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

Laporan Sementara
Praktikum Jaringan Komputer

Firewall NAT

Farrel Ganendra - 5024231036

2025

1 Pendahuluan

1.1 Latar Belakang

Praktikum modul 4 mengenai Firewall dan NAT ini dilakuakn untuk memberikan pemahaman dasar mengenai keamanan jaringan dan manajemen lalu lintas data. Perlindungan jaringan adalah hal yang sangat pentingg di era digital yang penuh dengan ancaman siber ini. Sehingga kita memerlukakn Firewall yang berfungsi sebagai pengendali lalu lintas data yang masuk dan keluar jaringan. Selain masalah keamanan, keterbatasan IP Addresss juga menjadi masalah yang terus berkembang, meskipun sudah ada IPv6, masih sedikit perangkat di dunia yang bisa menggunakannya. Sehingga solusi lain pun muncul yaitu sistem NAT. NAT memungkinkan banyak perangkat di jaringan lokal untuk mengakses internet menggunakan satu alamat IP publik, sekaligus menambah lapisan keamanan.

Topik ini sangatlah relevan di mana keamanan jaringan menjadi prioritas utama dalam perusahaan, layanan cloud, hingga sistem IoT. Melalui praktikum ini, praktikan diharapkan menjadi lebih siap menghadapi tantangan dalam membangun dan mengelola jaringan modern yang aman dan reliable.

1.2 Dasar Teori

Network Address Translation (NAT) adalah teknik yang digunakan untuk mengubah alamat IP sumber atau tujuan dalam paket jaringan. Salah satu bentuk paling umum adalah Masquerade, yang digunakan untuk memungkinkan banyak perangkat di jaringan lokal (LAN) mengakses internet melalui satu alamat IP publik. NAT tipe ini bersifat dinamis, sangat cocok untuk koneksi dengan IP publik yang berubah-ubah seperti pada jaringan rumah. Dengan begitu, kita dapat menghemat penggunaan IP Address karena tidak semua device perlu ip address nya sendiri melainkan cukup 1 router. Sementara itu, untuk mengalihkan koneksi dari port tertentu pada IP publik ke IP dan port tertentu di jaringan lokal (Misal untuk mempublish sebuah website yang di host di dalam perangkat dalam jaringan lokal atau lainnya), kita dapat melakukan Port Forwarding. Port forwarding dapat kita ibaratkan sebagai "jembatan" yang memungkinkan lalu lintas data melintasi "pagar" jaringan (router/firewall) dan sampai ke perangkat yang tepat di dalam jaringan. Cara melakukannya berbeda beda tergantung dengan jenis router yang digunakan.

Untuk menjaga keamanan jaringan lokal, kita memerlukan pengaman yang biasa disebut sebagai firewall. Salah satu komponen penting dalam pengelolaan firewall adalah filter rules, filter rules adalah aturan yang digunakan untuk mengontrol lalu lintas data yang melewati router atau perangkat firewall. Terdapat tiga tindakan utama dalam filter rules: Accept, Drop, dan Reject. Accept berarti lalu lintas diizinkan melewati firewall. Drop berarti lalu lintas dibuang secara diam-diam tanpa memberi respons ke pengirim, yang membuatnya berguna untuk mempersulit pemetaan jaringan oleh penyerang. Sedangkan Reject menolak koneksi secara eksplisit dengan mengirimkan pesan penolakan ke pengirim. Dengan filter rules ini, kita dapat mengatur siapa saja yang boleh mengakses layanan dalam jaringan serta melindungi perangkat dari akses yang tidak sah.

Pada firewall modern, terdapat fitur yang memungkinkan sistem untuk melacak status koneksi dari paket-paket data yang lewat. Dengan connection tracking, firewall dapat membedakan apakah paket tersebut merupakan koneksi baru, koneksi yang sudah ada, atau bagian dari koneksi yang tidak sah. Informasi ini sangat penting dalam implementasi firewall stateful, di mana keputusan untuk menerima atau menolak paket bisa didasarkan pada konteks koneksi sebelumnya, bukan hanya berdasarkan alamat dan port.

Untuk menjaga keamanan jaringan secara keseluruhan, penting juga untuk menerapkan proteksi router dari akses luar. Router sebagai gerbang utama jaringan memiliki risiko tinggi menjadi target serangan. Oleh karena itu, akses ke antarmuka administrasi router (misalnya SSH, Winbox, atau HTTP) sebaiknya dibatasi hanya dari jaringan lokal atau IP tertentu. Selain itu, layanan dan port yang tidak digunakan sebaiknya dinonaktifkan. Dengan menerapkan aturan firewall yang ketat, memblokir koneksi tidak dikenal, dan hanya mengizinkan akses yang sah, router dapat terlindungi dari eksploitasi dan penyusupan.

2 Tugas Pendahuluan

1. Untuk memungkinkan akses dari jaringan luar ke web server lokal dengan IP 192.168.1.10 dan port 80, kita perlu mengatur Port Forwarding menggunakan Destination NAT (dst-nat). Konfigurasi ini mengarahkan permintaan yang masuk ke alamat IP publik router pada port 80 ke alamat IP dan port internal server. (https://forum.mikrotik.com/viewtopic.php?t=193457)

2. Firewall sebaiknya diterapkan terlebih dahulu karena firewall berfungsi sebagai pengaman utama yang mengontrol lalu lintas data masuk dan keluar berdasarkan aturan yang ditetapkan, sehingga melindungi jaringan dari akses yang tidak sah dan potensi serangan.Meskipun NAT memberikan lapisan keamanan tambahan dengan menyembunyikan struktur internal jaringan, tanpa Firewall, jaringan tetap rentan terhadap serangan. (https://www.cloudcomputing.id/berita/firewall-berperan-penting-untuk-network-security)

3. Tanpa filter firewall, router akan menerima dan meneruskan semua lalu lintas data tanpa penyaringan, yang dapat menyebabkan beberapa masalah serius seperti Keamanan yang rentan, Penyalahgunaan sumber daya, Kebocoran data, dan pada beberapa kasus, kinerja jaringan juga dapat menurun. (https://www.cloudcomputing.id/berita/firewall-berperan-penting-untuk-network-security)