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

Laporan Sementara
Praktikum Jaringan Komputer

Firewall dan NAT

Kadek Candra Dwi Yanti - 5024231067

2025

1 Pendahuluan

1.1 Latar Belakang

Keamanan dan pengelolaan jaringan komputer merupakan aspek penting dalam mendukung kelancaran komunikasi dan pertukaran data di era digital saat ini. Seiring dengan semakin besarnya ketergantungan organisasi dan individu terhadap koneksi internet, risiko serangan siber seperti akses tidak sah, pencurian data, dan penyebaran malware juga meningkat signifikan. Oleh karena itu, diperlukan mekanisme pengamanan yang efektif untuk melindungi jaringan dari ancaman tersebut. Firewall sebagai salah satu perangkat keamanan jaringan berperan penting dalam menyaring dan mengontrol lalu lintas data yang masuk dan keluar, berdasarkan aturan tertentu yang dapat memblokir akses berbahaya dan memastikan hanya data yang valid yang dapat melewati jaringan internal. Di sisi lain, keterbatasan alamat IP publik yang tersedia menjadi kendala tersendiri dalam menghubungkan banyak perangkat ke internet secara bersamaan. Network Address Translation (NAT) hadir sebagai solusi teknologi yang memungkinkan penggunaan satu alamat IP publik untuk melayani banyak perangkat dengan melakukan penerjemahan alamat IP lokal ke alamat global secara dinamis dan efisien.

Permasalahan yang dihadapi dalam pengelolaan jaringan adalah bagaimana mengimplementasikan firewall dan NAT secara tepat agar jaringan dapat terlindungi dengan baik sekaligus mengoptimalkan penggunaan alamat IP yang terbatas. Selain itu, pemahaman tentang connection tracking yang merupakan bagian dari firewall stateful juga menjadi penting dalam mengenali status koneksi sehingga dapat meningkatkan keamanan dan performa jaringan. Urgensi pembelajaran topik ini sangat tinggi mengingat firewall dan NAT sudah menjadi teknologi dasar yang digunakan di berbagai lingkungan jaringan modern, termasuk pada perusahaan, instansi pemerintahan, hingga penyedia layanan internet. Dengan menguasai konsep dan konfigurasi firewall serta NAT, maka kesiapan dalam menghadapi tantangan pengamanan jaringan dapat ditingkatkan, sekaligus mendukung efisiensi penggunaan sumber daya jaringan. Praktikum ini memberikan kesempatan untuk menerapkan teori dalam kondisi nyata sehingga peserta dapat memahami secara langsung mekanisme kerja, kelebihan, dan kendala yang mungkin ditemui saat menggunakan firewall dan NAT dalam pengelolaan jaringan.

Dalam konteks teknologi saat ini, firewall dan NAT menjadi fondasi utama dalam menjaga keamanan serta kelancaran komunikasi data, terutama di tengah berkembangnya layanan cloud computing, Internet of Things (IoT), dan meningkatnya serangan siber yang semakin canggih. Oleh karena itu, pembelajaran praktis mengenai konfigurasi dan manajemen firewall serta NAT sangat relevan dan diperlukan untuk memperkuat kemampuan teknis dalam bidang jaringan komputer.

1.2 Dasar Teori

1. Firewall

   Firewall adalah perangkat atau sistem keamanan jaringan yang berfungsi untuk mengontrol lalu lintas data yang masuk dan keluar pada sebuah jaringan komputer. Firewall bertindak sebagai pengaman dengan cara memfilter paket data berdasarkan aturan yang telah ditentukan, sehingga hanya paket data yang memenuhi kriteria yang boleh melewati jaringan. Dengan kata lain, firewall berfungsi sebagai “satpam digital” yang menjaga agar hanya trafik yang sah dan aman yang dapat mengakses jaringan internal. Firewall dapat memberikan tiga jenis tindakan

terhadap paket data, yaitu menerima (accept), menolak dengan mengirim pesan error (reject), atau membuang paket tanpa balasan (drop). Keberadaan firewall menjadi sangat penting karena jaringan yang terkoneksi ke internet rentan terhadap berbagai ancaman seperti serangan hacker, virus, dan akses tidak sah yang dapat membahayakan sistem. Sebelum adanya firewall, metode pengamanan jaringan hanya menggunakan Access Control List (ACL) yang memiliki keterbatasan karena tidak mampu melakukan inspeksi mendalam terhadap isi data yang melewati jaringan.

