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

Laporan Sementara
Praktikum Jaringan Komputer

Firewall & NAT

Sebastian Adirian Nugraha - 5024231010

2025

1 Pendahuluan

1.1 Latar Belakang

Dalam perkembangan teknologi informasi dan komunikasi, jaringan komputer memainkan peran sentral dalam menghubungkan berbagai perangkat untuk bertukar data dan informasi. Namun, pertumbuhan pesat jumlah perangkat yang terhubung menimbulkan tantangan dalam hal ketersediaan alamat IP. Untuk mengatasi keterbatasan tersebut, digunakanlah teknologi Network Address Translation (NAT) yang memungkinkan banyak perangkat di jaringan lokal dengan alamat IP privat untuk mengakses internet melalui satu alamat IP publik. Selain efisiensi penggunaan IP, NAT juga memberikan lapisan perlindungan dasar karena perangkat internal tidak langsung terekspos ke jaringan luar, meskipun fungsi utamanya bukan untuk keamanan.

Di sisi lain, meningkatnya ancaman keamanan jaringan seperti peretasan, malware, dan serangan dari luar membuat perlindungan terhadap lalu lintas data menjadi sangat penting. Di sinilah peran firewall menjadi krusial sebagai sistem penyaring lalu lintas jaringan berdasarkan aturan yang ditentukan. Firewall dapat memblokir akses yang mencurigakan atau tidak sah, serta mencegah komunikasi dari dan ke sumber yang tidak terpercaya. Dengan menggabungkan NAT dan firewall dalam arsitektur jaringan, administrator dapat mengelola konektivitas secara efisien sekaligus menjaga sistem dari ancaman eksternal, menciptakan jaringan yang stabil, efisien, dan aman.

1.2 Dasar Teori

Firewall adalah sistem keamanan jaringan yang berfungsi untuk memantau dan mengontrol lalu lintas data yang masuk dan keluar dari suatu jaringan berdasarkan aturan yang telah ditentukan. Firewall bertindak sebagai penghalang antara jaringan internal yang dipercaya (seperti LAN) dan jaringan eksternal yang tidak dipercaya (seperti internet), untuk mencegah akses tidak sah serta melindungi sistem dari serangan seperti malware, intrusi, dan eksploitasi. Firewall dapat berupa perangkat keras (hardware), perangkat lunak (software), atau kombinasi keduanya, dan dapat dikonfigurasi untuk mengizinkan, memblokir, atau membatasi koneksi berdasarkan alamat IP, port, protokol, atau isi dari paket data.

NAT (Network Address Translation) adalah mekanisme dalam jaringan komputer yang digunakan untuk menerjemahkan alamat IP privat di dalam jaringan lokal menjadi alamat IP publik (dan sebaliknya) saat berkomunikasi dengan jaringan luar, seperti internet. NAT memungkinkan banyak perangkat di jaringan lokal dengan IP privat untuk mengakses internet menggunakan satu alamat IP publik, sehingga menghemat penggunaan IP publik dan meningkatkan keamanan jaringan karena perangkat internal tidak langsung terlihat dari luar. Selain itu, NAT juga digunakan dalam port forwarding untuk memungkinkan akses dari luar ke perangkat tertentu di dalam jaringan lokal.

Port forwarding adalah teknik dalam jaringan yang digunakan untuk mengarahkan koneksi dari luar (internet) ke perangkat tertentu di dalam jaringan lokal melalui port tertentu. Dengan port forwarding, ketika ada permintaan ke alamat IP publik router pada port tertentu (misalnya port 80), router akan meneruskan permintaan tersebut ke alamat IP dan port internal yang telah ditentukan (misalnya ke server lokal di 192.168.1.10:80). Teknik ini umum digunakan untuk mengizinkan akses dari luar ke layanan seperti web server, FTP, atau kamera CCTV yang berada di balik router dengan NAT, sehingga perangkat dari internet dapat terhubung ke layanan di dalam jaringan lokal.

2 Tugas Pendahuluan

1. Untuk mengakses web server lokal dari jaringan luar dapat dilakukan dengan menggunakan Port Forwarding. Port Forwarding menghubungkan port internal yang berada pada host (192.168.1.10) ke port external yang menggunakan External IP atau Public IP. Port yang tersedia pada masing-masing ip adalah 6512 Port. Misal, dari host lokal ke router kita gunakan IP Internal (192.168.1.10) diexpose pada port 80 internal. Lalu untuk kita broadcast ke public IP kita dapat kita dapat pilih port internal tadi dihubungkan dengan port external bebas. Jika dihubungkan pada port external 25565 dan public ip kita misal 168.12.128.100, maka web server lokal kita dapat diakses melalui 168.12.128.100:25565 (PublicIP:PortExternal).

2. Firewall perlu diterapkan terlebih dahulu karena faktor keamanan. Jika NAT dibuat terlebih dahulu dan suatu traffic sudah terbuat, maka terdapat kemungkinan traffic yang tidak diinginkan terjadi, karena NAT tidak memfilter traffic berdasarkan keamanan tetapi translasi.

3. Jika Firewall tidak diterapkan maka, semua traffic dari luar bisa saja mengaskes semua jaringan lokal.