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

Laporan Sementara
Praktikum Jaringan Komputer

Firewall & NAT

Muhammad Tamim Nugraha - 5024231060

2025

1 Pendahuluan

1.1 Latar Belakang

Perkembangan teknologi jaringan komputer yang semakin pesat membawa kebutuhan akan keamanan dan efisiensi dalam pengelolaan jaringan. Jaringan komputer tidak hanya menghubungkan perangkat dalam skala kecil, tetapi juga memungkinkan akses ke sumber daya global seperti internet. Namun, konektivitas yang luas ini membuka peluang bagi berbagai ancaman keamanan, seperti akses tidak sah, serangan malware, dan penyalahgunaan data.

Untuk menjaga keamanan jaringan, diperlukan alat dan teknik yang mampu mengontrol aliran data masuk dan keluar jaringan. Firewall adalah salah satu komponen penting yang berfungsi sebagai garis pertahanan pertama dengan cara menyaring dan memblokir trafik yang mencurigakan atau berbahaya berdasarkan kebijakan keamanan yang diterapkan. Dengan firewall, administrator jaringan dapat mengatur hak akses dan melindungi jaringan dari berbagai ancaman.

Di sisi lain, keterbatasan jumlah alamat IP publik yang tersedia juga menjadi tantangan dalam pengelolaan jaringan, terutama bagi organisasi yang memiliki banyak perangkat. Network Address Translation (NAT) hadir sebagai solusi dengan memungkinkan banyak perangkat dalam jaringan lokal menggunakan alamat IP privat untuk terhubung ke internet melalui satu atau beberapa alamat IP publik. Selain menghemat penggunaan alamat IP, NAT juga menambah lapisan keamanan dengan menyembunyikan alamat IP internal dari jaringan eksternal.

Praktikum ini bertujuan untuk memberikan pemahaman langsung mengenai konfigurasi firewall dan NAT, sehingga mahasiswa dapat mengaplikasikan konsep keamanan dan manajemen alamat IP dalam jaringan komputer. Melalui pengalaman praktis ini, diharapkan mahasiswa dapat merancang jaringan yang tidak hanya terkoneksi dengan baik tetapi juga aman dan efisien.efisien.

1.2 Dasar Teori

1.3 Firewall

Firewall adalah sistem keamanan jaringan yang berfungsi untuk mengontrol dan memantau lalu lintas data yang masuk maupun keluar dari sebuah jaringan berdasarkan aturan tertentu. Fungsi utama firewall adalah melindungi jaringan dari akses tidak sah dan serangan yang berpotensi membahayakan sistem. Firewall dapat berupa perangkat keras atau perangkat lunak, dan sering digunakan untuk membatasi akses berdasarkan alamat IP, port, serta jenis protokol yang digunakan.

Jenis firewall yang umum digunakan antara lain:

- **Packet Filtering Firewall**, yang bekerja dengan menyaring paket berdasarkan header paket seperti alamat IP dan port.

- **Stateful Inspection Firewall**, yang selain memeriksa header paket juga memantau status koneksi sehingga lebih aman.
- **Application Layer Firewall**, yang mampu menginspeksi data pada tingkat aplikasi untuk deteksi ancaman lebih spesifik.

1.4 Network Address Translation (NAT)

Network Address Translation (NAT) adalah teknik yang digunakan untuk mengubah alamat IP pada header paket data yang melewati sebuah router atau firewall. Fungsi utama NAT adalah menghubungkan jaringan lokal yang menggunakan alamat IP privat dengan jaringan publik seperti internet menggunakan satu atau beberapa alamat IP publik.

Ada beberapa jenis NAT, yaitu:

- **Static NAT**, yang memetakan alamat IP privat ke alamat IP publik secara tetap.
- **Dynamic NAT**, yang memetakan alamat IP privat ke alamat IP publik dari sebuah pool secara dinamis.
- **Port Address Translation (PAT)** atau NAT Overload, yang memungkinkan banyak perangkat menggunakan satu alamat IP publik dengan membedakan berdasarkan nomor port.

NAT juga berfungsi sebagai lapisan keamanan tambahan karena menyembunyikan alamat IP asli perangkat dalam jaringan lokal dari dunia luar.

