Vol. 6, No. 1, April 2025, hal. 68-76

Jurnal Computer Science and Information Technology (CoSciTech)

p-ISSN: 2723-567X
e-ISSN: 2723-5661

http://ejurnal.umri.ac.id/index.php/coscitech/index

Implementasi *access control list (ACL)* sebagai metode proteksi dan *traffic control* pada infrastruktur jaringan *local area network (LAN)*

Miftahur Rahman[*1], Moh. Dasuki[2]
Email: [1]miftahurrahman@unmuhjember.ac.id, [2]moh.dasuki22@unmuhjember.ac.id

[1,2]Program Studi Teknik Informatika, Fakultas Teknik, Universitas Muhammadiyah Jember

Diterima: 23 April 2025 | Direvisi: 29 April 2025 | Disetujui: 22 Mei 2025

Abstrak

PT. Hidatech Indonesia merupakan salah satu perusahaan di Kabupaten Jember yang berjalan di bidang teknologi yaitu menyediakan layanan kursus, pelatihan, pembuatan *software*, dan penjualan *hardware.* Infrastruktur jaringan pada perusahaan tersebut kerap mengalami penyerangan *cyber* seperti jaringan *trouble, server down,* dan gangunan operasional lainnya. Hal ini disebabkan banyaknya *user* yang mengakses jaringan tersebut tanpa adanya proteksi dan kontrol lalu lintas jaringan. Oleh sebab itu, dibutuhkan strategi untuk memproteksi atau melindungi dan mengkontrol *traffic* jaringan komputer dari serangan siber, salah satu strateginya adalah dengan menerapkan *Access Control List (ACL).* Adapun tahapan atau metode penelitian yang dilakukan pada penelitian ini meliputi pengumpulan data, desain, implementasi, dan pengujian. Menghasilkan penelitian bahwa Jaringan divisi ruang pimpinan (192.168.10.0) dapat mengakses server FTP (192.168.50.20) maupun server Web (192.168.50.20). Jaringan divisi ruang pemasaran (192.168.20.0) hanya diijinkan akses server Web (192.168.50.20). Jaringan divisi soft. development (192.168.30.0) dan divisi course pelatihan (192.168.40.0) tidak diijinkan mengakses keduanya server Web dan server FTP, sementara divisi server memiliki akses penuh ke semua divisi didalam jaringan tersebut dengan persentase keberhasilannya adalah 100%. Dari hasil penelitian ini diharapkan dapat diterapkan terhadap jaringan riil sebagai keamanan dan kontrol lalu lintas pada jaringan di PT. Hidatech.

Kata kunci: *Access Control List, Traffic Control*, Jaringan Komputer, *LAN, Cisco Packet Tracer*

Implementation of Access Control List (ACL) as a Protection and Traffic Control Method in Local Area Network (LAN) Infrastructure

Abstract

PT. Hidatech Indonesia is one of the companies in Jember Regency that operates in the field of technology, namely providing course services, training, software development, and hardware sales. The company's network infrastructure often experiences cyber attacks such as network trouble, server downs, and other operational disruptions. This is due to the large number of users accessing the network without network traffic protection and control. Therefore, a strategy is needed to protect or protect and control computer network traffic from cyber attacks, one of the strategies is to implement an Access Control List (ACL). The stages or research methods carried out in this study include data collection, design, implementation, and testing. Resulting in research that the network of the division of the lead room (192.168.10.0) can access FTP servers (192.168.50.20) and Web servers (192.168.50.20). Soft division network. development (192.168.30.0) and training course divisions (192.168.40.0) are not allowed to access both Web servers and FTP servers, while server divisions have full access to all divisions within the network with a 100% success rate. From the results of this research, it is hoped that it can be applied to the real network as security and traffic control on the network at PT. Hidatech.

Keyword: *Access Control List, Traffic Control, Computer Network, LAN, Cisco Packet Tracer*

1. PENDAHULUAN

Jaringan komputer saat ini memiliki peranan penting dalam berbagai aspek kehidupan, terutama dalam mendukung komunikasi global, pengelolaan data, dan automasi dalam berbagai bidang seperti dalam bidang pembelajaraan dan pendidikan, sektor medis, pemerintahan, perusahan dan sebagainya[1]. Jaringan komputer sendiri merupakan seperangkat komputasi yang saling terhubung yang dapat bertukar data dan berbagi sumber daya satu sama lain [2]. Perangkat jaringan ini agar terhubung menggunakan protokol komunikasi tertentu, untuk dapat mengirimkan informasi melalui teknologi fisik kabel ataupun nirkabel [3]. Jaringan komputer yang lingkup areanya global disebut dengan internet [4][5]. Pengguna internet saat ini begitu pesat berdasarkan data statistik dari www.datareportal.com per tahun 2024 bahwa jumlah pengguna internet di seluruh dunia mencapai sekitar 5.35 miliar pengguna, jumlah ini hampir sama dengan 67% populasi global, jumlah ini terus meningkat, mengingat rata-rata beberapa negara sudah mempunyai penetrasi internet yang tinggi [6]. Sedangkan di Indonesia sendiri menurut Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) mengumumkan bahwa jumlah pengguna internet tahun 2024 mencapai sekitar 221.5 juta jiwa dari total populasi 278.6 juta jiwa penduduk Indonesia tahun 2023. Dari hasil survei penetrasi internet Indonesia tersebut, maka tingkat penetrasi internet Indonesia menyentuh angka 79.5%. Dibandingkan dengan periode sebelumnya, maka ada peningkatan sekitar 1.4% [7].