2. Jenis-Jenis Firewall

   Ada beberapa tipe firewall berdasarkan cara kerjanya. Pertama, Packet Filtering, yang memeriksa paket data berdasarkan IP, port, dan protokol, tapi tidak melihat isi data. Kedua, Stateful Inspection, yang bisa mengenali status koneksi sehingga hanya mengizinkan paket yang bagian dari koneksi yang sah. Ketiga, Application Layer Firewall, yang mampu memeriksa isi aplikasi seperti HTTP dan FTP, serta memblokir konten tertentu. Selain itu, ada juga Next Generation Firewall (NGFW) yang menggabungkan berbagai fitur keamanan canggih, termasuk inspeksi paket secara mendalam hingga enkripsi SSL. Firewall juga bisa berupa perangkat lunak atau perangkat keras tergantung kebutuhan.

3. Network Address Translation (NAT)

   Network Address Translation adalah teknologi yang digunakan untuk mengatasi keterbatasan alamat IP publik dengan cara menerjemahkan alamat IP lokal dalam sebuah jaringan ke alamat IP publik yang digunakan untuk komunikasi di internet. Dengan NAT, banyak perangkat di jaringan lokal dapat menggunakan satu alamat IP publik secara bersamaan. Hal ini sangat efisien mengingat jumlah alamat IPv4 publik yang terbatas. NAT biasanya diimplementasikan pada perangkat router yang menghubungkan jaringan lokal dengan internet. Saat perangkat dalam jaringan lokal mengirim data ke internet, alamat IP lokalnya diganti menjadi alamat IP publik oleh router, dan saat data kembali, alamat IP publik diterjemahkan kembali ke IP lokal asli.

4. Jenis-Jenis NAT

   NAT terbagi menjadi tiga jenis utama. Static NAT menghubungkan satu alamat IP lokal ke satu alamat IP publik secara tetap, cocok untuk server yang butuh alamat tetap. Dynamic NAT menggunakan alamat IP publik yang tersedia dalam pool secara dinamis, tapi jika alamat habis maka koneksi tidak bisa dilakukan. Sedangkan Port Address Translation (PAT) adalah jenis NAT yang paling banyak dipakai karena memungkinkan banyak perangkat menggunakan satu IP publik dengan membedakan berdasarkan nomor port, sehingga sangat efisien.

5. Connection Tracking

   Connection Tracking merupakan fitur yang mengawasi dan mencatat status koneksi jaringan yang sedang berlangsung. Fitur ini memungkinkan firewall atau router untuk mengenali apakah paket data yang masuk adalah bagian dari koneksi yang sudah terverifikasi atau merupakan koneksi baru. Dengan adanya connection tracking, perangkat jaringan dapat mengizinkan paket balasan yang sah tanpa perlu memeriksa ulang secara detail setiap paket, sehingga meningkatkan efisiensi dan keamanan jaringan. Connection tracking mencatat informasi penting seperti alamat sumber dan tujuan, nomor port, protokol, dan status koneksi, yang sangat berguna

untuk proses penyaringan dan NAT. Fitur ini merupakan dasar dari firewall stateful yang lebih canggih dibandingkan firewall stateless.

2 Tugas Pendahuluan

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

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?

   Jawaban:

   Jenis NAT yang digunakan untuk mengakses web server lokal (192.168.1.10) dari jaringan luar adalah Static NAT, karena Static NAT menyediakan pemetaan satu-ke-satu antara IP privat server dan IP publik yang tetap, memungkinkan server lokal diakses secara konsisten dari luar jaringan. Konfigurasi NAT dilakukan dengan menandai interface lokal sebagai ip nat inside dan interface jaringan luar sebagai ip nat outside, kemudian memetakan IP lokal ke IP publik menggunakan perintah ip nat inside source static. Penjelasan ini dapat ditemukan pada halaman 19–20 jurnal Design And Configuration Of Static Network Address Translation Techniques, dan juga didukung oleh penjelasan serta implementasi Static NAT pada halaman 53–54 jurnal Implementasi Static NAT Terhadap Jaringan VLAN yang mengonfirmasi bahwa Static NAT sangat cocok digunakan agar server lokal dapat diakses dari luar jaringan secara stabil dan aman.

