JURNAL TAMPIASIH
INSTITUT TEKNOLOGI DAN KESEHATAN ASPIRASI
E-ISSN : 2986 - 8742

# Perancangan Keamanan Jaringan Menggunakan Firewall dan Access Control List (ACL) dengan Metode System Development Life Cycle (SDLC)

**Muhammad Nasir[1], Nurul Umami[2],**
[1]Teknologi Informasi, Universitas Teknologi Mataram, Indonesia
[2]Teknologi Informasi, Institut Teknologi dan Kesehatan Aspirasi, Indonesia

Email : nasir@utm.ac.id , nurulumamy27@gmail.com[2]

**ABSTRAK**

Keamanan jaringan merupakan aspek penting dalam menjaga kerahasiaan, integritas, dan ketersediaan data pada suatu organisasi. Penelitian ini bertujuan merancang sistem keamanan jaringan menggunakan Firewall dan Access Control List (ACL) dengan pendekatan System Development Life Cycle (SDLC). Tahapan penelitian meliputi perencanaan, analisis kebutuhan, perancangan, implementasi, pengujian, dan evaluasi. Firewall digunakan untuk melakukan penyaringan lalu lintas jaringan, sedangkan ACL digunakan untuk mengatur hak akses berdasarkan alamat IP, tujuan, protokol, dan layanan jaringan. Hasil perancangan menunjukkan bahwa kombinasi Firewall dan ACL dapat digunakan untuk membentuk kebijakan akses yang lebih terkontrol, sehingga lalu lintas yang sesuai kebijakan dapat diizinkan dan akses yang tidak sesuai dapat dibatasi. Penelitian ini menghasilkan rancangan keamanan jaringan yang sistematis dan dapat dikembangkan sesuai kebutuhan organisasi.

***Kata Kunci:*** Keamanan Jaringan, Firewall, Access Control List, ACL, SDLC.

**ABSTRACT**

*Network security is a crucial aspect of maintaining the confidentiality, integrity, and availability of an organization's data. This study aims to design a network security system utilizing a firewall and Access Control Lists (ACLs) through the System Development Life Cycle (SDLC) approach. The research stages encompass planning, requirements analysis, design, implementation, testing, and evaluation. The firewall is employed to filter network traffic, while ACLs are used to manage access rights based on IP addresses, destinations, protocols, and network services. The design results demonstrate that combining a firewall and ACLs enables the establishment of more controlled access policies, allowing traffic that complies with the policy while restricting unauthorized access. This research yields a systematic network security design that can be further developed to meet the organization's specific needs.*

***Keywords:*** *Network Security, Firewall, Access Control List, ACL, SDLC.*

***Corresponding author:** nasir@utm.ac.id

## PENDAHULUAN

Perkembangan teknologi informasi telah menjadikan jaringan komputer sebagai salah satu komponen utama dalam mendukung aktivitas organisasi, baik untuk pertukaran informasi, penggunaan aplikasi, komunikasi internal, maupun akses terhadap layanan berbasis internet. Ketergantungan terhadap jaringan tersebut menyebabkan aspek keamanan menjadi semakin penting karena setiap perangkat yang terhubung dapat menjadi bagian dari jalur komunikasi data. Data yang berpindah melalui jaringan harus mendapatkan perlindungan agar tidak mudah diakses oleh pihak yang tidak memiliki kewenangan. Permasalahan keamanan tidak hanya berkaitan dengan serangan dari jaringan eksternal, tetapi juga dapat berasal dari akses internal yang tidak sesuai dengan kebijakan organisasi. Oleh karena itu, pengelolaan keamanan jaringan perlu dilakukan melalui mekanisme yang mampu mengidentifikasi, mengendalikan, dan membatasi lalu lintas berdasarkan aturan yang telah ditetapkan. Penelitian mengenai keamanan jaringan menunjukkan bahwa penerapan mekanisme filtering dapat digunakan untuk mengendalikan komunikasi antara jaringan dan sumber daya yang dilindungi. Firmansyah dan Wahyudi menunjukkan bahwa penerapan firewall berbasis kebijakan dapat membatasi akses menuju server dari client sesuai aturan yang ditetapkan. (Firmansyah & Wahyudi, 2021) Kondisi tersebut menunjukkan bahwa keamanan jaringan tidak cukup hanya mengandalkan konektivitas, tetapi membutuhkan mekanisme pengendalian akses yang dirancang berdasarkan kebutuhan. Firewall menjadi salah satu teknologi yang dapat digunakan untuk melakukan penyaringan terhadap lalu lintas data yang masuk maupun keluar dari jaringan. Firewall bekerja dengan menerapkan aturan tertentu sehingga paket data dapat diperiksa sebelum diteruskan menuju tujuan. Dalam implementasinya, firewall dapat dikombinasikan dengan ACL untuk memberikan pengendalian yang lebih terarah terhadap komunikasi jaringan. Putra, Ispandi, dan Lubis menjelaskan bahwa firewall dapat digunakan untuk menyaring paket yang masuk dan keluar dari jaringan, sementara ACL dapat digunakan sebagai mekanisme filtering pada perangkat jaringan. (Putra et al., 2023) Dengan demikian, penerapan firewall dan ACL dapat menjadi salah satu pendekatan dalam membangun sistem keamanan jaringan yang memiliki kebijakan akses yang lebih terstruktur.

