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

Laporan Sementara
Praktikum Jaringan Komputer

Modul Firewall NAT

Syela Akhul Khalimi - 5024231015

2025

1 Pendahuluan

1.1 Latar Belakang

Kemajuan teknologi informasi dan komunikasi yang sangat cepat telah mengintegrasikan jaringan komputer ke dalam berbagai aspek kehidupan modern, termasuk sektor pendidikan, ekonomi, dan administrasi publik. Dengan semakin tingginya permintaan terhadap konektivitas jaringan, keamanan dan efektivitas sistem jaringan menjadi prioritas utama yang harus dipertimbangkan.

Firewall merupakan perpaduan teknologi perangkat keras dan perangkat lunak yang berfungsi sebagai penghalang antara berbagai segmen jaringan komputer untuk mempertahankan keamanan informasi. Dalam definisi lain, firewall adalah sistem proteksi jaringan komputer yang bertugas melindungi perangkat dari ancaman eksternal. Fungsi utama firewall adalah mengatur dan membatasi akses dari jaringan luar ke jaringan internal yang bersifat privat. Firewall beroperasi sebagai pengatur komunikasi antara berbagai jenis jaringan yang memiliki karakteristik berbeda. Melalui firewall, data pada komputer atau server yang terhubung dapat terlindungi dari akses tidak sah melalui internet. Ketika ada upaya pembukaan atau modifikasi informasi sensitif atau situs web oleh pihak yang tidak berwenang, firewall akan secara otomatis memblokir aktivitas tersebut.

NAT (Network Address Translation) adalah mekanisme pemetaan alamat IP yang memungkinkan perangkat jaringan memberikan alamat IP publik kepada perangkat-perangkat dalam jaringan lokal, sehingga multiple alamat IP privat dapat mengakses alamat IP publik. Secara sederhana, NAT berfungsi mentransformasikan alamat IP agar perangkat dalam jaringan lokal dapat terhubung dengan alamat host di internet menggunakan alamat IP publik yang tersedia dalam jaringan tersebut. NAT melakukan konversi alamat IP privat supaya dapat mengakses alamat host internet melalui pemanfaatan alamat IP publik pada jaringan yang bersangkutan.

Melalui kegiatan praktikum ini, diharapkan mahasiswa dapat menguasai konsep dasar dan penerapan firewall beserta NAT dalam sistem jaringan komputer. Praktikum ini menyediakan peluang untuk melakukan konfigurasi berbagai kebijakan firewall, mengimplementasikan metode NAT, serta melakukan evaluasi terhadap pengaruh dan keuntungannya dalam pengelolaan jaringan yang terjamin keamanannya dan beroperasi secara optimal.

1.2 Dasar Teori

Network Address Translation (NAT) merupakan teknologi fundamental yang digunakan untuk mengubah atau menerjemahkan alamat IP dari satu jaringan ke jaringan lain, khususnya dari alamat IP privat yang berada di jaringan internal ke alamat IP publik di jaringan eksternal dan sebaliknya. Teknologi ini memiliki peran yang sangat penting dalam jaringan komputer yang ingin menghubungkan perangkat-perangkat di jaringan lokal atau private network ke internet atau public network tanpa harus memberikan setiap perangkat alamat IP publik yang unik dan terpisah.

NAT bekerja dengan cara menempatkan sebuah perangkat khusus, yang biasanya berupa router atau firewall NAT, sebagai gateway atau gerbang penghubung antara jaringan internal dan jaringan eksternal. Ketika perangkat yang berada di jaringan internal mengirimkan data ke luar jaringan, misalnya ke internet, maka NAT akan secara otomatis mengganti alamat IP sumber dari paket data tersebut dengan alamat IP publik yang dimiliki oleh gateway. Sebaliknya, ketika data balasan datang dari jaringan eksternal, NAT akan menerjemahkan kembali alamat IP tujuan ke alamat IP privat perangkat internal yang sesuai dengan komunikasi tersebut. Dalam implementasinya, NAT memiliki

