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

Laporan Sementara
Praktikum Jaringan Komputer

Firewall & NAT

Aaron Smeraldo Olivier Manik - 5024231070

2025

1 Pendahuluan

1.1 Latar Belakang

Dalam era digital saat ini, komunikasi data melalui jaringan komputer telah menjadi bagian penting dalam berbagai aktivitas, baik di lingkungan akademik, bisnis, maupun pemerintahan. Namun, seiring dengan meningkatnya penggunaan jaringan, risiko terhadap keamanan data juga semakin tinggi. Oleh karena itu, diperlukan mekanisme pengamanan yang efektif untuk melindungi jaringan dari akses tidak sah dan potensi serangan siber. Salah satu mekanisme utama yang digunakan adalah Firewall.

Firewall berfungsi sebagai penghalang antara jaringan internal yang dipercaya dan jaringan eksternal yang tidak dipercaya, seperti internet. Dengan menggunakan aturan-aturan tertentu (rules), firewall dapat menyaring lalu lintas data yang masuk dan keluar dari jaringan, sehingga hanya trafik yang diizinkan yang dapat melewati sistem.

Selain itu, dalam pengelolaan jaringan, diperlukan juga teknik untuk mengatur alamat IP agar dapat digunakan secara efisien, terutama ketika terdapat keterbatasan alamat IP publik. Di sinilah peran Network Address Translation (NAT) menjadi penting. NAT memungkinkan perangkat dalam jaringan lokal menggunakan alamat IP privat dan tetap dapat mengakses internet menggunakan satu atau beberapa IP publik. Hal ini tidak hanya menghemat penggunaan alamat IP publik, tetapi juga memberikan lapisan tambahan dalam hal keamanan.

Praktikum ini bertujuan untuk memberikan pemahaman praktis kepada mahasiswa mengenai konsep dan implementasi firewall dan NAT dalam jaringan komputer. Melalui konfigurasi langsung, mahasiswa diharapkan mampu mengidentifikasi dan mengelola trafik jaringan, serta memahami bagaimana firewall dan NAT bekerja dalam situasi nyata. Pemahaman ini sangat penting dalam membekali mahasiswa dengan keterampilan dasar dalam perancangan dan pengelolaan sistem jaringan yang aman dan efisien.

1.2 Dasar Teori

1.2.1 Firewall

Firewall adalah sistem keamanan jaringan yang berfungsi untuk memantau dan mengontrol lalu lintas jaringan berdasarkan aturan yang telah ditentukan. Firewall dapat berupa perangkat keras (*hardware*), perangkat lunak (*software*), atau kombinasi keduanya. Tujuan utama dari firewall adalah untuk mencegah akses yang tidak sah ke atau dari jaringan privat.

Secara umum, firewall bekerja dengan cara menyaring paket data berdasarkan parameter seperti alamat IP, port, dan protokol. Berdasarkan cara kerjanya, terdapat beberapa jenis firewall, antara lain:

- **Packet Filtering Firewall**: Menyaring paket berdasarkan informasi header seperti IP sumber, IP tujuan, port, dan protokol.

- **Stateful Inspection Firewall**: Selain menyaring paket, firewall ini juga memeriksa status koneksi sehingga lebih aman dibandingkan packet filtering biasa.
- **Application Layer Firewall**: Bekerja pada level aplikasi dan mampu memahami protokol aplikasi seperti HTTP, FTP, dan DNS.
- **Next Generation Firewall (NGFW)**: Firewall modern yang menggabungkan berbagai fitur seperti *Deep Packet Inspection (DPI)*, antivirus, dan pencegahan intrusi (*Intrusion Prevention System* atau IPS).

1.3 NAT (Network Address Translation)

Network Address Translation (NAT) adalah proses yang dilakukan oleh perangkat jaringan (biasanya router) untuk mengubah alamat IP dalam header paket saat melewati perangkat tersebut. NAT digunakan untuk menghubungkan jaringan privat dengan jaringan publik (internet) tanpa harus memberikan alamat IP publik ke setiap perangkat di jaringan lokal.

Jenis-jenis NAT antara lain:

- **Static NAT**: Memetakan satu alamat IP privat ke satu alamat IP publik secara tetap.
- **Dynamic NAT**: Memetakan alamat IP privat ke salah satu dari sekumpulan IP publik yang tersedia.
- **Port Address Translation (PAT)** atau *NAT Overload*: Memetakan banyak alamat IP privat ke satu alamat IP publik dengan membedakan berdasarkan nomor port.

NAT sangat berguna dalam menghemat penggunaan alamat IP publik dan sekaligus menambah lapisan keamanan, karena alamat IP privat tidak terlihat langsung dari internet.

1.4 Hubungan Firewall dan NAT

Firewall dan NAT sering digunakan secara bersamaan dalam sistem jaringan modern. NAT menyembunyikan alamat IP privat dan membantu menghubungkan jaringan internal ke internet, sementara firewall mengontrol akses masuk dan keluar berdasarkan kebijakan keamanan.