Access Control List merupakan mekanisme yang dapat digunakan untuk menentukan apakah lalu lintas jaringan tertentu diperbolehkan atau ditolak berdasarkan parameter yang telah ditentukan. Parameter tersebut dapat mencakup alamat sumber, alamat tujuan, protokol, maupun port layanan. Penerapan ACL memungkinkan administrator jaringan untuk menentukan hubungan komunikasi yang diperbolehkan antara satu jaringan dengan jaringan lainnya. Hal tersebut menjadi penting terutama pada lingkungan yang memiliki beberapa kelompok pengguna dan sumber daya dengan tingkat akses berbeda. Sebagai contoh, jaringan pengguna umum dapat diberikan akses terhadap layanan internet, tetapi tidak diberikan akses langsung terhadap server tertentu yang berisi data internal. Sebaliknya, kelompok administrator dapat diberikan hak akses yang lebih luas sesuai dengan tugas dan kewenangannya. Penelitian Rahman dan Dasuki memperlihatkan bahwa ACL dapat digunakan untuk mengatur akses antarjaringan dan membedakan layanan yang dapat diakses oleh setiap kelompok jaringan. Pada penelitian tersebut, aturan ACL digunakan untuk memberikan akses berbeda kepada beberapa divisi terhadap server web dan FTP. (M. Rahman & Dasuki, 2025) Hal ini memperlihatkan bahwa ACL tidak hanya berfungsi sebagai mekanisme pemblokiran, tetapi juga dapat menjadi instrumen penerapan kebijakan akses jaringan. Selain itu, penelitian mengenai penerapan VLAN dan ACL menunjukkan bahwa segmentasi jaringan yang disertai pengaturan akses dapat digunakan untuk meningkatkan pengendalian komunikasi antarsegmen jaringan. (T. Rahman & Aprianto, 2025) Berdasarkan kondisi tersebut, perancangan

firewall dan ACL perlu dilakukan secara sistematis agar aturan yang diterapkan tidak mengganggu layanan yang sah. Kesalahan dalam menentukan aturan dapat menyebabkan layanan yang dibutuhkan pengguna ikut terblokir atau sebaliknya membuka akses yang seharusnya dibatasi. Oleh sebab itu, diperlukan suatu metode pengembangan yang dapat mengarahkan proses perancangan mulai dari identifikasi kebutuhan sampai tahap evaluasi.

Salah satu metode yang dapat digunakan untuk memberikan tahapan sistematis dalam pengembangan sistem adalah System Development Life Cycle (SDLC). SDLC merupakan pendekatan yang membagi proses pengembangan ke dalam beberapa tahapan sehingga kebutuhan sistem dapat dianalisis sebelum sistem dirancang dan diterapkan. Dalam konteks penelitian keamanan jaringan, SDLC dapat diadaptasi melalui tahapan perencanaan, analisis, desain, implementasi, pengujian, serta evaluasi atau pemeliharaan. Tahap perencanaan digunakan untuk menentukan tujuan dan ruang lingkup sistem keamanan. Tahap analisis digunakan untuk mengidentifikasi kondisi jaringan, perangkat, kebutuhan pengguna, layanan, serta potensi akses yang perlu dikendalikan. Tahap desain digunakan untuk menyusun rancangan topologi dan kebijakan firewall serta ACL. Selanjutnya, tahap implementasi digunakan untuk menerapkan rancangan pada lingkungan jaringan atau lingkungan simulasi. Tahap pengujian dilakukan untuk memastikan bahwa aturan yang diterapkan mampu membedakan lalu lintas yang diizinkan dan ditolak. Adapun tahap evaluasi dilakukan untuk menilai kesesuaian hasil penerapan dengan kebutuhan keamanan yang telah ditetapkan. Pendekatan bertahap tersebut relevan dengan penelitian keamanan jaringan karena konfigurasi keamanan tidak seharusnya dilakukan tanpa didahului analisis kebutuhan. Penelitian terkait ACL pada jaringan LAN, misalnya, menggunakan tahapan pengumpulan data, desain, implementasi, dan pengujian untuk menghasilkan pengendalian akses yang sesuai dengan kebutuhan jaringan. (M. Rahman & Dasuki, 2025) Dengan menggunakan SDLC, penelitian ini menempatkan firewall dan ACL bukan hanya sebagai konfigurasi teknis, tetapi sebagai bagian dari proses perancangan sistem keamanan yang memiliki tujuan, kebutuhan, aturan, serta mekanisme evaluasi yang jelas.

