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

Laporan Sementara
Praktikum Jaringan Komputer

Firewall NAT

Andrew Marlin - 5024231020

2025

1 Pendahuluan

1.1 Latar Belakang

Dalam era digital saat ini, keamanan jaringan komputer menjadi aspek krusial bagi organisasi maupun individu. Ancaman siber seperti peretasan, malware, dan serangan Distributed Denial of Service (DDoS) terus berkembang baik dari segi kuantitas maupun kompleksitas. Oleh karena itu, diperlukan mekanisme pertahanan yang kuat untuk melindungi aset informasi dan infrastruktur jaringan.

Firewall berperan sebagai garda terdepan dalam sistem keamanan jaringan. Fungsinya adalah untuk memonitor dan mengontrol lalu lintas data yang masuk dan keluar dari jaringan berdasarkan seperangkat aturan keamanan yang telah ditentukan. Dengan adanya firewall, akses yang tidak sah atau berpotensi berbahaya dapat dicegah, sehingga integritas, kerahasiaan, dan ketersediaan data dalam jaringan dapat terjaga.

Di sisi lain, Network Address Translation (NAT) adalah teknologi yang memungkinkan beberapa perangkat dalam jaringan lokal (LAN) untuk berbagi satu alamat IP publik ketika terhubung ke internet. Selain menghemat penggunaan alamat IP publik yang terbatas, NAT juga memberikan lapisan keamanan tambahan dengan menyembunyikan alamat IP internal perangkat di belakang alamat IP publik tunggal. Hal ini mempersulit pihak luar untuk secara langsung mengidentifikasi dan menargetkan perangkat individual di dalam jaringan lokal.

Praktikum mengenai Firewall dan NAT dirancang untuk memberikan mahasiswa atau peserta pelatihan pemahaman mendalam mengenai:

- Konsep dasar Firewall: Jenis-jenis firewall (misalnya, packet filtering, stateful inspection, proxy), cara kerja, dan arsitekturnya.
- Konsep dasar Firewall: Jenis-jenis firewall (misalnya, packet filtering, stateful inspection, proxy), cara kerja, dan arsitekturnya.
- Konfigurasi Firewall: Membuat dan menerapkan aturan-aturan firewall (rules/policies) untuk mengizinkan atau memblokir lalu lintas berdasarkan berbagai parameter seperti alamat IP sumber/tujuan, port, dan protokol.
- Konsep dasar NAT: Jenis-jenis NAT (Static NAT, Dynamic NAT, Port Address Translation/PAT), cara kerja, dan manfaatnya.
- Konfigurasi NAT: Mengimplementasikan berbagai skenario NAT untuk memungkinkan konektivitas internet bagi jaringan lokal dan mempublikasikan layanan internal ke jaringan eksternal.
- Pengujian dan Verifikasi: Melakukan pengujian untuk memastikan firewall dan NAT berfungsi sesuai dengan konfigurasi yang diterapkan dan mampu menangani skenario lalu lintas jaringan yang berbeda.

Melalui praktikum ini, peserta diharapkan mampu mengaplikasikan pengetahuan teoritis ke dalam skenario praktis, mengembangkan keterampilan teknis dalam mengkonfigurasi perangkat jaringan, serta memahami pentingnya firewall dan NAT dalam membangun infrastruktur jaringan yang aman dan efisien.

1.2 Dasar Teori

Firewall bertindak sebagai benteng pertahanan pertama yang mengontrol lalu lintas data yang masuk dan keluar dari sebuah jaringan. Prinsip kerjanya adalah dengan melakukan inspeksi terhadap setiap paket data dan memutuskan apakah paket tersebut diizinkan lewat atau harus diblokir, berdasarkan serangkaian aturan keamanan yang telah dikonfigurasi sebelumnya. Aturan ini bisa didasarkan pada berbagai kriteria, seperti alamat IP sumber dan tujuan, nomor port, serta protokol yang digunakan. Dengan kemampuannya menyaring lalu lintas, firewall secara efektif mencegah upaya peretasan, membatasi penyebaran ancaman dari dalam jaringan, dan memastikan bahwa hanya komunikasi yang sah yang dapat terjadi, sehingga menjaga integritas dan kerahasiaan data.

