Simulasi Topologi Jaringan Berbasis ACL Menggunakan *Cisco Packet Tracer*

Ahmad Harmain, Idham, Muhammad Guntara, I Gusti Ayu Diah Gita Kartika Santi, Husain

Universitas Bumigora, Mataram, Indonesia

Correspondence : *e-mail*: husain@universitasbumigora.ac.id

Abstrak

Penelitian ini bertujuan untuk mensimulasikan topologi jaringan berbasis Access Control List *(ACL) menggunakan perangkat lunak Cisco Packet Tracer. ACL digunakan untuk mengatur lalu lintas jaringan dengan memfilter paket berdasarkan alamat IP, protokol, dan port tertentu, sehingga meningkatkan keamanan jaringan. Proses simulasi melibatkan perancangan topologi jaringan, konfigurasi perangkat, penerapan aturan ACL, serta pengujian dan optimasi kinerja ACL. Hasil simulasi menunjukkan bahwa penerapan ACL dalam lingkungan virtual mampu merepresentasikan pengendalian akses secara efektif dan efisien. Studi ini juga menegaskan manfaat edukatif dari Cisco Packet Tracer dalam mendukung pembelajaran konsep keamanan jaringan secara praktis.*

Kata kunci: *Access Control List (ACL), Cisco Packet Tracer, Simulasi Jaringan, Keamanan Jaringan.*

Abstract

This study aims to simulate an Access Control List *(ACL)-based network topology using Cisco Packet Tracer software. ACLs are utilized to regulate network traffic by filtering packets based on IP addresses, protocols, and specific ports, thereby enhancing network security. The simulation process includes network topology design, device configuration, ACL rule implementation, as well as testing and optimization. The simulation results demonstrate that ACL deployment in a virtual environment can effectively and efficiently represent access control. This study also highlights the educational benefits of Cisco Packet Tracer in supporting practical learning of network security concepts.*

Keywords*: Access Control List (ACL), Cisco Packet Tracer, Network Simulation, Network Security.*

1. Pendahuluan

Keamanan jaringan menjadi salah satu komponen vital dalam pembangunan infrastruktur teknologi informasi yang andal. Di era digital saat ini, ancaman terhadap jaringan komputer semakin kompleks dan beragam. Oleh karena itu, diperlukan mekanisme pengamanan yang efektif dan efisien untuk mengatur dan membatasi akses terhadap sumber daya jaringan. Salah satu teknik pengamanan tersebut adalah penggunaan *Access Control List* (ACL). ACL merupakan serangkaian aturan yang digunakan untuk menyaring lalu lintas jaringan berdasarkan parameter tertentu seperti alamat IP sumber dan tujuan, protokol, serta nomor port [1], [2]. ACL terbagi menjadi dua jenis utama, yaitu ACL standar dan ACL ekstensi. ACL standar hanya memfilter lalu lintas berdasarkan alamat IP sumber, sedangkan ACL ekstensi dapat menyaring berdasarkan kombinasi alamat IP sumber dan tujuan, protokol (seperti TCP atau UDP), serta port tertentu [2], [3]. Dengan kemampuan ini, ACL menjadi alat yang sangat fleksibel dalam mengatur lalu lintas jaringan dan menerapkan kebijakan keamanan sesuai kebutuhan organisasi. Efisiensi dan efektivitas ACL dalam membatasi akses juga telah banyak dibuktikan melalui penelitian dan implementasi dalam lingkungan jaringan berskala kecil hingga besar [1], [3].

