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

Laporan Sementara
Praktikum Jaringan Komputer

Firewall & NAT

Mohammad Rizky Ibrahim Diswarin - 5024231055

2025

1 Pendahuluan

1.1 Latar Belakang

Pertumbuhan trafik internet yang pesat, dipicu oleh semakin banyaknya pengguna layanan daring dan perangkat pintar, turut meningkatkan potensi jaringan terhadap berbagai ancaman siber. Serangan seperti peretasan, Distributed Denial of Service (DDoS), dan penyebaran malware dapat menggangu operasional jaringan serta membahayakan informasi penting.

Firewall berfungsi memeriksa setiap paket data berdasarkan aturan keamanan tertentu untuk menentukan apakah paket tersebut layak diteruskan, ditolak, atau dibuang. Dengan menerapkan pendekatan berlapis, seperti memprioritaskan pemblokiran sebelum pemberian izin, firewall mampu menyaring hanya trafik yang aman untuk keluar masuk jaringan.

Network Address Translation (NAT) bekerja dengan menerjemahkan alamat IP privat ke alamat IP publik dan sebaliknya. Proses ini memungkinkan banyak perangkat dalam jaringan lokal menggunakan satu alamat IP publik, sekaligus melindungi struktur jaringan internal. Di sisi lain, Connection Tracking mencatat status koneksi untuk memastikan hanya paket balasan yang sah yang diperbolehkan lewat, sehingga proses penyaringan menjadi lebih cerdas dan aman.

2 Dasar Teori

2.1 Firewall

Firewall merupakan mekanisme pengamanan yang mengatur arus lalu lintas data yang masuk maupun keluar dalam sebuah jaringan komputer. Fungsinya adalah menyaring dan mengendalikan akses sesuai dengan kebijakan keamanan yang telah ditentukan. Firewall dapat diimplementasikan sebagai perangkat lunak yang berjalan di dalam sistem operasi, ataupun sebagai perangkat keras mandiri. Umumnya, firewall menganalisis informasi pada header paket data—seperti alamat IP sumber dan tujuan, nomor port, serta jenis protokol—untuk memutuskan apakah paket tersebut boleh diteruskan atau harus ditolak. Berdasarkan cara kerjanya, firewall diklasifikasikan menjadi beberapa tipe, antara lain: Packet Filtering Firewall, Stateful Inspection Firewall, dan Application Layer Firewall.

2.2 Network Address Translation (NAT)

NAT bertugas menerjemahkan alamat IP antara jaringan lokal dan internet. Mekanisme ini mendukung efisiensi pemanfaatan IPv4 dan memberikan tambahan keamanan dengan menyembunyikan alamat asli perangkat internal.

Tabel 1: Jenis NAT dan Contoh Penggunaannya

Jenis	Penjelasan	Penggunaan Umum
Static NAT	Satu IP publik untuk satu IP privat	Server web di jaringan lokal
Dynamic NAT	Alamat IP publik diambil dari pool	Jaringan kantor skala menengah
PAT (Port Address Translation)	Banyak host menggunakan satu IP publik melalui port yang berbeda	Akses klien ke internet

Contoh konfigurasi PAT di Mikrotik:

```
ip firewall nat add chain=srcnat out-interface=ether1 action=masquerade comment="PAT
    ke Internet"
```

2.3 Connection Tracking

Connection Tracking mencatat informasi koneksi seperti alamat, port, protokol, dan status koneksi untuk memungkinkan firewall bertindak secara stateful. Teknologi ini membantu membedakan antara paket balasan yang sah dan paket yang mencurigakan, sehingga meningkatkan ketepatan dan keamanan proses filtrasi.

Contoh implementasi menggunakan iptables di Linux:

```
# Mengizinkan koneksi balasan
iptables -A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
# Menolak paket yang tidak valid
iptables -A INPUT -m conntrack --ctstate INVALID -j DROP
```

Tugas Pendahuluan

1. **Bagaimana cara memberikan akses ke web server internal (192.168.1.10:80) dari luar jaringan?**
   Untuk melakukan port forwarding, diperlukan konfigurasi `dst-nat` pada router:

   ```
   ip firewall nat add chain=dstnat protocol=tcp dst-port=80 action=dst-nat to-
       addresses=192.168.1.10 to-ports=80 comment="Forward HTTP ke server internal"

   ```

   Dengan aturan ini, permintaan HTTP dari internet ke IP publik router pada port 80 akan diarahkan ke server lokal 192.168.1.10.
   Disarankan menambahkan aturan firewall sebelum proses NAT untuk membatasi akses hanya dari alamat tertentu:

   ```
   ip firewall filter add chain=forward src-address=203.0.113.0/24 dst-port=80
       protocol=tcp action=accept comment="Izinkan HTTP dari subnet tepercaya"
   ip firewall filter add chain=forward dst-port=80 protocol=tcp action=drop
       comment="Blokir HTTP selain yang diizinkan"

   ```

2. **Mana yang harus diterapkan terlebih dahulu: firewall atau NAT? Jelaskan alasannya.**
   Firewall harus dijalankan sebelum NAT. Hal ini bertujuan untuk menyaring trafik yang tidak sah sejak awal, sehingga tidak membebani tabel NAT dan menghindari masuknya trafik mencurigakan. Urutan ideal adalah sebagai berikut:

   a) **Filter:** Memfilter trafik berdasarkan parameter seperti alamat, port, dan protokol.

   b) **Translate:** Melakukan NAT pada paket yang sudah lolos filter.

   c) **Route:** Mengarahkan paket ke tujuan akhir sesuai tabel routing.

Jika NAT dilakukan lebih dahulu, paket asing berbahaya bisa mengaburkan identitasnya, menyulitkan deteksi firewall dan memenuhi tabel NAT dengan data tidak valid.

3. **Apa dampaknya jika router tidak memiliki firewall? Sebutkan minimal tiga.**
   Port yang terbuka berpotensi menjadi celah bagi serangan eksploitasi, di mana pihak tidak bertanggung jawab dapat menyusup untuk memperoleh akses tidak sah atau menyebarkan malware. Hal ini bisa menyebabkan kebocoran data, dan memungkinkan penyerang dari luar jaringan (internet) untuk menjangkau serta mengendalikan perangkat-perangkat di dalam jaringan lokal.