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

Laporan Sementara
Praktikum Jaringan Komputer

Modul Firewall & NAT

Ignasius Deva - 5024231003

2025

1 Pendahuluan

1.1 Latar Belakang

Perkembangan teknologi dan komunikasi telah membuat sebuah kemudahan untuk semua orang dengan mudahnya mengakses internet dan berkomunikasi jarak jauh hanya dengan beberapa detik saja. Namun dibalik kemudahan tersebut terdapat ancaman yang serius yang dapat dieksploitasi oleh orang-orang tertentu dengan maksud yang buruk, hal ini disebut hacking. Untuk dapat menanggulangi masalah cyber seperti ini, dibutuhkan adanya proteksi agar data kita di internet dapat terjaga dengan aman. Dengan adanya sistem pertahanan seperti Firewall dan Network Address Translation (NAT) sebagai proteksi di internet, mereka sudah menjadi bagian yang krusial di dalam arsitektur jaringan modern.

1.2 Dasar Teori

Firewall adalah sistem keamanan jaringan yang bertugas mengatur dan mengontrol traffic data dari sebuah jaringan dengan tujuan untuk menjaga keamanan data. Fungsinya dari firewall ini secara sistematis adalah memilah suatu koneksi dapat diteruskan, ditolak, atau diabaikan. Firewall modern zaman sekarang berkembang dari Access Control List (ACL) yang hanya bisa menyaring berdasarkan alamat IP atau port saja, tetapi dengan Next Generation Firewall (NGFW) sekarang firewall ini mampu melakukan investigasi pada tiap packet hingga data enkripsinya. Action yang dapat dilakukan oleh sebuah firewall adalah : Accept (mengizinkan traffic untuk melewati jaringan), Reject (menolak traffic untuk melalui jaringan dan memberikan error massage), dan Drop (menolak traffic tanpa memberikan error massage).

Network Address Translation (NAT) adalah teknik pengubahan alamat IP dalam paket data yang memungkinkan banyak perangkat dalam jaringan lokal menggunakan satu alamt IP publik untuk mengakses internet. Nat ini sangat penting dalam mengatasi keterbatasannya jumlah IP publik (IPv4). Jenis-jenis dari NAT meliputi : Static NAt (1 IP lokal dipetakan ke 1 IP publik secara tetap), Dynamic NAT (IP lokal yang dipetakan secara dinamis ke IP berbagi satu IP publik dengan membedakan koneksi berdasarkan nomor port. Nat ini umumnya dijalankan oleh router dan membutuhkan traslation table untuk mengtranslasi koneksi agar tetap lancar dan tidak tertukar.

Connection Tracking adalah mekanisme yang digunakan untuk memantau kinerja dan status pada setiap koneksi pada firewall dan NAT. Sistem ini menyimpan informasi penting dari koneksi seperti alamat IP, nomor port, protokol, serta status koneksi (connection state). Dengan mengetahui status koneksi, sistem dapat secara otomatis mengizinkan paket yang baik, dan menolak koneksi baru yang mencurigakan. Connection tracking membantu dalam meningkatkan keamanan melalui firewall, mempermudah proses NAT dengan pelacakan koneksi aktif, mengurangi beban pemrosesan paket yang tidak relevan, dan memberikan kontrol lebih detail terhadap trafik 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 ke local dan port 80 dari jaringan luar,harus dilakukan konfigurasi port forwarding atau Destination NAT pada router (meneruskan request dari IP publik ke IP private). Beberapa konfig parameter yang diubah di Firewall > NAT pada server adalah Chain to dstnat, protocol to tcp, dst.port to 80, action to dst-nat, To Address to 192.168.1.10, To Ports to 80.
Referensi : https://www.tembolok.id/cara-setting-akses-server-lokal-menggunakan-jaringan-internet

2. Menurutmu, mana yang lebih penting diterapkan terlebih dahulu di jaringan: NAT atau Firewall? Jelaskan alasanmu.
-.Sebaiknya firewall diterapkan terlebih dahulu karena firewall berfungsi sebagai pengaman utama yang mengfilter traffic. Tanpa adanya firewall jaringan akan rentan terhadap berbagai ancaman seperti malware, DDos, dst. NAT sendiri berfungsi untuk menerjemahkan alat IP private ke publik sehingga bukan merupakan prioritas utama (dibanding dengan firewall).
Referensi : https://www.slideshare.net/slideshow/firewall-network-address-translation-nat-proxy-server/40897624

3. Apa dampak negatif jika router tidak diberi filter firewall sama sekali?
-.Jika router tidak diberi filter firewall, jaringan menjadi rentan terhadap akses tidak sah, malware, dan serangan DDoS. Selain itu, lalu lintas berbahaya bisa masuk tanpa pengawasan, menyebabkan konsumsi bandwidth berlebih dan potensi pelanggaran kebijakan keamanan. Firewall penting untuk melindungi jaringan dari ancaman tersebut.
Referensi : https://id.safetydetectives.com/blog/apa-itu-firewall-dan-bisakah-dia-melindungi-komputer-anda-sepenuhnya

Berikan referensi dari jawaban yang kamu berikan