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

Laporan Sementara Praktikum Jaringan Komputer

Firewall dan NAT

Nur Rahman Fauzan - 5024231069

Sabtu, 31 Mei 2025

1 Pendahuluan

Berisi deskripsi awal praktikum yang dilakukan pada hari itu

2 Latar Belakang

eiring pesatnya perkembangan teknologi informasi, kebutuhan akan akses internet semakin meningkat. Banyak organisasi dan institusi kini mengandalkan layanan web dan aplikasi berbasis jaringan untuk menjalankan operasional sehari-hari, termasuk layanan internal yang berjalan pada server lokal. Namun, tanpa perlindungan yang memadai, server lokal rentan terhadap serangan dari luar, seperti pemindaian port, eksploitasi celah keamanan, dan percobaan akses tidak sah. Di sisi lain, keterbatasan alamat IP publik memaksa banyak perangkat di jaringan lokal untuk berbagi satu alamat publik melalui teknik NAT.

Ketika firewall tidak diterapkan dengan benar, lalu lintas berbahaya dapat masuk ke dalam jaringan, mengakibatkan potensi pencurian data, gangguan layanan, atau penyebaran malware. Sebaliknya, tanpa konfigurasi NAT yang tepat, server lokal tidak dapat diakses dari luar, yang menghambat layanan penting seperti web server atau aplikasi internal. Oleh karena itu, pemahaman dan penerapan kedua mekanisme firewall sebagai pengawal keamanan dan NAT sebagai penerjemah alamat menjadi sangat krusial dalam desain dan manajemen jaringan modern.

3 Dasar Teori

3.1 Firewall

Firewall adalah perangkat lunak atau perangkat keras yang berfungsi sebagai “satpam” digital, memantau dan mengendalikan lalu lintas data masuk maupun keluar jaringan berdasarkan kebijakan keamanan yang telah ditetapkan. Dengan firewall, organisasi dapat mencegah akses tidak sah, serangan malware, dan eksploitasi celah keamanan.

3.1.1 Jenis-jenis Firewall

- **Packet Filtering:** Memeriksa paket berdasarkan IP, port, dan protokol saja.
- **Stateful Inspection:** Menganalisis status koneksi untuk memastikan paket merupakan bagian dari sesi sah.
- **Application Layer Firewall:** Menginspeksi konten aplikasi (HTTP, FTP) dan dapat memblokir konten tertentu.
- **Next Generation Firewall (NGFW):** Menggunakan deep packet inspection dan dukungan SSL/TLS.
- **Circuit Level Gateway:** Bekerja pada level koneksi (session) tanpa menginspeksi payload.

- **Software Firewall:** Firewall berbasis perangkat lunak yang dipasang pada host.
- **Hardware Firewall:** Perangkat fisik yang diletakkan di perbatasan jaringan.
- **Cloud Firewall:** Firewall yang dijalankan di lingkungan komputasi awan.

3.2 Network Address Translation (NAT)

NAT adalah teknik yang memungkinkan banyak perangkat di jaringan privat menggunakan satu atau lebih alamat IP publik untuk berkomunikasi dengan jaringan eksternal. NAT mengubah alamat IP dan/atau port paket yang keluar/masuk.

3.2.1 Jenis-jenis NAT

- **Static NAT:** One-to-one mapping antara alamat lokal dan publik.
- **Dynamic NAT:** Mapping dari lokal ke alamat publik yang tersedia di pool.
- **Port Address Translation (PAT):** Banyak lokal ke satu publik dengan membedakan port.

3.2.2 Cara Kerja NAT

Saat perangkat lokal mengirim paket ke internet, NAT router mengganti *source address*: `inside local` menjadi `inside global`. Saat paket balasan tiba, router menerjemahkan `inside global` kembali ke `inside local` berdasarkan tabel NAT.

3.2.3 Istilah Penting di NAT

- *Inside Local Address*: Alamat IP privat sumber.
- *Inside Global Address*: Alamat IP publik yang mewakili sumber.
- *Outside Local Address*: Alamat tujuan menurut perspektif dalam.
- *Outside Global Address*: Alamat IP publik tujuan asli.

3.3 Connection Tracking

Connection Tracking adalah fitur stateful yang mencatat status setiap koneksi (alamat, port, protokol, dan state) sehingga firewall dan NAT dapat membedakan paket sah dan tidak sah.

3.3.1 Cara Kerja Connection Tracking

Sistem mencatat tuple koneksi saat sesi dimulai, kemudian otomatis mengizinkan paket balasan berdasarkan entry tabel tanpa perlu pemeriksaan ulang pola aturan.

3.3.2 Manfaat Connection Tracking

- Meningkatkan efisiensi firewall stateful.
- Mendukung NAT dinamis dengan mapping port.
- Mengurangi beban pemrosesan pada router.
- Memungkinkan kontrol trafik lebih granular.

4 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 port forwarding (DNAT) pada router untuk menerjemahkan alamat IP publik dan port ke server lokal. Contoh pada Cisco IOS:

```
ip nat inside source static tcp 192.168.1.10 80 interface GigabitEthernet0/0 80
```

2. Menurutmu, mana yang lebih penting diterapkan terlebih dahulu di jaringan: NAT atau Firewall? Jelaskan alasanmu.
Jawaban: Firewall sebaiknya diterapkan sebelum NAT agar hanya lalu lintas yang sesuai kebijakan keamanan yang diterjemahkan alamatnya. Ini meningkatkan keamanan dengan memblokir paket berbahaya lebih awal.

3. Apa dampak negatif jika router tidak diberi filter firewall sama sekali?
Jawaban: Tanpa firewall, router menjadi pintu terbuka lebar yang memungkinkan pemindaian port, akses tidak sah, serangan DDoS, dan masuknya malware tanpa deteksi.