BAB II
TINJAUAN PUSTAKA

2.1 Penelitian Terdahulu

Dalam penelitian ini, studi literatur digunakan untuk memahami lebih mendalam teori, metode, serta hasil dari penelitian-penelitian sebelumnya yang relevan dengan topik yang sedang diteliti. Studi literatur ini memberikan landasan yang kuat dalam merumuskan pendekatan penelitian, sekaligus membantu dalam mengidentifikasi celah penelitian yang dapat diisi melalui studi ini. Selain itu, sejumlah studi juga menyoroti pentingnya pengamanan jaringan pada arsitektur modern seperti Software Defined Network (SDN) yang belum dilengkapi fitur keamanan bawaan sejak awal pengembangannya, sehingga rentan terhadap serangan DdoS [10]. Berikut adalah tabel yang merangkum beberapa studi literatur yang relevan. Tabel 2.1 berikut ini memuat informasi penting dari penelitian terdahulu terkait topik yang sedang diteliti:

Tabel 2.1 Penelitian Terdahulu

No	Penulis Dan Tahun	Insight	Hasil	Metode
1.	Firmansyah & Wahyudi (2021)	Analisis performa ACL dengan metode Firewall Policy Base (FPB)	Zone-Based Policy Firewall mampu membatasi akses berdasarkan zona, menyembunyikan hop count, dan menyederhanakan manajemen ACL.	Simulasi jaringan dengan Cisco Packet Tracer menggunakan metode SPDLC (6 tahap), serta pengujian konektivitas UDP & HTTP untuk mengukur efektivitas

				firewall berdasarkan zona.
2.	Kusnanto, Y., et al. (2024)	Penerapan Zero Trust Architecture (ZTA) untuk meningkatkan keamanan jaringan melalui pendekatan berbasis simulasi.	Penerapan ZTA mampu mengurangi resiko serangan siber secara signifikan, dengan penurunan throughput sebesar 5% dan peningkatan latency sebesar 5 ms.	Simulasi menggunakan tools Iperf3 dan Wireshark untuk mengukur performa jaringan sebelum dan sesudah penerapan ZTA, khususnya dalam menghadapi serangan man-in-the-middle, DDoS, dan insider threats.
3.	Wahyudi (2023)	Proteksi jaringan menggunakan Access Control List pada Local	Implementasi ACL efektif dalam membatasi akses tidak sah dan meningkatkan keamanan	Perancangan dan implementasi ACL pada jaringan lokal menggunakan Cisco Packet

		Area Network.	jaringan lokal, dengan konfigurasi yang tepat sesuai kebutuhan jaringan.	Tracer, dengan pengujian konektivitas dan aksesibilitas layanan jaringan.
4.	Ge, Y., & Zhu, Q. (2023)	Penerapan Zero Trust untuk meningkatkan ketahanan siber dalam infrastruktur jaringan.	Model Zero Trust meningkatkan ketahanan siber dengan verifikasi kontinu dan kebijakan akses adaptif, efektif dalam menghadapi ancaman internal dan external.	Pendekatan teori permainan dinamis dan pembelajaran untuk mencapai otomatisasi dalam model Zero Trust, dengan studi kasus implementasi nyata.

2.2 Access Control List (ACL)

Access Control List (ACL) merupakan teknik pengamanan jaringan yang bertugas menyaring lalu lintas berdasarkan aturan-aturan yang ditentukan administrator jaringan. ACL memungkinkan atau menolak lalu lintas berdasarkan alamat IP sumber atau tujuan, port, dan protokol yang digunakan. Pada dasarnya, ACL bekerja dengan cara memfilter packet berdasarkan kondisi tertentu yang ditetapkan dalam daftar kontrol akses[11]. ACL banyak digunakan dalam jaringan tradisional untuk membatasi akses antara zona-zona tertentu dalam jaringan, seperti

antara jaringan internal dan external. Salah satu keunggulan utama ACL adalah kemampuannya untuk memberikan perlindungan dasar terhadap lalu lintas tidak sah. Namun, ACL juga memiliki keterbatasan, terutama dalam hal deteksi ancaman dinamis, autentikasi pengguna, dan segmentasi yang lebih granular. Dalam konteks penelitian ini, ACL digunakan sebagai representasi dari pendekatan Firewall Policy-Based, dimana aturan disusun secara statis berdasarkan kebijakan organisasi. Meskipun efisien dalam lingkungan jaringan kecil, pendekatan ini memiliki resiko keamanan ketika dihadapkan pada serangan lateral atau eksploitasi dari dalam jaringan[12][13].

2.3 Firewall Policy Base (Zone-Based Firewall)

Firewall Policy Base atau Zone-Based Policy Firewall adalah salah satu pendekatan pengamanan jaringan berbasis Access Control List (ACL) yang berfungsi untuk membatasi lalu lintas jaringan berdasarkan zona-zona yang telah didefinisikan. Metode ini menyusun aturan-aturan akses secara statis di antara zona internal dan external, dengan mempertimbangkan IP address, port, serta protokol tertentu. Kelebihannya terletak pada implementasi yang sederhana dan efisien untuk jaringan berskala kecil hingga menengah. Firewall Policy Base (FPB) dapat menyederhanakan manajemen kontrol akses dengan mengelompokkan perangkat berdasarkan zona, serta menyembunyikan hop count untuk meningkatkan privasi lalu lintas jaringan[14], [15].

