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

Laporan Sementara
Praktikum Jaringan Komputer

Firewall& NAT

Muhammad Risang Radityatama - 5024231028

2025

1 Pendahuluan

1.1 Latar Belakang

Kemampuan jaringan dalam menghubungkan sebuah perangkat atau komputer dengan perangkat lainnya memberikan banyak keuntungan dan kemudahan dalam hal komunikasi dan transfer file. Keuntungan-keuntungan ini membuat jaringan diminati oleh banyak orang dan organisasi untuk memudahkan pekerjaan. Namun, keuntungan yang ditawarkan oleh jaringan komputer seperti kemampuan untuk mengirimkan informasi dan file dari jarak jauh juga dapat berbalik menjadi ancaman bila disalahgunakan. Seseorang yang berniat jahat dapat memanfaatkan jaringan untuk menyusupkan malware atau spyware yang dapat mencuri data melalui jaringan sebagai perantara. Maka dari itu, dalam sebuah sistem jaringan diperlukan sebuah sistem keamanan untuk mencegah hal tersebut. Firewall ada sebagai jawaban dari permasalahan ini. Firewall dapat mengatur koneksi dan komunikasi yang terjadi pada jaringan sehingga dapat melakukan pemblokiran akses dari alamat yang mencurigakan.

Selain dapat mengundang orang dengan niat yang tidak baik, popularitas teknologi jaringan membuat pengguna internet semakin banyak. Semakin banyak pengguna yang menggunakan jaringan dalam internet tentu saja membuat alamat IP yang ditawarkan menjadi semakin sedikit. Untuk menyiasati hal ini, cara yang dapat dilakukan salah satunya adalah dengan menggunakan NAT. NAT (network address translation) merupakan sebuah proses yang dapat membuat satu jaringan lokal hanya perlu memiliki satu alamat IP publik untuk terhubung ke internet. Dengan begitu, maka jaringan lokal yang terdiri dari banyak perangkat hanya akan memerlukan satu alamat IP sehingga menghemat penggunaan alamat. Dalam teknoogi jaringan modern, pemahaman akan firewall dan NAT menjadi suatu hal yang penting karena berkaitan dengan keamanan data dan perancangan sistem jaringan. Maka dari itu, dilaksanakan praktikum jaringan komputer modul firewall dan NAT untuk lebih memahami mengenai bagaimana firewall dan NAT bekerja beserta cara mengaplikasikannya.

1.2 Dasar Teori

Firewall merupakan sebuah perangkat keamanan jaringan yang dapat memisahkan antara jaringan internal yang terpercaya dengan jaringan luar/external yang dianggap berbahaya atau tidak dapat dipercaya keamanannya. Firewall memisahkan jaringan internal dengan jaringan external berdasarkan preset atau aturan yang telah ditetapkan. Firewall dapat berupa hardware maupun software.Cara kerja firewall sedikit berbeda antar jenisnya, namun secara umum firewall bekerja dengan memeriksa setiap paket data yang keluar dan masuk pada jaringan lalu membandingkan isinya dengan aturan-aturan yang sudah ditentukan oleh pengguna/operator. Adapun jenis-jenis firewall yaitu stateless firewall atau disebut juga sebagai packet filtering, stateful firewall, application level gateways, dan next generation firewall. Stateless firewall atau packet filtering merupakan firewall generasi pertama dan yang paling sederhana, dengan kemampuan untuk memeriksa paket data lalu membandingkan asal, tujuan, dan port data tersebut dengan aturan yang sudah ditentukan untuk memutuskan apakah paket data tersebut akan dibiarkan lewat atau dihentikan. Kesederhanaan stateless firewall membuatnya menjadi pilihan yang murah dan tidak sulit untuk disetup, namun kekurangannya adalah tidak bisa melihat apa isi data dari paket yang dikirim atau diterima. Stateful firewall merupakan firewall dengan kemampuan tambahan untuk memeriksa isi dari paket data, sehingga dapat melindungi jaringan dari paket-paket berbahaya yang menyamarkan address dan portnya. Application level gateway meru-

pakan firewall dengan tingkat keamanan tinggi yang beroperasi pada tingkat aplikasi dan memiliki kemampuan untuk memeriksa alamat dan port data, isi paket data, dan protocol aplikasi (misalnya HTTP atau FTP) yang digunakan untuk mengirim atay menerima paket data tersebut. Kekurangan dari application level gateway adalah potensi terjadinya latensi akibat ketergantungannya terhadap proxy. Next generation firewall merupakan firewall generasi terbaru yang memiliki kemampuan untuk memeriksa paket data lebih dalam (deep packet inspection) dan sistem pertahanan yang proaktif dalam mengidentifikasi ancaman berdasarkan lalu lintas jaringan.