Berdasarkan uraian tersebut, penelitian ini berfokus pada perancangan keamanan jaringan menggunakan Firewall dan Access Control List (ACL) dengan metode SDLC. Perancangan diarahkan untuk menghasilkan mekanisme pengendalian lalu lintas jaringan berdasarkan kebijakan akses yang telah ditentukan. Firewall digunakan sebagai lapisan pengamanan terhadap lalu lintas jaringan, sedangkan ACL digunakan untuk mengatur akses berdasarkan sumber, tujuan, dan layanan yang diperbolehkan. Penelitian ini diharapkan dapat memberikan rancangan yang sistematis sehingga administrator jaringan dapat mengetahui jenis akses yang diperbolehkan, akses yang harus dibatasi, serta alasan penerapan setiap aturan. Pengujian dilakukan dengan membandingkan kondisi akses terhadap kebijakan yang telah dirancang. Akses yang sesuai dengan aturan diharapkan dapat diteruskan, sedangkan akses yang tidak sesuai diharapkan dapat ditolak. Pendekatan tersebut sejalan dengan hasil penelitian sebelumnya yang menunjukkan bahwa ACL dapat digunakan sebagai mekanisme proteksi dan pengendalian traffic pada infrastruktur LAN. (M. Rahman & Dasuki, 2025) Dengan demikian, kontribusi penelitian ini terletak pada penyusunan proses perancangan keamanan jaringan yang mengintegrasikan Firewall dan ACL melalui tahapan SDLC. Hasil penelitian diharapkan tidak hanya berupa konfigurasi perangkat, tetapi juga dokumentasi kebutuhan, desain keamanan, aturan akses, skenario pengujian, serta evaluasi hasil penerapan. Rancangan tersebut dapat menjadi dasar pengembangan sistem keamanan jaringan yang lebih terstruktur dan dapat disesuaikan dengan perubahan kebutuhan organisasi.

## METODE PENELITIAN

Penelitian ini menggunakan pendekatan System Development Life Cycle (SDLC) sebagai metode utama dalam proses perancangan keamanan jaringan. Pemilihan SDLC didasarkan pada kebutuhan penelitian untuk menghasilkan proses yang sistematis mulai dari identifikasi permasalahan sampai evaluasi rancangan. Penelitian dilaksanakan melalui beberapa tahapan, yaitu perencanaan, analisis, perancangan, implementasi, pengujian, dan evaluasi. Pada tahap perencanaan, dilakukan identifikasi terhadap tujuan penelitian dan kebutuhan keamanan jaringan yang akan dirancang. Permasalahan yang menjadi perhatian adalah kebutuhan pengendalian lalu lintas jaringan agar komunikasi antarjaringan dapat berjalan sesuai dengan kebijakan akses. Tahap berikutnya adalah analisis terhadap kondisi jaringan, yang meliputi identifikasi perangkat jaringan, segmentasi jaringan, alamat IP, layanan yang digunakan, serta hubungan komunikasi antara client dan server. Data yang diperoleh pada tahap analisis digunakan sebagai dasar untuk menentukan aturan keamanan. Metode pengumpulan data dapat dilakukan melalui observasi terhadap topologi jaringan, dokumentasi konfigurasi perangkat, wawancara dengan pengelola jaringan apabila penelitian dilakukan pada objek nyata, serta studi pustaka untuk memperkuat landasan teknis penelitian. Studi terdahulu mengenai ACL menunjukkan bahwa tahapan pengumpulan data, desain, implementasi, dan pengujian dapat digunakan dalam penelitian pengendalian traffic jaringan. (M. Rahman & Dasuki, 2025) Selain itu, penelitian mengenai firewall menunjukkan bahwa perancangan sistem filtering perlu mempertimbangkan perangkat yang digunakan karena implementasi firewall dapat berbeda antara perangkat jaringan. (Putra et al., 2023) Oleh karena itu, tahap analisis dalam penelitian ini menjadi dasar untuk menentukan bentuk konfigurasi yang sesuai dengan lingkungan jaringan. Setelah kebutuhan berhasil diidentifikasi, penelitian dilanjutkan ke tahap desain untuk menerjemahkan kebutuhan keamanan menjadi rancangan teknis yang dapat diimplementasikan.