Perkembangan internet yang sangat pesat ini berpotensi terhadap terjadinya ancaman penyerangan *cyber*. *Cyber attack* atau penyerangan dunia maya adalah tindakan yang dilakukan melalui jaringan komputer untuk memanipulasi, merusak, atau mencuri informasi dari sistem target secara ilegal. Pada umumnya serangan siber ini dapat menimbulkan dampak yang signifikan terhadap sebuah organisasi, seperti kerusakan reputasi, kerugian finansial, hilangnya produktivitas, dan sebagiannya [8]. Penyerangan *cyber* dapat dilakukan terhadap bermacam tingkatan, mulai dari yang sederhana hingga yang kompleks, serangan yang lebih kompleks seringkali tidak mudah terdeteksi dan dapat menimbulkan dampak jangka panjang pada sebuah organisasi[9]. Penyerangan siber tidak hanya menyerang pada jaringan internet yang lingkup areanya global, namun juga dapat menyerang pada jaringan yang lingkup areanya terbatas secara geografis, seperti area dalam satu gedung, laboratorium, atau sekolah, dalam hal ini disebut dengan *Local Area Network (LAN)* [10].

PT. Hidatech Indonesia merupakan salah satu perusahaan di Kabupaten Jember yang berjalan di bidang teknologi yaitu menyediakan layanan kursus, pelatihan, pembuatan *software*, dan penjualan *hardware* [11]. Infrastruktur jaringan pada perusahaan tersebut kerap mengalami penyerangan *cyber* seperti jaringan *trouble*, *server down*, dan gangunan operasional lainnya. Hal ini disebabkan banyaknya *user* yang mengakses jaringan tersebut tanpa adanya proteksi dan kontrol lalu lintas jaringan. Oleh sebab itu, dibutuhkan strategi untuk memproteksi atau melindungi dan mengkontrol *traffic* jaringan komputer dari serangan siber, salah satu strateginya adalah dengan menerapkan *Access Control List (ACL).*

Access Control List atau *ACL* adalah metode proteksi atau keamanan jaringan yang mengatur akses ke sumber daya melalui daftar aturan. Fitur *ACL* menentukan siapa yang dapat mengakses sumber daya di jaringan dan tingkat akses yang diperbolehkan. Biasanya digunakan dalam konfigurasi *firewall* dan *router*, *ACL* membantu memfilter lalu lintas berdasarkan alamat *IP*, *port*, atau *protocol*. *ACL* diklasifikasikan menjadi dua jenis. Salah satunya adalah *ACL standard* yang memfilter lalu lintas berdasarkan alamat *IP* sumber dan yang lainnya adalah *ACL extended* yang memberikan kontrol lebih fleksibel, seperti pemfilteran berdasarkan alamat *IP* tujuan, jenis protokol dan *port* tertentu [12].

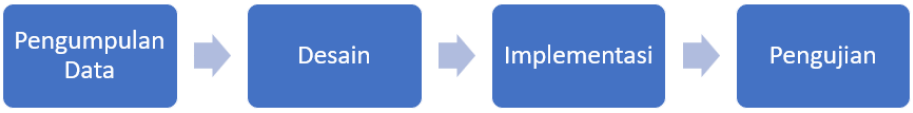
Penelitan terkait yang pernah dilakukan oleh [13] menghasilkan penelitian bahwa penerapan *ACL* berhasil dilakukan untuk membatasi sebuah jaringan agar *client* tidak dapat mengakses ke *client* tertentu, penelitian tersebut fokus tentang penerapan *ACL standard* pada jaringan *VLAN* PT Cakramedia Indocyber. Penelitian lainnya dilakukan oleh [14] menghasilkan penelitian bahwa dengan menggunakan *ACL extended* alamat IP dapat membantu *router* secara tepat dalam membatasi hak akses pada setiap jaringan *VLAN* maupun jaringan *AP* dalam menentukan alamat *network* mana saja yang bisa saling terhubung dan berkomunikasi untuk dapat mengakses *FTP server* maupun *web server*, penelitian tersebut fokus penerapan *ACL extended* pada jaringan *VLAN*. Berdasarkan penelitian sebalumnya yang diungkapkan bahwa penggunaaan *ACL* terbukti efektif dalam menyaring atau membatasi lalu lintas jaringan agar terhindar dari serangan siber.

Fokus penelitian yang akan dilakukan ini adalah mensimulasikan jaringan *Local Area Network (LAN)* atau jaringan dalam lingkup area yang terbatas dalam satu gedung dalam hal ini yaitu PT Hidatech Indonesia sebagai objek penelitian, menggunakan aplikasi simulasi *Cisco Packet Tracer* versi 8.2.2 yang akan mengimplementasikan metode *ACL* dengan cara akan dilakukan konfigurasi dengan mengkombinasikan konfigurasi ACL di berbagai router hal ini agar menjadi lebih efisien, metode ini akan diterapkan pada jaringan perusahaan tersebut sebagai proteksi dan kontrol lalu lintas jaringan terhadap ancaman serangan siber, dimana hasil simulasi ini nantinya digunakan sebagai usulan perancangan infrastruktur jaringan yang baru pada perusahaan tersebut. *Cisco Packet Tracer* adalah *software* simulasi jaringan yang komprehensif yang dikembangkan oleh Perusahaan Cisco Systems, Inc. untuk mengajarkan dan mempelajari cara membuat topologi jaringan dan meniru jaringan komputer modern. Perangkat ini menawarkan kombinasi unik antara pengalaman simulasi dan visualisasi yang realistis, kemampuan penilaian dan penulisan aktivitas, serta peluang kolaborasi dan kompetisi multi-pengguna. Fitur-fiturnya yang inovatif membantu penggunanya berkolaborasi, memecahkan masalah, dan mempelajari konsep jaringan dalam lingkungan sosial yang menarik dan dinamis [15].

Berdasarkan penjelasan yang sudah diuraikan diatas, sehingga rumusan masalah yang dapat dibuat pada penelitian ini adalah "bagaimana menerapkan *Access Control List (ACL)* Sebagai Metode Proteksi dan *Traffic Control* Pada Infrastruktur Jaringan *Local Area Network (LAN)* Menggunakan *Software* Simulasi *Cisco Packet Tracer* versi 8.2.2?".