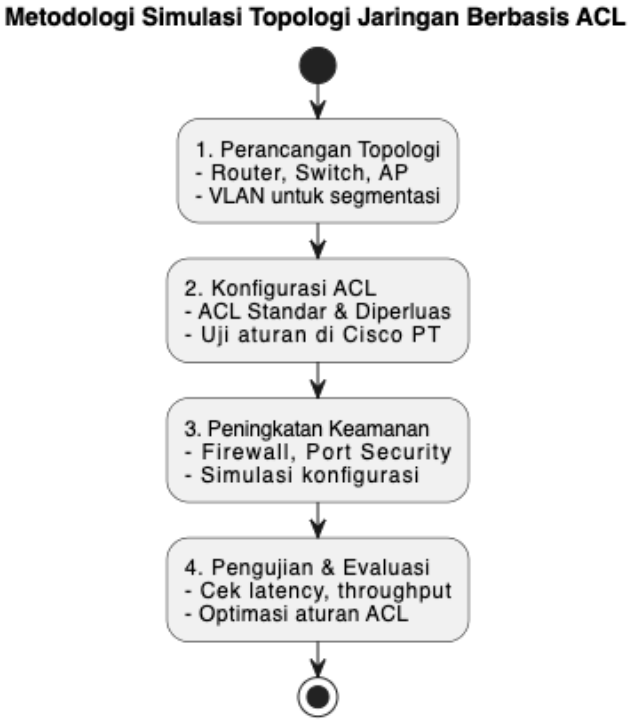
Untuk mempelajari dan mengimplementasikan ACL secara praktis, diperlukan media yang mendukung simulasi jaringan secara interaktif dan realistis. Salah satu perangkat lunak simulasi jaringan yang banyak digunakan adalah Cisco Packet Tracer. Aplikasi ini memungkinkan pengguna untuk merancang topologi jaringan, mengonfigurasi perangkat, dan melakukan simulasi lalu lintas serta keamanan jaringan [4], [5]. Cisco Packet Tracer memberikan lingkungan pembelajaran yang dinamis tanpa memerlukan perangkat keras fisik, sehingga sangat ideal untuk pembelajaran akademik maupun pelatihan

teknis di bidang jaringan komputer [5], [6]. Proses simulasi jaringan berbasis ACL dalam Cisco Packet Tracer meliputi beberapa tahapan penting. Tahap pertama adalah merancang topologi jaringan yang melibatkan perangkat seperti router, switch, dan host. Tahap berikutnya adalah konfigurasi perangkat dan penerapan aturan ACL sesuai skenario keamanan yang diinginkan [7], [8]. Setelah konfigurasi selesai, dilakukan pengujian terhadap lalu lintas jaringan untuk memastikan bahwa aturan ACL telah bekerja dengan benar. Hasil dari simulasi ini kemudian dapat digunakan untuk mengevaluasi efektivitas desain keamanan dan melakukan optimasi aturan jika diperlukan [3], [10].

Studi ini bertujuan untuk mensimulasikan topologi jaringan berbasis ACL menggunakan Cisco Packet Tracer, dengan fokus pada perancangan arsitektur jaringan, penerapan aturan ACL, serta evaluasi dan optimasi konfigurasi keamanan. Hasil dari penelitian ini diharapkan dapat memberikan wawasan praktis mengenai implementasi ACL di lingkungan jaringan simulasi, serta meningkatkan pemahaman teknis terkait manajemen dan pengendalian lalu lintas jaringan.

2. Metode Penelitian

Penelitian ini menggunakan pendekatan kuantitatif eksperimental melalui simulasi jaringan komputer dengan memanfaatkan perangkat lunak *Cisco Packet Tracer*. Tujuan utama dari metode ini adalah untuk mengevaluasi efektivitas dan efisiensi konfigurasi *Access Control List* (ACL) dalam mengamankan jaringan, serta mengamati dampaknya terhadap kinerja jaringan.



Gambar 1. Metodologi Penelitian

Perancangan Topologi Jaringan:

- Merancang topologi jaringan yang mencakup *router*, *switch*, dan perangkat penting lainnya.
- Memastikan topologi mencakup pengaturan jaringan yang melibatkan *access point nirkabel* dan kemungkinan VLAN untuk segmentasi lalu lintas jaringan.

Konfigurasi ACL

- Mengkonfigurasi ACL standar dan diperluas pada *router* dan *switch* untuk mengontrol akses ke jaringan.
- Menggunakan perintah khusus di Cisco Packet Tracer untuk menerapkan ACL tersebut, dan uji berbagai aturan serta dampaknya terhadap lalu lintas jaringan.