Dalam beberapa sistem operasi jaringan, seperti router MikroTik atau sistem berbasis Linux dengan `iptables`, konfigurasi NAT dan firewall dilakukan pada platform yang sama, memungkinkan integrasi yang lebih efisien antara pengalamatan 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?
   Untuk dapat mengakses web server lokal yang memiliki alamat IP 192.168.1.10 dan

berjalan pada port 80 dari jaringan luar (internet), diperlukan konfigurasi NAT berupa Destination NAT (DNAT) atau juga dikenal sebagai port forwarding. Konfigurasi ini bertujuan untuk meneruskan permintaan dari jaringan luar yang datang ke IP publik router pada port 80, ke alamat IP privat server lokal di jaringan internal. Misalnya, jika router memiliki alamat IP publik 203.0.113.1, maka permintaan dari luar ke alamat tersebut pada port 80 akan diarahkan ke 192.168.1.10:80. Dengan konfigurasi ini, pengguna dari internet dapat mengakses layanan web server lokal seolah-olah server tersebut berada langsung di internet. Implementasi NAT ini dapat dilakukan pada router menggunakan tools seperti MikroTik atau iptables di Linux, dengan memastikan bahwa firewall tidak memblokir koneksi masuk ke port yang digunakan. Selain itu, port yang digunakan juga harus benar-benar terbuka dan layanan web server berjalan dengan baik di server tujuan.

2. Menurutmu,mana yang lebih penting di terapkan terlebih dahulu di jaringan: NAT atau Firewall? Jelaskan alasanmu.
   Menurut saya, NAT (Network Address Translation) lebih penting untuk diterapkan terlebih dahulu dalam jaringan sebelum firewall. Hal ini dikarenakan NAT berperan sebagai fondasi utama agar perangkat-perangkat dalam jaringan lokal yang menggunakan alamat IP privat dapat terhubung ke internet melalui satu atau beberapa alamat IP publik. Tanpa konfigurasi NAT, perangkat di jaringan internal tidak akan mampu mengakses layanan di luar jaringan karena alamat IP privat tidak dapat dirutekan di internet. NAT juga secara tidak langsung memberikan lapisan perlindungan awal dengan menyembunyikan struktur alamat IP internal dari dunia luar. Sementara itu, firewall memang sangat penting untuk menjaga keamanan jaringan, namun perannya lebih kepada mengatur dan membatasi lalu lintas data yang sudah berjalan. Dengan kata lain, firewall bekerja setelah konektivitas dasar melalui NAT sudah tersedia. Oleh karena itu, dalam proses implementasi jaringan yang terhubung ke internet, NAT sebaiknya diterapkan terlebih dahulu agar jaringan memiliki akses keluar, dan selanjutnya firewall dapat dikonfigurasi untuk mengamankan lalu lintas data yang terjadi.

3. Apa dampak negatif jika router tidak diberi filter firewall sama sekali?
   Jika router tidak diberi filter firewall sama sekali, maka jaringan menjadi rentan terhadap berbagai ancaman keamanan, baik dari dalam maupun luar jaringan. Berikut adalah beberapa dampak negatif yang dapat terjadi:

   Pertama, seluruh lalu lintas data dari luar dapat masuk ke jaringan tanpa pengawasan atau pembatasan, termasuk lalu lintas yang bersifat berbahaya. Hal ini memungkinkan penyerang dari internet untuk melakukan pemindaian port, eksploitasi celah keamanan, atau bahkan masuk ke perangkat di jaringan internal secara langsung.

   Kedua, tidak adanya firewall membuka kemungkinan serangan seperti DDoS (Distributed Denial of Service), yang dapat menyebabkan jaringan menjadi lambat atau bahkan tidak dapat diakses. Selain itu, malware atau worm yang tersebar di inter-

net juga bisa masuk dengan mudah dan menyebar ke seluruh perangkat di jaringan lokal.

Ketiga, kebocoran data bisa terjadi karena tidak ada pengaturan atau kontrol terhadap data yang keluar dari jaringan. Informasi sensitif dapat secara tidak sengaja atau sengaja dikirim ke pihak luar tanpa terdeteksi.

Terakhir, dari sisi manajemen jaringan, tanpa firewall, administrator tidak memiliki alat untuk membatasi akses berdasarkan IP, port, atau protokol, sehingga sulit untuk mengendalikan siapa yang boleh mengakses apa. Hal ini dapat menyebabkan penyalahgunaan sumber daya jaringan dan turunnya performa jaringan secara keseluruhan.

Dengan demikian, tidak menggunakan firewall pada router sama saja dengan membiarkan jaringan terbuka sepenuhnya terhadap berbagai ancaman, yang dapat membahayakan integritas, kerahasiaan, dan ketersediaan sistem informasi di dalamnya.