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

Laporan Sementara
Praktikum Jaringan Komputer

Firewall dan NAT

Gilang Gallan Indrana - 5024231030

31 Mei 2025

1 Pendahuluan

1.1 Latar Belakang

Dalam era digital yang semakin berkembang, kebutuhan akan jaringan komputer yang aman dan efisien menjadi sangat penting, terutama seiring meningkatnya ketergantungan individu maupun organisasi terhadap koneksi internet. Namun, konektivitas global ini tidak lepas dari berbagai risiko seperti pencurian data, serangan siber, dan eksploitasi sistem oleh pihak yang tidak bertanggung jawab. Oleh karena itu, dibutuhkan sistem proteksi yang dapat menjaga integritas jaringan sekaligus mengatur lalu lintas data yang masuk dan keluar. Salah satu teknologi fundamental yang berperan dalam hal ini adalah firewall, yang berfungsi sebagai pengendali akses antar jaringan berdasarkan aturan tertentu. Dengan adanya firewall, administrator jaringan dapat memfilter data berdasarkan alamat IP, port, dan protokol, serta mencegah akses ilegal ke sistem. Selain firewall, teknologi Network Address Translation (NAT) juga memiliki peran vital dalam manajemen jaringan modern. NAT memungkinkan banyak perangkat di dalam jaringan lokal menggunakan satu alamat IP publik untuk mengakses internet, sehingga sangat membantu dalam menghemat alokasi IP publik yang terbatas. Tidak hanya efisien dari sisi teknis, NAT juga memberikan perlindungan tambahan dengan menyembunyikan struktur jaringan internal dari dunia luar. Salah satu implementasi NAT yang paling umum digunakan adalah Port Address Translation (PAT), di mana banyak koneksi dibedakan berdasarkan port, memungkinkan banyak perangkat berbagi satu IP publik. Dalam praktiknya, NAT biasanya dikombinasikan dengan firewall untuk menciptakan sistem jaringan yang aman, stabil, dan efisien. Sebagai pelengkap, fitur Connection Tracking semakin memperkuat sistem keamanan jaringan dengan melacak status koneksi antar perangkat. Fitur ini memungkinkan firewall untuk mengenali apakah suatu paket merupakan koneksi baru, koneksi sah yang sedang berlangsung, atau bahkan koneksi tidak valid yang harus diblokir. Dengan adanya connection tracking, proses filtering dan NAT menjadi lebih cerdas dan tepat sasaran. Oleh karena itu, pemahaman mengenai firewall, NAT, dan connection tracking sangat penting bagi setiap administrator jaringan untuk membangun sistem yang mampu memenuhi kebutuhan konektivitas sekaligus menjamin keamanan informasi di era serba terkoneksi ini.

1.2 Dasar Teori

Dalam infrastruktur jaringan komputer, Firewall dan Network Address Translation (NAT) merupakan dua komponen utama yang memiliki peran krusial dalam menjaga keamanan serta mengatur lalu lintas data antar jaringan internal dan eksternal. Firewall berfungsi sebagai sistem pengamanan yang memfilter lalu lintas jaringan berdasarkan aturan tertentu, layaknya penjaga gerbang digital yang menentukan apakah suatu data diperbolehkan masuk atau keluar dari jaringan. Firewall bisa dikonfigurasi untuk menerima (accept), menolak (reject), atau mengabaikan (drop) lalu lintas data berdasarkan parameter seperti alamat IP, nomor port, dan jenis protokol. Seiring perkembangan teknologi, firewall hadir dalam berbagai jenis, mulai dari packet filtering yang hanya memeriksa header data, hingga Next Generation Firewall (NGFW) yang mampu melakukan deep packet inspection dan mengenali konten terenkripsi. Peran firewall sangat penting untuk mencegah akses ilegal, serangan siber, hingga penyebaran malware dalam jaringan lokal. Di sisi lain, NAT (Network Address Translation) merupakan mekanisme penting yang digunakan untuk mengatasi keterbatasan jumlah alamat IP publik di dunia. NAT bekerja dengan menerjemahkan alamat IP privat yang digunakan dalam jaringan