Peningkatan Keamanan:

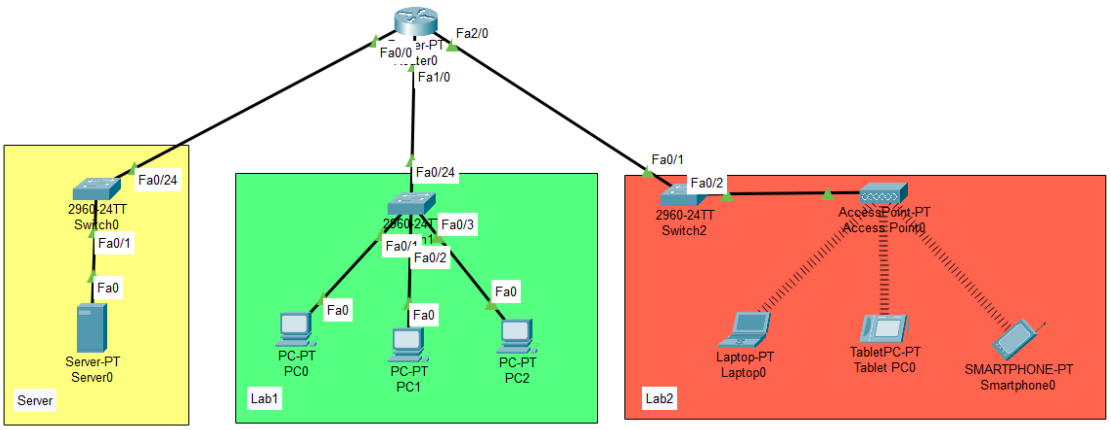
- Mengimplementasikan langkah-langkah keamanan tambahan seperti *firewall* dan *port security* untuk meningkatkan keamanan jaringan.
- Menggunakan Cisco Packet Tracer untuk mensimulasikan konfigurasi keamanan ini dan amati dampaknya terhadap kinerja dan keamanan jaringan.

Pengujian:
- Melakukan pengujian untuk mengevaluasi kinerja jaringan dengan ACL yang diterapkan. Ini mencakup pemeriksaan kehilangan paket, keterlambatan transmisi, dan *throughput* jaringan secara keseluruhan.
- Mengoptimalkan aturan ACL agar efisien dan tidak menurunkan performa jaringan.

3. Hasil dan Pembahasan

3.1. Topologi Jaringan

Pada simulasi ini dirancang sebuah sistem jaringan lokal berbasis Cisco Packet Tracer yang terdiri atas tiga segmen utama, yaitu jaringan Server, jaringan Lab1, dan jaringan Lab2. Setiap segmen dihubungkan ke satu buah router pusat melalui interface yang berbeda, yaitu Fa0/0 untuk jaringan Server, Fa1/0 untuk jaringan Lab1, dan Fa2/0 untuk jaringan Lab2 yang berisi perangkat wireless. Masing-masing segmen merepresentasikan ruang atau kelompok kerja yang terpisah dan memiliki hak akses yang berbeda terhadap sumber daya jaringan.



Gambar 2. Rancangan Topologi

Gambar 1 menggambarkan sebuah rancangan topologi yang dibuat untuk menerapkan konfigurasi *Access Control List* (ACL). Jaringan Lab1 terdiri dari tiga unit PC yang terhubung melalui satu switch, mewakili jaringan kabel (wired) untuk kebutuhan pengguna tetap. Sementara itu, jaringan Lab2 terdiri dari perangkat wireless seperti laptop, tablet, dan smartphone yang terhubung melalui Access Point, yang selanjutnya disambungkan ke router. Server diletakkan pada segmen jaringan tersendiri dan berperan sebagai pusat layanan (*web server*) yang akan diakses oleh perangkat klien yang diizinkan. Perancangan topologi ini bertujuan untuk mengimplementasikan *Access Control List* (ACL) sebagai metode pembatasan hak akses antar segmen, serta untuk menguji bagaimana konfigurasi ACL dapat memfilter lalu lintas jaringan secara selektif dan terarah.

3.2. Pembagian Alamat IP Address

Setiap perangkat yang digunakan dalam simulasi ini diberikan alamat IP statis sesuai dengan segmen jaringan masing-masing. Pembagian IP address disesuaikan dengan penggunaan subnet kelas C dengan subnet mask 255.255.255.0 atau /24, sehingga masing-masing segmen memiliki ruang alamat tersendiri yang terisolasi secara logis. Segmen Server menggunakan subnet 192.168.1.0/24, *Lab1* menggunakan 192.168.2.0/24, dan *Lab2* menggunakan 192.168.3.0/24.

