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

Laporan Sementara
Praktikum Jaringan Komputer

Firewall & NAT

Natania Christin Agustina - 5024231014

2025

1 Pendahuluan

1.1 Latar Belakang

Di era digital yang semakin berkembang pesat, jaringan komputer menjadi tulang punggung komunikasi dan pertukaran data di berbagai bidang seperti bisnis, pendidikan, pemerintahan, hingga kehidupan sehari-hari. Jaringan yang terkoneksi dengan internet memungkinkan akses informasi yang cepat dan efisien, namun juga membuka peluang bagi berbagai ancaman keamanan seperti serangan siber, malware, dan akses tidak sah. Oleh karena itu, perlindungan jaringan menjadi aspek yang sangat penting untuk memastikan data dan sistem tetap aman dan terpercaya. Salah satu teknologi utama dalam menjaga keamanan jaringan adalah firewall, yang berfungsi sebagai penjaga gerbang digital. Firewall memantau dan menyaring lalu lintas data berdasarkan aturan tertentu, sehingga hanya data yang memenuhi kriteria keamanan yang diizinkan masuk atau keluar jaringan. Dengan keberadaan firewall, risiko serangan dari luar seperti hacking, virus, dan akses ilegal dapat diminimalisir sehingga jaringan menjadi lebih aman dan stabil. Selain itu, masalah keterbatasan alamat IP publik menjadi tantangan dalam mengelola jaringan yang terus berkembang. Banyaknya perangkat yang membutuhkan koneksi internet membuat penggunaan IP publik per perangkat menjadi tidak efisien. Untuk mengatasi hal ini, teknologi Network Address Translation (NAT) hadir sebagai solusi dengan memungkinkan beberapa perangkat di jaringan lokal menggunakan satu alamat IP publik saja untuk terhubung ke internet. NAT tidak hanya membantu menghemat penggunaan alamat IP publik yang terbatas, tetapi juga berfungsi menyembunyikan alamat IP asli perangkat dalam jaringan lokal, sehingga memberikan lapisan tambahan perlindungan terhadap serangan. Dengan pemahaman yang baik tentang firewall dan NAT, pengelolaan jaringan dapat dilakukan secara lebih optimal, menjaga keamanan sekaligus efisiensi sumber daya jaringan. Oleh sebab itu, materi mengenai firewall dan NAT menjadi sangat penting dalam pembelajaran jaringan komputer dan keamanan siber di era modern ini.

1.2 Dasar Teori

- Firewall
  Firewall adalah sistem keamanan yang berfungsi sebagai penyaring atau penjaga lalu lintas data yang masuk dan keluar dari jaringan komputer. Dalam analogi sederhana, firewall dapat dianggap sebagai “satpam digital” yang memantau dan mengatur siapa saja yang diizinkan untuk berkomunikasi dengan jaringan internal. Firewall bekerja berdasarkan seperangkat aturan yang ditentukan oleh administrator jaringan, dan dapat memutuskan apakah suatu paket data harus diterima (accept), ditolak dengan pemberitahuan (reject), atau dibuang tanpa memberikan respon sama sekali (drop). Keberadaan firewall menjadi sangat penting, terutama dalam konteks meningkatnya ketergantungan terhadap koneksi internet dan banyaknya ancaman siber yang terus berkembang. Sebelum kehadiran firewall, sistem keamanan jaringan banyak bergantung pada Access Control List (ACL), yang hanya mampu mengatur lalu lintas berdasarkan IP dan port tanpa memperhatikan isi dari data yang dikirim. Pendekatan tersebut memiliki banyak kelemahan, karena tidak mampu menganalisis atau menyaring lalu lintas data secara cerdas dan menyeluruh. Oleh karena itu, firewall hadir sebagai solusi yang lebih komprehensif, mampu menganalisis data tidak hanya dari identitas asal dan tujuan, tetapi juga dari konteks dan isi komunikasi. Terdapat beberapa jenis firewall yang dikembangkan untuk memenuhi kebu-

tuhan keamanan dengan tingkat yang berbeda-beda. Berikut adalah jenis-jenis firewall beserta penjelasannya:

