (NAT), yaitu metode yang memungkinkan sebuah IP publik digunakan oleh beberapa perangkat. Metode inilah yang memungkinkan IPv4 untuk digunakan hingga saat ini walau jumlah perangkat yang ada di dunia sudah lebih dari 4,3 Miliar. Biasanya, NAT ini ada di router yang jadi penghubung antara jaringan lokal dan internet. dimana jika ada perangkat di dalam jaringan lokal kirim data ke internet, alamat IP-nya bakal diubah

jadi alamat IP publik dulu sama router. Pas data dari internet mau balik ke perangkat tadi, NAT akan ganti lagi alamat publik itu jadi IP lokal si pengirim. Dalam NAT terdapat beberapa istilah penting yaitu Inside Local Address (IP lokal perangkat di jaringan dalam), Inside Global Address (IP publik yang mewakili perangakt dari dalam jaringan ke dunia luar), Outside Local Address (IP tujuan dari sisi luar yang udah diterjemahkan di dalam jaringan), Outside Global Address (IP asli dari tujuan di luar jaringan). NAT memiliki beberapa jenis yaitu, Static NAT, Dynamic NAT, dan Port Address Translation(PAT). Selain itu dalam NAT terdapat Connetion Tracking yang melakukan tracking dan pencatatan IP mana yang tengah berhubungan dengan IP mana, kapan terjadinya hubungan ini, route yang diambil, dan status dari hubungan.

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 mengakses web server lokal dari jaringan luar dapat digunakan Static NAT karena web server lokal tidak perlu untuk berganti-ganti IP.
   sumber: Muhammad, D. R., & Arisandy, Y. (2021). Analisis pengaruh konfigurasi Network Address Translator (NAT) statik berbasis web menggunakan WireShark. ResearchGate.

2. Menurutmu, mana yang lebih penting diterapkan terlebih dahulu di jaringan: NAT atau Firewall? Jelaskan alasanmu.
   Firewall lebih penting untuk diterapkan terlebih dahulu, karena firewall berguna untuk memfilter akses dan menjaga keamanan data. NAT hanya berfungsi untuk membagi satu IP publik ke beberapa perangkat dan tidak secara langsung melindungi data.
   sumber: Fauzie, A. (2016). Analisis penerapan firewall sebagai sistem keamanan jaringan komputer dengan metode iptables [Undergraduate thesis, UIN Syarif Hidayatullah Jakarta]. UIN Jakarta Institutional Repository.

3. Apa dampak negatif jika router tidak diberi filter firewall sama sekali?
   Tanpa adanya firewall sama sekali, data yang ada di perangkat komputer akan rawan untuk diakses oleh pihak lain. Biasanya melalui sebuah file malware atau virus yang terinstall secara sendirinya ketika mengakses website.
   sumber: Widharma, I. G. S. (2020). Pengamanan sistem jaringan komputer dengan teknologi firewall. ResearchGate.