Router sebagai perangkat pengatur lalu lintas jaringan memiliki tiga interface yang masing-masing terkoneksi langsung ke ketiga segmen tersebut. Server dan perangkat klien diberikan IP secara manual agar mempermudah proses konfigurasi dan pengujian. Adapun detail alokasi alamat IP untuk seluruh perangkat ditampilkan pada Tabel 1.

Tabel 1. Pembagian alamat IP Address

Perangkat	Interface	IP Address	Subnet
Router0	Fa0/0	192.168.1.1	255.255.255.0
Router0	Fa1/0	192.168.2.1	255.255.255.0
Router0	Fa2/0	192.168.3.1	255.255.255.0
Server0	Fa0	192.168.1.2	255.255.255.0
PC0	Fa0	192.168.2.2	255.255.255.0
PC1	Fa0	192.168.2.3	255.255.255.0
PC2	Fa0	192.168.2.4	255.255.255.0
Laptop0	WLAN	192.168.3.2	255.255.255.0
TabletPC0	WLAN	192.168.3.3	255.255.255.0
Smartphone0	WLAN	192.168.3.4	255.255.255.0

3.3. Pembagian Hak Akses

Sebagai bagian dari implementasi keamanan jaringan, dilakukan pembatasan hak akses antar segmen dengan menggunakan konfigurasi *Access Control List* (ACL) pada *router*. ACL digunakan untuk mengatur trafik berdasarkan alamat IP sumber dan tujuan sehingga hanya perangkat yang diizinkan saja yang dapat berkomunikasi ke segmen tertentu. Dalam simulasi ini, hak akses dibatasi sesuai dengan kebijakan pada Tabel 2.

Tabel 2. Kebijakan Hak Akses

Ruangan	Status
Lab1	Diizinkan mengakses *Web Server* dan tidak diizinkan mengakses ke *Lab2*
Lab2	Tidak diizinkan mengakses kemanapun

3.4. Konfigurasi

Access Control List (ACL) diterapkan pada router untuk menyaring lalu lintas jaringan antar segmen berdasarkan kebijakan yang telah ditentukan sebelumnya. Konfigurasi dilakukan dengan menggunakan *Extended* ACL, yang memungkinkan penyaringan berdasarkan alamat IP sumber dan tujuan, serta jenis protokol. Dua daftar ACL dibuat dan diterapkan pada *interface router* yang terhubung ke segmen *Lab1* dan *Lab2*.

ACL pertama, yaitu `access-list 101`, diterapkan pada interface fa1/0 (arah masuk dari *Lab1*). Daftar ini mengizinkan perangkat di Lab1 untuk mengakses Server (192.168.1.2), namun memblokir akses dari Lab1 ke Lab2. Semua trafik lainnya diizinkan sebagai fallback rule agar tidak terjadi pemblokiran total.

ACL kedua, yaitu *access-list 102*, diterapkan pada interface fa2/0 (arah masuk dari Lab2). ACL ini memblokir semua akses dari *Lab2* ke *Server* maupun ke *Lab1*. Seperti pada ACL sebelumnya, aturan permit ip any any juga disertakan di akhir sebagai izin umum untuk trafik yang tidak disebutkan secara eksplisit.

Konfigurasi ACL 101

```
Router(config)#access-list 101 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
Router(config)#access-list 101 deny ip 192.168.2.0 0.0.0.255 192.168.3.0 0.0.0.255
Router(config)#access-list 101 permit ip any any
Router(config)#interface fa1/0
Router(config-if)#ip access-group 101 in
Router(config-if)#ex
```

Konfigurasi ACL 102

```
Router(config)#access-list 102 deny ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
Router(config)#access-list 102 deny ip 192.168.3.0 0.0.0.255 192.168.2.0 0.0.0.255
Router(config)#access-list 102 permit ip any any
Router(config)#interface fa2/0
Router(config-if)#ip access-group 102 in
```

