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

Laporan Sementara
Praktikum Jaringan Komputer

Modul Firewall & NAT

Muhammad Zia Alhambra - 5024231059

2025

1 Pendahuluan

1.1 Latar Belakang

Dalam pengembangan dan pemeliharaan jaringan komputer, terutama yang terhubung ke Internet, dua konsep penting memainkan peran sentral dalam memastikan efisiensi operasional dan keamanan: firewall dan Network Address Translation (NAT). Seiring dengan meningkatnya permintaan akan perangkat yang terhubung ke Internet, administrator jaringan harus menghadapi dua tantangan utama—kekurangan alamat IP dan meningkatnya ancaman siber. NAT dan firewall, meskipun memiliki tujuan yang berbeda secara fundamental, sering kali diimplementasikan bersama dalam gateway jaringan atau router untuk mengatasi masalah ini secara efektif.

Firewall adalah mekanisme keamanan jaringan yang dirancang untuk memantau dan mengatur lalu lintas yang masuk dan keluar dari jaringan berdasarkan kumpulan aturan yang telah ditentukan. Berperan sebagai penghalang pelindung antara jaringan internal yang tepercaya dan jaringan eksternal yang tidak tepercaya (seperti Internet), firewall memainkan peran kritis dalam mencegah akses tidak sah, mendeteksi aktivitas berbahaya, dan menegakkan kebijakan keamanan organisasi. Firewall dapat diimplementasikan dalam bentuk perangkat keras, perangkat lunak, atau kombinasi keduanya. Tergantung pada kompleksitas dan desainnya, firewall tersedia dalam beberapa jenis, termasuk firewall penyaringan paket, firewall inspeksi status, firewall lapisan aplikasi, dan firewall generasi berikutnya (NGFW).

1.2 Dasar Teori

Firewall penyaring paket beroperasi dengan memeriksa header setiap paket dan membuat keputusan penyaringan berdasarkan atribut seperti alamat IP sumber dan tujuan, nomor port, serta protokol transportasi yang digunakan. Firewall berstatus (stateful firewalls) lebih canggih, karena tidak hanya memeriksa header paket tetapi juga memelihara status koneksi aktif, memungkinkan mereka membuat keputusan yang lebih sadar konteks. Firewall lapisan aplikasi memperdalam pemeriksaan ini dengan menganalisis lalu lintas yang terkait dengan aplikasi tertentu, seperti HTTP atau FTP, memungkinkan deteksi ancaman yang lebih canggih. Solusi paling komprehensif, yang dikenal sebagai Next- Generation Firewalls, menggabungkan fungsi firewall tradisional dengan kemampuan canggih seperti sistem deteksi/pencegahan intrusi (IDS/IPS), pemeriksaan paket mendalam, dan intelijen ancaman real-time.

Dasar teoretis firewall terletak pada penggunaan logika berbasis aturan. Aturan-aturan ini, sering kali disusun sebagai daftar kontrol akses (ACL), mendefinisikan kondisi di mana paket diizinkan atau ditolak untuk melewati. Firewall menerapkan logika Boolean untuk mengevaluasi apakah paket tertentu sesuai dengan aturan, sehingga menerapkan postur keamanan yang diinginkan. Mereka juga dapat mempertahankan tabel koneksi saat ini untuk membedakan antara sesi baru dan yang sudah ada, terutama dalam model inspeksi berbasis status.

Meskipun firewall berfokus pada pengendalian lalu lintas untuk tujuan keamanan, Network Address Translation (NAT) menangani tantangan yang berbeda: ketersediaan alamat IPv4 yang terbatas. NAT memungkinkan beberapa perangkat di jaringan lokal pribadi (LAN) mengakses internet menggunakan satu alamat IP publik. NAT mencapai ini dengan memodifikasi informasi alamat IP dalam header paket saat paket berpindah antara jaringan pribadi dan publik. Ada beberapa jenis NAT, termasuk static NAT, dynamic NAT, dan Port Address Translation (PAT), yang juga dikenal sebagai NAT overload.

Static NAT menyediakan pemetaan satu-ke-satu antara alamat IP pribadi dan publik, biasanya digunakan ketika perangkat di jaringan internal perlu diakses dari luar, seperti server web atau email. NAT dinamis mengalokasikan alamat IP publik dari kumpulan alamat yang tersedia ke perangkat internal sesuai kebutuhan, sementara PAT memungkinkan banyak perangkat berbagi satu alamat IP publik dengan membedakan sesi berdasarkan nomor port. Bentuk terakhir ini paling sering digunakan di jaringan rumah dan bisnis kecil karena efisiensinya dalam menghemat alamat IP.

Dari perspektif teoretis, NAT beroperasi dengan memodifikasi bidang sumber atau tujuan dalam header IP dan TCP/UDP paket, sesuai dengan tabel terjemahan yang dikelola oleh router atau perangkat gateway. Meskipun NAT menyediakan lapisan keamanan tidak langsung dengan menyembunyikan alamat IP internal, ini bukanlah fitur keamanan secara langsung; melainkan alat untuk mengelola penomoran IP dan memfasilitasi konektivitas. Oleh karena itu, mengandalkan NAT saja tanpa menerapkan kebijakan firewall akan mengekspos jaringan pada risiko keamanan yang signifikan.

