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

Laporan Sementara
Praktikum Jaringan Komputer

Firewall dan NAT

Muhammad Fahri Fadillah - 5024231063

2025

1 Pendahuluan

1.1 Latar Belakang

Dalam era digital yang semakin berkembang, keamanan jaringan menjadi prioritas utama dalam setiap organisasi. Seiring dengan meningkatnya ketergantungan pada teknologi informasi dan komunikasi, ancaman terhadap data dan informasi organisasi semakin beragam dan kompleks. Salah satu metode yang paling umum digunakan untuk mengamankan jaringan komputer adalah Firewall dan Network Address Translation (NAT). Firewall berfungsi sebagai penjaga yang mengatur lalu lintas data yang masuk dan keluar dari jaringan, sedangkan NAT memungkinkan penggunaan satu alamat IP publik untuk banyak perangkat dalam jaringan yang sama, mengatasi keterbatasan jumlah alamat IP yang tersedia.

Keamanan jaringan tidak hanya mengandalkan perangkat keras dan perangkat lunak, tetapi juga pada pengelolaan koneksi yang cermat. Salah satu teknik yang mendukung pengelolaan tersebut adalah Connection Tracking, yang memungkinkan pengawasan dan pelacakan koneksi data yang terjadi dalam jaringan. Dengan begitu, diharapkan organisasi dapat mengurangi risiko ancaman yang mungkin timbul dari luar maupun dari dalam jaringan.

Modul ini akan mengulas konsep dasar dari Firewall, NAT, dan Connection Tracking beserta jenis-jenis serta cara kerjanya. Dengan pemahaman yang lebih mendalam tentang ketiga teknologi ini, diharapkan individu atau organisasi dapat merancang dan menerapkan sistem keamanan yang lebih efektif untuk menjaga integritas, kerahasiaan, dan ketersediaan data serta informasi dalam jaringan.

1.2 Dasar Teori

Firewall adalah sebuah sistem keamanan jaringan yang berfungsi untuk mengontrol dan mengawasi aliran data yang masuk dan keluar dari jaringan komputer. Secara sederhana, firewall berperan seperti "satpam digital" yang memeriksa setiap data yang ingin melewati jaringan, memastikan data tersebut sesuai dengan kebijakan yang telah ditentukan. Jika ada data yang tidak sesuai atau mencurigakan, firewall akan memblokirnya atau memberikan respon error. Dalam konteks keamanan jaringan, firewall berfungsi untuk melindungi perangkat dalam jaringan dari ancaman eksternal seperti hacker, virus, atau malware. Terdapat berbagai jenis firewall, antara lain Packet Filtering yang memeriksa data berdasarkan IP, port, dan protokol tanpa menginspeksi isi data, serta Stateful Inspection yang lebih canggih dengan kemampuan untuk mengenali koneksi yang sah atau tidak. Jenis lainnya adalah Application Layer Firewall, yang dapat memeriksa isi aplikasi dan bahkan memblokir konten tertentu, serta Next Generation Firewall (NGFW) yang menawarkan pemeriksaan lebih mendalam termasuk enkripsi SSL.

Sementara itu, Network Address Translation (NAT) adalah teknologi yang memungkinkan banyak perangkat dalam suatu jaringan lokal untuk menggunakan satu alamat IP publik ketika mengakses internet. NAT ini menjadi solusi untuk mengatasi keterbatasan jumlah alamat IP publik yang tersedia. Sebagai contoh, alamat IPv4 yang terbatas ini dapat digunakan secara efisien dengan mengubah alamat IP lokal perangkat menjadi IP publik. Ada beberapa jenis NAT, termasuk Static NAT yang menghubungkan satu alamat IP lokal ke satu IP publik secara permanen, Dynamic NAT yang memetakan alamat IP lokal ke IP publik dari kumpulan IP yang tersedia, dan Port Address Translation (PAT) yang memungkinkan banyak perangkat berbagi satu alamat IP publik dengan membedakan setiap koneksi berdasarkan nomor port.