3.5. Pengujian

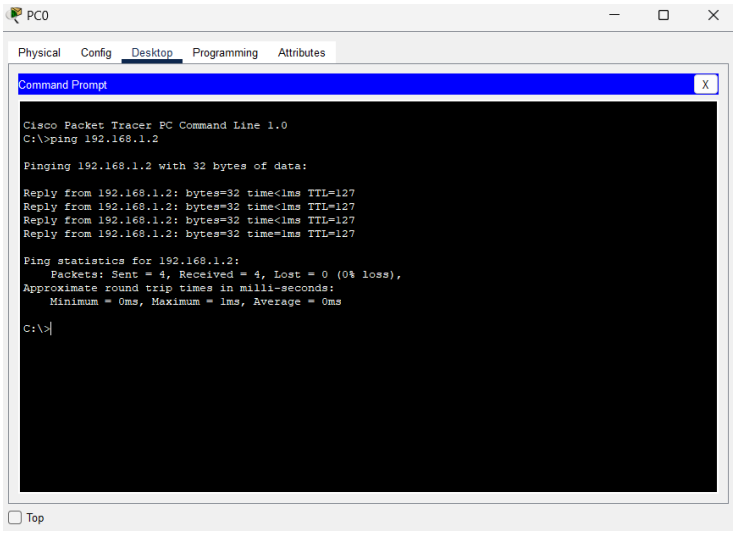
Pengujian dilakukan untuk memastikan bahwa konfigurasi ACL yang diterapkan pada router bekerja sesuai dengan kebijakan akses antar segmen jaringan. Setiap skenario diuji menggunakan metode ping untuk menguji konektivitas antar perangkat, serta akses HTTP untuk menguji komunikasi aplikasi pada layer yang lebih tinggi. Hasil pengujian dibagi menjadi dua bagian berdasarkan lokasi sumber trafik, yaitu dari Lab1 dan dari Lab2.

3.5.1 Pengujian *Lab1*

Pengujian dilakukan dari perangkat yang berada dalam segmen Lab1 (192.168.2.0/24), yaitu PC0 dan PC1. Tujuannya adalah untuk menguji apakah perangkat di Lab1 dapat mengakses server, serta apakah dapat berkomunikasi dengan perangkat di segmen Lab2.

a. PC0 Ping ke Server

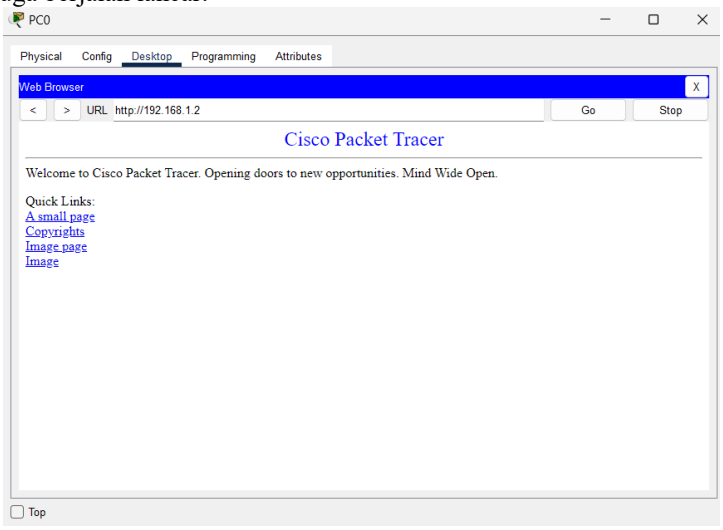
Uji konektivitas menggunakan perintah ping dari PC0 ke alamat IP server (192.168.1.2). Hasil menunjukkan bahwa PC0 berhasil menerima balasan dari server, yang berarti akses dari Lab1 ke Server diizinkan oleh ACL.