2. METODE PENELITIAN

Adapun tahapan atau metode penelitian yang dilakukan pada penelitian ini meliputi pengumpulan data, desain, implementasi, dan pengujian yang ditunjukkan pada gambar berikut ini:



Gambar 1. Tahapan Penelitian

2.1. Pengumpulan Data

Tahap pertama pengumpulan data adalah proses sistematis dalam memperoleh informasi atau fakta dari berbagai sumber untuk dianalisis dan digunakan dalam pengambilan keputusan, penelitian, atau evaluasi. Proses ini bertujuan untuk mendapatkan data yang akurat, relevan, dan dapat dipercaya. Metode pengumpulan data yang dilakukan pada penelitian ini adalah observasi dan studi literatur.

2.2. Desain

a. Topologi Jaringan

Pada tahap ini tim peneliti akan membuat dan mengembangkan desain topologi jaringan yang akan dibangun berdasarkan topologi yang sedang berjalan, pembuatannya dibantu dengan *Software* simulasi *Cisco Packet Tracer* versi 8.2.2.

b. Analisis Kebutuhan

Analisis kebutuhan adalah proses sistematis untuk mengidentifikasi, mengumpulkan, dan mengevaluasi kebutuhan suatu sistem, proyek, atau organisasi sebelum tahap perancangan atau implementasi. Proses ini bertujuan untuk memastikan bahwa solusi yang dikembangkan dapat memenuhi kebutuhan pengguna atau stakeholder dengan efektif.

2.3. Implementasi

Tahapan ini akan mengimplementasikan semua yang telah dirancang sebelumnya. Pada tahapan ini akan terlihat sejauh mana pengembangan yang akan dibangun memberikan pengaruh terhadap sistem yang sudah ada. Pada tahap ini tim peneliti akan melakukan konfigurasi kebutuhan pengalamatan IP, konfigurasi *routing RIP*, konfigurasi *ACL*. Berikut contoh konfigurasi *ACL* jaringan komputer:

```
#access-list 100 deny tcp any 192.168.2.0 0.0.0.255 eq 80
#access-list 100 permit ip any any
#interface FastEthernet0/0
#ip access-group 100 out
```

Keterangan:

- *ACL extended* (100) diterapkan sebagai *outbound* pada *interface* yang sama untuk memfilter jenis lalu lintas tertentu.

2.4. Pengujian

Pengujian yang akan dilakukan adalah test koneksi masing-masing divisi jaringan untuk memastikan apakan konfigurasi yang dilakukan sesuai dengan aturan atau *policy* kontrol lalu lintas jaringan yang sudah dibuat. Berikut beberapa pengujian yang akan dilakukan:

a. Pengujian test koneksi menggunakan protokol *Internet Control Message Protocol (ICMP)* yang merupakan salah satu jenis protokol layer 3 (tiga) yang biasa digunakan untuk pengecekan dan mengindikasi *error* pada saat transmisi dalam sebuah jaringan. Contoh: `#ping [IP tujuan]` atau `#tracert [IP tujuan]`
b. *Test browsing* dan *FTP* dengan mengakses *service HTTP* atau *Web* dan *FTP server*. *FTP (File Transfer Protocol)* adalah protokol jaringan standar yang memungkinkan pemindahan file secara aman antara klien dan server di dalam jaringan. Sedangkan *HTTP (Hypertext Transfer Protocol)* adalah layanan yang memungkinkan akses berbasis web ke antarmuka manajemen perangkat.

3. HASIL DAN PEMBAHASAN

3.1. Pengumpulan Data

a. Observasi

Tim peneliti mengamati secara langsung kondisi objek penelitian, dalam hal ini adalah PT Hidatech Indonesia. Observasi dilakukan pada tanggal 9 November 2024 di Perusahaan tersebut untuk mengetahui infrastruktur atau topologi jaringan yang

sudah ada dengan mengidentifikasi sistem yang sedang berjalan kemudian mencoba untuk mengembangkan sistem seperti apa yang akan diperlukan pada sistem jaringan tersebut. Hasil dari observasi terdapat temuan bahwa infrastruktur jaringan pada perusahaan tersebut kerap mengalami penyerangan cyber seperti jaringan trouble, server down, dan gangunan operasional lainnya. Hal ini disebabkan banyaknya user yang mengakses jaringan tersebut tanpa adanya proteksi dan kontrol lalu lintas jaringan.