- Packet Filtering Firewall:
  Jenis ini merupakan bentuk firewall paling dasar. Ia bekerja dengan memeriksa header dari setiap paket data yang masuk atau keluar, berdasarkan kriteria seperti alamat IP sumber dan tujuan, nomor port, serta protokol yang digunakan. Jika paket sesuai dengan aturan, maka akan diteruskan, dan jika tidak, akan diblokir. Namun, packet filtering tidak memahami konteks atau status koneksi, sehingga rentan terhadap beberapa jenis serangan.
- Stateful Inspection Firewall:
  Lebih canggih dibanding packet filtering, jenis ini dapat mengenali status dari suatu koneksi. Firewall akan mencatat koneksi yang sah dan hanya mengizinkan lalu lintas data yang merupakan bagian dari koneksi yang telah diotorisasi. Ini memungkinkan penyaringan data yang lebih dinamis dan kontekstual.
- Application Layer Firewall:
  Firewall ini beroperasi pada lapisan aplikasi dan mampu memeriksa isi dari lalu lintas data, seperti HTTP, FTP, atau DNS. Dengan demikian, ia dapat mendeteksi dan memblokir konten tertentu atau aktivitas mencurigakan pada tingkat aplikasi. Umumnya, jenis ini menggunakan sistem proxy untuk bertindak sebagai perantara antara pengguna dan server.
- Next Generation Firewall (NGFW):
  Merupakan evolusi dari firewall tradisional, NGFW menawarkan kemampuan inspeksi mendalam terhadap paket data (deep packet inspection), termasuk data yang terenkripsi. Selain itu, NGFW juga memiliki fitur-fitur tambahan seperti deteksi serangan siber, identifikasi aplikasi secara spesifik, dan integrasi dengan sistem keamanan lainnya.
- Circuit Level Gateway:
  Firewall ini bekerja pada lapisan sesi koneksi TCP. Ia tidak memeriksa isi data, melainkan hanya memastikan apakah koneksi antara sumber dan tujuan telah sah. Meskipun ringan dalam penggunaan sumber daya, tingkat keamanannya lebih rendah karena tidak menyaring konten.
- Software Firewall:
  Merupakan aplikasi yang dipasang di perangkat seperti komputer atau server. Software firewall menawarkan fleksibilitas dalam pengaturan keamanan setiap perangkat secara individual, meskipun dapat mempengaruhi kinerja sistem tergantung pada spesifikasi perangkat kerasnya.
- Hardware Firewall:
  Biasanya berupa perangkat fisik yang dipasang di antara jaringan internal dan koneksi luar (misalnya internet). Hardware firewall menawarkan performa yang tinggi dan andal untuk lingkungan jaringan besar karena dapat menyaring lalu lintas sebelum mencapai sistem internal.
- Cloud Firewall:
  Jenis firewall ini berjalan di lingkungan cloud dan sangat cocok untuk organisasi yang mengandalkan layanan cloud secara ekstensif. Cloud firewall memberikan perlindungan terhadap lalu lintas data yang melewati infrastruktur cloud, serta mendukung skalabilitas dan fleksibilitas tinggi.

Dengan beragam jenis dan kemampuannya, firewall menjadi komponen yang sangat penting dalam menjaga keamanan jaringan dari ancaman yang terus berkembang. Di tengah derasnya arus data digital dan meningkatnya kompleksitas sistem informasi, penerapan firewall yang tepat dapat memberikan perlindungan berlapis terhadap data sensitif, menjaga privasi, serta menjamin stabilitas dan keandalan sistem jaringan secara keseluruhan.

- Network Address Translation (NAT)
  NAT (Network Address Translation) adalah suatu teknik yang digunakan dalam jaringan komputer untuk mengubah alamat IP pada paket data ketika paket tersebut melewati perangkat perantara, biasanya berupa router. Tujuan utama dari NAT adalah untuk menghemat penggunaan alamat IP publik, yang jumlahnya terbatas, sekaligus memberikan fleksibilitas dalam pengelolaan jaringan internal. Dengan menggunakan NAT, banyak perangkat dalam jaringan lokal (LAN) dapat berbagi satu alamat IP publik yang sama untuk mengakses layanan di internet. Permasalahan utama yang mendorong penggunaan NAT adalah keterbatasan jumlah alamat IPv4 yang tersedia secara global, yaitu sekitar 4,3 miliar. Jumlah ini tidak mencukupi untuk mengakomodasi semua perangkat yang kini terhubung ke internet. Oleh karena itu, NAT menjadi solusi yang sangat efektif, karena memungkinkan perangkat-perangkat dengan alamat IP privat (seperti 192.168.x.x atau 10.x.x.x) untuk tetap bisa berkomunikasi dengan dunia luar melalui satu atau beberapa IP publik. NAT memiliki beberapa jenis dengan fungsi dan mekanisme kerja yang berbeda. Berikut merupakan jenis-jenis dari NAT :