beberapa jenis yang berbeda sesuai dengan kebutuhan jaringan. Static NAT merupakan jenis yang paling sederhana dimana satu alamat IP privat diterjemahkan ke satu alamat IP publik secara tetap dan permanen. Dynamic NAT memungkinkan beberapa alamat IP privat diterjemahkan ke sejumlah alamat IP publik yang tersedia secara dinamis dari pool alamat yang telah ditentukan sebelumnya. Sementara itu, Port Address Translation atau PAT memungkinkan banyak alamat IP privat diterjemahkan ke satu alamat IP publik dengan cara membedakan port komunikasi yang digunakan, dan jenis ini juga dikenal dengan istilah NAT Overload. Penggunaan NAT memberikan berbagai manfaat signifikan dalam pengelolaan jaringan. Pertama, NAT dapat menghemat penggunaan alamat IP publik karena memungkinkan banyak perangkat di jaringan lokal berbagi satu alamat IP publik, sehingga penggunaan alamat IP publik menjadi lebih efisien dan ekonomis. Kedua, NAT memberikan lapisan keamanan tambahan dengan menyembunyikan alamat IP privat dari jaringan luar, sehingga dapat meminimalkan risiko ancaman dan serangan dari luar jaringan. Ketiga, NAT memungkinkan konektivitas yang seamless dengan memungkinkan perangkat yang memiliki alamat IP privat untuk mengakses internet atau jaringan eksternal lainnya.

Firewall adalah perangkat keamanan jaringan yang memiliki fungsi utama untuk memantau dan menyaring lalu lintas data yang masuk dan keluar dari suatu jaringan berdasarkan aturan keamanan yang telah ditetapkan dan dikonfigurasi sebelumnya. Firewall dapat berupa perangkat keras atau hardware, perangkat lunak atau software, atau bahkan kombinasi dari keduanya tergantung pada kebutuhan dan kompleksitas jaringan yang akan dilindungi. Cara kerja firewall didasarkan pada prinsip pemeriksaan setiap paket data yang melewati jaringan. Setiap paket data ini akan dianalisis secara mendetail berdasarkan berbagai parameter penting seperti alamat IP sumber dan tujuan, nomor port yang digunakan, jenis protokol komunikasi, dan pola serangan tertentu yang telah diidentifikasi sebelumnya. Berdasarkan hasil analisis tersebut, firewall kemudian akan membuat keputusan apakah paket data tersebut akan diizinkan untuk melewati jaringan (accept), ditolak akses (reject), atau diabaikan begitu saja tanpa respon (drop). Firewall memiliki beberapa metode kerja utama yang berbeda dalam menganalisis dan memproses lalu lintas jaringan. Packet Filtering merupakan metode yang memeriksa setiap paket data secara individual berdasarkan aturan-aturan tertentu yang telah ditetapkan. Stateful Inspection adalah metode yang lebih canggih karena dapat melacak status koneksi yang sedang berlangsung dan memeriksa paket berdasarkan konteks koneksi tersebut. Proxy Service bertindak sebagai perantara atau mediator antara dua jaringan dan memverifikasi paket secara terpusat dengan kontrol yang lebih ketat. Berdasarkan teknologi dan cara kerjanya, firewall dapat dikategorikan ke dalam beberapa jenis yang berbeda. Packet Filtering Firewall merupakan jenis yang paling dasar yang memfilter paket berdasarkan alamat IP, nomor port, dan protokol yang digunakan. Proxy Firewall memiliki kemampuan untuk memproses dan memverifikasi isi paket pada level aplikasi sehingga memberikan kontrol yang lebih detail. Stateful Inspection Firewall dapat memeriksa status koneksi dan memfilter paket berdasarkan konteks komunikasi yang sedang berlangsung. Unified Threat Management atau UTM Firewall menggabungkan berbagai fitur keamanan seperti firewall tradisional, antivirus, dan sistem pencegahan intrusi dalam satu perangkat. Next-Generation Firewall atau NGFW menyediakan inspeksi paket yang lebih detail dan berbagai fitur keamanan tambahan yang lebih canggih. NAT Firewall menggabungkan fungsi NAT dengan firewall untuk memblokir komunikasi yang tidak diminta atau tidak diinginkan dari jaringan luar. Fungsi firewall dalam jaringan komputer sangat beragam dan komprehensif. Firewall bertugas mengontrol dan memantau aliran data dalam jaringan untuk memastikan hanya lalu lintas yang legitimate yang dapat melewati sistem. Firewall juga mencatat aktivitas pengguna dan lalu lintas jaringan melalui fitur logging yang bergu-

