BAB I
PENDAHULUAN

1.1 Latar Belakang

Dalam perkembangan dunia digital yang terus meningkat, perlindungan jaringan menjadi aspek krusial bagi keberlangsungan aktivitas organisasi. Salah satu metode tradisional yang banyak digunakan untuk mengontrol akses adalah Access Control List (ACL) dengan pendekatan Firewall Policy Base (FPB), dimana akses antarzona jaringan diatur berdasarkan aturan spesifik. Metode ini dikenal karena kesederhanaannya dan efektivitasnya dalam jaringan berskala kecil atau sederhana [1]. Namun, dengan semakin meningkatnya kompleksitas jaringan modern, metode ini mulai menunjukkan sejumlah kelemahan dalam menghadapi ancaman siber yang semakin canggih.

Keterbatasan Firewall Policy Base (FPB) meliputi ketidak mampuan untuk mencegah ancaman internal seperti lateral movement, kurangnya segmentasi granular untuk membatasi penyebaran ancaman, serta ketergantungan pada aturan statis yang memerlukan pembaruan manual. Selain itu, metode ini tidak mendukung autentikasi berkelanjutan, sehingga perangkat atau pengguna yang berhasil melewati firewall dapat beroperasi tanpa deteksi lebih lanjut. Penelitian menunjukkan bahwa lebih dari 60% pelanggaran data terjadi karena kontrol akses yang tidak memadai, dan sekitar 80% serangan siber berhasil akibat kurangnya pengelolaan akses granular dalam jaringan [2], [3].

Zero Trust Architecture (ZTA) hadir sebagai pendekatan alternatif untuk menjawab tantangan tersebut. Dengan filosofi "Never Trust, Always Verify", ZTA menuntut validasi setiap permintaan akses tanpa memandang lokasi pengguna atau perangkat, baik dari dalam maupun luar jaringan. Pendekatan ini memperkuat keamanan dengan melakukan verifikasi secara terus-menerus berdasarkan identitas, perangkat, lokasi, dan konteks lainnya.[4].

Keunggulan utama ZTA terletak pada kebijakan seperti Micro-segmentation, Multi-Factor Authentication (MFA), dan Least Privilege Access. Micro-segmentation membagi jaringan menjadi segmen-segmen kecil untuk membatasi pergerakan lateral penyerang, sehingga mencegah eksploitasi meluas

jika terjadi pelanggaran keamanan. MFA memastikan hanya pengguna yang terverifikasi melalui beberapa lapisan autentikasi yang dapat mengakses sumber daya penting. dan pembatasan hak akses memperkecil potensi penyalahgunaan[5].

Penelitian menunjukkan bahwa penerapan ZTA dapat mengurangi insiden keamanan hingga 30% dan menghemat biaya mitigasi pelanggaran data hingga $1,76 juta per insiden [6]. Namun, implementasi ZTA juga memiliki tantangan, termasuk dampak terhadap performa jaringan, seperti peningkatan latency dan jitter, yang memerlukan evaluasi mendalam untuk memastikan keefektifan pendekatan ini [7].

Penelitian ini dilakukan untuk mengevaluasi serta membandingkan kinerja pendekatan FPB dan ZTA dengan menggunakan simulasi jaringan melalui perangkat lunak GNS3, Wireshark, dan Iperf3. Evaluasi difokuskan pada metrik performa seperti throughput, latency, jitter, dan packet loss. Dengan tujuan untuk menjawab pertanyaan penelitian mengenai perbandingan kinerja kedua metode dalam hal kontrol akses dan performanya, hasil penelitian ini diharapkan dapat memberikan rekomendasi bagi organisasi dalam memilih pendekatan keamanan jaringan yang paling sesuai dengan kebutuhan dan perkembangan ancaman siber[8] [9].

Oleh karena itu, penelitian ini bertujuan untuk mengevaluasi dan membandingkan secara menyeluruh dua pendekatan keamanan jaringan, yakni Firewall Policy Base (FPB) dan Zero Trust Architecture (ZTA), baik dari sisi efektivitas kontrol akses maupun dampaknya terhadap performa jaringan. Hasil dari penelitian ini diharapkan dapat menjadi landasan dalam menentukan strategi keamanan jaringan yang adaptif dan efisien untuk menghadapi kompleksitas ancaman siber modern.

1.2 Rumusan Masalah

1. Bagaimana perbedaan penerapan konsep Zero Trust Architecture (ZTA) dibandingkan dengan pendekatan Firewall Policy Base (FPB) dalam mengatasi keterbatasan sistem keamanan jaringan berbasis Access Control List (ACL)?
2. Bagaimana perbandingan performa jaringan antara metode Zero Trust Architecture (ZTA) dan Firewall Policy Base (FPB), dilihat dari parameter throughput, latency, jitter, dan packet loss berdasarkan hasil pengujian ?

1.3 Tujuan Penelitian

1. Menerapkan pendekatan Zero Trust Architecture (ZTA) sebagai solusi terhadap keterbatasan sistem keamanan keamanan jaringan yang bertujuan menutup celah keamanan yang terdapat pada metode Firewall Policy Base (FPB) berbasis Access Control List (ACL).
2. Menganalisis dan membandingkan performa serta efektivitas kontrol akses dari metode FPB dan ZTA berdasarkan parameter jaringan dan indikator keamanan utama.

1.4 Batasan Masalah

1. Penelitian dilakukan dalam lingkungan simulasi menggunakan perangkat lunak seperti GNS3, Wireshark, dan Iperf3 untuk memastikan pengukuran parameter teknis dapat dilakukan secara terkontrol dan terukur.
2. Simulasi dilakukan dalam lingkungan jaringan yang terdiri dari tiga zona utama: server, pengguna internal, dan pengguna exsternal.
3. Fokus evaluasi performa jaringan hanya mencakup parameter seperti kecepatan transmisi data (throughput), waktu tunda (latency), ketidakstabilan koneksi (jitter), serta kehilangan paket (packet loss), tanpa mempertimbangkan biaya maupun kebutuhan perangkat keras fisik.
4. Kebijakan keamanan yang diimplementasikan pada arsitektur Zero Trust dalam simulasi ini terbatas pada segmentasi mikro, otentikasi dua faktor (MFA), dan pembatasan akses sesuai kebutuhan minimum pengguna (Least Privilege Access).

5. Penelitian tidak dilakukan pada jaringan fisik nyata dan sepenuhnya berbasis pada simulasi perangkat lunak demi menjaga konsistensi dan pengendalian variabel.