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

Laporan Sementara
Praktikum Jaringan Komputer

NAT dan Firewall

Sultan Syafiq Rakan - 5024231009

2025

1 Pendahuluan

1.1 Latar Belakang

Firewall dan Network Address Translation (NAT) merupakan dua komponen penting dalam pengelolaan dan keamanan jaringan modern. Firewall berfungsi sebagai sistem keamanan yang memantau dan mengontrol lalu lintas jaringan masuk dan keluar berdasarkan aturan yang telah ditentukan, bertindak seperti penjaga gerbang untuk melindungi jaringan dari akses tidak sah, serangan siber, atau ancaman seperti malware. Dengan memfilter data berdasarkan informasi seperti alamat IP, port, dan protokol, firewall memastikan hanya koneksi yang diizinkan yang dapat mengakses jaringan, menjaga privasi dan integritas data. Sementara itu, NAT memungkinkan perangkat di jaringan lokal dengan alamat IP pribadi, seperti 192.168.1.x, untuk berkomunikasi dengan internet melalui satu alamat IP publik dengan memodifikasi header paket data, termasuk alamat IP dan port. Teknik ini, yang sering digunakan dalam bentuk Port Forwarding, memungkinkan akses dari internet ke layanan lokal seperti web server, sekaligus menyembunyikan struktur jaringan internal untuk meningkatkan keamanan. Dalam praktiknya, firewall dan NAT bekerja bersama di router, di mana NAT mengatur penerusan data dan firewall memastikan hanya lalu lintas yang sesuai aturan yang diizinkan, menciptakan keseimbangan antara aksesibilitas dan keamanan jaringan.

2 Dasar Teori

Firewall

Firewall adalah sistem keamanan jaringan yang berfungsi untuk mengontrol dan memantau lalu lintas jaringan masuk dan keluar berdasarkan aturan keamanan yang telah ditentukan. Firewall bertindak seperti "penjaga gerbang" yang memfilter data berdasarkan informasi seperti alamat IP, port, dan protokol (misalnya, TCP atau UDP). Tujuannya adalah melindungi jaringan atau perangkat dari akses tidak sah, serangan siber, atau ancaman seperti malware dan peretasan. Firewall dapat diimplementasikan dalam perangkat keras (seperti pada router), perangkat lunak (seperti Windows Firewall), atau kombinasi keduanya. Ada beberapa jenis firewall, seperti packet-filtering, stateful inspection, dan application-layer firewall, yang masing-masing memiliki cara berbeda dalam memeriksa dan mengatur lalu lintas jaringan. Dalam konteks keamanan, firewall sangat penting untuk menjaga privasi dan integritas data dalam jaringan lokal, terutama saat terhubung ke internet.

NAT (Network Address Translation)

NAT adalah teknik yang digunakan router atau gateway untuk memetakan alamat IP pribadi (private IP) dalam jaringan lokal ke alamat IP publik yang digunakan di internet. NAT memungkinkan banyak perangkat dalam jaringan lokal (misalnya, dengan IP seperti 192.168.1.x) untuk berbagi satu alamat IP publik saat berkomunikasi dengan jaringan luar. Ini dilakukan dengan mengubah header paket data, seperti alamat IP sumber atau tujuan,

dan sering kali nomor port. Salah satu fungsi utama NAT adalah **Port Forwarding** (Destination NAT), yang memungkinkan akses dari internet ke perangkat tertentu di jaringan lokal, seperti web server, dengan meneruskan permintaan dari port tertentu di IP publik ke IP dan port lokal. Selain menghemat alamat IP publik, NAT juga memberikan lapisan keamanan tambahan dengan menyembunyikan struktur jaringan lokal dari dunia luar.

Hubungan Firewall dan NAT

Firewall dan NAT sering bekerja bersama dalam router untuk mengatur lalu lintas jaringan. NAT menentukan bagaimana alamat dan port diterjemahkan, sedangkan firewall memastikan bahwa hanya lalu lintas yang diizinkan yang dapat melewati aturan NAT. Misalnya, saat mengatur akses ke web server lokal (IP: 192.168.1.10, port 80) dari internet, NAT akan meneruskan permintaan dari IP publik ke IP lokal, dan firewall harus dikonfigurasi untuk mengizinkan koneksi ke port tersebut agar akses berhasil. Kombinasi keduanya memungkinkan akses yang aman dan terkontrol ke layanan dalam jaringan lokal sambil menjaga keamanan dari ancaman eksternal.

3 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?

   (a) External Port: Port 8080

   (b) Internal IP: 192.168.1.10

   (c) Internal Port: Port 80.

   (d) Protokol: TCP.

   (e) Action : Forward request dari port luar ke IP dan port dalam.

2. Menurutmu, mana yang lebih penting diterapkan terlebih dahulu di jaringan: NAT atau Firewall? Jelaskan alasanmu.
   Firewall harus diterapkan terlebih dahulu karena keamanan adalah fondasi utama dalam jaringan. NAT, meskipun penting untuk fungsionalitas seperti akses eksternal, namun tidak memberikan perlindungan terhadap ancaman. Dengan firewall yang sudah aktif, NAT dapat diatur dengan aman. Hal ini memastikan jaringan tetap terlindungi dengan tetap memenuhi kebutuhan aksesibilitas.

3. Apa dampak negatif jika router tidak diberi filter firewall sama sekali?
   Ancaman dari internet akan masuk dengan bebas tanpa ada penyaring ataupun filter yang menjaga sistem dari ancaman seperti virus, malware, dsb.