   Referensi:

   Parthasarathy, R., & Ayyappan, P. (2020). Design And Configuration Of Static Network Address Translation Techniques Method Using Cisco Packet Tracer Tool. International Journal of Scientific & Technology Research, 9(11), 19–20.

   Link Referensi

   Natali, J., Fajrillah, & Diansyah, T.M. (2016). Implementasi Static NAT Terhadap Jaringan VLAN Menggunakan IP Dynamic Host Configuration Protocol (DHCP). Jurnal Ilmiah Informatika, 1(1), 53–54.

   Link Referensi

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

   jawaban:

   Firewall harus diterapkan terlebih dahulu sebelum NAT karena firewall berperan sebagai garis pertahanan utama yang mengontrol dan memfilter lalu lintas jaringan untuk mencegah akses tidak sah dan serangan siber. Firewall menyaring paket berdasarkan aturan keamanan sehingga hanya trafik yang aman yang diteruskan. Sedangkan NAT berfungsi untuk menerjemahkan alamat IP internal menjadi alamat publik dan menyembunyikan IP asli dari jaringan luar, yang merupakan fitur pendukung keamanan, bukan pengaman utama. Cahyawati et al. (2023) menjelaskan bahwa firewall harus diposisikan sebagai lapisan pertama dalam sistem keamanan jaringan, sedangkan NAT biasanya merupakan bagian dari konfigurasi firewall yang berfungsi setelah proses filtering (hlm. 204-206). Selain itu, Sutiyo et al. (2023) menyatakan bahwa

firewall memberikan perlindungan efektif dengan memblokir akses tidak sah dan mendeteksi ancaman, sementara NAT membantu menjaga kerahasiaan IP internal tanpa menggantikan fungsi firewall (hlm. 66-68). Oleh karena itu, penerapan firewall lebih prioritas untuk keamanan jaringan yang optimal sebelum NAT dijalankan.

Referensi:

Cahyawati, R. K., Agustin, F. F., Arum, K. S., & Saputro, I. A. (2023). Perancangan keamanan jaringan menggunakan metode firewall security port. Seminar Nasional AMIKOM Surakarta (SEMNASA), 3031-5581, 203–210. **Link Referensi**

Sutiyo, F. R. A., Cahya, B., Saputra, Y. E., & Elfarizi, M. (2023). Implementasi firewall pada mikrotik untuk keamanan jaringan. Jurnal JOCOTIS - Journal Science Informatica and Robotics, 1(2).

Link Referensi

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

   jawaban:

   - Jaringan komputer yang terhubung ke internet sangat rentan terhadap serangan seperti virus, backdoor, port scan, hacker, dan serangan Denial of Service (DoS/DDos) jika tanpa firewall. (Sinaga dkk., 2020, hlm. 5)
   - Firewall berfungsi untuk membatasi akses dan memfilter trafik jaringan agar hanya yang aman yang dapat melewati jaringan. Tanpa firewall, akses tidak terbatas dan jaringan mudah dimasuki pihak tak berwenang. (Sinaga dkk., 2020, hlm. 3-4)
   - Tidak ada mekanisme pencatatan aktivitas mencurigakan sehingga sulit untuk mendeteksi dan menanggulangi serangan secara efektif. (Abidin, 2021, hlm. 87)
   - Port-port terbuka tanpa pembatasan dapat dimanfaatkan untuk eksploitasi oleh penyerang, melemahkan keamanan jaringan. (Abidin, 2021, hlm. 89-90)
   - Kinerja jaringan dapat terganggu, misalnya koneksi sering putus dan server rentan hang atau terinfeksi virus karena serangan tidak terhalang. (Sinaga dkk., 2020, hlm. 5-6)
   - Risiko backdoor dan akses ilegal meningkat tanpa adanya filter untuk membatasi akses remote yang tidak sah. (Sinaga dkk., 2020, hlm. 5)

   Referensi:

Sinaga, H. H., Sitompul, O. S., & Saleh, M. U. (2020). Implementasi dan Perbandingan Firewall Security Menggunakan Mikrotik dan M0n0wall Pada Local Area Network, hlm. 3-6. **Link Referensi**

Abidin, N. (2021). Optimalisasi Firewall Pada Jaringan Komputer Berskala Luas, hlm. 84-94. **Link Referensi**