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

Laporan Sementara
Praktikum Jaringan Komputer

Firewall dan NAT

Arhya Hafidz Hafidin - 5024231042

2025

1 Pendahuluan

1.1 Latar Belakang

Dalam manajemen jaringan komputer, aspek keamanan memiliki peranan yang sangat krusial untuk menjaga data dan sistem dari berbagai ancaman eksternal. Dua teknologi utama yang sering dimanfaatkan untuk tujuan ini adalah Firewall dan Network Address Translation (NAT). Firewall berfungsi untuk menyaring lalu lintas jaringan berdasarkan aturan tertentu, sehingga hanya koneksi yang diperbolehkan yang bisa mengakses jaringan. Sementara itu, NAT memungkinkan perangkat dalam jaringan lokal untuk berkomunikasi dengan jaringan luar menggunakan satu alamat IP publik, sekaligus menyembunyikan alamat IP internal sebagai langkah tambahan dalam perlindungan keamanan.

Melalui kegiatan praktikum ini, akan dipelajari bagaimana cara kerja serta penerapan firewall dan NAT dalam konteks jaringan komputer. Dengan melakukan konfigurasi aturan dasar pada firewall dan menerapkan NAT, peserta akan memahami bagaimana sistem kontrol akses dan keamanan jaringan dapat dikelola secara efisien. Praktikum ini juga dirancang untuk memberikan pengalaman langsung dalam pengelolaan keamanan jaringan, yang merupakan keterampilan fundamental dalam dunia profesional di bidang teknologi informasi.

1.2 Dasar Teori

Dalam pengelolaan jaringan komputer, keamanan merupakan aspek yang sangat penting untuk menjaga data dan sistem tetap terlindungi dari berbagai ancaman eksternal. Dua teknologi utama yang sering digunakan dalam upaya ini adalah Firewall dan Network Address Translation (NAT). Firewall berfungsi untuk memfilter lalu lintas jaringan berdasarkan aturan tertentu, sehingga hanya koneksi yang diizinkan yang dapat melewati jaringan. Sementara itu, NAT memungkinkan perangkat dalam jaringan lokal menggunakan satu alamat IP publik untuk berkomunikasi dengan jaringan luar, sekaligus menyembunyikan alamat IP internal guna menambah lapisan perlindungan.

Praktikum ini bertujuan untuk mempelajari cara kerja dan penerapan firewall serta NAT dalam lingkungan jaringan komputer. Melalui konfigurasi aturan dasar pada firewall dan implementasi NAT, dapat dipahami bagaimana pengendalian akses dan perlindungan jaringan dilakukan secara efektif. Praktikum ini juga dirancang untuk membekali keterampilan praktis dalam mengelola keamanan jaringan, yang menjadi fondasi penting di dunia profesional teknologi informasi.

2 Tugas Pendahuluan

1. Untuk dapat mengakses web server lokal dengan alamat IP 192.168.1.10 pada port 80 dari jaringan luar, perlu dilakukan konfigurasi NAT jenis Destination NAT (DNAT), yang juga dikenal sebagai port forwarding. Konfigurasi ini berfungsi untuk mengarahkan permintaan dari jaringan luar yang masuk ke alamat IP publik router pada port 80 agar diteruskan ke alamat IP dan port server lokal yang sesuai, yaitu 192.168.1.10:80. Dengan cara ini, ketika pengguna dari luar mengakses IP publik router melalui browser atau aplikasi, permintaan tersebut akan secara otomatis diteruskan ke web server di jaringan internal. Konfigurasi ini memungkinkan layanan web di dalam jaringan lokal dapat diakses secara aman dan terkendali dari luar jaringan.

2. Dalam penerapan keamanan jaringan, firewall sebaiknya diutamakan untuk diterapkan terlebih dahulu dibandingkan NAT. Hal ini karena firewall berperan sebagai lini pertahanan utama yang

menyaring lalu lintas jaringan berdasarkan aturan tertentu, sehingga mampu mencegah akses yang tidak sah dan melindungi sistem dari ancaman eksternal seperti malware atau serangan siber. Sementara itu, NAT berfungsi mengatur translasi alamat IP agar perangkat dalam jaringan lokal dapat berkomunikasi dengan jaringan luar, namun tidak secara langsung memberikan perlindungan terhadap ancaman keamanan. Oleh karena itu, meskipun NAT juga penting, firewall perlu diterapkan lebih dahulu untuk memastikan lalu lintas jaringan yang masuk dan keluar sudah berada dalam kendali yang aman. Setelah itu, NAT dapat digunakan untuk mendukung komunikasi jaringan secara efisien tanpa mengesampingkan aspek keamanan yang telah diatur oleh firewall.

3. Jika router tidak diberi filter firewall sama sekali, jaringan menjadi sangat rentan terhadap berbagai ancaman dari luar. Tanpa adanya penyaringan lalu lintas, setiap koneksi yang masuk akan diterima tanpa pengecekan, sehingga membuka peluang bagi serangan seperti peretasan, penyebaran malware, pencurian data, hingga serangan DDoS. Ketiadaan firewall juga berarti tidak adanya kontrol akses, sehingga pihak luar dapat dengan mudah mencoba mengakses perangkat internal jaringan tanpa izin. Hal ini dapat menyebabkan kompromi sistem, gangguan operasional, bahkan kerusakan atau kehilangan data penting. Selain itu, router yang menerima seluruh lalu lintas tanpa penyaringan bisa mengalami penurunan kinerja karena harus memproses data yang sebenarnya tidak diperlukan. Dalam skala yang lebih luas, terutama di lingkungan organisasi atau institusi, kegagalan dalam menerapkan firewall dapat menyebabkan kerugian finansial dan menurunkan reputasi akibat kebocoran data atau gangguan layanan. Oleh karena itu, firewall merupakan komponen penting yang tidak boleh diabaikan dalam pengelolaan keamanan jaringan.