Tahap desain dilakukan dengan menyusun rancangan topologi jaringan dan kebijakan keamanan yang akan diterapkan pada firewall dan ACL. Rancangan topologi menggambarkan hubungan antara jaringan eksternal, perangkat firewall atau router, switch, client, dan server. Dalam rancangan tersebut, setiap jaringan diberikan alamat IP atau subnet yang sesuai sehingga sumber dan tujuan komunikasi dapat diidentifikasi. Setelah topologi ditentukan, dibuat kebijakan akses atau security policy yang menjadi dasar konfigurasi. Kebijakan tersebut dapat berupa aturan yang mengizinkan jaringan internal mengakses internet, mengizinkan kelompok administrator mengakses server tertentu, membatasi jaringan pengguna umum terhadap server internal, serta menolak akses dari sumber yang tidak dikenal. ACL kemudian dirancang berdasarkan parameter seperti source IP, destination IP, protocol, dan destination port. Apabila penelitian menggunakan perangkat Cisco, ACL dapat diterapkan pada interface router sesuai arah lalu lintas yang direncanakan. Sementara itu, firewall dapat digunakan untuk menerapkan filtering terhadap lalu lintas masuk dan keluar. Penentuan aturan harus dilakukan berdasarkan prinsip kebutuhan akses sehingga hanya komunikasi yang diperlukan yang diberikan izin. Penelitian Firmansyah dan Wahyudi menunjukkan bahwa firewall berbasis kebijakan dapat digunakan untuk membatasi akses menuju server dari client tertentu. (Firmansyah & Wahyudi, 2021) Penelitian Rahman dan Dasuki juga menunjukkan bahwa ACL dapat memberikan hak akses berbeda kepada kelompok jaringan terhadap layanan server tertentu. (M. Rahman & Dasuki, 2025) Oleh karena itu, rancangan penelitian ini menggunakan pendekatan allow berdasarkan kebutuhan dan deny terhadap akses yang tidak sesuai kebijakan. Setiap aturan didokumentasikan agar administrator dapat mengetahui fungsi, sumber, tujuan, layanan, dan tindakan yang diberikan. Dokumentasi tersebut juga penting pada tahap pengujian karena setiap rule harus memiliki skenario pengujian yang sesuai.

Tahap implementasi dilakukan dengan menerapkan rancangan yang telah dibuat pada perangkat jaringan atau lingkungan simulasi. Apabila penelitian dilakukan menggunakan simulator, konfigurasi dapat diterapkan pada perangkat virtual yang tersedia di lingkungan simulasi. Implementasi dimulai dengan konfigurasi dasar perangkat jaringan, pemberian alamat IP pada interface, konfigurasi routing apabila diperlukan, kemudian dilanjutkan dengan penerapan firewall dan ACL. ACL ditempatkan pada interface yang tepat berdasarkan arah lalu lintas yang hendak dikendalikan. Setiap rule dibuat berdasarkan hasil analisis dan rancangan kebijakan yang telah ditentukan sebelumnya. Setelah konfigurasi diterapkan, dilakukan pemeriksaan terhadap konfigurasi untuk memastikan tidak terdapat kesalahan sintaks maupun aturan yang bertentangan. Tahap implementasi tidak hanya berorientasi pada keberhasilan konfigurasi, tetapi juga memastikan bahwa layanan jaringan yang sah tetap dapat digunakan. Hal ini penting karena aturan keamanan yang terlalu ketat dapat mengakibatkan gangguan terhadap aktivitas pengguna. Sebaliknya, aturan yang terlalu longgar dapat menyebabkan akses yang seharusnya dibatasi tetap tersedia. Penelitian mengenai implementasi firewall dan ACL menunjukkan bahwa konfigurasi ACL dapat digunakan untuk menyaring paket data yang masuk dan keluar dari jaringan. Penelitian Rahman dan Dasuki juga memperlihatkan bahwa penerapan ACL dapat menghasilkan perbedaan hak akses antarsegmen jaringan sesuai dengan kebijakan yang ditentukan. Dengan demikian, implementasi dalam penelitian ini dilakukan secara bertahap dan setiap konfigurasi dicatat sebagai bagian dari dokumentasi penelitian.

