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

Laporan Sementara
Praktikum Jaringan Komputer

Firewall & NAT

Ferdie Ewaldo Djohan - 5024231017

2025

1 Pendahuluan

1.1 Latar Belakang

Perkembangan teknologi informasi dan komunikasi yang pesat telah membuat internet menjadi kebutuhan pokok bagi organisasi dan individu di seluruh dunia. Namun, ketergantungan yang tinggi terhadap internet juga membuka celah keamanan yang signifikan bagi jaringan komputer. Sebelum teknologi firewall berkembang, keamanan jaringan hanya mengandalkan Access Control List (ACL) yang memiliki keterbatasan dalam membedakan isi dari data yang melewati jaringan. Kondisi ini menciptakan banyak celah keamanan yang dapat dimanfaatkan oleh pihak-pihak yang tidak bertanggung jawab untuk melakukan serangan terhadap infrastruktur jaringan. Di sisi lain, pertumbuhan pesat jumlah perangkat yang terhubung ke internet menimbulkan masalah lain yang tidak kalah penting, yaitu keterbatasan alamat IPv4. Dengan hanya tersedia sekitar 4,3 miliar alamat IPv4 di seluruh dunia, sementara jumlah perangkat yang membutuhkan akses internet terus bertambah secara eksponensial, diperlukan solusi yang dapat mengoptimalkan penggunaan alamat IP publik yang terbatas tersebut. Tanpa adanya mekanisme yang tepat, krisis alamat IP akan menghambat perkembangan internet dan akses digital bagi masyarakat luas.

1.2 Dasar Teori

Firewall merupakan sistem keamanan jaringan yang berfungsi sebagai penjaga digital atau "satpam" bagi jaringan komputer. Firewall beroperasi dengan memonitor dan mengontrol lalu lintas data yang masuk dan keluar dari jaringan berdasarkan aturan keamanan yang telah ditetapkan sebelumnya. Setiap paket data yang melewati firewall akan diperiksa dan dievaluasi, kemudian firewall akan memutuskan apakah paket tersebut boleh diteruskan (accept), ditolak dengan pesan error (reject), atau langsung diabaikan tanpa respon (drop). Teknologi firewall telah berkembang dari yang sederhana seperti packet filtering hingga teknologi canggih seperti Next Generation Firewall (NGFW) yang mampu melakukan deep packet inspection dan analisis konten aplikasi. Network Address Translation (NAT) adalah teknologi yang memungkinkan multiple perangkat dalam jaringan lokal untuk mengakses internet menggunakan satu alamat IP publik. NAT bekerja dengan cara menerjemahkan alamat IP privat dari perangkat internal menjadi alamat IP publik ketika berkomunikasi dengan internet, dan sebaliknya ketika menerima respon dari server eksternal. Teknologi ini tidak hanya mengatasi masalah keterbatasan alamat IPv4, tetapi juga memberikan lapisan keamanan tambahan dengan menyembunyikan struktur jaringan internal dari dunia luar. Terdapat beberapa jenis NAT, mulai dari Static NAT yang melakukan pemetaan satu-ke-satu, Dynamic NAT yang menggunakan pool alamat IP, hingga Port Address Translation (PAT) yang paling efisien karena dapat melayani banyak perangkat dengan satu IP publik melalui pembedaan nomor port. Connection Tracking merupakan fitur pelacakan koneksi yang berfungsi sebagai "resepsionis jaringan" intelligent yang mencatat semua informasi penting dari setiap koneksi yang melewati sistem. Teknologi ini menyimpan data seperti alamat sumber dan tujuan, nomor port, protokol yang digunakan, serta status koneksi untuk memungkinkan router atau firewall mengenali apakah suatu paket data merupakan bagian dari koneksi yang sah atau tidak. Connection tracking memberikan foundation bagi operasi stateful firewall dan NAT, serta meningkatkan efisiensi dan keamanan jaringan dengan memungkinkan sistem untuk membedakan antara koneksi yang legitimate dan traffic yang mencurigakan. Ketiga teknologi ini saling berkaitan dan bekerja secara sinergis dalam infrastruktur jaringan modern. Firewall menyediakan perlindungan keamanan, NAT

mengatasi keterbatasan alamat IP sambil memberikan keamanan tambahan, sementara connection tracking memungkinkan kedua teknologi tersebut bekerja secara stateful dan efisien. Pemahaman yang mendalam tentang ketiga teknologi ini sangat penting bagi administrator jaringan untuk dapat merancang, mengimplementasikan, dan mengelola infrastruktur jaringan yang aman, efisien, dan scalable.

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 lokal dari jaringan luar, perlu dilakukan port mapping atau port forwarding pada router NAT. Saat seseorang dari internet mengakses IP publik pada port 80, router akan meneruskan traffic tersebut ke server web internal di 192.168.1.10. Port forwarding pada dasarnya adalah jenis khusus dari NAT atau address translation yang digunakan untuk tujuan spesifik yaitu mempublikasikan server internal ke internet publik. Rule NAT setiap kali seseorang mencoba terhubung pada TCP port 80 dengan alamat IP tujuan public router, maka akan diteruskan ke 192.168.1.1 (IP internal server). (https://www.homenethowto.com/ports-and-nat/port-forward/) (https://networklessons.com/cisco/ccie-routing-switching/cisco-ios-nat-port-forwarding)

2. Menurutmu, mana yang lebih penting diterapkan terlebih dahulu di jaringan: NAT atau Firewall? Jelaskan alasanmu.
   Menurut saya firewall lebih penting diterapkan terlebih dahulu dibandingkan NAT. Hal ini dikarenakan firewall merupakan dasar dari keamanan perangkat dan merupakan pertahanan utama. Firewall bertindak sebagai gatekeeper, sedangkan NAT bertindak sebagai translator. Firewall memeriksa header paket dari traffic yang masuk dan menolak yang tidak diinginkan atau berbahaya. (https://www.itsasap.com/blog/3-top-risks-of-not-having-a-firewall) (https://www.onsip.com/voip-resources/voip-fundamentals/what-are-nat-and-firewall-traversals) (https://security.stackexchange.com/que
   important-is-nat-as-a-security-layer)

3. Apa dampak negatif jika router tidak diberi filter firewall sama sekali?
   Tidak memiliki firewall saam saja dengan tidak memiliki keamanan, hacker atau cyber criminal dapat mengakses dan menyusup ke jaringan. Semua perangkat di jaringan yang saam dapat diserang atau diakses datanya seperti pin rekening dan lain lain.(https://www.itsasap.com/blog/3-top-risks-of-not-having-a-firewall) (https://www.comparitech.com/blog/information-security/what-is-a-router-firewall/)