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

Laporan Sementara
Praktikum Jaringan Komputer

Firewall & NAT

Joycelyn Emmanuella Passandaran - 5024231001

2025

1 Pendahuluan

1.1 Latar Belakang

Seiring dengan meningkatnya penggunaan jaringan komputer dan keterhubungan antar perangkat melalui internet, kebutuhan akan sistem keamanan jaringan yang baik menjadi semakin penting. Lalu lintas data yang terbuka tanpa pengamanan dapat menjadi celah bagi berbagai ancaman seperti akses tidak sah, serangan siber, dan penyalahgunaan sumber daya jaringan. Oleh karena itu, penerapan firewall dan Network Address Translation (NAT) menjadi salah satu langkah utama dalam menjaga keamanan dan kestabilan jaringan. Firewall berperan dalam mengatur lalu lintas berdasarkan aturan yang ditentukan, sedangkan NAT memungkinkan banyak perangkat dalam jaringan lokal mengakses internet melalui satu alamat IP publik. Melalui praktikum ini, praktikan diharapkan dapat memahami fungsi serta cara kerja firewall dan NAT dalam pengelolaan dan perlindungan jaringan. Selain itu, praktikan juga akan mengenal konsep connection tracking sebagai pendukung utama dalam filtering dan translasi alamat IP. Dengan melakukan praktikum ini, praktikan diharapkan mampu mengimplementasikan konfigurasi dasar firewall dan NAT serta memahami perannya dalam membatasi akses dan menjaga keamanan jaringan dari ancaman eksternal.

1.2 Dasar Teori

Firewall merupakan sistem keamanan jaringan yang berfungsi mengatur dan mengontrol lalu lintas data yang masuk maupun keluar dari suatu jaringan berdasarkan aturan yang ditentukan. Firewall dapat melakukan tiga aksi utama terhadap paket data: menerima (accept), menolak dengan balasan error (reject), atau membuang tanpa respon (drop). Awalnya, keamanan jaringan hanya mengandalkan Access Control List (ACL) yang terbatas karena tidak dapat mengevaluasi konteks komunikasi. Terdapat beberapa jenis firewall seperti packet filtering yang menyaring berdasarkan IP dan port, stateful inspection yang dapat mengenali status koneksi, serta application layer firewall yang mampu menganalisis lalu lintas hingga ke level aplikasi. Selain itu, terdapat Next Generation Firewall (NGFW) yang mendukung inspeksi lebih dalam termasuk trafik terenkripsi.

Network Address Translation (NAT) adalah metode yang digunakan untuk menerjemahkan alamat IP privat ke alamat IP publik, sehingga memungkinkan banyak perangkat dalam satu jaringan lokal untuk mengakses internet menggunakan satu alamat IP publik. NAT sangat penting mengingat terbatasnya jumlah alamat IPv4. Jenis NAT yang umum digunakan meliputi static NAT (satu IP lokal ke satu IP publik), dynamic NAT (mengambil IP publik dari pool), dan Port Address Translation (PAT) atau masquerade, yang mengizinkan banyak perangkat menggunakan satu IP publik dengan membedakan berdasarkan port koneksi. Proses NAT dicatat dalam tabel NAT yang berisi informasi koneksi agar sistem dapat meneruskan data masuk ke perangkat yang benar.

Connection Tracking adalah fitur yang mencatat status koneksi jaringan secara real time. Informasi yang disimpan mencakup alamat IP sumber dan tujuan, port, protokol, serta status koneksi. Fitur ini penting dalam pengambilan keputusan firewall dan proses NAT, karena memungkinkan sistem mengenali apakah suatu paket merupakan bagian dari koneksi aktif, koneksi baru, atau koneksi tidak sah. Dengan connection tracking, router dapat mengizinkan trafik yang sah dan menolak trafik yang mencurigakan tanpa perlu memproses ulang setiap paket dari awal. Dalam konteks perlindungan router dari akses luar, pengaturan firewall dan NAT perlu dikonfigurasi untuk memblokir semua koneksi yang tidak dibutuhkan dari luar, hanya membuka port yang diperlukan, serta memanfaatkan fitur

connection tracking untuk mencegah akses tidak sah dan potensi serangan dari jaringan eksternal.

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 memungkinkan akses dari jaringan luar ke web server lokal dengan IP 192.168.1.10, jenis NAT yang digunakan adalah Static NAT. Static NAT menetapkan hubungan tetap antara alamat IP privat dan alamat IP publik, sehingga perangkat dari luar dapat selalu mengakses server menggunakan IP publik tersebut. Dalam konfigurasinya, interface yang mengarah ke jaringan internal diatur sebagai IP NAT inside, sedangkan interface yang terhubung ke internet ditetapkan sebagai IP NAT outside. Selanjutnya, pemetaan IP dilakukan menggunakan perintah IP NAT inside source static, yang secara eksplisit menghubungkan IP internal server dengan IP publik yang tersedia.
   Refrensi:
   Soetam Rizky Wicaksono dan Ronald Dwi Nompunu (2013) *Konfigurasi NAT (Network Address Translation) untuk Laboratorium Majemuk di Lingkup Perguruan Tinggi*. Program Studi Sistem Informasi, Universitas Ma Chung, Oktober 2013.
   Link Refrensi

2. Menurutmu, mana yang lebih penting diterapkan terlebih dahulu di jaringan: NAT atau Firewall? Jelaskan alasanmu.
   Firewall lebih penting untuk diterapkan terlebih dahulu di jaringan karena fungsinya sebagai garis pertahanan utama yang mengatur dan mengontrol akses masuk dan keluar dari jaringan. Firewall dapat melindungi jaringan dari ancaman eksternal dengan memfilter lalu lintas berdasarkan aturan keamanan, sehingga mencegah serangan dan akses tidak sah sejak awal. Sedangkan NAT lebih berfokus pada pengelolaan alamat IP dan memungkinkan banyak perangkat berbagi satu IP publik, yang penting untuk konektivitas, tetapi tidak secara langsung melindungi jaringan dari ancaman.
   Refrensi:
   Riadi, I. (2011) *Optimalisasi Keamanan Jaringan Menggunakan Pemfilteran Aplikasi Berbasis Mikrotik*. Program Studi Sistem Informasi, Universitas Ahmad Dahlan, Februari 2011.
   Link Refrensi

3. Apa dampak negatif jika router tidak diberi filter firewall sama sekali?
   Jika router tidak dilengkapi dengan filter firewall, jaringan akan sangat rentan terhadap berbagai ancaman dari luar. Tanpa firewall, tidak ada pengaturan yang membatasi atau memeriksa lalu lintas data yang masuk dan keluar, sehingga perangkat di dalam jaringan bisa dengan mudah diakses oleh pihak yang tidak berwenang. Hal ini membuka peluang bagi serangan seperti pencurian data, penyebaran virus atau malware, hingga serangan denial-of-service yang bisa membuat layanan jaringan terganggu atau bahkan mati total. Selain itu, tanpa perlindungan firewall, risiko eksploitasi celah keamanan meningkat, yang dapat menyebabkan kerusakan sistem dan hilangnya data penting.
   Refrensi:
   Aprilianto, D., Fadila, T. and Muslim, M.A. (2017) *Sistem Pencegahan UDP DNS Flood dengan*

Filter Firewall pada Router Mikrotik. Jurusan Ilmu Komputer, FMIPA, Universitas Negeri Semarang, Mei 2017.

Link Refrensi