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

Laporan Sementara
Praktikum Jaringan Komputer

Firewall dan NAT

Salman Al Ghifary - 5024221003

2025

1 Pendahuluan

1.1 Latar Belakang

Seiring meningkatnya penggunaan jaringan komputer dan internet, kebutuhan akan sistem keamanan jaringan menjadi semakin penting. Serangan siber seperti peretasan dan malware dapat mengganggu bahkan merusak sistem, sehingga perlindungan terhadap jaringan harus diperkuat.Salah satu teknologi utama untuk menjaga keamanan jaringan adalah firewall, yang berfungsi menyaring dan mengontrol lalu lintas data berdasarkan aturan tertentu. Selain itu, keterbatasan alamat IP publik diatasi dengan Network Address Translation (NAT), yang memungkinkan banyak perangkat dalam jaringan lokal mengakses internet menggunakan satu IP publik. Untuk mendukung kedua teknologi ini, digunakan Connection Tracking, yaitu sistem yang memantau status setiap koneksi agar firewall dan NAT dapat bekerja lebih efisien dan aman. Praktikum ini bertujuan untuk memberikan pemahaman mengenai fungsi dan implementasi firewall, NAT, dan connection tracking sebagai dasar penting dalam keamanan jaringan modern.

1.2 Dasar Teori

Dalam dunia jaringan komputer yang semakin kompleks, Firewall, Network Address Translation (NAT), dan Connection Tracking adalah tiga pilar utama yang bekerja sama untuk memastikan keamanan, efisiensi, dan kelancaran komunikasi.

Bayangkan Firewall sebagai penjaga gerbang digital untuk jaringan Anda. Mirip satpam yang teliti, ia mengawasi setiap data yang mencoba masuk atau keluar, memastikan hanya lalu lintas yang sah dan aman yang diperbolehkan lewat. Sebelum adanya firewall, jaringan sangat rentan karena hanya mengandalkan daftar kontrol akses yang kurang canggih. Berbagai jenis firewall, dari yang sederhana memeriksa paket data hingga Next Generation Firewall (NGFW) yang mampu menganalisis konten terenkripsi, kini menjadi garis pertahanan pertama. Entah itu perangkat lunak yang terinstal di komputer atau perangkat keras khusus di pintu gerbang jaringan, firewall beroperasi berdasarkan serangkaian aturan ketat: data bisa diizinkan masuk, ditolak dengan pemberitahuan, atau bahkan diblokir tanpa jejak sama sekali, semua disesuaikan dengan kebijakan keamanan organisasi.

Sementara itu, Network Address Translation (NAT) adalah solusi cerdas untuk mengatasi keterbatasan alamat IP publik di internet. Daripada setiap perangkat di rumah atau kantor memerlukan alamat IP publiknya sendiri (yang jumlahnya sangat terbatas), NAT memungkinkan banyak perangkat berbagi satu alamat IP publik tunggal. Ini seperti banyak penghuni yang berbagi satu alamat rumah saat mengirim surat ke luar. Jenis NAT bervariasi, namun yang paling umum adalah Port Address Translation (PAT), yang memungkinkan ribuan perangkat lokal untuk mengakses internet melalui satu IP publik dengan membedakan setiap koneksi berdasarkan nomor port. Proses ini umumnya terjadi di router yang secara dinamis mengubah alamat IP lokal menjadi IP publik saat data keluar, dan sebaliknya saat data masuk, semua tercatat rapi dalam "tabel NAT".

Terakhir, Connection Tracking adalah fitur pengawas yang cerdas dan teliti. Ini seperti seorang resepsionis yang mencatat setiap detail percakapan atau "koneksi" yang sedang berlangsung—siapa bicara dengan siapa, kapan dimulai, dan lewat jalur mana. Ketika sebuah perangkat memulai komunikasi, connection tracking mencatatnya. Jadi, ketika balasan datang, sistem sudah tahu bahwa itu adalah bagian dari percakapan yang sah dan langsung mengizinkannya lewat, tanpa perlu pemeriksaan ulang yang memakan waktu. Ini sangat penting karena memungkinkan firewall untuk berfungsi

lebih cerdas (dikenal sebagai stateful firewall), membantu NAT mengelola banyak koneksi secara efisien, mengurangi beban kerja router, dan secara keseluruhan meningkatkan keamanan dengan cepat mengidentifikasi dan memblokir lalu lintas yang mencurigakan atau tidak sah.
Singkatnya, Firewall menjaga perbatasan jaringan, NAT memungkinkan banyak perangkat berbagi identitas di internet, dan Connection Tracking melacak setiap percakapan untuk memastikan semua berjalan lancar dan aman. Ketiganya bersinergi menciptakan lingkungan jaringan yang terlindungi dan efisien di era digital saat ini.

2 Tugas Pendahuluan

2.1. 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 (IP: 192.168.1.10, port 80) dari internet, Anda perlu mengonfigurasi Port Forwarding pada router Anda. Ini akan mengarahkan permintaan dari **IP publik router Anda di port 80 (misalnya, 203.0.113.5:80) langsung ke IP dan port web server internal Anda (192.168.1.10:80).

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

Firewall harus diprioritasin Alasannya, NAT memfasilitasi konektivitas (membuka jalur), sementara Firewall bertugas melindungi dan mengontrol jalur tersebut. Membuka jalur tanpa pengamanan firewall akan membuat jaringan sangat rentan terhadap serangan dari internet. Keamanan harus menjadi prioritas utama.

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

Jika router tidak memiliki filter firewall sama sekali, jaringan akan terekspos penuh pada ancaman eksternal. Ini berarti risiko sangat tinggi terhadap serangan siber (peretasan, malware, DDoS), pencurian data, kompromi sistem (dijadikan botnet), penurunan kinerja jaringan, dan pelanggaran privasi.