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

Laporan Sementara
Praktikum Jaringan Komputer

Firewall dan NAT

Bintang Arya Mahendra - 5024231058

2025

1 Pendahuluan

1.1 Latar Belakang

Dengan semakin luasnya penggunaan jaringan komputer dan internet, keamanan dan efisiensi pengelolaan lalu lintas data menjadi hal yang sangat penting. Firewall berperan sebagai pelindung jaringan dengan menyaring akses berdasarkan aturan tertentu, sementara NAT memungkinkan banyak perangkat lokal berbagi satu IP publik. Untuk mendukung keduanya, fitur Connection Tracking digunakan agar router dapat mengenali status setiap koneksi yang terjadi. Praktikum modul 4 ini bertujuan untuk memahami konsep dan konfigurasi dasar dari ketiga fitur tersebut dalam pengelolaan jaringan.

1.2 Dasar Teori

Firewall adalah sistem keamanan jaringan yang mengatur lalu lintas data masuk dan keluar berdasarkan aturan tertentu. Ia berfungsi seperti penjaga gerbang digital, memutuskan apakah data diizinkan lewat, ditolak, atau dibuang. Firewall membantu melindungi jaringan dari akses tidak sah seperti malware atau hacker. Sebelum firewall, keamanan jaringan mengandalkan Access Control List (ACL), namun ACL hanya memfilter berdasarkan alamat dan port tanpa melihat konteks koneksi. Kini, firewall hadir dengan berbagai jenis, seperti Packet Filtering, Stateful Inspection, Application Layer Firewall, Next Generation Firewall (NGFW), Circuit Level Gateway, software firewall, hardware firewall, hingga cloud firewall. Masing-masing jenis memiliki keunggulan dalam cara kerja dan kedalaman analisis terhadap paket data.

Firewall bekerja berdasarkan aturan yang ditentukan oleh administrator. Setiap data diperiksa, lalu diputuskan apakah akan diterima (accept), ditolak dengan pemberitahuan (reject), atau dibuang tanpa balasan (drop). Sementara itu, Network Address Translation (NAT) memungkinkan banyak perangkat di jaringan lokal mengakses internet menggunakan satu IP publik. NAT sangat penting karena jumlah IP publik terbatas, sedangkan jumlah perangkat terus bertambah. NAT bekerja dengan mengganti IP privat dan port lokal dengan IP publik dan port baru saat perangkat mengakses internet, lalu mencocokkannya saat data kembali.

Jenis NAT meliputi Static NAT (satu IP lokal ke satu IP publik), Dynamic NAT (penggantian dari pool IP publik), dan Port Address Translation (PAT) yang paling efisien karena membedakan koneksi berdasarkan port. Dalam NAT dikenal istilah seperti Inside Local Address, Inside Global Address, Outside Local Address, dan Outside Global Address yang menggambarkan asal dan tujuan alamat sebelum dan sesudah translasi.

Connection Tracking adalah fitur yang mencatat status koneksi jaringan secara dinamis, termasuk IP, port, protokol, dan status koneksi (baru, aktif, atau tidak valid). Fitur ini membantu firewall dan NAT dalam mengenali koneksi yang sah, mengurangi beban kerja router, dan meningkatkan keamanan jaringan. Dengan Connection Tracking, paket yang merupakan bagian dari koneksi aktif akan langsung diizinkan tanpa pemeriksaan berulang, sedangkan koneksi asing dapat langsung ditolak.

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, diperlukan konfigurasi *Destination NAT* (DNAT) atau *port forwarding*, yaitu dengan mengarahkan permintaan dari IP publik ke alamat IP lokal tertentu dalam jaringan internal. Dalam kasus ini, lalu lintas yang datang ke IP publik pada port 80 harus diteruskan ke IP 192.168.1.10 port 80. Konfigurasi pada router dapat dilakukan dengan menentukan `chain=dstnat`, `protocol=tcp`, `dst-port=80`, lalu menetapkan `action=dst-nat` ke `to-address=192.168.1.10` dan `to-port=80`. Konfigurasi ini memungkinkan akses dari luar ke server web lokal dengan aman dan terkendali.
   Referensi: MikroTik Documentation: NAT Configuration. *https://help.mikrotik.com/docs/display/ROS/NAT*

2. **Menurutmu, mana yang lebih penting diterapkan terlebih dahulu di jaringan: NAT atau Firewall? Jelaskan alasanmu.**
   Firewall lebih penting untuk diterapkan terlebih dahulu karena fungsinya sebagai garis pertahanan pertama dalam menjaga keamanan jaringan. Firewall dapat memfilter dan mengendalikan lalu lintas berdasarkan aturan yang ditetapkan, sehingga dapat mencegah akses tidak sah dan potensi serangan dari luar sebelum data diteruskan ke dalam jaringan. Sementara itu, NAT lebih berperan dalam pengalamatan dan penerjemahan paket. Tanpa firewall, NAT dapat membuka akses langsung ke jaringan internal tanpa perlindungan.
   Referensi: Odom, W. (2020). *CCNA 200-301 Official Cert Guide, Volume 1*. Cisco Press.

3. **Apa dampak negatif jika router tidak diberi filter firewall sama sekali?**
   Jika router tidak diberi filter firewall sama sekali, maka semua lalu lintas data akan diteruskan tanpa pemeriksaan atau pembatasan. Hal ini sangat berisiko karena dapat menyebabkan:

   - Akses tidak sah ke perangkat internal.
   - Meningkatnya kemungkinan serangan malware dan eksploitasi celah keamanan.
   - Kebocoran data penting akibat kurangnya kontrol lalu lintas.
   - Terjadinya gangguan layanan karena serangan seperti DDoS.

   Oleh karena itu, firewall diperlukan untuk memfilter paket yang masuk dan keluar guna menjaga stabilitas dan keamanan sistem jaringan.
   Referensi: Stallings, W. (2020). *Network Security Essentials: Applications and Standards* (6th ed.). Pearson.