Gambar 3. Hasil Ping dari PC0 ke Server

b. PC0 Ping ke Web Server

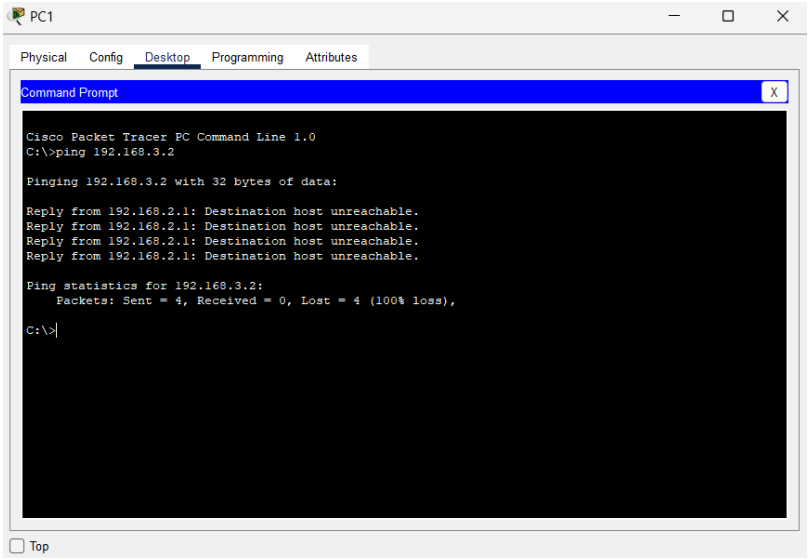
PC0 mengakses layanan web pada server melalui browser dengan memasukkan alamat http://192.168.1.2. Halaman web berhasil ditampilkan, yang menandakan bahwa komunikasi pada layer aplikasi juga berjalan lancar.



Gambar 4. Tampilan Web dari browser PC0

c. PC1 Ping ke Laptop0

PC1 melakukan pengujian ping ke Laptop0 (192.168.3.2) yang berada di segmen Lab2. Hasil pengujian menunjukkan bahwa ping gagal, yang berarti ACL telah berhasil memblokir akses dari Lab1 ke Lab2.



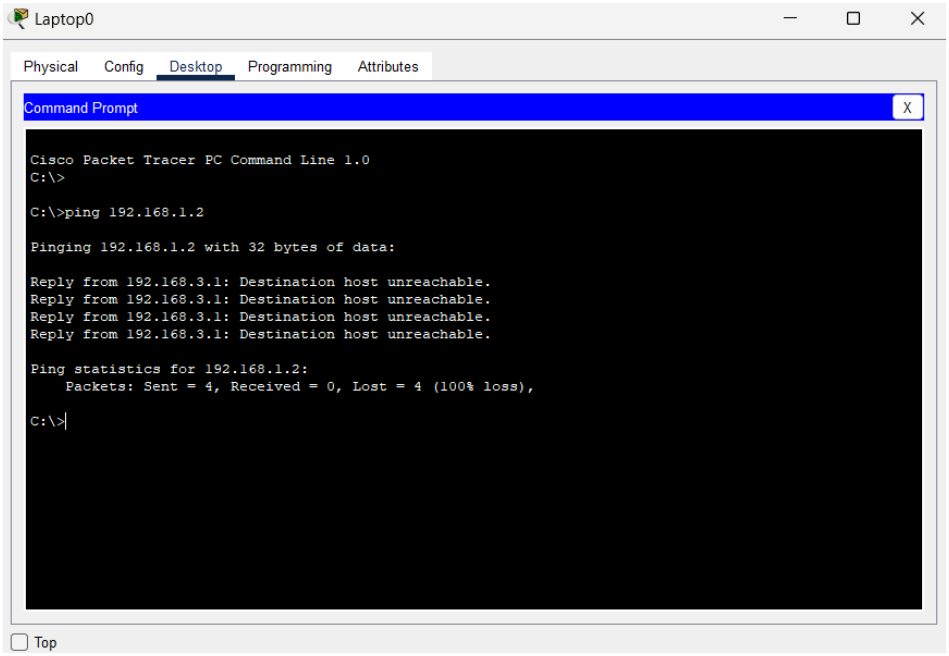
Gambar 5. Hasil ping gagal dari PC1 ke Laptop0

3.5.2 Pengujian *Lab2*

Pengujian ping dari Laptop0 ke Server (192.168.1.2) menunjukkan hasil gagal, yang mengindikasikan bahwa akses dari Lab2 ke Server telah dibatasi sepenuhnya oleh ACL.