lokal menjadi alamat IP publik ketika perangkat mengakses internet, dan sebaliknya. Proses ini memungkinkan banyak perangkat di jaringan internal berbagi satu IP publik untuk koneksi internet. NAT hadir dalam beberapa varian, seperti static NAT (one-to-one mapping), dynamic NAT (mengambil IP dari pool), dan PAT (Port Address Translation) yang paling efisien karena memungkinkan banyak perangkat menggunakan satu IP publik dengan membedakan setiap koneksi berdasarkan port. Fungsi NAT sangat penting terutama dalam lingkungan rumah dan kantor, karena tidak hanya menghemat penggunaan IP publik, tetapi juga menambah lapisan keamanan dengan menyembunyikan struktur jaringan internal dari dunia luar. Sebagai pelengkap fungsi firewall dan NAT, terdapat fitur Connection Tracking yang memungkinkan sistem mencatat dan mengenali status dari setiap koneksi yang lewat. Connection tracking bekerja secara stateful, mencatat informasi penting seperti alamat IP sumber dan tujuan, port, protokol, serta status koneksi (baru, diterima, tidak valid, dsb). Dengan informasi ini, firewall dapat mengambil keputusan lebih akurat dan efisien misalnya, langsung mengizinkan paket balasan dari koneksi yang sah tanpa memeriksa ulang seluruh aturan. Connection tracking juga sangat penting dalam implementasi NAT, karena memastikan setiap alur koneksi dapat ditelusuri dengan tepat agar data kembali ke perangkat yang benar. Secara keseluruhan, sinergi antara firewall, NAT, dan connection tracking membentuk sistem pertahanan dan pengelolaan jaringan yang kuat, efisien, dan aman dari berbagai ancaman eksternal.

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?

   Jika ingin mengakses web server lokal (dengan IP 192.168.1.10 dan berjalan di port 80) dari jaringan luar seperti internet, maka konfigurasi NAT jenis Destination NAT (dst-nat) atau yang lebih dikenal dengan port forwarding perlu dilakukan di router yang terhubung ke jaringan publik. NAT berfungsi untuk menerjemahkan alamat IP privat yang digunakan di jaringan lokal menjadi alamat IP publik yang dikenali oleh jaringan luar, dan sebaliknya. Dalam kasus ini, ketika ada permintaan dari internet yang ditujukan ke IP publik router pada port 80, router harus diarahkan untuk meneruskannya ke alamat IP lokal server (192.168.1.10) pada port yang sama. Konfigurasi ini sangat penting karena alamat IP 192.168.1.10 adalah bagian dari alamat IP privat (RFC 1918) dan tidak dapat diakses langsung dari internet. Oleh karena itu, router bertindak sebagai perantara yang "membuka jalan" dari dunia luar ke server lokal dengan cara meneruskan lalu lintas yang masuk ke port yang ditentukan. Hal ini biasanya dilakukan untuk keperluan seperti hosting website pribadi, layanan FTP, atau aplikasi lain yang ingin diakses dari luar jaringan lokal. Tanpa konfigurasi NAT ini, permintaan dari luar jaringan tidak akan tahu ke mana harus diarahkan karena tidak ada peta yang menunjukkan bahwa permintaan tersebut sebenarnya ditujukan ke IP lokal tertentu. Maka dari itu, penerapan destination NAT menjadi syarat utama untuk menjembatani komunikasi antara jaringan publik dengan server privat.

   Sumber: Citraweb. "Forwarding Dengan Fitur NAT." `https://citraweb.com/artikel_lihat.php?id=75` Cloudflare. "What is NAT?" `https://www.cloudflare.com/learning/network-layer/what-is-nat/`

2. Menurutmu, mana yang lebih penting diterapkan terlebih dahulu di jaringan: NAT atau Firewall?

Jelaskan alasanmu.

