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

Laporan Sementara
Praktikum Jaringan Komputer

Firewall dan NAT

Akhmad Rizqullah Ridlohi - 5024231037

2025

1 Pendahuluan

1.1 Latar Belakang

Pada modul ini, praktikan akan memelajari bagaimana Firewall dan NAT, praktikan akan memahami apa itu Firewall dan NAT dan akan mengetahui bagaimana Firewall dan NAT bekerja pada aplikasinya.

1.2 Dasar Teori

Firewall adalah sistem keamanan jaringan yang berfungsi untuk memantau dan mengontrol lalu lintas jaringan masuk dan keluar berdasarkan aturan keamanan yang telah ditentukan. Tujuan utama firewall a dalah untuk mencegah akses tidak sah ke atau dari jaringan pribadi. Terdapat beberapa jenis firewall yang digunakan sesuai kebutuhan dan skala infrastruktur jaringan. Packet filtering firewall adalah jenis paling dasar yang memeriksa paket data berdasarkan alamat IP sumber dan tujuan, port, dan protokol, namun tidak dapat melacak status koneksi. Stateful inspection firewall bekerja lebih canggih dengan memeriksa status dari setiap koneksi jaringan, sehingga mampu menentukan apakah paket merupakan bagian dari koneksi yang sah. Application layer firewall beroperasi pada lapisan aplikasi OSI dan mampu memfilter lalu lintas berdasarkan jenis aplikasi (seperti HTTP, FTP), memberikan tingkat keamanan yang lebih tinggi. Next-Generation Firewall (NGFW) menggabungkan fitur dari firewall tradisional dengan teknologi tambahan seperti inspeksi paket mendalam (DPI), pencegahan intrusi (IPS), dan kontrol aplikasi. Circuit level gateway memonitor sesi TCP dan UDP, serta memastikan bahwa sesi dimulai dengan benar sebelum memungkinkan data ditransfer tetapi circuit level gateway tidak bisa mengecek isi data yang dikirimkan.Software firewall yang berjalan di sistem operasi dan memberikan perlindungan untuk satu perangkat, serta hardware firewall yang berupa perangkat fisik khusus untuk mengamankan seluruh jaringan. Selain itu, terdapat cloud firewall, yaitu firewall berbasis cloud yang dikelola oleh penyedia layanan untuk melindungi infrastruktur cloud dan layanan berbasis internet. Cara kerja firewall secara umum melibatkan penyaringan lalu lintas berdasarkan aturan yang ditetapkan administrator jaringan; ketika lalu lintas jaringan diterima, firewall mengevaluasi paket terhadap aturan dan memutuskan apakah akan mengizinkan atau memblokir paket tersebut.

Network Address Translation (NAT) adalah teknik yang digunakan dalam jaringan komputer untuk mengubah alamat IP pada paket data saat mereka melewati router atau firewall. NAT memungkinkan beberapa perangkat dalam jaringan lokal menggunakan satu alamat IP publik yang sama untuk akses ke internet, sehingga menghemat penggunaan IP dan memberikan tingkat keamanan tambahan dengan menyembunyikan alamat aslinya. Cara kerja NAT adalah dengan mencatat setiap koneksi yang keluar dari jaringan lokal ke internet dan menggantikan alamat IP lokal dan/atau port sumber dengan alamat IP publik dan port tertentu, serta menyimpan informasi translasi tersebut di tabel NAT untuk memetakan respons yang kembali. Terdapat beberapa jenis NAT, yaitu: Static NAT yang menerjemahkan satu alamat IP lokal ke satu alamat IP publik secara permanen; Dynamic NAT yang memetakan alamat IP lokal ke alamat IP publik dari kumpulan alamat yang tersedia secara dinamis,dan Port Address Translation (PAT) yang memetakan banyak alamat IP lokal ke satu alamat IP publik dengan membedakan sesi berdasarkan nomor port.

Connection tracking adalah fitur pengamat lalu lintas jaringan, ia akan mencatat setiap koneksi yang terhubung .Connection tracking melakukan manajemen trafik dengan cara menyimpan informasi penting dari koneksi yang terjadi yang dimana informasi tersebut akan digunakan untuk proses firewall filtering dan NAT.

2 Tugas Pendahuluan

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

1. Menggunakan Port Address Translation,dimana permintaan dari jaringan luar akan diproses dulu dalam NAT, dan di NAT akan diolah sesuai port yang dituju dan nantinya akan diarahkan ke port tersebut.
2. Tergantung kebutuhan, jika ingin menggunakan internet yang aman maka prioritaskan firewall, dan jika ingin menggunakan IP publik yang sama dalam setiap jaringan lokal maka gunakanlah NAT (Modul Firewall dan NAT)
3. Maka perangkat akan rentan terhadap serangan dari luar, karena tidak adanya pengecekan terlebih dahulu sebelum pengiriman suatu data dan validasi koneksi Modul Firewall dan NAT.