a. Laptop0 Ping ke Server

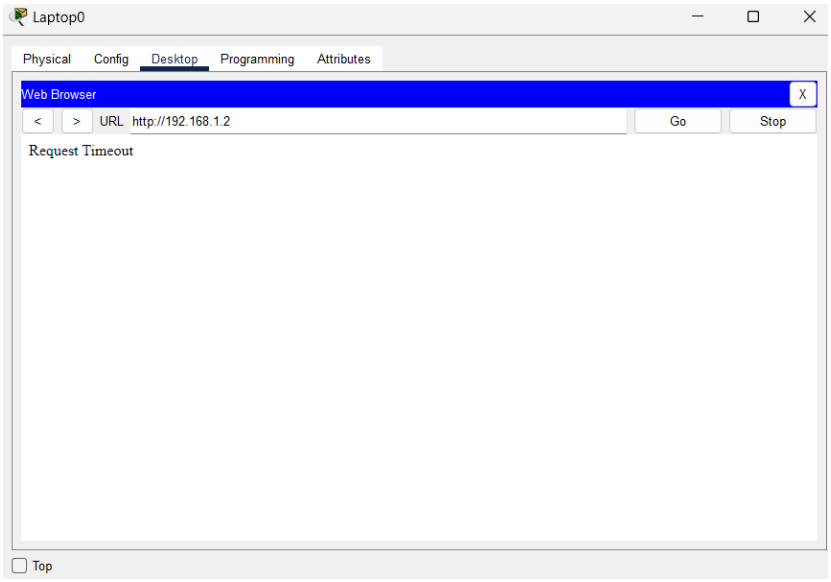
Pengujian ping dari Laptop0 ke Server (192.168.1.2) menunjukkan hasil gagal, yang mengindikasikan bahwa akses dari Lab2 ke Server telah dibatasi sepenuhnya oleh ACL.



Gambar 6. Hasil ping dari Laptop0 ke Server

b. Laptop0 Ping ke Web Server

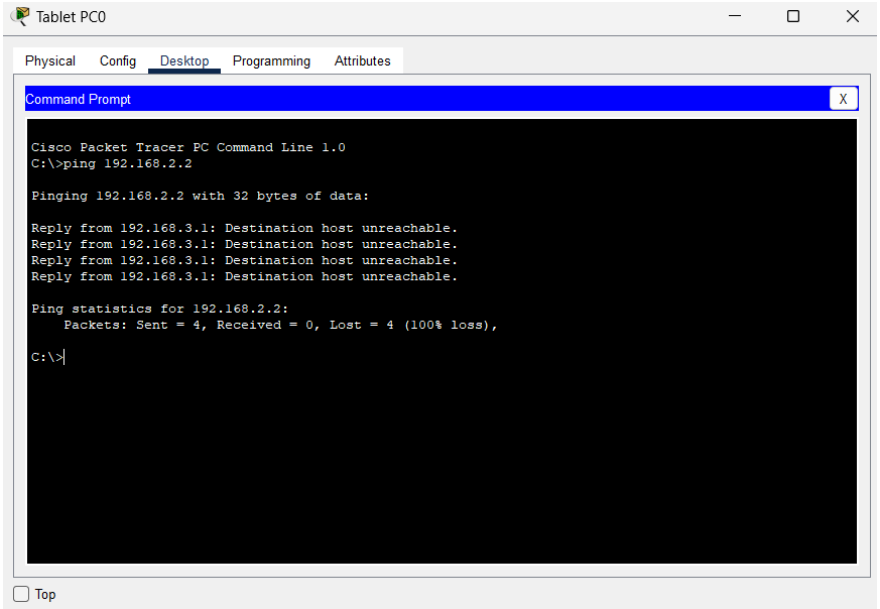
Laptop0 mencoba mengakses web server dengan memasukkan alamat http://192.168.1.2 di browser. Hasil menunjukkan halaman tidak dapat ditampilkan, yang memperkuat bukti bahwa trafik dari Lab2 ke Server benar-benar terblokir pada semua layer komunikasi.



Gambar 7. Tampilan gagal akses Web Server

c. Tablet PC0 Ping ke PC0

TabletPC0 mencoba melakukan ping ke PC0 (192.168.2.2) yang berada di Lab1. Sama seperti sebelumnya, hasil pengujian menyatakan ping gagal, menunjukkan bahwa Lab2 tidak dapat berkomunikasi keluar ke segmen lain, sesuai kebijakan pada ACL.