Sementara itu, Network Address Translation (NAT) adalah sebuah mekanisme yang memungkinkan banyak perangkat dalam jaringan lokal (LAN) yang menggunakan alamat IP privat untuk berbagi satu atau beberapa alamat IP publik ketika berkomunikasi dengan jaringan eksternal seperti internet. Fungsi utama NAT adalah untuk mengatasi keterbatasan jumlah alamat IPv4 publik. Namun, NAT juga memberikan lapisan keamanan tambahan secara implisit dengan menyembunyikan struktur alamat IP internal jaringan. Ketika perangkat dari jaringan internal mengirimkan data ke internet, NAT akan mengganti alamat IP privat sumber dengan alamat IP publik router atau gateway. Sebaliknya, ketika ada balasan dari internet, NAT akan menerjemahkannya kembali ke alamat IP privat yang sesuai di dalam jaringan lokal. Hal ini membuat perangkat di dalam jaringan lokal tidak secara langsung terekspos ke internet, sehingga lebih sulit bagi pihak luar untuk melakukan pemindaian atau serangan langsung.

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 ke web server lokal Anda yang memiliki alamat IP 192.168.1.10 dan berjalan pada port 80 dari jaringan luar atau internet, Anda perlu mengonfigurasi sebuah mekanisme NAT yang dikenal sebagai Port Forwarding atau Destination NAT (DNAT) pada router Anda. Konfigurasi ini bekerja dengan cara memetakan sebuah port tertentu pada alamat IP publik router Anda ke alamat IP dan port spesifik dari server web internal. Ketika permintaan dari internet tiba di alamat IP publik router pada port yang telah ditentukan (misalnya, port 80 publik atau port lain seperti 8080), router akan meneruskan lalu lintas tersebut ke alamat IP internal 192.168.1.10 pada port 80 menggunakan protokol TCP, yang merupakan protokol standar untuk trafik web HTTP. Router secara otomatis akan menangani translasi alamat sumber dan tujuan sehingga komunikasi dua arah antara klien di internet dan server web lokal dapat terjalin seolah-olah mereka terhubung langsung, padahal server internal tetap aman di belakang NAT.

2. Menurutmu, mana yang lebih penting diterapkan terlebih dahulu di jaringan: NAT atau Firewall? Jelaskan alasanmu.
   Dalam perdebatan mengenai mana yang lebih krusial untuk diimplementasikan terlebih dahulu antara NAT dan Firewall, Firewall secara umum dianggap memiliki prioritas yang lebih tinggi. Alasan utamanya adalah karena firewall menyediakan lapisan keamanan fundamental dengan bertindak sebagai penghalang pertama yang mengontrol semua lalu lintas data yang masuk dan keluar jaringan berdasarkan aturan yang telah ditentukan, sehingga secara aktif mencegah

akses tidak sah dan berbagai ancaman siber sejak awal. Meskipun NAT menawarkan keuntungan sekunder berupa penyembunyian topologi IP internal yang dapat mempersulit pengintaian langsung dari luar, fungsi utamanya adalah konservasi alamat IP dan memfasilitasi konektivitas. Mengandalkan NAT sebagai satu-satunya benteng pertahanan sangatlah tidak disarankan, karena layanan yang sengaja diekspos melalui port forwarding tetap rentan tanpa adanya inspeksi dan penyaringan dari firewall. Oleh karena itu, membangun perimeter keamanan dasar dengan firewall adalah langkah awal yang lebih esensial, baru kemudian diikuti dengan konfigurasi NAT untuk kebutuhan konektivitas dan manajemen alamat, dengan firewall tetap menjaga integritas keamanan jaringan.

3. Apa dampak negatif jika router tidak diberi filter firewall sama sekali?
   Jika sebuah router yang terhubung ke internet dioperasikan tanpa filter firewall sama sekali, dampak negatif yang ditimbulkan bisa sangat signifikan dan membahayakan. Ketiadaan firewall akan membuka pintu lebar bagi akses tidak sah ke dalam router itu sendiri maupun ke seluruh perangkat di jaringan internal, membuat mereka rentan terhadap berbagai upaya peretasan dan eksploitasi. Jaringan akan menjadi sasaran empuk bagi penyebaran malware, seperti virus dan worm, yang dapat merusak sistem atau mencuri data. Lebih lanjut, router dan layanan di dalamnya dapat menjadi korban serangan Denial of Service (DoS) atau Distributed Denial of Service (DDoS) yang bertujuan melumpuhkan konektivitas jaringan dengan membanjirinya menggunakan lalu lintas berbahaya. Pencurian data sensitif dan pelanggaran privasi menjadi risiko nyata karena penyerang dapat lebih mudah menembus pertahanan yang tidak ada. Selain itu, sumber daya jaringan yang tidak terlindungi dapat disalahgunakan oleh pihak luar untuk melancarkan serangan ke target lain atau aktivitas ilegal lainnya, serta akan terjadi kurangnya kontrol dan visibilitas terhadap lalu lintas jaringan, yang membuat deteksi dan respons terhadap insiden keamanan menjadi sangat sulit.