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

Laporan Sementara
Praktikum Jaringan Komputer

Firewall & NAT

Michael - 5024231022

2025

1 Pendahuluan

1.1 Latar Belakang

Seiring dengan berkembangnya zaman, terutama pada sektor teknologi informasi, jaringan komputer telah menjadi landasan penting dalam berbagai aspek kehidupan. Aspek-aspek ini mencakup ekonomi, pendidikan, politik, hingga hal-hal normal dalam kehidupan sehari-hari seperti misalnya menonton youtube, video call, e-learning, dan masih banyak lagi. Ini karena dengan adanya jaringan komputer, dapat terbentuk konektivitas antar perangkat. Konektivitas antar perangkat ini memungkinkan pertukaran data secara cepat dan efisien. Hal ini merupakan fondasi utama dari sistem informasi modern.

Namun di balik kemudahan dan kecepatan yang ditawarkan oleh jaringan komputer, terdapat beberapa tantangan besar yang harus dihadapi. Hal tersebut adalah aspek keamanan jaringan. Meningkatnya aktivitas pengguna di internet serta ketergantungan terhadap koneksi jaringan membuat sistem menjadi semakin rentan terhadap berbagai ancaman seiring dengan perkembangan teknologi jaringan komputer, mulai dari serangan siber, peretasan, hingga penyebaran malware yang dapat berakibat fatal bagi para pengguna internet. Oleh karena itu, dibutuhkan suatu mekanisme perlindungan yang dapat mengatur dan memantau lalu lintas data yang masuk dan keluar dari jaringan.

Untuk menyelesaikan masalah tersebut, Firewall dikembangkan sebagai solusi dalam perlindungan jaringan komputer. Firewall bekerja sebagai penjaga perangkat elektronik yang dapat menentukan apakah suatu data diizinkan untuk masuk atau keluar dari jaringan berdasarkan aturan-aturan yang sudah ditentukan sebelumnya. Dengan adanya firewall, organisasi dapat mencegah akses tak dikenal dan membatasi komunikasi dengan sumber-sumber berbahaya dari luar jaringan. Dengan begitu, kemungkinan terjadinya masalah keamanan menjadi semakin rendah.

Selain itu, jumlah alamat IP publik yang terbatas juga menjadi permasalahan tersendiri di era modern ini, terutama di tempat yang dikhususkan untuk banyak orang dan perangkat elektronik. Untuk mengatasi keterbatasan tersebut, dikembangkan sebuah teknologi bernama Network Address Translation (NAT). NAT memungkinkan banyak perangkat dalam jaringan lokal untuk terkoneksi ke internet hanya dengan menggunakan satu alamat IP publik. Ini berarti, penggunaan IP dapat menjadi lebih efisien serta memungkinkan adanya peningkatan fleksibilitas koneksi.

Oleh karena munculnya fitur-fitur ini, praktikum jaringan komputer dengan topik seputar FIrewall dan NAT menjadi sangat krusial dalam memberikan pengalaman langsung. Praktikum ini bertujuan untuk meningkatkan pemahaman serta kemampuan praktikan dalam memanfaatkan Firewall dan NAT. Dengan bekal ini, praktikan diharapkan mampu meningkatkan pemahamannya terhadap Firewall dan NAT yang menjadi salah satu fondasi penting pada internet dan komunikasi digital saat ini.

1.2 Dasar Teori

1. Firewall
   Secara umum, Firewall merupakan sistem keamanan jaringan yang berfungsi sebagai pengatur lalu lintas data antara jaringan internal dan eksternal suatu komputer. Firewall memeriksa setiap data yang masuk dan keluar dari jaringan dengan menggunakan aturan keamanan yang telah

ditentukan oleh sistem sebagai referensinya. Firewall dapat memberikan tiga jenis tanggapan terhadap akses suatu lalu lintas data, yaitu accept, reject, dan drop. Tanpa adanya fitur ini, komputer akan menjadi rentan terhadap berbagai ancaman siber hingga malware.

Pada jaringan komputer, beberapa Firewall yang sering digunakan adalah sebagai berikut:

- Packet Filtering
- Stateful Inspection
- Application Layer Firewall
- Next Generation Firewall
- Circuit Level Gateway
- Software Firewall
- Hardware Firewall
- Cloud Firewall

2. Network Address Translation (NAT)
   NAT adalah mekanisme yang memungkinkan sebuah alamat IP publik untuk digunakan oleh banyak perangkat dalam suatu jaringan lokal untuk mengakses internet bersama-sama. Hal ini sangat membantu dalam lingkungan di mana jumlah IP publik terbatas sedangkan jumlah penggunanya banyak, sehingga memungkinkan efisiensi IP.

   Secara umum, NAT dapat dikategorikan sebagai berikut:

   - Static NAT
   - Dynamic NAT
   - Port Address Translation

3. Connection Tracking
   Connection Tracking merpakan fitur pelacakan koneksi yang digunakan dalam firewall dan NAT dengan tujuan untuk memantau status setiap koneksi jaringan. Sistem ini dapat mencatat informasi-informasi penting seperti alamat sumber dan tujuan, nomor port, protokol, serta status koneksi. Informasi-informasi ini penting untuk meningkatkan keamanan pada jaringan lokal tersebut.

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? Agr bisa mengakses web server lokal (IP: 192.168.1.10, port 80) dari jaringan luar, diperlukan port forwarding menggunakan konfigurasi Static NAT. Ini karena Static NAT dapat meneruskan permintaan dari IP publik router ke IP lokal web server. Untuk implementasinya, cukup diperoleh IP web server lokal dan IP router beserta portnya. Setelah diberikan penamaan, lakukan setup dan penentuan port. Setelah itu, semua permintaan yang masuk ke IP router cukup dirouting ke IP web server lokal.

Referensi:
- https://www.noip.com/support/knowledgebase/general-port-forwarding-guide

2. Menurutmu, mana yang lebih penting diterapkan terlebih dahulu di jaringan: NAT atau Firewall? Jelaskan alasanmu. Dari dasar teori, diketahui bahwa NAT merupakan sebuah sistem jaringan yang memungkinkan efisiensi alamat IP pada suatu jaringan publik, sedangkan Firewall merupakan sebuah sistem keamanan yang memastikan agar sebuah perangkat selalu aman dari berbagai ancaman siber. Oleh karena itu, saya pribadi merasa bahwa Firewall jauh lebih penting karena NAT tanpa Firewall akan membuat komputer yang terhubung menjadi rentan terhadap masalah-masalah eksternal.

   Referensi:
   - https://www.geeksforgeeks.org/network-address-translation-nat/
   - https://www.geeksforgeeks.org/introduction-of-firewall-in-computer-network/

3. Apa dampak negatif jika router tidak diberi filter firewall sama sekali? Sesuai fungsi dari fitur Firewall, router yang tidak dilindungi oleh Firewall akan menjadi rentan terhadap berbagai ancaman eksternal, seperti eksploitas, virus malware, peretasan, dan ancaman-ancaman lainnya.

   Referensi:
   - https://www.geeksforgeeks.org/introduction-of-firewall-in-computer-network/