NAT atau network address translation merupakan sistem yang dapat mengubah satu atau lebih alamat IP lokal menjadi satu atau lebih alamat IP publik dan sebaliknya untuk menyediakan akses internet bagi perangkat yang terhubung pada jaringan lokal. Selain mengubah alamat IP, NAT juga dapat mengubah atau melakukan masking pada port. NAT umumnya beroperasi pada firewall yang terpasang di router. NAT bekerja dengan mengubah IP address dari perangkat-perangkat yang terhubung pada jaringan lokal menjadi alamat yang terdaftar pada IP publik global, sehingga perangkat-perangkat yang terhubung pada jaringan lokal akan menggunakan alamat lokalnya masing-masing untuk berkomunikasi di dalam jaringan lokal dan bila akan berkomunikasi melalui internet maka alamat-alamat lokal dari perangkat-perangkat dalam jaringan akan dikonversi menjadi alamat yang terdaftar pada alamat IP publik di internet. Ada 3 jenis NAT, yaitu static NAT, dynamic NAT, dan port address translation (PAT). Static NAT melakukan konversi one-to-one antara IP lokal dengan IP publik secara statis, yang artinya satu alamat IP publik hanya akan ditranslasikan menjadi satu alamat IP lokal yang sudah ditentukan dan sebaliknya, sehingga alamat IP lokal lain tidak akan ditranslasikan menjadi alamat publik tersebut. Static NAT tidak efisien dalam segi biaya, karena bila IP publiknya tidak gratis, maka perlu membeli satu IP publik untuk satu perangkat dalam jaringan, sehingga static NAT lazimnya hanya digunakan untuk perangkat yang memerlukan alamat IP yang tetap dan eksklusif, misalnya web server. Dynamic NAT melakukan konversi alamat IP lokal ke alamat IP publik yang telah disediakan dalam sebuah pool. Dynamic NAT memungkinkan berbagai perangkat dalam jaringan lokal untuk terhubung dengan internet secara dinamis, yang artinya perangkat bisa mengakses internet dari jaringan lokal selama masih ada alamat IP publik yang tersedia dalam pool. Kekurangan dynamic NAT sama dengan static NAT, yaitu tidak efisien dalam biaya, karena bila IP publiknya tidak gratis maka harus membeli banyak IP publik untuk membuat sebuah pool. Kapasitas pool yang terbatas akan membatasi jumlah perangkat yang dapat terhubung ke internet dalam satu waktu. Port address translation atau PAT melakukan konversi alamat IP dari perangkat-perangkat dalam jaringan lokal menjadi alamat IP publik dengan port yang berbeda-beda, sehingga memungkinkan banyak perangkat dalam satu jaringan lokal untuk menggunakan satu alamat IP publik saja dengan port dari alamat IP publik tersebut sebagai alat identifikasi. PAT merupakan yang paling sering digunakan di antara tiga metode yang telah disebutkan karena paling efisien dalam biaya. Dengan PAT, hanya perlu dilakukan pembelian terhadap satu IP publik namun perangkat yang dapat mengakses internet dapat menjadi sangat banyak.

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?

   Konfigurasi yang akan dibuat adalah konfigurasi NAT statis. NAT statis dipilih karena alamat lokal dari sebuah web server cenderung tidak berubah, sehingga akan memudahkan akses

apabila menggunakan NAT statis yang dapat mengonversi satu alamat publik menjadi alamat web server tersebut. Misalnya alamat lokal web server tersebut, yaitu 192.168.1.10:80, dipasangkan menggunakan NAT statis dengan alamat pubik 10.10.10.1.

Referensi:

https://support.huawei.com/enterprise/en/doc/EDOC1100034071/7f3ef931/introduction-to-nat#dc_fd_NAT_0004

https://www.geeksforgeeks.org/network-address-translation-nat/

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

   Firewall lebih penting untuk diterapkan terlebih dahulu karena firewall merupakan sistem keamanan dasar yang perlu ada di setiap jaringan untuk menghindari komunikasi data dari alamat-alamat yang tidak diinginkan. Bila tidak ada firewall, maka paket-paket data dapat melintas bebas tanpa aturan di jaringan, memungkinkan data-data jahat seperti malware dan spyware untuk menyusup ke perangkat pengguna. NAT juga pada umumnya dipasang atau dioperasikan di firewall pada router, sehingga firewall tentu saja harus dipasang lebih dulu dibanding NAT.

   Referensi:

   https://www.geeksforgeeks.org/network-address-translation-nat/

   https://www.fortinet.com/resources/cyberglossary/firewall

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

   Jika router tidak diberi filter firewall sama sekali, maka komunikasi data pada jaringan akan berjalan bebas tanpa aturan. Perangkat dalam jaringan dapat menerima dan mengirim data ke seluruh alamat di internet tanpa terkecuali, memberikan kebebasan akses namun juga memberi jalan tanpa halangan bagi orang-orang yang berniat jahat. Karena tidak ada aturan yang menyaring komunikasi data, maka para hacker dapat mengirimkan malware, spyware, bahkan ransomware dengan mudah ke perangkat-perangkat dalam jaringan, yang dapat berakibat pada kerugian bagi pengguna jaringan, baik kerugian privasi akibat spyware maupun kerugian materi akibat malware dan ransomware.

   Referensi:

   https://www.fortinet.com/resources/cyberglossary/firewall

   https://www.cisco.com/site/us/en/learn/topics/security/what-is-a-firewall.html