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

Laporan Sementara
Praktikum Jaringan Komputer

Firewall dan NAT

Bernanddus Nathaniel Arthur - 5024231041

2025

1 Pendahuluan

1.1 Latar Belakang

Perkembangan teknologi jaringan yang pesat telah membawa dampak signifikan pada cara kita berinteraksi dan bertukar informasi. Namun, seiring dengan kemajuan ini, ancaman keamanan siber juga semakin meningkat. Data-data penting perusahaan dan individu menjadi sasaran empuk bagi pihak tidak bertanggung jawab, sehingga diperlukan sebuah mekanisme perlindungan yang kuat. Dalam konteks ini, firewall hadir sebagai garda terdepan dalam menjaga keamanan jaringan. Firewall berfungsi sebagai sistem keamanan yang memantau dan mengontrol lalu lintas jaringan masuk dan keluar berdasarkan aturan keamanan yang telah ditetapkan. Selain firewall, implementasi Network Address Translation (NAT) juga menjadi krusial dalam arsitektur jaringan modern. NAT memungkinkan banyak perangkat dalam jaringan lokal untuk berbagi satu alamat IP publik, sehingga tidak hanya menghemat penggunaan alamat IP, tetapi juga menambahkan lapisan keamanan dengan menyembunyikan topologi internal jaringan dari internet. Praktikum modul Firewall dan NAT ini akan memberikan pemahaman mendalam mengenai prinsip kerja, konfigurasi, dan implementasi kedua teknologi ini dalam menciptakan jaringan yang aman, efisien, dan terlindungi dari berbagai ancaman siber. Sebelum adanya firewall, keamanan jaringan sangat bergantung pada Access Control List (ACL) yang hanya mampu melakukan pemeriksaan sederhana tanpa dapat membedakan isi dari lalu lintas data. Hal ini meninggalkan banyak celah keamanan yang rentan dimanfaatkan oleh pihak tidak bertanggung jawab, terutama mengingat internet kini telah menjadi kebutuhan pokok bagi berbagai organisasi. Oleh karena itu, firewall, yang diibaratkan sebagai "satpam digital", menjadi esensial untuk memantau dan mengontrol lalu lintas jaringan berdasarkan aturan yang telah ditetapkan (Modul Firewall NAT, sub-bab 1.1). Di samping firewall, Network Address Translation (NAT) memainkan peran penting dalam mengatasi keterbatasan alamat IPv4 yang semakin menipis sekaligus meningkatkan efisiensi penggunaan alamat IP publik. Dengan NAT, banyak perangkat dalam jaringan lokal dapat berbagi satu alamat IP publik untuk mengakses internet, layaknya "banyak penghuni yang berbagi satu alamat rumah di dunia maya" (Modul Firewall NAT, sub-bab 1.2). Gabungan antara firewall yang mengontrol lalu lintas dan NAT yang mengelola alamat IP, didukung oleh fitur Connection Tracking yang melacak status koneksi secara detail, akan membentuk sistem keamanan jaringan yang kokoh dan efisien.

1.2 Dasar Teori

Firewall adalah fondasi keamanan jaringan, berfungsi sebagai penjaga gerbang yang mengontrol lalu lintas data masuk dan keluar berdasarkan aturan yang telah ditetapkan. Tujuannya jelas: mencegah akses tidak sah dan melindungi jaringan internal dari ancaman eksternal seperti malware dan serangan siber. Perjalanan evolusi firewall, dari penyaringan paket sederhana hingga Next Generation Firewall (NGFW) dengan kemampuan inspeksi

mendalam, menunjukkan bagaimana teknologi ini beradaptasi untuk menghadapi kompleksitas ancaman siber yang terus berkembang. Melalui kebijakan accept, reject, atau drop, firewall memastikan hanya lalu lintas yang sah yang dapat melewati batas jaringan, menjadi garda terdepan dalam menjaga integritas dan kerahasiaan data.

Sejalan dengan fungsi firewall, Network Address Translation (NAT) berperan penting dalam mengatasi keterbatasan alamat IPv4 sekaligus meningkatkan keamanan jaringan. NAT memungkinkan banyak perangkat dalam jaringan lokal berbagi satu alamat IP publik saat mengakses internet, layaknya banyak "penghuni" yang berbagi satu "alamat rumah" di dunia maya. Mekanisme ini bekerja dengan menerjemahkan alamat IP privat internal ke alamat IP publik saat paket keluar, dan sebaliknya saat paket masuk, dengan Port Address Translation (PAT) sebagai metode yang paling umum dan efisien. Kedua teknologi ini, baik firewall maupun NAT, sangat ditopang oleh Connection Tracking, sebuah fitur cerdas yang melacak status setiap koneksi. Dengan informasi ini, firewall dapat mengizinkan lalu lintas yang sah secara efisien dan menolak yang tidak valid, sementara NAT dapat mengelola terjemahan alamat dengan akurat. Kombinasi sinergis dari firewall, NAT, dan Connection Tracking ini membentuk benteng keamanan jaringan yang kokoh dan efisien, melindungi dari berbagai tantangan keamanan siber.

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?
   Jawaban: Gunakan *pengalihan port* (Static NAT atau Destination NAT). Semua permintaan yang masuk ke alamat publik dan port tertentu akan diteruskan ke alamat IP dan port server di dalam jaringan.
   Contoh parameter:
   - IP Eksternal Router: 123.123.123.1
   - Port Eksternal: 80
   - IP Internal Server: 192.168.1.10
   - Port Internal: 80

2. **Menurutmu, mana yang lebih penting diterapkan terlebih dahulu di jaringan: NAT atau Firewall? Jelaskan alasanmu.**
   Jawaban: Dari sisi konektivitas, NAT harus diaktifkan terlebih dahulu agar perangkat beralamat IP privat dapat mengakses Internet. Namun untuk menjaga keamanan, *firewall* sebaiknya dipasang lebih awal ia akan memeriksa dan menolak lalu lintas berbahaya sebelum atau sesudah proses NAT.

3. **Apa dampak negatif jika router tidak diberi filter firewall sama sekali?**
   Jawaban: Tanpa firewall, router akan meneruskan seluruh paket tanpa penyaringan, mengakibatkan:

- Rentan terhadap serangan malware, botnet, dan peretasan.
- Layanan internal (misal web/file server) dapat diakses siapa saja.
- Tidak ada proteksi terhadap trafik mencurigakan.
- Risiko kebocoran data dan pelanggaran privasi pengguna meningkat.