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

Laporan Sementara
Praktikum Jaringan Komputer

Firewall dan NAT

Hilmy Abid Syafi Abiyyu - 5024231029

2025

1 Pendahuluan

1.1 Latar Belakang

Keamanan dan pengelolaan lalu lintas data dalam jaringan komputer adalah hal penting yang harus diperhatikan untuk menjaga stabilitas dan integritas sebuah sistem. Salah satu komponen penting dalam sistem jaringan adalah firewall, yang berfungsi sebagai pengontrol lalu lintas data masuk dan keluar berdasarkan aturan tertentu. Penerapan filter rules seperti accept, drop, dan reject, administrator jaringan dapat menentukan jenis koneksi apa saja yang diizinkan atau diblokir untuk meningkatkan keamanan jaringan.

Network Address Translation (NAT) juga berperan penting dalam manajemen jaringan, terutama dalam menghubungkan jaringan lokal dengan jaringan publik. Fitur seperti masquerade memungkinkan beberapa perangkat dalam jaringan lokal menggunakan satu alamat IP publik untuk mengakses internet, sementara port forwarding digunakan untuk mengarahkan koneksi dari luar ke layanan tertentu di dalam jaringan. NAT tidak hanya memudahkan koneksi, tetapi juga menambah lapisan keamanan dengan menyembunyikan struktur internal jaringan.

Untuk memastikan keamanan lebih lanjut, sistem jaringan juga memanfaatkan fitur connection tracking yang dapat memantau status koneksi dan membantu dalam pembuatan aturan firewall yang dinamis. Kombinasi fitur-fitur ini dapat melindungi router dari akses luar yang tidak sah, mencegah potensi serangan seperti port scanning atau brute force.

1.2 Dasar Teori

Firewall adalah sistem keamanan jaringan yang berfungsi untuk mengatur dan mengontrol lalu lintas data berdasarkan aturan tertentu yang disebut filter rules. Filter rules terdiri dari tindakan seperti accept, drop, dan reject. Tindakan accept akan mengizinkan paket data melewati firewall, drop akan membuang paket tanpa memberikan respon ke pengirim, sementara reject juga membuang paket tetapi dengan memberikan pesan penolakan. Dengan aturan-aturan ini, firewall mampu memfilter lalu lintas yang diperbolehkan dan yang harus diblokir demi menjaga keamanan sistem jaringan.

Network Address Translation (NAT) adalah teknik yang digunakan untuk mengubah alamat IP sumber atau tujuan dalam paket data saat melalui router, sehingga memungkinkan perangkat-perangkat dalam jaringan lokal untuk berkomunikasi dengan jaringan luar seperti internet. Salah satu jenis NAT adalah masquerade, yang memungkinkan banyak perangkat menggunakan satu alamat IP publik. Selain itu, ada pula port forwarding yang memungkinkan pengalihan koneksi dari luar menuju alamat dan port tertentu dalam jaringan lokal, biasanya digunakan untuk mengakses layanan internal dari luar. NAT juga berkontribusi dalam menyembunyikan struktur internal jaringan dari akses eksternal.

Fitur connection tracking pada firewall digunakan untuk melacak status koneksi jaringan, seperti koneksi baru, koneksi yang sedang aktif, atau koneksi yang sudah ditutup. Firewall dapat membuat keputusan yang lebih cerdas dan dinamis dalam mengelola lalu lintas. Connection tracking dapat dikombinasikan dengan filter rules untuk meningkatkan perlindungan router dari akses luar yang tidak sah.

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?

   Mengakses web server lokal dengan IP 192.168.1.10 dan port 80 dari jaringan luar (internet) dilakukan dengan cara membuat konfigurasi NAT berupa port forwarding atau static NAT di router dengan tujuan agar setiap permintaan dari internet yang masuk ke alamat IP publik router pada port 80 secara otomatis diteruskan ke alamat IP lokal 192.168.1.10 pada port yang sama. Sehingga, server lokal tersebut dapat diakses dari luar jaringan menggunakan alamat IP publik router, walaupun server menggunakan alamat IP private di jaringan internal.

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

   Firewall lebih penting untuk diterapkan terlebih dahulu sebelum NAT. Firewall bertugas memfilter lalu lintas data berdasarkan aturan keamanan yang telah ditentukan, sehingga hanya trafik yang aman dan sah yang diizinkan masuk atau keluar dari jaringan. Fungsinya yaitu sebagai pertahanan utama terhadap berbagai ancaman keamanan seperti serangan dari luar, malware, dan akses tidak sah. NAT berperan dalam mentranslate alamat IP privat ke IP publik untuk memungkinkan komunikasi dengan jaringan luar, tetapi tidak dirancang untuk menangkal serangan. Maka dari itu, firewall harus diaktifkan terlebih dahulu untuk memastikan bahwa semua traffic yang melewati NAT sudah melalui proses penyaringan.

3. Apa dampak negatif jika router tidak diberi filter firewall sama sekali?

   Jika router tidak dilengkapi dengan filter firewall sama sekali, jaringan menjadi rentan terhadap serangan dari luar, semua trafik masuk bisa langsung mencapai device internal tanpa penyaringan, sehingga memungkinkan terjadinya akses ilegal, serangan brute force, penyebaran malware, atau pencurian data. Selain itu, jaringan juga bisa dijadikan bagian dari botnet atau terkena serangan DDoS sehingga bisa merugikan mulai dari kerusakan sistem, hilangnya data, dan terganggunya layanan secara keseluruhan.

Link Referensi Tugas Pendahuluan Nomor 1
Link Referensi Tugas Pendahuluan Nomor 2
Link Referensi Tugas Pendahuluan Nomor 3