Firewall merupakan komponen yang lebih penting dan sebaiknya diterapkan terlebih dahulu dalam perancangan jaringan sebelum NAT. Hal ini karena firewall berfungsi sebagai garis pertahanan utama yang mengatur dan mengamankan lalu lintas data yang masuk dan keluar dari jaringan. Firewall melakukan penyaringan berdasarkan aturan yang ditentukan administrator, seperti alamat IP, port, dan protokol, serta memastikan bahwa hanya lalu lintas yang sah dan diizinkan yang dapat melewati jaringan. Dengan kata lain, firewall melindungi jaringan dari akses yang tidak sah, serangan malware, peretasan, dan berbagai ancaman siber lainnya. Sementara itu, NAT (Network Address Translation) berfungsi untuk menerjemahkan alamat IP privat ke alamat IP publik agar perangkat dalam jaringan lokal bisa terhubung ke internet. Fungsi utama NAT adalah penghematan IP publik dan memungkinkan komunikasi antara jaringan privat dan jaringan publik. Meskipun NAT secara tidak langsung memberikan efek perlindungan dengan menyembunyikan struktur internal jaringan, ia tidak mampu melakukan deteksi atau pemblokiran terhadap lalu lintas berbahaya. Oleh karena itu, dalam skala keamanan dan urgensi, firewall memegang peran yang lebih penting sebagai filter dan penjaga gerbang jaringan. Mengutamakan firewall memastikan bahwa semua koneksi yang diizinkan oleh NAT sudah terlebih dahulu melewati proses verifikasi dan pengamanan, sehingga jaringan tidak hanya fungsional tetapi juga aman sejak awal.

Sumber: Cloudflare. “What is a Firewall?” https://www.cloudflare.com/learning/ddos/glossary/firewall/ Cyberhub. “Fungsi, Manfaat, dan Jenis Firewall.” https://cyberhub.id/pengetahuan-dasar/fungsi-manfaat-firewall

3. Apa dampak negatif jika router tidak diberi filter firewall sama sekali?
Jika sebuah router tidak dilengkapi dengan filter firewall, maka seluruh lalu lintas data baik yang sah maupun berbahaya akan dibiarkan melewati jaringan tanpa pengawasan atau kontrol. Hal ini sangat berisiko karena membuka celah besar bagi berbagai jenis serangan, seperti unauthorized access (akses ilegal), port scanning, DDoS attack (serangan beruntun yang melumpuhkan jaringan), hingga pencurian data. Tanpa firewall, router tidak akan bisa membedakan antara koneksi yang berasal dari pengguna sah dan koneksi dari pihak berbahaya yang mencoba menyusup atau mengambil alih sistem. Selain itu, router yang tidak memiliki filter firewall akan membiarkan semua layanan terbuka dapat diakses dari luar, termasuk layanan yang seharusnya hanya tersedia secara lokal seperti SSH, Telnet, atau web interface administrasi. Hal ini bisa dimanfaatkan oleh penyerang untuk mengeksploitasi kerentanan sistem dan mendapatkan akses penuh ke dalam jaringan. Bahkan perangkat-perangkat seperti printer, kamera CCTV, atau server lokal dapat menjadi target serangan apabila tidak dilindungi oleh aturan firewall. Oleh karena itu, absennya firewall bukan hanya menurunkan keamanan jaringan, tetapi juga memperbesar risiko kerugian data, kerusakan sistem, dan kompromi terhadap privasi pengguna. Firewall berperan penting dalam memblokir akses yang tidak sah dan mendeteksi lalu lintas yang mencurigakan sejak awal.

Sumber:

Kaspersky. “What is a firewall and why do you need one?” https://www.kaspersky.com/resource-center/definitions/what-is-a-firewall Kominfo - Ditjen Aptika. “Keamanan Jaringan Internet dan Firewall.” https://aptika.kominfo.go.id/2017/06/keamanan-jaringan-internet-da