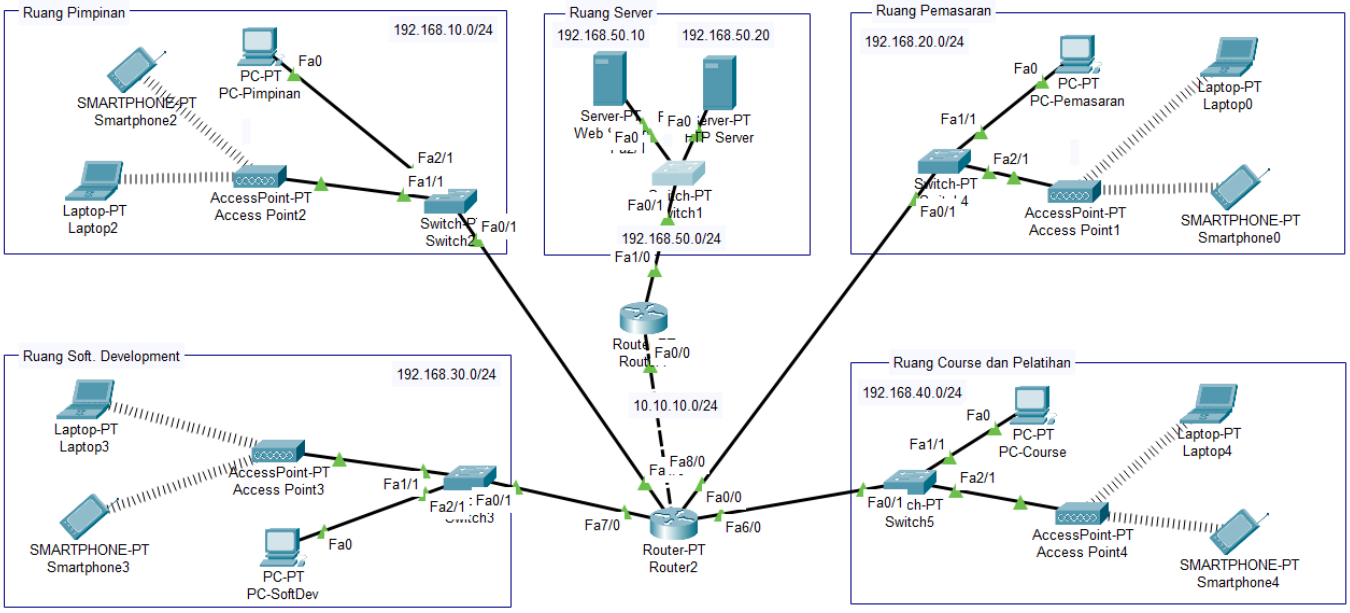
b. Studi Literatur

Studi literatur merupakan bagian penting dari proses penelitian yang akan dilakukan. Hal ini melibatkan pengumpulan, peninjauan, dan analisis karya-karya ilmiah dan referensi yang berkaitan dengan topik penelitian. Tujuan utama penelitian literatur adalah untuk memahami latar belakang teori, tren penelitian, dan kesenjangan literatur yang ada untuk menjadi landasan penelitian yang akan dilakukan.

3.2. Desain

a. Topologi Jaringan

Pada tahap ini tim peneliti akan membuat dan mengembangkan desain topologi jaringan yang akan dibangun berdasarkan topologi yang sedang berjalan, pembuatannya dibantu dengan *Software* simulasi *Cisco Packet Tracer* versi 8.2.2, berikut pengembangan topologinya:



Gambar 2. Topologi Jaringan

b. Analisis Kebutuhan

Setelah dirancang desain topologi jaringan, pada tahap ini adalah analisis kebutuhan. Kebutuhan yang diperlukan pada penelitian ini, berdasarkan gambar 2 bahwa infrastruktur yang dibangun terdapat 5 divisi, antara lain: (1) Divisi Ruang Server, (2) Divisi Ruang Pimpingan, (3) Divisi Ruang Pemasaran, (4) Divisi Ruang Software Development, dan (5) Divisi Course dan Pelatihan.

Selanjutnya dibutuhkan pembuatan aturan-aturan atau *policy* kontrol lalu lintas jaringan sesuai dengan kebutuhan objek penelitian agar serangan *cyber* dapat dicegah. Berdasarkan gambar 2 adapun aturan yang akan dibuat dapat diskenariokan sebagai berikut:

1). Jaringan Divisi Ruang Pimpinan diijinkan mengakses *Server FTP* dan *Server Web*.
2). Jaringan Divisi Ruang Pemasaran tidak diijinkan mengakses *Server FTP* yang ada pada Jaringan Divisi Ruang Server, namun diijinkan mengakses *Server Web*.
3). Jaringan Divisi Ruang Soft. Development dan Divisi Ruang Course Pelatihan tidak diijinkan mengakses *Server Web* dan *Server FTP* yang ada pada Jaringan Divisi Ruang Server.
4). Divisi Ruang Server dapat mengakses seluruh Divisi dalam topologi jaringan tersebut.

3.3. Implementasi

a. Pengalamatan

Sebelum melakukan konfigurasi pastikan pemetaan pengalamatan sudah dibuat, pemetaan IP ini sebagai identitas masing-masing perangkat untuk bisa digunakan pada infrastruktur jaringn ini:

Tabel 1. Daftar IP Address

No	Device Name	Interface/Port	IP Address	Network	Gateway
1	Router1	Fa1/0	192.168.50.1/24	192.168.50.0	
		Fa0/0	10.10.10.1/24	10.10.10.0	
2	Router2	Fa8/0	10.10.10.2/24	10.10.10.0	
		Fa1/0	192.168.10.1/24	192.168.10.0	
		Fa0/0	192.168.20.1/24	192.168.20.0	
		Fa7/0	192.168.30.1/24	192.168.30.0	
		Fa7/0	192.168.40.1/24	192.168.40.0	
3	PC Server Web	Fa	192.168.50.10/24	192.168.50.0	192.168.50.1
4	PC Server FTP	Fa	192.168.50.20/24	192.168.50.0	192.168.50.1
5	PC-Pimpinan	Fa	192.168.10.2/24	192.168.10.0	192.168.10.1
6	PC-Pemasaran	Fa	192.168.20.2/24	192.168.20.0	192.168.20.1
7	PC-SoftDef	Fa	192.168.30.2/24	192.168.30.0	192.168.30.1
8	PC-Course	Fa	192.168.40.2/24	192.168.40.0	192.168.40.1

Tabel 1 diatas dapat dijelaskan bahwa pembagian IP yang sudah dibuat selanjutnya akan dikonfigurasi pada masing-masing perangkat jaringan, sehingga semua perangkat mimiliki identitas atau IP address. Pada jaringan tersebut terdapat 2 (dua) router, agar semua jaringan saling terhubung diperlukan konfigurasi protokol routing. Pada penelitian ini menggunakan protokol routing dinamis jenis RIP. *Routing Information Protocol* (RIP) adalah salah satu protokol perutean dinamis pertama kali yang digunakan dalam jaringan komputer untuk mendistribusikan informasi perutean antar router. RIP menggunakan algoritma *distance vector*.

b. Konfigurasi Routing RIP

Konfigurasi routing *RIP (Routing Information Protocol)* pada Router1 dan Router2 di topologi jaringan yang sudah dibuat berfungsi untuk memungkinkan seluruh jaringan saling terhubung dan berkomunikasi, khususnya antar subnet yang terhubung ke router-router tersebut.