Tahap terakhir dalam metode penelitian adalah pengujian dan evaluasi. Pengujian dilakukan untuk mengetahui apakah konfigurasi firewall dan ACL telah berjalan sesuai dengan rancangan keamanan. Skenario pengujian dibuat berdasarkan aturan yang telah ditentukan, sehingga terdapat minimal dua kondisi, yaitu akses yang seharusnya diizinkan dan akses yang seharusnya ditolak. Pengujian konektivitas dapat dilakukan menggunakan ping untuk melihat keterjangkauan antarperangkat, sedangkan pengujian layanan dapat dilakukan berdasarkan protokol dan port yang digunakan. Misalnya, apabila suatu client diizinkan mengakses web server melalui HTTP atau HTTPS, maka pengujian dilakukan untuk memastikan layanan tersebut dapat diakses. Sebaliknya, apabila suatu jaringan tidak diizinkan mengakses server tertentu, pengujian dilakukan untuk memastikan komunikasi tersebut ditolak. Hasil pengujian dicatat dalam tabel yang berisi sumber, tujuan, layanan, aturan, hasil yang diharapkan, dan hasil aktual. Evaluasi dilakukan dengan membandingkan hasil aktual dengan hasil yang diharapkan. Apabila hasil pengujian tidak sesuai, konfigurasi dianalisis kembali untuk menemukan penyebabnya, kemudian dilakukan perbaikan pada tahap implementasi. Siklus evaluasi tersebut dapat dilakukan sampai konfigurasi memenuhi kebutuhan keamanan yang telah ditetapkan. Pendekatan pengujian semacam ini juga digunakan dalam penelitian ACL yang mengevaluasi perbedaan akses antarsegmen jaringan berdasarkan aturan yang diterapkan. Dengan demikian, metode SDLC dalam penelitian ini menghasilkan alur yang sistematis dari identifikasi kebutuhan hingga evaluasi konfigurasi keamanan jaringan.

## HASIL DAN PEMBAHASAN

Hasil penelitian berupa rancangan sistem keamanan jaringan yang mengintegrasikan firewall dan ACL untuk mengendalikan lalu lintas jaringan berdasarkan kebijakan akses. Rancangan terdiri atas jaringan eksternal, perangkat firewall/router, switch, jaringan client, dan server. Pada rancangan tersebut, firewall ditempatkan sebagai pengendali lalu lintas antara jaringan internal dan jaringan eksternal, sedangkan ACL diterapkan untuk mengatur komunikasi berdasarkan alamat sumber, alamat tujuan, protokol, dan layanan. Rancangan keamanan diawali dengan prinsip bahwa tidak seluruh perangkat dalam jaringan memiliki kebutuhan akses yang sama. Oleh karena itu, setiap kelompok jaringan diberikan hak akses berdasarkan fungsi dan kebutuhan operasionalnya. Jaringan

pengguna dapat diberikan akses terhadap layanan internet yang diperlukan, sedangkan akses terhadap server internal dibatasi berdasarkan kebutuhan. Administrator diberikan akses yang lebih luas terhadap perangkat atau server yang menjadi tanggung jawabnya. Sementara itu, lalu lintas yang berasal dari sumber yang tidak dikenal atau tidak sesuai dengan kebijakan dapat ditolak. Rancangan tersebut menunjukkan bahwa firewall dan ACL memiliki fungsi yang saling melengkapi. Firewall berperan sebagai mekanisme filtering pada batas jaringan, sedangkan ACL memberikan kontrol yang lebih spesifik terhadap aliran komunikasi. Penelitian Putra, Ispandi, dan Lubis menunjukkan bahwa firewall dengan ACL dapat digunakan untuk melakukan filtering paket yang masuk dan keluar dari jaringan. Hasil tersebut mendukung rancangan penelitian ini karena pengendalian lalu lintas perlu dilakukan berdasarkan kebijakan yang dapat diterjemahkan ke dalam rule. Selain itu, penelitian Firmansyah dan Wahyudi memperlihatkan bahwa kebijakan firewall dapat membatasi akses client menuju server. Berdasarkan hasil perancangan tersebut, sistem keamanan tidak hanya berfungsi sebagai penghalang akses, tetapi juga sebagai mekanisme untuk memastikan bahwa komunikasi jaringan berlangsung sesuai dengan kebutuhan.

