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

Laporan Sementara
Praktikum Jaringan Komputer

Firewall & NAT

Ahmad Akmal Defatra - 5024231005

2025

1 Pendahuluan

1.1 Latar Belakang

Pertumbuhan trafik internet yang sangat cepat, didorong juga dengan blooming user layanan internet dan smart device, sekaligus meningkatkan probabilitas jaringan terhadap ancaman siber. Risiko tersebut bisa berupa peretasan, serangan DDoS, dan penyebaran malware yang dapat mengganggu layanan serta membahayakan data sensitif.

Firewall bekerja dengan memeriksa setiap paket data berdasarkan aturan keamanan, memutuskan apakah paket tersebut harus diteruskan, ditolak, atau dibuang langsung. Dengan menerapkan aturan berlapis (misalnya blokir sebelum izinkan), firewall memastikan hanya trafik tepercaya yang dapat memasuki atau meninggalkan jaringan.

Network Address Translation (NAT) menerjemahkan alamat IP privat menjadi alamat publik dan sebaliknya, memungkinkan banyak perangkat privat menggunakan satu IP publik. Selain menghemat penggunaan IPv4, NAT juga menyembunyikan topologi internal dari dunia luar. Mekanisme Connection Tracking menambah kecerdasan dengan mencatat status koneksi sehingga hanya paket balasan sah yang diizinkan, meningkatkan efisiensi dan keamanan penyaringan.

2 Dasar Teori

2.1 Firewall

Firewall adalah lapisan pertahanan pertama yang mempertahankan keamanan jaringan dengan mengawasi dan memfilter paket data berdasarkan kebijakan yang telah ditentukan. Dengan memahami beragam tipe firewall, administrator dapat memilih solusi yang tepat untuk memenuhi kebutuhan performa dan keamanan lingkungan jaringan.

Tabel 1: Jenis Firewall dan Karakteristik Utama

Tipe	Ciri Khas	Kapan Digunakan
Packet Filtering	Memeriksa header (IP, port, protokol)	Gateway sederhana
Stateful Inspection	Melacak status koneksi (TCP/UDP)	Jaringan korporat
Application Layer	Deep packet inspection, blokir serangan aplikasi	Lingkungan kritis (bank, data center)

Aturan firewall dilakukan secara berurutan: pertama aturan blokir, kemudian NAT atau pembatasan akses, dan terakhir aturan izin untuk trafik tepercaya. Sebagai contoh, pada Mikrotik perintah berikut menolak akses Telnet:

```
1 ip firewall filter add chain=forward protocol=tcp dst-port=23 action=drop comment="
    Blokir Telnet"
```

2.2 Network Address Translation (NAT)

NAT berfungsi sebagai penerjemah alamat antara jaringan privat dan publik, memungkinkan banyak host internal menggunakan satu alamat IP eksternal. Teknik ini tidak hanya menghemat ruang alamat

IPv4, tetapi juga menambah lapisan keamanan dengan menyembunyikan alamat asli host.

Tabel 2: Mode NAT dan Contoh Implementasi

Mode	Deskripsi	Kegunaan
Static NAT	Mapping satu-ke-satu IP publik	Hosting web server
Dynamic NAT	Alamat publik diambil dari pool otomatis	Jaringan menengah
PAT (Overload)	Berbagai host berbagi satu IP publik, dibedakan port	Koneksi klien ke internet

Pada Mikrotik, PAT diaktifkan dengan:

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

2.3 Connection Tracking

Connection Tracking mencatat metadata setiap koneksi (alamat, port, protokol, status) agar firewall stateful dan NAT dinamis dapat membedakan paket resp valid dari paket yang tidak diharapkan. Dengan begitu, paket unsolicited secara otomatis ditolak, meningkatkan efisiensi dan keamanan.

Contoh implementasi pada Linux menggunakan iptables:

```
# Izin balasan koneksi
iptables -A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
# Buang paket invalid
iptables -A INPUT -m conntrack --ctstate INVALID -j DROP
```

Tugas Pendahuluan

1. **Bagaimana cara membuka akses ke web server internal (192.168.1.10:80) dari luar jaringan?**

   Untuk mewujudkan port forwarding, kita perlu menambahkan aturan *dst-nat* di 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"

   ```

   Setelah aturan ini diterapkan, setiap permintaan HTTP yang masuk ke alamat publik router pada port 80 akan dialihkan ke server lokal 192.168.1.10.

   Pastikan juga menambahkan rule firewall sebelum NAT untuk membatasi akses hanya dari alamat atau jaringan tertentu, misalnya:

   ```
   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 sebaiknya diterapkan lebih dulu: firewall atau NAT? Mengapa?**
   urutannya Firewall harus diutamakan sebelum NAT untuk mengurangi beban NAT Table dan juga antisipasi menolak paket berbahaya sejak awal. Alur idealnya:

   a) **Filter** – periksa paket masuk melalui aturan firewall (alamat, port, protokol). Dengan ini paket yang tidak valid akan langsung diabaikan.
   b) **Translate** – lakukan NAT pada paket yang lolos filter untuk mengganti alamat dan port.
   c) **Route** – setelah NAT, routing dilanjutkan sesuai route tabel.

   Jika NAT diterapkan lebih dulu, paket asing yang berpotensi berbahaya bisa mengubah alamat sehingga sulit dikenali dalam filter, dan tabel NAT akan terisi entry dari trafik mencurigakan.

3. **Apa konsekuensi jika router tidak mengaktifkan firewall sama sekali? Sebutkan minimal tiga.**
   Tanpa firewall, router akan meneruskan semua paket, termasuk paket berbahaya yang bisa mengeksploitasi device user. jika Firewall dimatikan, maka beberapa dampak negatif yang mungkin terjadi adalah:

   - *Serangan DDoS* - bisa langsung menyerang server internal yang bisa menyebabkan down-time. Hal ini karena tanpa filter, semua paket bisa langsung masuk tanpa adanya proses pemilahan
   - *akses layanan berbahaya* - karena port yang rentan seperti SSH, telnet dan database dapat diakses dari internet secara langsung oleh semua orang tanpa adanya proteksi.
   - *Penyebaran malware* - dengan jaringan yang terbuka dan tanpa proteksi, sebuah jaringan tanpa firewall bisa mendapat malware yang tersebar ke seluruh jaringan yang memicu kerusakan data.
   - *Pencurian bandwidth* - tanpa firewall, semua orang bisa langsung masuk dan memanfaatkan bandwidth internet user dari jauh, misalnya botnet menggunakan jaringan untuk spam atau mining.
   - *Infiltrasi IoT* - Smart device seperti sering memiliki keamanan lemah dan bisa dijadikan pintu masuk kedalam jaringan secara langsung.

   Oleh karena itu, implementasi firewall stateful dan filter NAT sangat krusial untuk melindungi jaringan privat.