1). Konfigurasi Router 1

Konfigurasi routing RIP Router 1 adalah mengenalkan subnet-subnet atau jaringan yang terhubunh langsung dengan router 1, dengan perintah seperti berikut:

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 192.168.50.0
Router(config-router)#network 10.10.10.0
Router(config-router)#no auto-summary
Router(config-router)#exit
Router(config)#
```

Gambar 3. Konfigurasi RIPv2 pada Router 1

Pada gambar 3 dapat dijelaskan bahwa konfigurasi RIP dilakukan dengan cara mengenalkan network tetangganya atau network yang terhubung secara langsung dengan Router 1 yaitu network 192.168.50.0 (network menuju server) dan 10.10.10.0 (network link antar router).

2). Konfigurasi Router 2

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 192.168.10.0
Router(config-router)#network 192.168.20.0
Router(config-router)#network 192.168.30.0
Router(config-router)#network 192.168.40.0
Router(config-router)#network 10.10.10.0
Router(config-router)#no auto-summary
Router(config-router)#exit
```

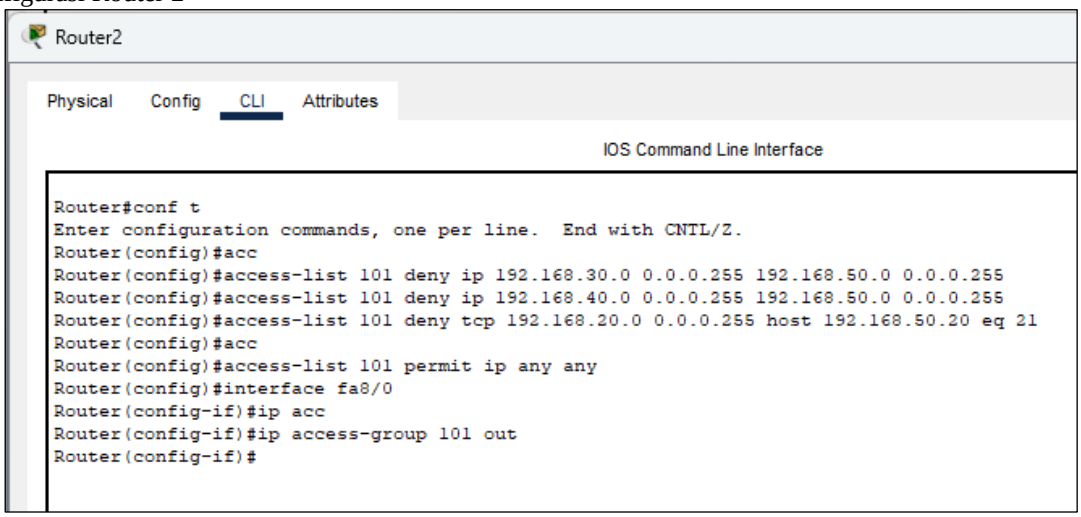
Gambar 4. Konfigurasi RIPv2 pada Router 2

Pada gambar 4 dapat dijelaskan bahwa konfigurasi RIP dilakukan dengan cara mengenalkan network tetangganya atau network yang terhubung secara langsung dengan Router 2 yaitu network 192.168.10.0 (network menuju ruang pimpinan), 192.168.20.0 (network menuju ruang pemasaran), 192.168.30.0 (network menuju ruang softdev), 192.168.10.0 (network menuju ruang ruang course) dan 10.10.10.0 (network link antar router).

c. Konfigurasi ACL

Untuk memfilter traffic atau lalu lintas jaringan sesuai skenario diatas, maka perlu dilakukan konfigurasi access control list (ACL), pada penelitian ini akan dilakukan konfigurasi dengan cara mengkombinasikan konfigurasi ACL di Router 1 dan Router 2 hal ini agar menjadi lebih efisien. ACL pada router 2 bertugas untuk memfilter lalu lintas dari berbagai divisi jaringan sebelum sampai ke router 1 (pre-filtering), sedangkan ACL pada router 1 bertugas untuk memfilter lalu lintas ke Server (destination). Sesuai topologi diatas (gambar 2), konfigurasi dilakukan Router 2 terlebih dulu, selanjutnya Router 1. Berikut konfigurasinya:

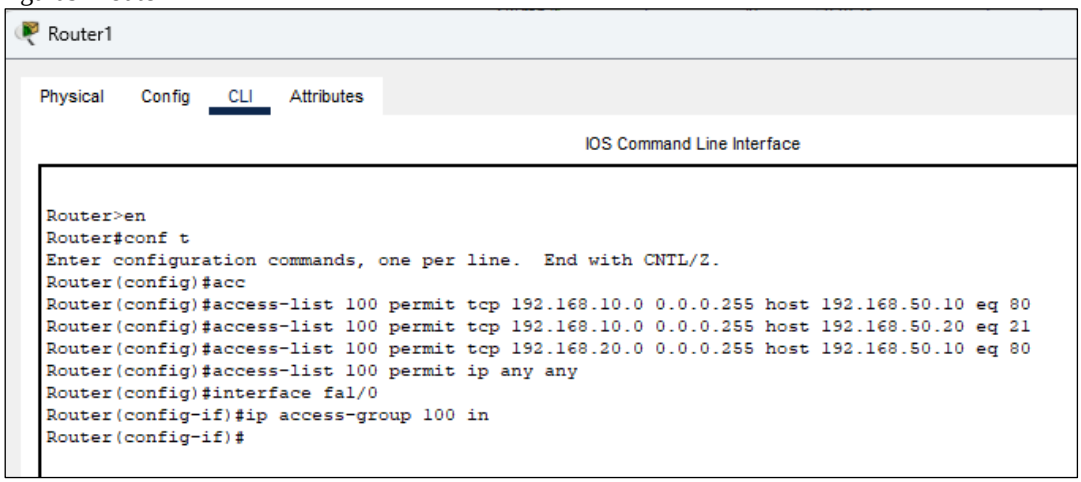
1). Konfigurasi Router 2



Gambar 5. Konfigurasi ACL pada Router 2

Pada gambar 5 dapat dijelaskan bahwa konfigurasi dilakukan bertujuan untuk tidak mengijinkan atau blokir network divisi Ruang SoftDev (192.168.30.0/24) ke divisi Server (192.168.50.0/24), blokir network divisi Ruang Course (192.168.40.0/24) ke divisi Server, dan blokir akses FTP (port 21) dari network divisi Ruang Pemasaran (192.168.20.0/24) ke Server FTP (192.168.50.20).