Hasil berikutnya berupa rancangan aturan ACL yang digunakan untuk mengontrol komunikasi antarjaringan. ACL dirancang dengan mempertimbangkan hubungan antara jaringan sumber dan jaringan tujuan. Sebagai contoh, jaringan pengguna umum dapat diberikan akses menuju layanan web dan DNS yang diperlukan untuk aktivitas internet, tetapi akses langsung terhadap server administrasi dapat dibatasi. Jaringan administrator dapat diberikan akses menuju server berdasarkan port layanan yang dibutuhkan. Sementara itu, akses dari jaringan eksternal menuju jaringan internal dapat ditolak kecuali terdapat layanan tertentu yang memang sengaja dipublikasikan. Pola aturan tersebut bertujuan menerapkan prinsip pembatasan akses berdasarkan kebutuhan. Setiap rule memiliki parameter yang jelas sehingga proses pengelolaan keamanan dapat dilakukan secara lebih terstruktur. Dalam implementasi ACL, urutan rule juga menjadi aspek penting karena perangkat jaringan akan memproses aturan berdasarkan urutan tertentu. Oleh sebab itu, aturan yang lebih spesifik perlu ditempatkan dengan tepat agar tidak tertutup oleh aturan yang lebih umum. Hasil penelitian Rahman dan Dasuki menunjukkan bahwa ACL dapat digunakan untuk membedakan hak akses antarjaringan terhadap layanan web dan FTP. Temuan tersebut memperkuat bahwa ACL dapat diterapkan untuk membangun kebijakan akses berbasis kelompok jaringan. Selain itu, penelitian Kurniati dan Dasmen mengenai simulasi ACL pada jaringan PT KAI Palembang menunjukkan penggunaan ACL sebagai bagian dari pengamanan jaringan dan pembatasan akses pengguna. (Kurniati & Dasmen, 2019) Berdasarkan hasil tersebut, penerapan ACL dalam penelitian ini diarahkan untuk menghasilkan aturan yang sederhana, terukur, dan mudah dievaluasi. Rule yang tidak diperlukan perlu dihindari karena dapat meningkatkan kompleksitas konfigurasi dan menyulitkan administrator ketika melakukan pemeliharaan.

Hasil pengujian rancangan dilakukan berdasarkan skenario akses yang telah ditentukan. Skenario pertama digunakan untuk menguji akses yang diizinkan, misalnya komunikasi dari jaringan internal menuju layanan internet atau server yang memang diperlukan. Apabila komunikasi tersebut berhasil dilakukan, maka rule dapat dinilai sesuai dengan kebijakan akses. Skenario kedua digunakan untuk menguji akses yang harus ditolak, misalnya akses dari jaringan pengguna menuju server internal yang tidak termasuk dalam hak aksesnya. Apabila komunikasi tidak dapat dilakukan sesuai dengan rule penolakan, maka mekanisme filtering telah bekerja sesuai rancangan. Pengujian juga dapat dilakukan terhadap beberapa protokol dan port untuk memastikan bahwa ACL tidak hanya membatasi berdasarkan alamat IP tetapi juga dapat mengendalikan jenis layanan tertentu apabila menggunakan extended ACL. Hasil penelitian sebelumnya menunjukkan bahwa ACL dapat digunakan untuk menghasilkan pembagian hak akses yang berbeda berdasarkan jaringan sumber dan layanan tujuan. Rahman dan Dasuki, misalnya, melaporkan bahwa beberapa divisi diberikan

akses berbeda terhadap web server dan FTP server sesuai kebijakan yang dirancang. Sementara itu, Firmansyah dan Wahyudi menunjukkan bahwa penerapan firewall policy dapat membatasi akses menuju server. Dengan demikian, hasil pengujian dalam penelitian ini dianalisis berdasarkan kesesuaian antara kondisi aktual dan kebijakan yang telah ditetapkan, bukan sekadar berdasarkan keberhasilan koneksi. Pengujian tersebut menjadi penting karena tujuan utama sistem keamanan adalah memastikan bahwa akses yang sah tetap tersedia dan akses yang tidak sah dapat dikendalikan. Apabila ditemukan akses yang seharusnya ditolak tetapi masih berhasil, rule perlu diperiksa kembali. Sebaliknya, apabila akses yang seharusnya diizinkan justru gagal, aturan perlu disesuaikan agar tidak mengganggu layanan operasional.