Connection Tracking merupakan fitur penting yang mendukung keamanan jaringan dengan melacak dan mengelola sesi koneksi yang terjadi dalam jaringan. Melalui connection tracking, router atau firewall dapat mencatat informasi terkait koneksi seperti alamat IP sumber dan tujuan, nomor port, serta status koneksi. Dengan cara ini, setiap koneksi yang datang bisa dikenali apakah valid atau tidak, yang sangat berguna untuk melindungi jaringan dari ancaman atau akses yang tidak sah. Misalnya, jika ada koneksi yang tidak tercatat sebelumnya, maka koneksi tersebut akan langsung ditolak karena dianggap sebagai ancaman. Connection tracking juga memungkinkan pengelolaan trafik jaringan yang lebih efisien dan membantu meminimalkan beban pada perangkat jaringan dengan hanya memproses koneksi yang sah.

Secara keseluruhan, firewall, NAT, dan connection tracking bekerja bersama-sama untuk menciptakan sistem keamanan yang lebih kuat dan efisien dalam sebuah jaringan. Firewall berperan sebagai pelindung utama dari ancaman eksternal, sementara NAT membantu memaksimalkan penggunaan alamat IP dan connection tracking memberikan kontrol lebih lanjut dalam mengelola dan melacak lalu lintas data yang masuk. Kombinasi ketiganya membentuk lapisan pertahanan yang efektif untuk menjaga integritas dan keamanan jaringan.

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?**
   Jawaban: Untuk mengakses web server lokal dengan IP 192.168.1.10 dan port 80 dari jaringan luar (internet), kamu perlu melakukan konfigurasi Port Forwarding pada NAT (Network Address Translation) di router. Port forwarding ini akan mengarahkan permintaan dari alamat IP publik router pada port 80 ke alamat IP lokal 192.168.1.10 port 80. Misalnya, jika alamat IP publik router adalah 123.45.67.89, maka permintaan dari internet ke http://123.45.67.89 akan diteruskan ke http://192.168.1.10 secara otomatis. Konfigurasi ini umumnya dilakukan dengan membuat aturan NAT tipe Destination NAT (DNAT) atau Static NAT, tergantung pada perangkat jaringan yang digunakan.

2. **Menurutmu, mana yang lebih penting diterapkan terlebih dahulu di jaringan: NAT atau Firewall? Jelaskan alasanmu.**
   Jawaban: Menurut saya, Firewall lebih penting untuk diterapkan terlebih dahulu dibandingkan NAT karena firewall berperan langsung dalam menjaga keamanan jaringan dari akses yang tidak sah atau serangan berbahaya. Firewall menyaring lalu lintas data berdasarkan aturan tertentu dan bisa mencegah masuknya trafik mencurigakan bahkan sebelum NAT memproses permintaan tersebut. Walaupun NAT juga memberikan lapisan keamanan dengan menyembunyikan IP internal, namun fungsi utamanya adalah untuk memetakan alamat IP, bukan untuk menyaring lalu lintas. Oleh karena itu, firewall lebih krusial sebagai pertahanan awal dalam arsitektur keamanan jaringan.

3. **Apa dampak negatif jika router tidak diberi filter firewall sama sekali?**
   Jawaban: Jika router tidak diberi filter firewall sama sekali, maka semua jenis lalu lintas, baik dari dalam maupun luar jaringan, dapat masuk dan keluar tanpa kontrol. Hal ini membuka celah keamanan yang sangat besar, karena memungkinkan serangan dari luar seperti port scanning, malware injection, DDoS (Distributed Denial of Service), atau akses ilegal terhadap perangkat

dalam jaringan lokal. Tanpa firewall, tidak ada mekanisme yang membatasi atau memantau aktivitas jaringan, sehingga risiko kebocoran data, peretasan, dan penyebaran virus menjadi sangat tinggi. Oleh karena itu, firewall merupakan komponen vital dalam menjaga integritas dan keamanan jaringan.