2). Konfigurasi Router 1



Gambar 6. Konfigurasi ACL pada Router 1

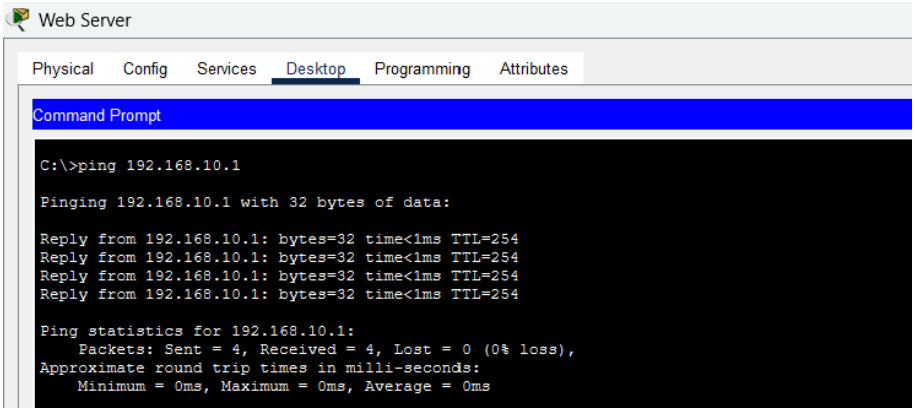
Pada gambar 6 dapat dijelaskan bahwa konfigurasi dilakukan bertujuan untuk mengijinkan network divisi Ruang Pimpinan (192.168.10.0/24) mengkases Server Web (port 80) dan FTP (port 21) dan mengijinkan network divisi Ruang Pemasan (192.168.20.0/24) hanya ke Server Web (port 80). Defaultnya, akses jaringan lainnya sesuai filtering utama sudah dikonfigurasi di Router 2.

3.4. Pengujian

Pengujian dilakukan berdasarkan skenario yang sudah dijelaskan sebelumnya, dengan protocol dan service berikut ini:

a. ICMP

Pada pengujian ICMP atau Ping, dilakukan dari sisi Server terhadap Client/Divisi-Divisi. Berdasarkan skenario bahwa sever dapat terhubung terhadap semua client/divisi. Hasilnya ditunjukkan pada gambar berikut:

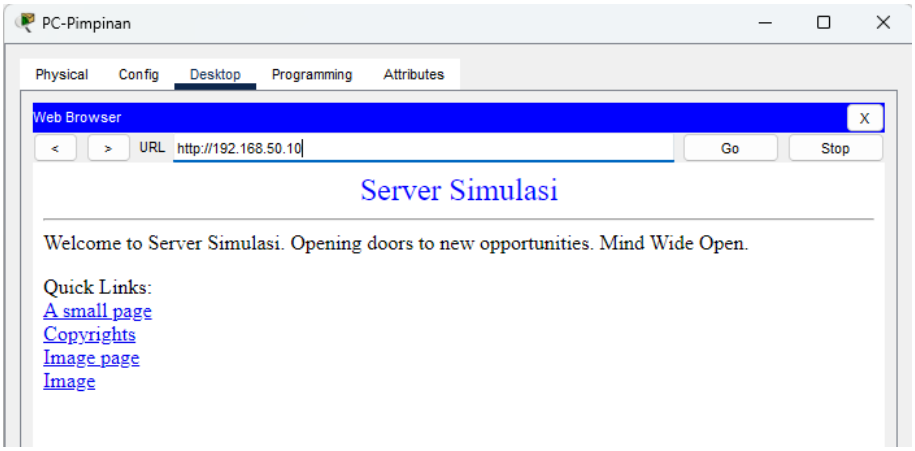


Gambar 7. Tes Koneksi Web Server ke Divisi Ruang Pimpinan

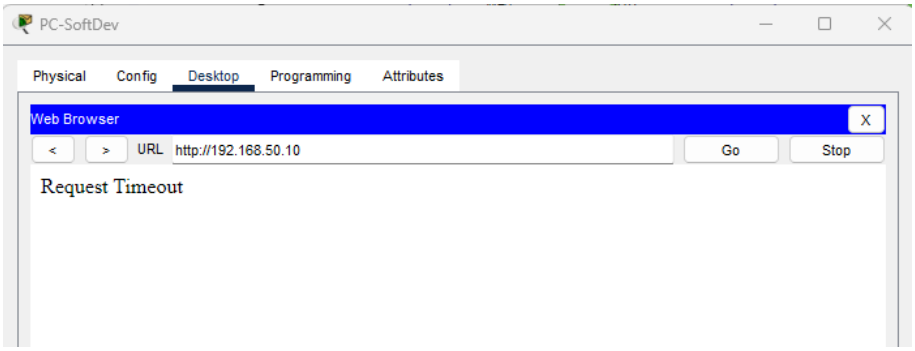
Pada gambar 7 dapat dijelaskan bahwa setelah dilakukan tes koneksi dari sisi web server terhadap jaringan divisi ruang pimpinan muncul pesan Reply, artinya bahwa jaringan tersebut sudah terhubung dan dapat berkomunikasi. Hal ini juga sama hasilnya pada divisi-divisi lainnya.

b. Web Server

Pada pengujian ini, dilakukan dari sisi Client/Divisi-Divisi terhadap Web Server. Berdasarkan skenario bahwa yang diijinkan mengakses web server adalah jaringan dari divisi Ruang Pimpinan dan Ruang Pemasaran, sedangkan divisi Ruang SoftDev dan Ruang Course tidak diijinkan. Hasilnya ditunjukkan pada gambar berikut:



Gambar 8. Tes Koneksi Divisi Ruang Pimpinan ke Web Server

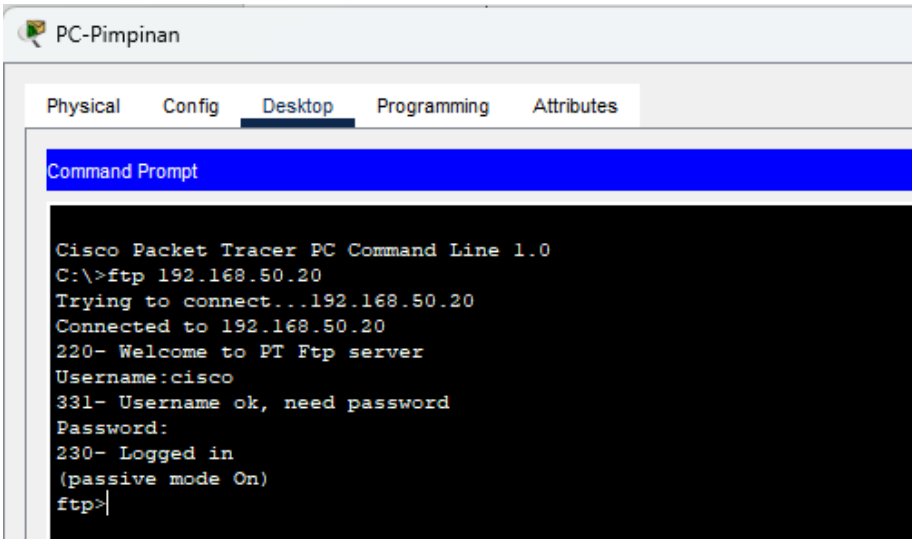


Gambar 9. Tes Koneksi Divisi Ruang SoftDev ke Web Server

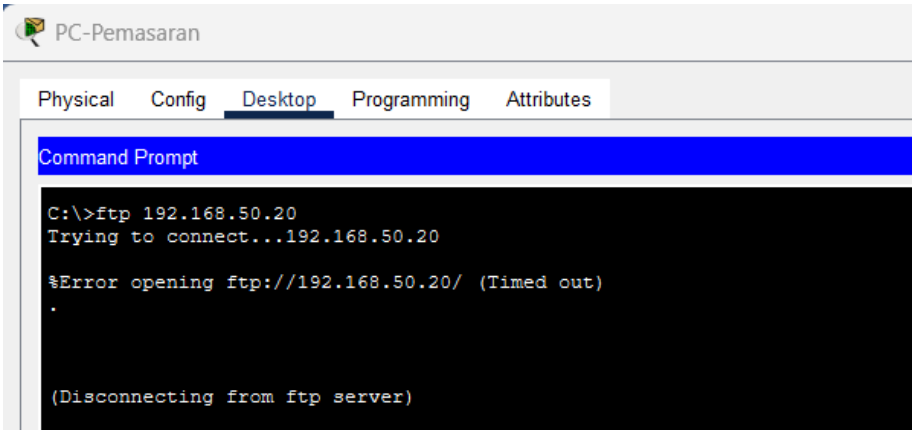
Pada gambar 8 dapat dijelaskan bahwa tes koneksi yang dilakukan berhasil terhubung, sedangkan pada gambar 9 adalah tampilan tidak terbuhung yaitu muncul pesan Request Timeout, hal ini karena divisi Ruang Covdev tidak diijikan akses Web Server. Hal ini juga sama hasilnya pada divisi-divisi lainnya sesuai skenario yang sudah dibuat.

c. FTP Server

Pada pengujian ini, dilakukan dari sisi Client/Divisi-Divisi terhadap FTP Server. Berdasarkan skenario bahwa hanya jaringan dari divisi Ruang Pimpinan yang dapat mengakses FTP server, selain itu tidak diijinkan. Hasilnya ditunjukkan pada gambar berikut:



Gambar 10. Tes Koneksi Divisi Ruang Pimpinan ke FTP Server



Gambar 11. Tes Koneksi Divisi Ruang Pemasaran ke FTP Server

Pada gambar 10 dapat dijelaskan bahwa tes koneksi yang dilakukan berhasil terhubung, sedangkan pada gambar 11 adalah tampilan ketika tidak terbuhung yaitu muncul pesan Disconnectung from ftp server, hal ini karena divisi Ruang Pemasaran tidak diijikan akses FTP Server. Hal ini juga sama hasilnya pada divisi-divisi lainnya sesuai skenario yang sudah dibuat. Pengujian-pengujian mulai dari protokol ICMP, akses ke layanan Web dan FTP server berhasil dilakukan sesuai skenario yang sudah dibuat, keberhasilan pengujian tersebut dapat dirinci pada tabel berikut ini:

Tabel 2. Pengujian dari sisi Client/Divisi Terhadap Server

Pengujian	Divisi	Network Address	Akses ke Web Server (192.168.50.10)	Akses ke FTP Server (192.168.50.20)	Persentase Keberhasilan
1	Ruang Pimpinan	192.168.10.0	Ya	Ya	100%
2	Ruang Pemasaran	192.168.20.0	Ya	Tidak	100%
3	Ruang SoftDev	192.168.30.0	Tidak	Tidak	100%
4	Ruang Course	192.168.40.0	Tidak	Tidak	100%

Tabel 3. Pengujian dari sisi Server Terhadap Client/Divisi

Pengujian	Divisi	IP Address	Akses ke Pimpinan	Akses ke Pemasaran	Akses ke SoftDev	Akses ke Course	Persentase Keberhasilan
1	PC Server Web	192.168.50.10	Ya	Ya	Ya	Ya	100%
2	PC Server FTP	192.168.50.20	Ya	Ya	Ya	Ya	100%

