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

Laporan Sementara
Praktikum Jaringan Komputer

Firewall dan NAT

Ernita kartika Weni - 5024231013

2025

1 Pendahuluan

1.1 Latar Belakang

Seiring bertambahnya ketergantungan masyarakat terhadap infrastruktur digital, perlindungan terhadap data dan kestabilan jaringan bukan lagi menjadi kebutuhan tambahan, melainkan sebuah keharusan. Di tengah kompleksitas lalu lintas data yang terus meningkat, dibutuhkan mekanisme pengelolaan dan pengamanan jaringan yang tidak hanya tangguh, tetapi juga adaptif terhadap dinamika ancaman siber. Salah satu solusi teknis yang esensial dalam konteks ini adalah implementasi firewall dan Network Address Translation (NAT). Firewall berperan sebagai pengendali lalu lintas jaringan dengan melakukan penyaringan data berdasarkan aturan yang telah ditentukan. Fungsinya adalah untuk mencegah akses tidak sah ke dalam sistem dan melindungi jaringan dari potensi serangan dari luar. Di sisi lain, Network Address Translation (NAT) memungkinkan jaringan lokal dengan alamat IP privat untuk berkomunikasi dengan jaringan publik, seperti internet, tanpa mengekspos alamat IP internal secara langsung. Selain itu, NAT juga berperan dalam menghemat penggunaan alamat IP publik yang jumlahnya terbatas. Praktikum ini bertujuan untuk memberikan pemahaman yang aplikatif mengenai konfigurasi dan penerapan firewall serta NAT dalam sistem jaringan komputer. Melalui praktikum ini, mahasiswa diharapkan mampu memahami konsep dasar, fungsi, serta implementasi dari kedua teknologi tersebut guna mendukung perancangan sistem jaringan yang aman, efisien, dan sesuai dengan kebutuhan dunia kerja serta perkembangan teknologi saat ini.

1.2 Dasar Teori

1. Firewall

Firewall adalah sistem keamanan jaringan yang dirancang untuk mengatur dan mengontrol lalu lintas data berdasarkan aturan tertentu yang ditentukan oleh administrator. Firewall bertugas menyaring lalu lintas masuk (*inbound*) dan keluar (*outbound*) dalam jaringan komputer dengan tujuan mencegah akses yang tidak sah dan melindungi sistem dari serangan eksternal. Firewall dapat diimplementasikan secara perangkat keras (*hardware-based*), perangkat lunak (*software-based*), atau gabungan dari keduanya. Firewall bekerja dengan membuat aturan atau kebijakan (*rules*) berdasarkan parameter seperti alamat IP sumber dan tujuan, port, serta protokol yang digunakan. Beberapa jenis firewall yang umum digunakan meliputi:

- **Packet Filtering Firewall**: Menyaring lalu lintas berdasarkan header paket, seperti alamat IP dan nomor port.
- **Stateful Inspection Firewall**: Memonitor status koneksi aktif dan menentukan izin lalu lintas berdasarkan konteks koneksi.
- **Application Layer Firewall (Proxy Firewall)**: Menganalisis lalu lintas hingga ke level aplikasi dan dapat memblokir konten tertentu.
- **Next Generation Firewall (NGFW)**: Menggabungkan kemampuan inspeksi mendalam dengan fitur tambahan seperti deteksi ancaman dan kontrol aplikasi.

Implementasi pada MikroTik:

Pada MikroTik, firewall dapat diimplementasikan melalui fitur `/ip firewall filter`. Administrator

dapat membuat aturan untuk menerima, menolak, atau menjatuhkan paket berdasarkan kriteria tertentu. Contoh aturan firewall di MikroTik:

```
/ip firewall filter add chain=input protocol=tcp dst-port=22 action=drop
```

Perintah di atas akan memblokir akses SSH (port 22) ke router MikroTik, sebagai bentuk pengamanan dari luar.

2. Network Address Translation (NAT)

Network Address Translation (NAT) adalah teknik yang digunakan untuk menerjemahkan alamat IP privat menjadi alamat IP publik, atau sebaliknya, ketika paket data melewati perangkat jaringan seperti router. NAT penting digunakan dalam jaringan lokal (LAN) karena alamat IP privat tidak dapat langsung digunakan di internet. Dengan NAT, banyak perangkat di jaringan lokal dapat mengakses internet menggunakan satu alamat IP publik.