  - Static NAT:
    Static NAT menerjemahkan satu alamat IP lokal ke satu alamat IP publik secara tetap (one-to-one mapping). Artinya, setiap perangkat yang ingin diakses dari luar akan selalu menggunakan alamat IP publik yang sama. Jenis ini umum digunakan untuk perangkat seperti server internal yang harus bisa diakses dari jaringan luar, misalnya server web atau server email. Namun, penggunaan static NAT cenderung boros karena memerlukan satu IP publik untuk setiap perangkat.
  - Dynamic NAT:
    Dynamic NAT menerjemahkan IP lokal ke IP publik yang tersedia dalam sebuah pool (kumpulan) IP publik. Ketika sebuah perangkat ingin mengakses internet, router akan secara dinamis memberikan IP publik yang tersedia dari pool tersebut. Namun, jika jumlah perangkat melebihi jumlah IP publik yang tersedia, maka koneksi tambahan akan ditolak. Meski lebih efisien dibanding static NAT, jenis ini masih bergantung pada ketersediaan IP publik yang cukup.
  - Port Address Translation (PAT):
    Port Address Translation (PAT) juga dikenal sebagai NAT overload, PAT adalah bentuk NAT yang paling banyak digunakan, terutama di jaringan rumah atau kantor kecil. PAT memungkinkan banyak perangkat lokal untuk berbagi satu alamat IP publik dengan membedakan setiap koneksi berdasarkan nomor port. Router akan mencatat informasi koneksi seperti IP dan port asal serta tujuan dalam sebuah translation table. Ketika data dari internet kembali, router akan mencocokkannya dengan tabel tersebut dan meneruskan data ke perangkat yang sesuai. PAT sangat efisien karena dapat melayani banyak perangkat hanya dengan satu IP publik.

Secara teknis, NAT bekerja dengan mencatat informasi dari setiap koneksi jaringan yang melewati router. Ketika sebuah perangkat di jaringan lokal mengirimkan data ke internet, router akan mengubah alamat IP sumber dari IP privat menjadi IP publik. Selain itu, NAT juga sering mengubah nomor port agar bisa membedakan antara beberapa koneksi yang berjalan secara bersamaan. Semua informasi ini dicatat dalam NAT table. Sebagai contoh, jika dua perangkat di jaringan lokal mengakses situs web yang sama secara bersamaan, mereka mungkin menggunakan port yang berbeda (misalnya port 50123 dan 50124). Router akan mencatat bahwa permintaan dari IP 192.168.1.2:50123 dan 192.168.1.3:50124 dikirim melalui IP publik 203.0.113.5, lalu ketika balasan dari situs web diterima, router akan mencocokkannya berdasarkan port dan mengirimkan kembali ke perangkat yang sesuai di jaringan internal. Salah satu kelebihan utama dari NAT adalah kemampuannya dalam menghemat dan mengelola penggunaan IP publik. Selain itu, karena NAT menyembunyikan alamat IP internal dari dunia luar, ia secara tidak langsung memberikan lapisan keamanan tambahan—pihak luar tidak dapat dengan mudah mengetahui struktur internal jaringan. Namun, NAT bukanlah solusi keamanan yang sepenuhnya andal. Fungsi utamanya lebih pada manajemen lalu lintas dan penghematan IP. NAT tidak secara eksplisit dirancang untuk mendeteksi atau memblokir serangan siber. Oleh karena itu, dalam implementasi nyata, NAT sering dikombinasikan dengan sistem firewall agar dapat memberikan perlindungan yang lebih menyeluruh terhadap ancaman dari luar.