1.5 Hubungan Firewall dan NAT

Firewall dan NAT sering bekerja bersama untuk menjaga keamanan dan mengelola alamat IP dalam jaringan. NAT memungkinkan perangkat dalam jaringan lokal dapat mengakses internet meskipun menggunakan alamat IP privat, sementara firewall mengatur dan membatasi akses serta melindungi jaringan dari ancaman yang berasal dari luar maupun dalam. Kombinasi kedua teknologi ini sangat penting dalam pengelolaan jaringan modern untuk menjamin konektivitas sekaligus keamanan.

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?
   Jika kamu ingin mengakses web server lokal dengan IP 192.168.1.10 pada port 80 dari jaringan luar, maka konfigurasi NAT yang perlu dibuat adalah Destination NAT (DNAT) atau yang biasa disebut port forwarding. Konfigurasi ini memungkinkan router untuk meneruskan permintaan yang datang dari jaringan luar ke alamat IP publik router pada port 80, kemudian mengarahkan lalu lintas tersebut ke alamat IP

lokal server di 192.168.1.10 pada port 80. Dengan demikian, pengguna dari luar jaringan dapat mengakses web server lokal seolah-olah server tersebut berada di jaringan publik. Pengaturan ini biasanya dilakukan dengan menambahkan aturan NAT pada router yang memetakan IP publik dan port tertentu ke IP privat dan port web server lokal.

2. Menurutmu,mana yang lebih penting di terapkan terlebih dahulu di jaringan: NAT atau Firewall? Jelaskan alasanmu.
   Menurut saya, NAT (Network Address Translation) sebaiknya diterapkan terlebih dahulu dalam sebuah jaringan. Hal ini karena NAT berfungsi sebagai fondasi utama yang memungkinkan perangkat dalam jaringan lokal yang menggunakan alamat IP privat dapat terhubung ke jaringan luar, seperti internet, melalui satu atau beberapa alamat IP publik. Tanpa NAT, perangkat dengan IP privat tidak dapat berkomunikasi secara langsung dengan jaringan eksternal karena IP privat tidak bisa dirutekan di internet. Setelah koneksi dasar melalui NAT terbentuk, firewall dapat diterapkan untuk mengatur dan mengamankan lalu lintas data yang masuk dan keluar jaringan. Firewall bertugas membatasi akses, memfilter paket, dan mencegah ancaman keamanan, sehingga sangat penting dalam menjaga keamanan jaringan. Namun, fungsi firewall baru bisa berjalan efektif jika konektivitas jaringan sudah tersedia terlebih dahulu, yang disediakan oleh NAT. Oleh karena itu, secara urutan, NAT lebih prioritas diterapkan terlebih dahulu agar jaringan dapat terkoneksi, kemudian firewall diterapkan untuk memperkuat keamanan jaringan tersebut.

3. Apa dampak negatif jika router tidak diberi filter firewall sama sekali?
   Jika router tidak diberi filter firewall sama sekali, maka jaringan akan sangat rentan terhadap berbagai ancaman keamanan dari luar maupun dalam. Tanpa adanya filter firewall, seluruh lalu lintas data yang masuk dan keluar dari jaringan tidak akan disaring atau dibatasi, sehingga semua jenis koneksi akan diizinkan secara bebas. Hal ini memungkinkan pihak yang tidak berwenang, termasuk peretas atau malware, untuk mengakses perangkat-perangkat di jaringan internal tanpa hambatan. Akibatnya, jaringan dapat mengalami kebocoran data, penyebaran virus atau worm, hingga serangan serius seperti hacking, brute force attack, atau Distributed Denial of Service (DDoS). Selain itu, tanpa firewall, tidak ada mekanisme untuk mengendalikan atau memblokir trafik yang mencurigakan atau tidak diinginkan, sehingga dapat menurunkan performa jaringan dan membahayakan kestabilan sistem. Dengan kata lain, ketiadaan firewall membuat jaringan sepenuhnya terbuka dan tidak terlindungi, yang dapat berujung pada kerugian besar baik secara teknis maupun operasional.