Jenis-jenis NAT yang umum digunakan, yaitu:

- **Static NAT**: Satu alamat IP privat dipetakan ke satu alamat IP publik secara permanen.
- **Dynamic NAT**: Alamat IP privat dipetakan ke salah satu dari kumpulan alamat IP publik yang tersedia secara dinamis.
- **Port Address Translation (PAT) / NAT Overload**: Banyak alamat IP privat dipetakan ke satu alamat IP publik dengan membedakan nomor port.

Implementasi pada MikroTik:

MikroTik menyediakan fitur NAT melalui menu `/ip firewall nat`. Salah satu implementasi yang paling umum adalah mengatur NAT agar klien lokal dapat mengakses internet menggunakan IP publik router MikroTik:

```
/ip firewall nat add chain=srcnat out-interface=ether1 action=masquerade
```

Perintah di atas mengaktifkan teknik *masquerading* yang merupakan bentuk dari NAT Overload. NAT ini secara otomatis menerjemahkan alamat IP privat ke alamat IP publik yang melekat pada antarmuka keluar (misalnya, ether1 sebagai koneksi internet).

3. Hubungan Firewall dan NAT dalam Keamanan Jaringan

Firewall dan NAT bekerja secara sinergis dalam infrastruktur jaringan modern. Firewall berperan sebagai pelindung yang menyaring lalu lintas data sesuai dengan kebijakan keamanan, sementara NAT menjembatani komunikasi antara jaringan privat dan publik dengan tetap menjaga kerahasiaan struktur jaringan internal. Pada perangkat seperti MikroTik, kedua fitur ini dapat dikonfigurasi secara bersamaan untuk membangun sistem jaringan yang aman, efisien, dan terkendali.Dengan memanfaatkan firewall dan NAT secara optimal, administrator jaringan dapat melindungi aset digital organisasi sekaligus memastikan kelancaran konektivitas antarjaringan, baik dalam skala kecil (rumah/kantor) maupun besar (korporat/ISP).

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?**

   Untuk mengakses web server lokal dari jaringan luar, perlu dibuat konfigurasi *Destination NAT (dst-nat)* pada router. Konfigurasi ini mengarahkan permintaan dari IP publik ke IP privat internal. Contoh konfigurasi pada MikroTik adalah sebagai berikut:

   ```
   /ip firewall nat add chain=dstnat dst-address=<IP_Publik> \
   protocol=tcp dst-port=80 action=dst-nat \
   to-addresses=192.168.1.10 to-ports=80
   ```

   Penjelasan:

   - `dst-address` adalah alamat IP publik router yang dapat diakses dari luar.
   - `protocol=tcp dst-port=80` digunakan karena layanan HTTP menggunakan port 80.
   - `to-addresses=192.168.1.10` adalah IP lokal dari server web.
   - `to-ports=80` meneruskan ke port HTTP pada server tersebut.

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

   Firewall sebaiknya diterapkan terlebih dahulu karena fungsinya sebagai lapisan pertahanan utama terhadap akses yang tidak sah. Firewall memungkinkan administrator untuk menyaring lalu lintas masuk dan keluar berdasarkan aturan tertentu. Dengan demikian, ancaman dari luar dapat diblokir sebelum mencapai sistem internal. Jika NAT diterapkan lebih dulu tanpa perlindungan firewall, maka lalu lintas yang diarahkan ke jaringan lokal tidak disaring dan berpotensi membahayakan perangkat internal.

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

   Tanpa filter firewall, router tidak dapat menyaring lalu lintas data secara selektif, sehingga semua jenis lalu lintas dapat masuk tanpa kontrol. Hal ini dapat menyebabkan:

   - Terbukanya celah keamanan yang memungkinkan serangan dari luar seperti *DDoS*, *brute-force login*, dan *port scanning*.
   - Perangkat internal menjadi target langsung serangan.
   - Penggunaan bandwidth yang tidak efisien akibat lalu lintas tidak penting.
   - Overload pada CPU router karena harus memproses semua lalu lintas masuk tanpa penyaringan.

Referensi:

- MikroTik Wiki - *NAT*: `https://wiki.mikrotik.com/wiki/Manual:IP/Firewall/NAT`
- MikroTik Wiki - *Firewall Filter*: `https://wiki.mikrotik.com/wiki/Manual:IP/Firewall/Filter`
- Kurose, J. F., & Ross, K. W. (2017). *Computer Networking: A Top-Down Approach* (7th ed.).
- Cisco. (2020). *Network Security Concepts and Policies* – Cisco Press.