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

Laporan Sementara
Praktikum Jaringan Komputer

Firewall dan NAT

Muhammad Jaysyurrahman - 5024231057

2025

1 Pendahuluan

1.1 Latar Belakang

Keamanan jaringan saat ini menjadi perhatian utama bagi banyak organisasi, mengingat semakin banyaknya ancaman yang dapat merusak data dan infrastruktur digital. Salah satu bentuk ancaman yang sering terjadi adalah peretasan, di mana individu atau kelompok yang tidak bertanggung jawab mencoba mengakses sistem jaringan tanpa izin. Oleh karena itu, perlindungan terhadap jaringan internal sangat penting. Firewall dan Network Address Translation (NAT) merupakan dua teknologi dasar yang digunakan untuk meningkatkan keamanan jaringan. Firewall berfungsi sebagai penghalang yang mengontrol lalu lintas yang masuk dan keluar dari jaringan, sedangkan NAT memungkinkan pengelolaan alamat IP yang terbatas dan juga berfungsi menyembunyikan perangkat dalam jaringan lokal dari akses langsung dari luar. Keduanya berperan penting dalam mencegah serangan dan membatasi potensi risiko yang dapat merusak sistem.
Melalui praktikum ini, kita dapat memahami cara mengonfigurasi dan mengelola firewall dan NAT dalam jaringan komputer. Dalam praktiknya, penerapan firewall dan NAT tidak hanya terbatas pada jaringan perusahaan besar, namun juga menjadi kebutuhan penting dalam jaringan rumahan atau kantor. Pemahaman mengenai keduanya sangat relevan mengingat ancaman yang semakin berkembang, seperti peretasan atau serangan DDoS. Oleh karena itu, praktikum ini bertujuan untuk memberikan wawasan yang lebih dalam tentang penerapan kedua teknologi tersebut.

1.2 Dasar Teori

Firewall adalah sistem pengamanan jaringan yang berfungsi untuk memfilter dan mengontrol lalu lintas data yang masuk atau keluar dari suatu jaringan. Secara umum, firewall bekerja dengan memeriksa paket data dan membandingkannya dengan aturan atau kebijakan yang telah ditetapkan. Aturan ini bisa berdasarkan beberapa parameter, seperti alamat IP sumber dan tujuan, port yang digunakan, serta jenis protokol yang terlibat. Firewall memainkan peran yang sangat penting dalam menjaga integritas dan kerahasiaan jaringan dari ancaman eksternal yang dapat merusak sistem informasi.
Secara teknis, firewall bekerja pada berbagai lapisan model OSI (Open Systems Interconnection), khususnya pada lapisan transport dan jaringan. Ada beberapa jenis firewall yang sering digunakan, yang dibedakan berdasarkan cara mereka memeriksa dan memfilter lalu lintas data:
1. Packet Filtering Firewall
Jenis firewall ini bekerja dengan memeriksa setiap paket data yang melewati jaringan berdasarkan aturan yang telah ditentukan. Aturan ini bisa berupa alamat IP sumber dan tujuan, nomor port, dan jenis protokol (TCP, UDP, ICMP, dll.). Meskipun sederhana, packet filtering firewall memiliki keterbatasan dalam memeriksa status koneksi, sehingga lebih rentan terhadap serangan yang lebih kompleks.
2. Stateful Inspection Firewall
Berbeda dengan packet filtering, stateful inspection firewall melacak status setiap koneksi yang sedang berlangsung. Ini memungkinkan firewall untuk memeriksa konteks dari paket yang diterima, memastikan apakah paket tersebut merupakan bagian dari koneksi yang sah. Sebagai contoh, jika sebuah perangkat di dalam jaringan lokal melakukan koneksi ke server di luar, stateful firewall akan memastikan bahwa respons dari server yang masuk adalah bagian dari koneksi yang sah dan bukan

dari serangan.

3. Proxy Firewall

Proxy firewall bekerja dengan cara menyembunyikan alamat asli perangkat di dalam jaringan lokal dari perangkat yang berada di luar. Proxy bertindak sebagai perantara antara pengguna dan server yang ingin diakses. Dengan menggunakan proxy, alamat IP asli perangkat di dalam jaringan lokal tidak terlihat oleh perangkat luar, sehingga menambah lapisan perlindungan terhadap potensi ancaman yang datang dari luar.

Firewall juga dapat dikategorikan menjadi software firewall dan hardware firewall. Software firewall lebih sering digunakan pada perangkat individu atau server, sedangkan hardware firewall lebih banyak digunakan pada perimeter jaringan untuk melindungi seluruh jaringan.

Network Address Translation (NAT) adalah teknik yang digunakan untuk menggantikan alamat IP di header paket data saat data tersebut melewati router atau firewall. NAT berfungsi untuk menghubungkan perangkat di jaringan privat (seperti jaringan lokal) dengan jaringan publik (internet), tanpa harus memberikan setiap perangkat di jaringan lokal alamat IP publik yang unik. NAT memungkinkan beberapa perangkat dalam jaringan lokal untuk berbagi satu alamat IP publik yang digunakan untuk mengakses internet.