Kombinasi fungsi NAT dan firewall umum ditemukan di sebagian besar router komersial dan perangkat keamanan. Dalam konfigurasi semacam itu, NAT mengelola penerjemahan alamat untuk koneksi keluar, sementara firewall menentukan lalu lintas mana yang diizinkan atau ditolak berdasarkan aturan keamanan. Bersama-sama, keduanya memberikan manfaat ganda: NAT memastikan penggunaan alamat IP yang efisien dan skalabel, sementara firewall menerapkan perbatasan keamanan yang melindungi sistem internal dari ancaman eksternal.

Namun, jika router tidak memiliki kemampuan penyaringan firewall sama sekali, jaringan menjadi sangat rentan terhadap berbagai ancaman. Tanpa penyaringan paket atau kontrol akses, lalu lintas berbahaya dari internet dapat mencapai perangkat internal tanpa batasan. Hal ini dapat menyebabkan akses tidak sah, kebocoran data, atau penyebaran malware dan ransomware di dalam jaringan. Selain itu, ketidakhadiran kontrol lalu lintas keluar berarti perangkat yang terkompromi di dalam jaringan dapat dengan mudah mentransmisikan data sensitif atau berkomunikasi dengan server komando dan kontrol di luar organisasi, memperburuk dampak dari pelanggaran keamanan apa pun.

Kesimpulannya, baik NAT maupun firewall merupakan komponen yang tak tergantikan dalam arsitektur jaringan modern. NAT memainkan peran vital dalam memfasilitasi komunikasi jaringan pribadi dengan internet publik sambil menghemat ruang alamat IP global. Di sisi lain, firewall sangat penting untuk menerapkan kebijakan keamanan dan melindungi jaringan dari ancaman internal maupun eksternal. Bersama-sama, keduanya membentuk lapisan dasar dari desain jaringan yang tangguh.

2 Tugas Pendahuluan

1. Untuk mengakses server web lokal (IP: 192.168.1.10, port 80) dari jaringan eksternal, Anda perlu mengonfigurasi Port Forwarding pada router Anda, yang merupakan jenis Destination NAT (DNAT).

   Langkah konfigurasi:

   - Masuk ke antarmuka admin router Anda.
   - Navigasi ke bagian Port Forwarding atau NAT.
   - Buat aturan baru:
     - Port Eksternal: 80
     - Protokol: TCP (karena HTTP menggunakan TCP)

- IP Internal: 192.168.1.10
- Port Internal: 80

- Pastikan alamat IP publik router bersifat statis atau gunakan Dynamic DNS (DDNS) jika tidak.

Referensi:

- Kurose, J. F., & Ross, K. W. (2021). Computer Networking: A Top-Down Approach (8th ed.). Pearson.
- Cisco. Port Forwarding and NAT Overview

2. Firewall harus diimplementasikan terlebih dahulu. Firewall adalah mekanisme keamanan yang mengontrol lalu lintas berdasarkan aturan (izinkan/tolak). NAT, meskipun menawarkan keamanan terbatas melalui penyamaran, pada dasarnya adalah metode untuk penerjemahan alamat, bukan penegakan keamanan. Jika Anda mengimplementasikan NAT tanpa firewall, lalu lintas yang tidak difilter masih dapat mencapai sistem internal melalui port yang diteruskan atau celah keamanan. Firewall melindungi jaringan Anda terlepas dari jenis alamat (publik atau privat), sementara NAT hanya memberikan perlindungan tidak langsung yang minimal.

   Referensi:

   - Stallings, W. (2013). Network Security Essentials: Applications and Standards (5th ed.). Pearson.
   - Pfleeger, C. P., & Pfleeger, S. L. (2015). Security in Computing (5th ed.). Pearson.

3. Berikut dampak negatif bila router tidak diberi filter firewall:

   (a) Peningkatan Kerentanan Terhadap Serangan:
   - Tanpa penyaringan paket, setiap koneksi masuk (misalnya, pemindaian port, uji coba malware) dapat mencapai perangkat internal.
   - Contoh: Serangan eksploit jarak jauh, serangan DoS, login paksa.

   (b) Akses Tidak Sah:
   - Layanan terbuka (seperti SSH, HTTP, SMB) mungkin dapat diakses, terutama jika NAT/pengalihan port dikonfigurasi.

   (c) Bocornya Data:
   - Tanpa kontrol atas lalu lintas keluar, informasi sensitif dapat dikirimkan oleh malware atau perangkat yang terkompromi.

   (d) Penyebaran Worm Jaringan atau Malware dengan Mudah:
   - Tanpa segmentasi atau penegakan aturan, malware dapat bergerak secara lateral antar perangkat.

   (e) Tidak Ada Logging atau Peringatan:
   - Tanpa firewall, Anda tidak memiliki visibilitas terhadap lalu lintas mencurigakan atau berbahaya.

   Referensi:

- Northcutt, S. (2005). Inside Network Perimeter Security (2nd ed.). Sams Publishing.
- NIST SP 800-41 Rev. 1 - Guidelines on Firewalls and Firewall Policy