



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

Laporan Sementara Praktikum Jaringan Komputer

Firewall dan NAT

Kenny Joe Neville - 5024231079

2025

1 Pendahuluan

1.1 Latar Belakang

Dalam era digital saat ini, keamanan jaringan komputer menjadi salah satu aspek krusial dalam menjaga integritas, kerahasiaan, dan ketersediaan data. Dengan semakin meningkatnya ancaman siber seperti serangan malware, peretasan, dan pencurian data, organisasi membutuhkan sistem keamanan yang andal untuk melindungi infrastruktur jaringan mereka. Salah satu solusi yang umum digunakan adalah firewall, yang berfungsi sebagai pertahanan utama untuk mengontrol lalu lintas jaringan berdasarkan aturan keamanan tertentu. Selain itu, Network Address Translation (NAT) memainkan peran penting dalam mengelola alamat IP, memungkinkan efisiensi penggunaan alamat serta memberikan lapisan tambahan untuk menyembunyikan struktur jaringan internal dari dunia luar.

1.2 Dasar Teori

Firewall adalah sistem keamanan jaringan yang dirancang untuk memantau dan mengontrol lalu lintas jaringan masuk dan keluar berdasarkan aturan keamanan yang telah ditentukan. Firewall dapat berupa perangkat keras, perangkat lunak, atau kombinasi keduanya, dan bekerja dengan memfilter paket data berdasarkan informasi seperti alamat IP, port, dan protokol. Fungsi utama firewall adalah mencegah akses tidak sah, melindungi dari ancaman siber, dan memastikan bahwa hanya lalu lintas jaringan yang diizinkan yang dapat masuk atau keluar dari jaringan. Network Address Translation (NAT) adalah teknik yang digunakan untuk memetakan alamat IP privat ke alamat IP publik, atau sebaliknya, untuk memungkinkan komunikasi antara jaringan lokal dan jaringan eksternal seperti internet. NAT memungkinkan banyak perangkat dalam jaringan lokal menggunakan satu alamat IP publik, sehingga menghemat penggunaan alamat IP dan meningkatkan keamanan dengan menyembunyikan alamat IP internal dari jaringan eksternal. NAT biasanya diimplementasikan pada router atau gateway dan sering kali dikombinasikan dengan firewall untuk meningkatkan keamanan jaringan.

2 Tugas Pendahuluan

Bagian ini berisi jawaban dari tugas pendahuluan yang telah anda kerjakan, beserta penjelasan dari jawaban tersebut.

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?**

Untuk mengakses web server lokal (192.168.1.10:80) dari jaringan luar, perlu dibuat konfigurasi Static NAT dengan port forwarding (PAT). Konfigurasi ini meneruskan permintaan dari IP publik router pada port 80 ke alamat IP privat server tersebut, sehingga lalu lintas dari luar dapat diarahkan ke server lokal dengan benar. Selain itu, antarmuka jaringan harus diatur sebagai inside untuk jaringan lokal dan outside untuk jaringan publik agar NAT berjalan efektif.

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

Firewall lebih penting diterapkan terlebih dahulu karena berfungsi sebagai pelindung utama jaringan dengan menyaring lalu lintas dan mencegah akses tidak sah, serangan malware, atau eksploitasi dari luar. Sementara NAT lebih fokus pada menghemat alamat IPv4 dengan menyembunyikan IP privat, namun perlindungan yang diberikannya bersifat tidak langsung dan bukan tujuan utamanya. Firewall juga bekerja pada semua jenis jaringan, termasuk IPv6, sedangkan NAT hanya relevan pada jaringan IPv4.

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

- Akses Tidak Sah: Siapa pun dari internet dapat mengakses semua port terbuka di jaringanmu yang dapat dieksploitasi untuk mendapatkan akses ke perangkat.
- Serangan Jaringan: Tanpa firewall, router rentan terhadap serangan seperti DDoS, port scanning, atau injeksi malware.
- Kebocoran Data: Data sensitif di jaringan lokal bisa diakses oleh pihak luar jika layanan tersebut tidak sengaja terekspos melalui NAT atau konfigurasi buruk.
- Penyalahgunaan Sumber Daya: Penyerang dapat memanfaatkan perangkat di jaringanmu untuk aktivitas ilegal.
- Kinerja Jaringan Terganggu: Lalu lintas berbahaya yang tidak difilter dapat membebani router, menyebabkan penurunan kinerja.

2.1 Referensi

- <https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/13772-12.html>
- <https://bminfotrade.com/blog/cyber-security/nat-and-firewall-explained-key-differences-and-their-role-in-network-security->