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

Laporan Sementara
Praktikum Jaringan Komputer

Firewall and NAT

Devlin Jeychovhinn Saputra - 5024231019

2025

1 Pendahuluan

1.1 Latar Belakang

Dalam era digital yang terus berkembang, keamanan jaringan menjadi salah satu aspek paling krusial dalam pengelolaan infrastruktur teknologi informasi. Akses terbuka terhadap internet membuat jaringan internal organisasi rentan terhadap berbagai ancaman dari luar seperti peretasan, serangan *malware*, hingga pencurian data. Untuk itu, diperlukan mekanisme pengamanan jaringan yang mampu mengontrol lalu lintas data, mendeteksi ancaman, dan mencegah akses yang tidak sah. Modul keempat ini membahas dua komponen utama dalam pengamanan dan pengelolaan lalu lintas jaringan, yaitu *Firewall* dan *Network Address Translation (NAT)*. Firewall berfungsi sebagai pengawas utama yang menyaring lalu lintas berdasarkan aturan tertentu, sedangkan NAT memungkinkan banyak perangkat dalam jaringan lokal mengakses internet menggunakan satu alamat IP publik. Keduanya merupakan fondasi penting dalam arsitektur jaringan modern, baik untuk kebutuhan personal, perusahaan, maupun institusi skala besar.

1.2 Dasar Teori

Firewall adalah sistem yang dirancang untuk mencegah akses yang tidak diinginkan ke atau dari jaringan pribadi. Firewall dapat berupa perangkat keras (hardware), perangkat lunak (software), atau gabungan keduanya yang menerapkan aturan untuk mengizinkan atau memblokir lalu lintas jaringan berdasarkan kriteria keamanan tertentu seperti alamat IP, port, dan protokol. Firewall memiliki beberapa jenis berdasarkan cara kerjanya, di antaranya: Packet Filtering, Stateful Inspection, Application Layer Firewall, hingga Next-Generation Firewall (NGFW). Kebijakan dasar firewall meliputi *accept*, *reject*, dan *drop*, yang mengatur bagaimana paket data ditangani saat melewati firewall.
Network Address Translation (NAT) adalah metode untuk mengubah alamat IP sumber atau tujuan dari paket IP. NAT memungkinkan banyak perangkat dalam jaringan lokal (dengan IP privat) untuk berkomunikasi ke jaringan luar (internet) melalui satu IP publik. Tiga jenis utama NAT adalah Static NAT, Dynamic NAT, dan Port Address Translation (PAT), dengan PAT menjadi yang paling umum digunakan karena efisiensinya dalam memanfaatkan IP publik. NAT biasanya diimplementasikan pada perangkat router atau firewall yang menjadi penghubung antara jaringan lokal dan jaringan luar.
Connection Tracking merupakan fitur penting dalam firewall dan NAT yang memungkinkan sistem mencatat status setiap koneksi jaringan. Dengan mengetahui apakah sebuah koneksi masih aktif, baru, atau tidak sah, sistem dapat memutuskan untuk mengizinkan atau memblokir koneksi tersebut secara lebih cerdas.

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?**

   Konfigurasi NAT yang diperlukan adalah port forwarding (Destination NAT). Dengan port forwarding, router publik akan meneruskan permintaan dari internet (misalnya pada IP publik x.x.x.x port 80) ke IP lokal 192.168.1.10 port 80. Konfigurasi ini memungkinkan perangkat dari luar jaringan mengakses layanan web server yang berada di jaringan lokal.

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

   Keduanya penting dan sering berjalan bersamaan, namun dalam konteks prioritas implementasi, Firewall lebih penting untuk diterapkan terlebih dahulu. Firewall bertugas menyaring dan mengamankan lalu lintas data berdasarkan aturan yang dibuat administrator jaringan. Jika firewall tidak ada, jaringan akan sangat rentan terhadap serangan dari luar, bahkan sebelum NAT sempat melakukan translasi alamat. Firewall adalah garis pertahanan utama yang membatasi akses terhadap jaringan lokal.

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

   Dampak negatifnya adalah jaringan menjadi terbuka sepenuhnya terhadap lalu lintas luar yang tidak dikenal atau berbahaya. Hal ini dapat menyebabkan masuknya trafik berbahaya seperti *malware*, *botnet*, atau serangan *DDoS*, eksploitasi celah keamanan pada layanan internal yang seharusnya tidak dapat diakses publik pencurian data, penyadapan koneksi, hingga pengambilalihan sistem oleh pihak tidak sah. Tanpa firewall, tidak ada mekanisme penyaringan atau pembatasan terhadap lalu lintas yang datang dari luar, sehingga risiko keamanan jaringan meningkat drastis.

   Referensi:

   - Cisco. (2020). *Introduction to Firewalls*. Cisco Networking Academy.
   - MikroTik Documentation. (2022). *Firewall and NAT Concepts*. `https://help.mikrotik.com/docs/display/ROS/Firewall`
   - Odom, W. (2021). *CCNA 200-301 Official Cert Guide*. Cisco Press.