Pembahasan hasil penelitian menunjukkan bahwa penggunaan firewall dan ACL dengan pendekatan SDLC memberikan kerangka yang lebih terstruktur dalam perancangan keamanan jaringan. SDLC membantu memastikan bahwa konfigurasi tidak langsung dilakukan tanpa melalui proses identifikasi kebutuhan, analisis kondisi jaringan, dan penyusunan kebijakan. Tahap perencanaan menentukan tujuan keamanan, tahap analisis mengidentifikasi kebutuhan akses, tahap desain menerjemahkan kebutuhan menjadi aturan, tahap implementasi menerapkan konfigurasi, sedangkan tahap pengujian dan evaluasi memastikan bahwa konfigurasi sesuai dengan rancangan. Pendekatan ini juga memberikan kemudahan dalam melakukan pemeliharaan karena setiap rule memiliki dasar kebutuhan yang dapat ditelusuri. Dari perspektif keamanan, firewall dan ACL dapat mengurangi ruang akses yang tersedia bagi pengguna atau sumber yang tidak memiliki kewenangan. Namun, efektivitas sistem tidak hanya ditentukan oleh keberadaan firewall dan ACL, tetapi juga oleh ketepatan konfigurasi, pengelolaan rule, pemantauan log, serta pembaruan kebijakan apabila kebutuhan jaringan berubah. Penelitian terbaru mengenai penerapan VLAN dan ACL juga menunjukkan bahwa segmentasi jaringan dapat dikombinasikan dengan ACL untuk membatasi komunikasi antarsegmen berdasarkan kebutuhan. Oleh karena itu, hasil penelitian ini menunjukkan bahwa keamanan jaringan sebaiknya dipandang sebagai proses berkelanjutan, bukan konfigurasi yang hanya dilakukan satu kali. Evaluasi berkala diperlukan untuk memastikan bahwa aturan yang diterapkan masih relevan dengan perkembangan perangkat, pengguna, layanan, dan kebutuhan organisasi. Dengan demikian, rancangan firewall dan ACL berbasis SDLC dapat menjadi dasar pengembangan keamanan jaringan yang lebih terkontrol, terdokumentasi, dan mudah dikembangkan pada tahap berikutnya.

## KESIMPULAN

Berdasarkan hasil perancangan dan pembahasan, dapat disimpulkan bahwa keamanan jaringan membutuhkan mekanisme pengendalian akses yang mampu membatasi lalu lintas berdasarkan kebijakan yang telah ditentukan. Firewall dapat digunakan sebagai mekanisme penyaringan lalu lintas pada batas jaringan, sedangkan Access Control List (ACL) dapat digunakan untuk mengatur akses berdasarkan sumber, tujuan, protokol, maupun layanan jaringan. Kombinasi kedua mekanisme tersebut memungkinkan administrator menentukan komunikasi yang diperbolehkan dan komunikasi yang harus ditolak. Dengan adanya aturan yang jelas, akses terhadap sumber daya jaringan dapat disesuaikan dengan kebutuhan masing-masing kelompok pengguna. Hasil penelitian terdahulu juga mendukung penggunaan firewall dan ACL sebagai mekanisme filtering dan pengendalian akses jaringan. Putra, Ispandi, dan Lubis menunjukkan bahwa ACL dapat digunakan sebagai bagian dari firewall untuk menyaring paket yang masuk dan keluar dari jaringan. Sementara itu, Rahman dan Dasuki menunjukkan bahwa ACL dapat menghasilkan pembagian hak akses yang berbeda antarjaringan berdasarkan layanan yang dibutuhkan. Dengan demikian, penerapan firewall

dan ACL dalam rancangan penelitian ini dapat digunakan sebagai salah satu pendekatan untuk meningkatkan pengendalian keamanan jaringan.

Penerapan metode SDLC memberikan tahapan yang sistematis dalam proses perancangan keamanan jaringan. Tahap perencanaan digunakan untuk menentukan tujuan dan ruang lingkup keamanan, tahap analisis digunakan untuk mengidentifikasi kebutuhan akses dan kondisi jaringan, tahap desain digunakan untuk menentukan topologi serta aturan firewall dan ACL, tahap implementasi digunakan untuk menerapkan konfigurasi, sedangkan tahap pengujian dan evaluasi digunakan untuk memastikan kesesuaian konfigurasi dengan kebutuhan. Pendekatan tersebut mengurangi risiko penerapan aturan secara sembarangan karena setiap konfigurasi memiliki dasar dari hasil analisis sebelumnya. Selain itu, dokumentasi yang dihasilkan pada setiap tahapan dapat membantu administrator memahami fungsi masing-masing aturan. Hal tersebut menjadi penting karena perubahan kebutuhan jaringan dapat menyebabkan perubahan terhadap kebijakan keamanan. Oleh sebab itu, penggunaan SDLC dalam penelitian ini tidak hanya memberikan struktur terhadap proses teknis, tetapi juga memberikan kerangka pengelolaan sistem keamanan yang dapat dievaluasi dan dikembangkan. Hasil penelitian mengenai keamanan jaringan dengan firewall juga menunjukkan pentingnya perencanaan dan penerapan filtering untuk melindungi informasi yang masuk maupun keluar dari jaringan.