4. KESIMPULAN

Berdasarkan implementasi konfigurasi *Access Control List (ACL)* sebagai proteksi dan kontrol lalu lintas pada infrastruktur jaringan berhasil dilakukan, hal ini terbukti bahwa pengujian yang dilakukan sudah sesuai dengan skenario yang sudah dibuat, yaitu Jaringan divisi ruang pimpinan (192.168.10.0) dapat mengakses server FTP (192.168.50.20) maupun server Web (192.168.50.20). Jaringan divisi ruang pemasaran (192.168.20.0) hanya diijinkan akses server Web (192.168.50.20). Jaringan divisi soft. development (192.168.30.0) dan divisi course pelatihan (192.168.40.0) tidak diijinkan mengakses keduanya server Web dan server FTP, sementara divisi server memiliki akses penuh ke semua divisi didalam jaringan tersebut dengan persentase keberhasilannya adalah 100%. Dari hasil penelitian tersebut diharapkan dapat diterapkan terhadap jaringan riil sebagai proteksi dan kontrol lalu lintas pada jaringan di PT. Hidatech. Saran kedepan, agar lebih kompleks jaringan yang akan dibangun sebaiknya juga diterapkan manajemen *bandwidth,* hal ini bertujuan agar tidak terjadi perebutan *bandwidth*.

Ucapan Terimakasih

Peneliti mengucapkan banyak terimakasih kepada LPPM Universitas Muhammadiyah Jember yang telah memberikan pembiayaan penelitian ini dan telah mendukung selama berjalannya kegiatan penelitian.

DAFTAR PUSTAKA

[1] M. Rahman, M. Dasuki, and H. Oktavianto, "Implementasi Manajemen Bandwidth Simple Queue Sebagai Optimalisasi Layanan Jaringan Internet Warga Menggunakan Metode NDLC," *J. Comput. Sci. Inf. Technol.*, vol. 5, no. 1, pp. 27–35, 2024, doi: 10.37859/coscitech.v5i1.6899.

[2] M. Rahman, R. B. Hadnwika, and A. I. Zahro, "Penerapan Model Network Development Life Cycle (NDLC) Pada Infrastruktur Jaringan Internet Kantor Desa Kemiri," *J. Publ. Tek. Inform.*, vol. 2, no. 3, 2023, doi: 10.55606/jupti.v2i3.1790.

[3] M. Rahman, "Implementasi Web Content Filtering Pada Jaringan RT/RW Net Menggunakan Pi-Hole DNS Server," *Gener. J.*, vol. 7, no. 1, pp. 50–60, 2023, doi: 10.29407/gj.v7i1.19818.

[4] M. Rahman *et al.*, "Optimalisasi Jangkauan Sinyal Wireless Fidelity Menggunakan Mi WiFi Range Extender Pro," *J. Comput. Sci. Inf. Technol.*, vol. 4, no. 1, pp. 164–171, 2023, doi: 10.37859/coscitech.v4i1.4630.

[5] M. A. S. iriansyah Prayitno, M. Rahman, and D. L. Pater, "Implementasi Manajemen Bandwidth Hierarchical Token Bucket (HTB) Menggunakan Metode Network Development Life Cycle (NDLC)," vol. 5, no. 2, pp. 120–128, 2024, doi: doi.org/10.37148/bios.v5i2.131.

[6] S. Kemp, "DIGITAL 2024 : Global Overview Report," *Datareportal*, 2024. https://datareportal.com/reports/digital-2024-global-overview-report (accessed Nov. 10, 2024).

[7] APJII, "APJII Jumlah Pengguna Internet Indonesia Tembus 221 Juta Orang," *APJII (Asosiasi Penyelenggara Jasa Internet Indonesia)*, 2024. https://apjii.or.id/berita/d/apjii-jumlah-pengguna-internet-indonesia-tembus-221-juta-orang (accessed Nov. 10, 2024).

[8] I. Agrafiotis, J. R. C. Nurse, M. Goldsmith, S. Creese, and D. Upton, "A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate," *J. Cybersecurity*, vol. 4, no. 1, pp. 1–15, 2018, doi: 10.1093/cybsec/tyy006.

[9] M. D. Musielewicz, "The Spectrum of Cyber Attack," *Air Sp. Power J.*, vol. 34, no. 4, pp. 91–100, 2020, [Online]. Available: https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-34_Issue-4/V-Musielewicz.pdf

[10] D. D. Clark, K. T. Pogran, and D. P. Reed, "An Introduction to Local Area Networks," *Proc. IEEE*, vol. 66, no. 11, pp. 1497–1517, 1978, doi: 10.1109/PROC.1978.11152.

[11] Admin, "Profil Perusahaan," *PT Hidatech Indonesia*, 2024. https://hidatechindonesia.com/profil/ (accessed Nov. 11, 2024).

[12] Y. Kannan, "Access Control List (ACL) Compliance Verification and Alarm Systems: Strengthening Network Security," *Int. J. Multidiscip. Res.*, vol. 6, no. 1, pp. 1–7, 2024, doi: 10.36948/ijfmr.2024.v06i01.12734.

[13] F. Fahrizal and B. A. Candra, "Implementasi Access Control List Dalam Perancangan Virtual Local Area Network Pada PT Cakramedia Indocyber," *JEIS J. Elektro Dan Inform. Swadharma*, vol. 2, no. 2, pp. 36–43, 2022, doi: 10.56486/jeis.vol2no2.204.

[14] O. J. Usior and E. Sediyono, "Simulasi Extended ACL pada Jaringan VLAN Menggunakan Aplikasi Cisco Packet Tracer," *Aiti J. Teknol. Inf.*, vol. 20, no. 1, pp. 32–47, 2023, doi: 10.24246/aiti.v20i1.32-47.

[15] I. Cisco Systems, "Cisco Packet Tracer," *Cisco Networking Academy*, 2024. https://www.netacad.com/cisco-packet-tracer (accessed Nov. 12, 2024).