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 : Konfigurasi NAT yang akan saya buat adalah menggunakan Port Address Translation (PAT), khususnya dalam bentuk Static PAT atau yang lebih dikenal sebagai port forwarding. Hal ini dikarenakan saya ingin mengarahkan permintaan dari jaringan luar yang masuk melalui IP publik pada port 80 ke alamat IP lokal 192.168.1.10 port 80. Teknik ini memungkinkan satu IP publik digunakan untuk melayani banyak perangkat di jaringan lokal dengan membedakan koneksi berdasarkan nomor port, sehingga lebih efisien dan hemat dibandingkan menggunakan Static NAT atau Dynamic NAT yang membutuhkan lebih banyak IP publik. Dengan menggunakan PAT, router dapat meneruskan koneksi masuk ke server lokal berdasarkan port tertentu, memungkinkan akses dari internet ke layanan yang berjalan di jaringan internal.
   Referensi :
   - www.geeksforgeeks.org/advanced-nat-techniques-port-address-translation
   - www.techtarget.com/searchnetworking/definition/Port-Address-Translation-PAT
   - www.zenarmor.com/docs/network-basics/what-is-port-address-translation-pat
2. Menurutmu, mana yang lebih penting diterapkan terlebih dahulu di jaringan: NAT atau Firewall? Jelaskan alasanmu.
   Jawaban : Menurut saya, yang lebih penting diterapkan terlebih dahulu di jaringan adalah firewall. Hal ini dikarenakan firewall berfungsi sebagai satpam digital yang menjaga pintu masuk dan keluar jaringan komputer. Firewall akan memeriksa semua lalu lintas data berdasarkan aturan tertentu, apakah diizinkan lewat (accept), ditolak dengan pesan (reject), atau dibuang begitu saja (drop). Fungsi ini sangat penting karena sebelum ada firewall, pengamanan jaringan hanya mengandalkan Access Control List (ACL) yang tidak bisa mengenali isi data secara mendalam, sehingga lebih rentan terhadap serangan. Firewall juga hadir sebagai solusi utama ketika internet mulai menjadi kebutuhan pokok, tapi juga membuka celah besar untuk serangan dari luar. Dengan adanya firewall, jaringan internal bisa tetap aman karena akses dari luar yang mencurigakan bisa langsung diblokir. Terlebih lagi, jenis firewall modern seperti Stateful Inspection atau Next Generation Firewall (NGFW) mampu mendeteksi status koneksi dan isi data secara mendalam, termasuk data yang dienkripsi, sehingga memberikan perlindungan yang jauh lebih canggih. Sedangkan NAT (Network Address Translation) lebih berperan dalam pengelolaan IP dan konektivitas. Fungsi utama NAT adalah memungkinkan banyak perangkat di jaringan lokal untuk mengakses internet dengan satu IP publik, yang memang sangat efisien mengingat keterbatasan alamat IPv4. Namun, tanpa perlindungan dari firewall, koneksi internet yang difasilitasi oleh NAT tetap bisa menjadi jalan masuk bagi serangan dari luar. Oleh karena itu, firewall sebaiknya diterapkan terlebih dahulu sebelum NAT, karena fungsi utamanya adalah melindungi jaringan dari ancaman, sedangkan NAT lebih berfokus pada penghematan IP dan konektivitas keluar masuk jaringan.
   Referensi :
   - www.geeksforgeeks.org/network-address-translation-nat
   - www.geeksforgeeks.org/introduction-of-firewall-in-computer-network

- www.paloaltonetworks.com/cyberpedia/types-of-firewalls
- www.zscaler.com/resources/security-terms-glossary/what-is-next-generation-firewall

3. Apa dampak negatif jika router tidak diberi filter firewall sama sekali?
   Jawaban : Jika router tidak dilengkapi dengan filter firewall, dampak negatifnya bisa sangat serius, khususnya dalam hal keamanan jaringan. Tanpa adanya firewall, lalu lintas data dari luar dapat langsung masuk ke jaringan internal tanpa melalui proses penyaringan, sehingga jaringan menjadi sangat rentan terhadap berbagai ancaman seperti port scanning, brute force, serangan DDoS, hingga penyebaran malware. Informasi penting seperti file server atau database juga berisiko diakses oleh pihak yang tidak berwenang karena tidak adanya sistem yang membatasi akses. Selain itu, arus data keluar dan masuk dari jaringan menjadi tidak terkendali, yang memungkinkan perangkat-perangkat dalam jaringan mengakses situs atau layanan yang berbahaya tanpa terdeteksi. Jika salah satu perangkat terinfeksi, virus atau malware dapat dengan mudah menyebar ke seluruh jaringan karena tidak ada sistem pertahanan yang menghentikannya. Lebih parahnya lagi tanpa fitur pencatatan dan pemantauan dari firewall, administrator jaringan akan kesulitan dalam mendeteksi aktivitas mencurigakan atau potensi serangan. Oleh karena itu, keberadaan firewall sangat penting untuk menjaga keamanan, mengatur akses, dan melindungi jaringan dari berbagai ancaman.
   Referensi :

   - www.cisco.com/site/us/en/learn/topics/security/what-is-a-firewall.html
   - www.paloaltonetworks.com/cyberpedia/what-is-a-firewall
   - www.fortinet.com/resources/cyberglossary/firewall