Namun, metode ini memiliki keterbatasan signifikan dalam menghadapi serangan yang bersifat dinamis seperti serangan lateral movement dan tidak menyediakan autentikasi berkelanjutan. Karena aturan bersifat statis, pembaruan harus dilakukan secara manual dan rentan terhadap kelalaian manusia. Oleh karena itu, dalam konteks jaringan modern dengan kebutuhan keamanan yang lebih adaptif, Firewall Policy Base (FPB) perlu dibandingkan secara langsung dengan pendekatan yang lebih mutakhir seperti Zero Trust Architecture (ZTA) guna mengukur efektivitas dan efisiensi masing-masing dalam menghadapi ancaman siber yang berkembang[16].

2.4 Zero Trust Architecture (ZTA)

Zero Trust Architecture (ZTA) merupakan pendekatan keamanan jaringan yang menghilangkan kepercayaan implisit terhadap perangkat atau pengguna di dalam maupun di luar jaringan. ZTA mengharuskan setiap entitas yang ingin mengakses sumber daya jaringan untuk melalui proses verifikasi yang ketat dan berkelanjutan. Prinsip utama ZTA adalah "Never Trust, Always Verify." Pendekatan ini mencakup strategi seperti pemisahan jaringan menjadi segmen-segmen kecil untuk membatasi pergerakan lateral dalam jaringan (micro-segmentation), penggunaan autentikasi berlapis agar akses lebih aman (Multi-Factor Authentication/MFA), serta pembatasan hak akses minimum kepada pengguna berdasarkan kebutuhan spesifik (Least Privilege Access). Penelitian terdahulu oleh Kusnanto et al. (2024) dan Ge & Zhu (2023) menunjukkan bahwa penerapan ZTA dapat secara signifikan meningkatkan keamanan jaringan, meskipun terdapat trade-off berupa penurunan throughput dan peningkatan latency. Meski demikian, efektivitas ZTA dalam menangani serangan insider maupun outsider menjadikannya solusi adaptif untuk lingkungan jaringan modern yang kompleks[17], [18].

2.5 Perbandingan ACL dan ZTA dalam konteks keamanan Jaringan

Perbandingan antara ACL dan ZTA tidak hanya terletak pada teknis implementasi, tetapi juga filosofi pendekatan terhadap keamanan. ACL beroperasi dengan pendekatan preventif berbasis aturan statis, dimana akses diatur berdasarkan alamat IP, port, dan protokol. Pendekatan ini cenderung pasif dan lebih mudah diterapkan pada jaringan berskala kecil, namun memiliki keterbatasan dalam hal skalabilitas dan deteksi ancaman yang lebih dinamis. Di sisi lain, ZTA menerapkan verifikasi yang lebih aktif dan berkelanjutan terhadap setiap entitas yang ingin mengakses jaringan. Pendekatan ini memanfaatkan autentikasi berlapis, micro-segmentation, serta kebijakan berbasis identitas dan konteks, sehingga lebih adaptif terhadap perubahan dan ancaman yang kompleks. Walaupun penerapan ZTA memerlukan sumber daya dan infrastruktur yang lebih besar, pendekatan ini menawarkan fleksibilitas dan keamanan yang jauh lebih tinggi, terutama pada jaringan modern yang memiliki kebutuhan akses dan proteksi yang lebih granular.

Penelitian ini berupaya mengukur bagaimana kedua pendekatan ini mempengaruhi parameter performa jaringan seperti throughput, latency, jitter, dan packet loss, serta sejauh mana efektivitasnya dalam menyaring dan melindungi lalu lintas jaringan dari potensi ancaman[19].

Berdasarkan studi literatur pada Tabel 1, dapat disimpulkan bahwa baik Access Control List (ACL), Firewall Policy Base (FPB) maupun Zero Trust Architecture (ZTA) memiliki karakteristik dan keunggulan masing-masing yang dapat disesuaikan dengan kebutuhan serta kompleksitas jaringan. ACL dan Firewall Policy Base (FPB) cenderung lebih sederhana dalam hal implementasi, dengan Firewall Policy Base (FPB) menawarkan pengelompokan akses berdasarkan zona serta kemudahan dalam manajemen kebijakan akses. Keduanya cocok digunakan pada jaringan berskala kecil hingga menengah, dimana fokus utamanya adalah efisiensi dan kestabilan koneksi. Sementara itu, ZTA menawarkan tingkat keamanan yang lebih tinggi karena prinsip verifikasi berkelanjutan yang diterapkannya, yang membuat metode ini relevan untuk digunakan dalam skenario jaringan modern dengan tingkat resiko yang lebih besar.