Ada beberapa jenis NAT yang digunakan, di antaranya: Static NAT

Static NAT secara langsung memetakan satu alamat IP privat ke satu alamat IP publik. Ini berarti bahwa alamat IP privat yang ditentukan akan selalu menggunakan alamat IP publik yang sama setiap kali terhubung ke internet. Static NAT sering digunakan untuk perangkat yang membutuhkan akses langsung ke internet, seperti server web yang berada di dalam jaringan lokal.

Dynamic NAT

Berbeda dengan static NAT, dynamic NAT memungkinkan beberapa perangkat di jaringan lokal untuk menggunakan satu alamat IP publik, tetapi alamat IP publik yang digunakan bisa bervariasi. Alamat IP publik yang tersedia akan dipilih secara dinamis dari kumpulan alamat IP yang telah ditentukan oleh administrator jaringan.

Port Address Translation (PAT)

PAT, juga dikenal dengan istilah "overloading," adalah jenis NAT yang memungkinkan banyak perangkat di dalam jaringan lokal untuk berbagi satu alamat IP publik. PAT membedakan perangkat berdasarkan nomor port yang digunakan. Sebagai contoh, meskipun beberapa perangkat menggunakan alamat IP publik yang sama, mereka akan dibedakan dengan nomor port yang berbeda pada router atau firewall. PAT adalah jenis NAT yang paling sering digunakan pada jaringan rumah atau kantor kecil.

Secara keseluruhan, NAT memberikan beberapa keuntungan, seperti penghematan alamat IP publik yang terbatas dan peningkatan keamanan. Dengan menggunakan NAT, perangkat di jaringan lokal tidak dapat langsung diakses dari internet, sehingga menambah lapisan perlindungan terhadap potensi serangan dari luar.

Kombinasi firewall dan NAT dapat memberikan perlindungan yang lebih komprehensif bagi jaringan. Firewall membatasi dan memfilter akses yang tidak sah, sementara NAT menjaga agar perangkat di dalam jaringan privat tetap tersembunyi dari akses langsung. Penggunaan kedua teknologi ini dalam desain jaringan memberikan lapisan pengamanan yang lebih kuat, mencegah potensi ancaman dari luar untuk mengakses dan merusak sistem internal. Oleh karena itu, penting bagi administrator jaringan untuk mengonfigurasi dan mengelola firewall serta NAT dengan tepat agar jaringan tetap aman dan efisien.

2 Tugas Pendahuluan

Bagian ini berisi jawaban dari tugas pendahuluan yang telah anda kerjakan, beserta penjelasan dari jawaban tersebut

1. Untuk mengakses web server lokal yang berada di alamat IP 192.168.1.10 pada port 80 dari jaringan luar, perlu dilakukan konfigurasi NAT (Network Address Translation) pada router atau perangkat firewall. NAT yang digunakan adalah Port Forwarding (atau juga dikenal dengan NAT statis). Konfigurasi ini akan memetakan port 80 pada alamat IP publik router ke alamat IP privat 192.168.1.10 di jaringan lokal. Dengan demikian, setiap permintaan yang masuk ke alamat IP publik router pada port 80 akan diteruskan ke server lokal tersebut. Secara teknis, administrator jaringan dapat mengonfigurasi NAT dengan perintah seperti ip nat inside source static tcp 192.168.1.10 80 interface GigabitEthernet0/0 80, di mana interface GigabitEthernet0/0 adalah interface yang terhubung ke jaringan luar.

2. Dalam pengaturan jaringan, firewall sebaiknya diterapkan terlebih dahulu dibandingkan dengan NAT. Firewall berfungsi untuk melindungi jaringan dari akses yang tidak sah, serangan, dan ancaman lainnya dari luar jaringan, dengan cara menyaring lalu lintas yang masuk dan keluar berdasarkan kebijakan yang ditetapkan. Firewall mengamankan jaringan dari potensi kebocoran informasi atau kerusakan akibat perangkat yang tidak terotorisasi. Sedangkan NAT, meskipun berguna untuk memungkinkan perangkat di jaringan lokal untuk mengakses internet menggunakan satu alamat IP publik, lebih berfokus pada pengaturan lalu lintas data dalam konteks IP. Tanpa perlindungan yang memadai dari firewall, implementasi NAT saja tidak cukup untuk mencegah potensi ancaman dari luar jaringan. Oleh karena itu, firewall harus diprioritaskan untuk diterapkan terlebih dahulu.

3. Jika router tidak diberi filter firewall sama sekali, dampaknya dapat sangat merugikan bagi keamanan jaringan. Tanpa firewall, router tidak memiliki mekanisme untuk memblokir lalu lintas yang tidak diinginkan atau berbahaya, sehingga jaringan menjadi rentan terhadap serangan dari luar, seperti Distributed Denial of Service (DDoS), port scanning, atau intrusi dari pihak yang tidak sah. Selain itu, perangkat yang terhubung ke jaringan dapat menjadi sasaran empuk untuk malware atau virus yang dapat merusak atau mencuri data sensitif. Tanpa adanya perlindungan yang memadai, integritas dan kerahasiaan data yang dikirimkan melalui jaringan dapat terancam, yang pada akhirnya dapat mengarah pada kerugian finansial dan reputasi yang serius. Oleh karena itu, pemasangan filter firewall di router sangat penting untuk menjaga keamanan dan privasi jaringan.