na untuk audit dan investigasi keamanan. Selain itu, firewall memiliki kemampuan untuk memblokir akses tidak sah dan berbagai jenis serangan siber seperti malware, virus, dan serangan Distributed Denial of Service atau DDoS. Firewall dapat membatasi dan memonitor penggunaan bandwidth untuk mengoptimalkan kinerja jaringan. Firewall juga dapat memblokir konten atau situs web yang tidak diinginkan atau berbahaya. Yang tidak kalah penting, firewall berperan dalam mencegah kebocoran data atau informasi rahasia dari jaringan internal ke pihak yang tidak berwenang. NAT dan firewall merupakan dua komponen yang sangat penting dan saling melengkapi dalam sistem keamanan dan efisiensi jaringan komputer modern. NAT berperan utama dalam menerjemahkan alamat IP untuk menghubungkan jaringan privat ke jaringan publik dengan cara yang efisien dan aman, sehingga memungkinkan optimalisasi penggunaan sumber daya alamat IP. Sementara itu, firewall bertugas sebagai penjaga dan pengontrol lalu lintas data, memastikan bahwa hanya data yang aman dan diizinkan yang dapat melewati jaringan, sehingga melindungi sistem dari berbagai ancaman keamanan. Keduanya sering digunakan bersamaan dalam implementasi jaringan untuk memberikan perlindungan yang komprehensif dan pengelolaan jaringan yang optimal, menciptakan ekosistem jaringan yang tidak hanya efisien tetapi juga aman dari berbagai ancaman internal maupun eksternal.

2 Tugas Pendahuluan

1. Untuk mengakses web server lokal dengan IP 192.168.1.10 port 80 dari jaringan luar, diperlukan konfigurasi Port Forwarding atau Static NAT pada router/gateway yang menghubungkan jaringan lokal dengan internet. Konfigurasi ini melibatkan pembuatan aturan Destination NAT (DNAT) yang mengarahkan traffic yang masuk ke IP publik router port 80 menuju server internal 192.168.1.10 port 80, serta Source NAT (SNAT) untuk mengganti alamat sumber pada traffic balikan dari server ke client eksternal. Mapping yang dibuat adalah External IP publik router port 80 menuju Internal IP 192.168.1.10 port 80 menggunakan protokol TCP. Dalam implementasinya, perlu diperhatikan konfigurasi firewall yang mengizinkan traffic ke port 80, memastikan web server sudah berjalan dengan baik, serta mempertimbangkan aspek keamanan seperti penggunaan port non-standard untuk mengurangi risiko serangan, sehingga ketika ada request dari internet ke IP publik router, traffic akan diteruskan ke web server lokal dan response dikembalikan melalui jalur NAT yang telah dikonfigurasi.

2. Jika prioritasnya adalah konektivitas, maka NAT perlu diterapkan terlebih dahulu agar jaringan lokal bisa terhubung ke internet. Namun, jika prioritasnya adalah keamanan, maka firewall lebih penting untuk mencegah akses tidak sah. Idealnya, keduanya diterapkan bersamaan karena saling melengkapi: NAT untuk koneksi, firewall untuk perlindungan.

   https://mikbotam.net/peran-network-address-translation-nat-dalam-jaringan

3. Jika router tidak diberi firewall, jaringan menjadi sangat rentan terhadap berbagai ancaman seperti akses ilegal dari luar, pencurian dan kerusakan data, serangan DDoS yang mengganggu layanan, penyebaran malware ke perangkat lain dalam jaringan, serta potensi kehilangan reputasi akibat kebocoran data. Tanpa firewall, tidak ada penghalang yang menyaring lalu lintas berbahaya, sehingga membuka peluang besar bagi peretas untuk mengeksploitasi sistem. Oleh karena itu, firewall sangat penting untuk menjaga keamanan dan kestabilan jaringan.

   https://cyberhub.id/pengetahuan-dasar/cara-mengamankan-wi-fi