Berdasarkan skenario pengujian, keberhasilan rancangan keamanan ditentukan oleh kesesuaian antara akses aktual dengan kebijakan yang telah ditetapkan. Akses yang memang dibutuhkan harus tetap dapat berlangsung, sedangkan akses yang tidak memiliki kewenangan harus dapat dibatasi oleh firewall atau ACL. Dengan demikian, parameter keberhasilan bukan hanya kemampuan sistem dalam memblokir akses, tetapi juga kemampuannya mempertahankan ketersediaan layanan yang sah. Penerapan rule harus dilakukan secara hati-hati agar tidak menimbulkan konflik antaraturan. Administrator juga perlu melakukan evaluasi terhadap rule secara berkala untuk menghapus aturan yang tidak lagi diperlukan dan menyesuaikan aturan dengan perubahan kebutuhan organisasi. Penelitian mengenai implementasi ACL pada LAN menunjukkan bahwa aturan yang berbeda dapat digunakan untuk memberikan akses berbeda terhadap beberapa kelompok jaringan dan layanan server. Temuan tersebut memperkuat bahwa pengendalian akses dapat dirancang secara spesifik berdasarkan kebutuhan organisasi. Oleh karena itu, rancangan yang dihasilkan dalam penelitian ini dapat dikembangkan lebih lanjut melalui penambahan segmentasi jaringan, monitoring, pencatatan log, serta mekanisme keamanan lainnya sesuai dengan kebutuhan dan skala jaringan.

Secara keseluruhan, penelitian ini menunjukkan bahwa perancangan keamanan jaringan menggunakan Firewall dan Access Control List (ACL) dengan metode SDLC dapat menghasilkan pendekatan keamanan yang terstruktur dalam mengendalikan lalu lintas jaringan. Firewall berperan dalam melakukan filtering pada lalu lintas jaringan, sedangkan ACL memberikan pengaturan akses yang lebih spesifik terhadap sumber daya jaringan. SDLC memberikan alur pengembangan mulai dari perencanaan hingga evaluasi sehingga setiap tahap dapat didokumentasikan dan diperiksa. Rancangan ini dapat menjadi dasar bagi organisasi dalam membangun kebijakan keamanan jaringan yang lebih terkontrol. Untuk pengembangan penelitian selanjutnya, sistem dapat diperluas dengan penerapan VLAN untuk segmentasi jaringan, sistem monitoring dan logging, Intrusion Detection System, serta pengujian pada lingkungan jaringan nyata. Pengembangan tersebut diperlukan agar mekanisme keamanan tidak hanya berfokus pada filtering, tetapi juga mampu memberikan informasi mengenai aktivitas jaringan dan potensi kejadian keamanan. Dengan demikian, firewall dan ACL dapat ditempatkan sebagai bagian dari strategi keamanan jaringan yang lebih menyeluruh dan dapat disesuaikan dengan perkembangan kebutuhan organisasi.

**UCAPAN TERIMA KASIH**

Penulis mengucapkan terima kasih yang sebesar-besarnya kepada rekan-rekan sejawat yang telah memberikan masukan dan saran konstruktif demi menyempurnakan karya ilmiah ini.

**DAFTAR PUSTAKA**

Firmansyah, F., & Wahyudi, M. (2021). Analisis Performa Access Control List Menggunakan Metode Firewall Policy Base. *MATRIK: Jurnal Manajemen, Teknik Informatika Dan Rekayasa Komputer*, *20*(2), 283–292.

Kurniati, K., & Dasmen, R. N. (2019). The Simulation of Access Control List (ACLs) Network Security for Frame Relay Network at PT. KAI Palembang. *Lontar Komputer: Jurnal Ilmiah Teknologi Informasi*, *10*(1), 49.

Putra, A. A., Ispandi, I., & Lubis, B. O. (2023). Perancangan Firewall dan Spanning Tree Protocol Sebagai Sistem Keamanan Jaringan Komputer. *Jurnal Teknologi Informatika Dan Komputer*, *9*(1), 48–60.

Rahman, M., & Dasuki, M. (2025). Implementasi access control list (ACL) sebagai metode proteksi dan traffic control pada infrastruktur jaringan local area network (LAN). *Jurnal CoSciTech (Computer Science and Information Technology)*, *6*(1), 68–76.

Rahman, T., & Aprianto, Q. (2025). Implementation of VLAN and ACL for network security at SDIT Ibnu Hajar Bekasi. *Journal of Electrical Engineering and Computer (JEECOM)*, *7*(2), 564–571.