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

Praktikum Jaringan Komputer

Modul 4 – Firewall and NAT

I Gusti Ngurah Opaldi Partha Dwipayana – 5024221057

2025

1 Pendahuluan

1.1 Latar Belakang

Dalam era digital saat ini, keamanan jaringan menjadi salah satu aspek paling krusial dalam pengelolaan sistem informasi. Semakin meningkatnya ketergantungan terhadap jaringan internet juga disertai dengan bertambahnya ancaman terhadap integritas, kerahasiaan, dan ketersediaan data. Untuk itu, diperlukan solusi teknis yang mampu mengamankan jaringan dari akses yang tidak sah dan sekaligus memastikan konektivitas jaringan tetap berjalan secara efisien. Dua komponen penting yang berperan dalam sistem keamanan dan manajemen lalu lintas jaringan adalah Firewall dan Network Address Translation (NAT).

Firewall berfungsi sebagai penghalang antara jaringan internal dan jaringan eksternal (internet), yang bekerja dengan cara memfilter lalu lintas data berdasarkan aturan keamanan yang telah ditentukan. Firewall dapat mendeteksi dan memblokir aktivitas mencurigakan yang berpotensi membahayakan sistem, seperti serangan dari peretas, malware, atau akses ilegal. Sementara itu, NAT memiliki peran dalam menerjemahkan alamat IP privat ke alamat IP publik, sehingga perangkat dalam jaringan lokal dapat berkomunikasi dengan dunia luar menggunakan satu atau beberapa alamat IP yang legal. Selain membantu menghemat penggunaan alamat IP publik, NAT juga memberikan lapisan perlindungan tambahan dengan menyembunyikan struktur jaringan internal. Kombinasi penggunaan firewall dan NAT menjadi standar dalam desain jaringan modern karena keduanya saling melengkapi dalam menjaga keamanan sekaligus memastikan kelancaran komunikasi data.

1.2 Dasar Teori

Firewall atau adaptive security appliance adalah sebuah sistem atau kelompok sistem yang menerapkan sebuah access control policy terhadap lalu lintas jaringan yang melewati titik-titik akses dalam jaringan. Tugas firewall adalah untuk memastikan bahwa tidak ada tambahan diluar ruang lingkup yang diizinkan. Firewall bertanggung jawab untuk memastikan bahwa access control policy yang diikuti oleh semua pengguna di dalam jaringan tersebut. Firewall seperti halnya alat-alat jaringan lain dalam hal untuk mengontrol aliran lalu lintas jaringan. Namun, tidak seperti alat-alat jaringan lain, sebuah firewall harus mengontrol lalu lintas network dengan memasukkan faktor pertimbangan bahwa tidak semua paket-paket data yang dilihatnya adalah seperti yang terlihat. Firewall digunakan untuk mengontrol akses antara network internal sebuah organisasi internet.

Network Address Translation (NAT) adalah proses yang memungkinkan satu alamat IP unik untuk mewakili seluruh kelompok komputer. Dalam NAT, sebuah perangkat jaringan biasanya berupa router atau firewall dengan fitur NAT memberikan satu atau beberapa komputer dalam jaringan privat sebuah alamat IP publik. Dengan cara ini, NAT memungkinkan satu perangkat bertindak sebagai perantara atau agen antara jaringan lokal (privat) dengan jaringan publik, yaitu internet. Tujuan utama dari NAT adalah untuk menghemat penggunaan alamat IP publik, baik demi alasan keamanan maupun

efisiensi biaya. NAT menghemat alamat IP dengan memungkinkan jaringan IP privat yang menggunakan alamat IP yang tidak terdaftar untuk tetap dapat terhubung ke internet. Sebelum NAT meneruskan paket data antar jaringan yang dihubungkannya, NAT akan terlebih dahulu menerjemahkan alamat dari jaringan internal yang privat menjadi alamat yang sah dan unik secara globa

2 Tugas Pendahuluan

2.1 Soal

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?

2. Menurutmu, mana yang lebih penting diterapkan terlebih dahulu di jaringan: NAT atau Firewall? Jelaskan alasanmu.

3. Apa dampak negatif jika router tidak diberi filter firewall sama sekali?

2.2 Jawaban

1. Jika ingin mengakses web server lokal dengan alamat IP 192.168.1.10 pada port 80 dari jaringan luar (internet), maka jenis konfigurasi NAT yang perlu diterapkan adalah port forwarding atau Static NAT. Konfigurasi ini memungkinkan router untuk meneruskan permintaan dari alamat IP publik ke alamat IP privat di jaringan lokal. Sebagai contoh, jika seseorang mengakses alamat IP publik router pada port 80, NAT akan meneruskannya ke IP lokal 192.168.1.10 pada port yang sama. Dengan kata lain, NAT akan menerjemahkan permintaan eksternal menjadi permintaan internal yang ditujukan ke server lokal. Konfigurasi ini umum digunakan ketika layanan lokal (seperti web server atau CCTV) ingin diakses dari luar jaringan, namun tetap menggunakan satu IP publik.

2. NAT sebaiknya diterapkan terlebih dahulu karena fungsinya adalah menghubungkan jaringan lokal ke jaringan luar (internet) dengan menerjemahkan alamat IP. Tanpa NAT, jaringan private dengan IP seperti 192.168.x.x tidak dapat mengakses atau diakses dari internet karena IP tersebut tidak dikenali secara global. Setelah NAT dikonfigurasi, barulah firewall menjadi penting untuk melindungi sistem dari akses yang tidak sah. Firewall berfungsi sebagai penyaring dan pengontrol lalu lintas jaringan berdasarkan aturan keamanan. Jadi, NAT mendahului secara teknis agar komunikasi dapat terjadi, sementara firewall berfungsi untuk memastikan bahwa komunikasi tersebut tetap aman.

3. Dampak negatif jika router tidak diberi filter firewall sama sekali sangatlah serius. Tanpa firewall, seluruh perangkat di jaringan lokal menjadi terbuka terhadap lalu lintas dari luar tanpa penyaringan. Hal ini memungkinkan berbagai serangan seperti port scanning, brute force login, malware injection, hingga pengambilalihan sistem oleh peretas. Dalam konteks jaringan rumah maupun perusahaan, ketiadaan firewall dapat menyebabkan kebocoran data, gangguan layanan, dan

bahkan kerusakan perangkat. Oleh karena itu, firewall sangat penting untuk membatasi akses hanya untuk lalu lintas yang diizinkan dan mencegah eksploitasi dari pihak luar.