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

Laporan Sementara
Praktikum Jaringan Komputer

Firewall & NAT

Ahmad Faiq Fawwaz - 5024231032

2025

1 Pendahuluan

1.1 Latar Belakang

Dalam era digital seperti saat ini, jaringan komputer merupakan tulang punggung dari berbagai sistem informasi dan layanan teknologi. Kebutuhan terhadap akses internet yang cepat dan andal telah mendorong pengembangan infrastruktur jaringan yang semakin kompleks. Namun, semakin kompleksnya jaringan juga membawa tantangan baru, salah satunya adalah meningkatnya risiko terhadap serangan siber dan akses tidak sah ke dalam sistem. Oleh karena itu, aspek keamanan jaringan menjadi hal yang sangat krusial untuk diperhatikan, terutama pada sistem yang menangani data sensitif dan beroperasi dalam skala besar. Salah satu komponen penting dalam menjaga keamanan jaringan adalah penggunaan firewall. Firewall bertindak sebagai penjaga gerbang yang mengatur lalu lintas data masuk dan keluar dari suatu jaringan berdasarkan aturan yang telah ditentukan. Dengan kata lain, firewall mampu menyaring dan mengizinkan hanya lalu lintas yang dianggap aman untuk diteruskan ke jaringan internal. Firewall dapat berupa perangkat lunak maupun perangkat keras, dan implementasinya sangat bergantung pada kebutuhan serta skala jaringan yang digunakan. Selain firewall, teknik lain yang tak kalah penting adalah Network Address Translation (NAT). NAT memungkinkan perangkat-perangkat dalam jaringan lokal menggunakan satu atau beberapa alamat IP publik untuk mengakses internet. Hal ini tidak hanya menghemat penggunaan alamat IP publik yang terbatas, tetapi juga memberikan lapisan keamanan tambahan dengan menyembunyikan struktur jaringan internal dari dunia luar. Untuk menunjang fungsi firewall dan NAT, connection tracking menjadi fitur penting yang harus dipahami. Connection tracking mencatat setiap koneksi yang terjadi, termasuk status dan metadata dari koneksi tersebut. Dengan demikian, firewall dapat melakukan pemeriksaan yang lebih cerdas dan NAT dapat bekerja lebih efisien karena koneksi-koneksi dapat dikenali dan dipetakan dengan benar. Melalui praktikum ini, mahasiswa diharapkan dapat memahami cara kerja firewall dan NAT secara praktis serta bagaimana connection tracking berperan dalam meningkatkan keamanan dan efisiensi jaringan. Pemahaman ini akan sangat bermanfaat ketika mahasiswa menghadapi permasalahan nyata dalam pengelolaan dan pengamanan jaringan di dunia industri maupun penelitian.

2 Dasar Teori

Firewall adalah sistem pengamanan jaringan yang bertindak sebagai penghalang antara jaringan internal yang dipercaya dan jaringan eksternal yang tidak terpercaya, seperti internet. Tujuan utama firewall adalah mencegah akses tidak sah dan melindungi jaringan internal dari berbagai ancaman, seperti serangan DoS, malware, dan eksploitasi celah keamanan. Berdasarkan cara kerjanya, firewall dapat berupa packet filtering yang menyaring lalu lintas berdasarkan header paket, stateful inspection yang melacak status koneksi, application layer firewall yang menganalisis lalu lintas pada lapisan aplikasi, serta next generation firewall (NGFW) yang menggabungkan berbagai fitur keamanan lanjutan. Network Address Translation (NAT) adalah metode untuk memodifikasi alamat IP dalam header paket sehingga banyak perangkat di jaringan lokal dapat mengakses jaringan publik menggunakan satu atau beberapa alamat IP publik. NAT bermanfaat untuk menghemat penggunaan alamat IP publik, menyembunyikan struktur jaringan internal, dan mendukung topologi jaringan yang fleksibel, dengan jenis-jenis seperti static NAT, dynamic NAT, dan port address translation (PAT). Connection tracking adalah fitur yang memungkinkan sistem memantau dan mencatat setiap koneksi yang terjadi di ja-

ringan, sehingga firewall dapat membuat keputusan berdasarkan status koneksi, NAT dapat bekerja lebih efisien, dan administrator dapat melakukan monitoring serta meningkatkan keamanan jaringan dengan mendeteksi koneksi yang tidak valid.