Gambar 8. Hasil ping gagal dari TabletPC0 ke PC0

4. Kesimpulan

Simulasi topologi jaringan berbasis ACL menggunakan Cisco Packet Tracer membuktikan bahwa pengendalian akses dapat diterapkan secara efektif dalam lingkungan virtual. ACL memberikan fleksibilitas tinggi dalam mengatur lalu lintas jaringan berdasarkan berbagai parameter, seperti alamat IP, protokol, dan port. Melalui proses perancangan topologi, konfigurasi perangkat, penerapan aturan, serta pengujian, pengguna dapat memahami mekanisme kerja ACL dan dampaknya terhadap sistem jaringan.

Selain itu, Cisco Packet Tracer terbukti menjadi alat yang efektif untuk pembelajaran interaktif, karena memungkinkan eksperimen langsung tanpa memerlukan perangkat keras fisik. Hal ini sangat bermanfaat dalam konteks pendidikan dan pelatihan keamanan jaringan. Dengan demikian, simulasi ini tidak hanya mendukung pemahaman teknis, tetapi juga membekali pengguna dengan keterampilan praktis yang dapat diterapkan dalam dunia kerja nyata.

Daftar Pustaka

[1] K.-Y. Zeng and J.-H. Yang, "Towards the optimization of access control list," *Ruan Jian Xue Bao/Journal of Software*, 2007. [Online]. Available: https://www.scopus.com/pages/publications/34249336420

[2] Y. Cao and L. Ai, "Experimental simulation and comparative analysis of an access control list at different deployment locations," in *Proc. 2022 IEEE 2nd Int. Conf. on Computer Communication and Artificial Intelligence (CCAI)*, 2022. [Online]. Available: https://www.scopus.com/pages/publications/85134410894

[3] A. X. Liu, E. Torng, and C. R. Meiners, "Compressing network access control lists," *IEEE Trans. Parallel Distrib. Syst.*, vol. 22, no. 12, pp. 1969–1977, 2011. [Online]. Available: https://www.scopus.com/pages/publications/80055048663

[4] K. Kundu, S. Chaurasia, P. Pandey, and R. K. Gatla, "Simulating a local area network with Cisco Packet Tracer: A comprehensive IP packet switching network demonstration," in *Proc. Int. Conf. on Power Energy, Environment and Intelligent Control (PEEIC)*, 2023. [Online]. Available: https://www.scopus.com/pages/publications/85188092188

[5] Z. Trabelsi and H. Saleous, "Exploring the opportunities of Cisco Packet Tracer for hands-on security courses on firewalls," in *Proc. IEEE Global Engineering Education Conf. (EDUCON)*, 2019. [Online]. Available: https://www.scopus.com/pages/publications/85067503893

[6] I. B. Irawan Purnama, "Role of packet tracer in simulating server services on the client-server computer network," *J. Phys.: Conf. Ser.*, vol. 1477, no. 4, 2020. [Online]. Available: https://www.scopus.com/pages/publications/85087519104

[7] M. Feng, "Network security management and implementation based on ACL," in *Advances in Intelligent Systems and Computing*, vol. 887, pp. 199–203, 2019. [Online]. Available: https://www.scopus.com/pages/publications/85056824313

[8] S. Dhaka, "Traffic management and security in wired network," in *Communications in Computer and Information Science*, vol. 1076, pp. 278–285, 2019. [Online]. Available: https://www.scopus.com/pages/publications/85066909359

[9] S. H. Moz, M. A. Hosen, and N. F. I. Tanny, "Campus network configuration, monitoring and data flow simulation using Cisco Packet Tracer," in *Proc. 6th Int. Conf. on Inventive Computation Technologies (ICICT)*, 2023. [Online]. Available: https://www.scopus.com/pages/publications/85163466682

[10] F. H. Li and X. Cao, "Implementation of the demonstration center network ACL technology," in *Proc. Int. Conf. on Management, Information and Educational Engineering (MIEE)*, 2015. [Online]. Available: https://www.scopus.com/pages/publications/84957376892

[11] T. Ishikawa and N. Yoshiura, "Decreasing access control list processed in hardware," in *Lecture Notes in Computer Science*, vol. 5939, pp. 205–215, 2009. [Online]. Available: https://www.scopus.com/pages/publications/70350453941