3 Tugas Pendahuluan

Bagian ini berisi jawaban dari tugas pendahuluan yang telah anda kerjakan, beserta penjelasan dari jawaban tersebut.

1. **Apa yang dimaksud dengan Firewall dan sebutkan jenis-jenisnya!**
   FIrewall adalah sistem pengaman jaringan yang bekerja dengan cara menyaring lalu lintas data yang masuk dan keluar berdasarkan aturan yang telah ditentukan. Firewall berfungsi untuk melindungi jaringan dari ancaman eksternal seperti serangan hacker, malware, dan akses tidak sah. Jenis-jenis firewall meliputi:

   - **Packet Filtering**: Menyaring paket berdasarkan IP, port, dan protokol.
   - **Stateful Inspection**: Memahami status koneksi untuk menentukan izin lalu lintas.
   - **Application Layer Firewall**: Menyaring hingga ke tingkat aplikasi (misalnya HTTP/FTP).
   - **Next Generation Firewall (NGFW)**: Memiliki fitur deep packet inspection dan analisis SSL.
   - **Circuit Level Gateway**: Menilai keabsahan koneksi tanpa melihat isi data.
   - **Software Firewall**: Dipasang sebagai aplikasi di perangkat.
   - **Hardware Firewall**: Perangkat fisik yang menyaring lalu lintas sebelum masuk jaringan.
   - **Cloud Firewall**: Firewall berbasis cloud untuk melindungi infrastruktur cloud.

2. **Jelaskan apa itu NAT, sebutkan jenis-jenisnya dan bagaimana cara kerjanya!**
   NAT (Network Address Translation) adalah teknik untuk mengubah alamat IP dari paket data agar perangkat dalam jaringan lokal dapat berkomunikasi dengan jaringan publik menggunakan satu atau beberapa IP publik. Jenis-jenis NAT meliputi:

   - **Static NAT**: Satu IP lokal dihubungkan ke satu IP publik (satu-satu).
   - **Dynamic NAT**: IP lokal dipetakan ke IP publik dari kumpulan IP yang tersedia.
   - **Port Address Translation (PAT)**: Banyak IP lokal menggunakan satu IP publik, dibedakan berdasarkan port.

   Cara kerja NAT adalah dengan mencatat pemetaan antara IP lokal dan IP publik di tabel NAT. Saat perangkat dalam jaringan mengirim data ke internet, NAT mengganti IP sumber ke IP publik dan menyimpan informasinya. Saat ada balasan dari internet, NAT menggunakan tabel tersebut untuk meneruskan paket ke IP lokal yang sesuai.

3. **Apa itu Connection Tracking dan apa manfaatnya dalam firewall dan NAT?**
   Connection Tracking adalah mekanisme pelacakan status koneksi jaringan, seperti siapa yang sedang berkomunikasi, protokol yang digunakan, port sumber dan tujuan, serta status koneksi (baru, aktif, atau tidak valid). Fitur ini penting untuk implementasi firewall stateful karena memungkinkan identifikasi paket balasan yang sah. Dalam NAT, connection tracking digunakan

untuk mencocokkan koneksi masuk dengan koneksi yang sudah tercatat, sehingga memastikan bahwa hanya koneksi sah yang diteruskan. Manfaatnya mencakup peningkatan keamanan, efisiensi NAT, pengurangan beban router, dan kontrol lebih detail terhadap lalu lintas jaringan.