JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 9, No. 4, Desember 2024, Pp. 2357-2364

# IMPLEMENTASI ZERO TRUST ARCHITECTURE UNTUK MENINGKATKAN KEAMANAN JARINGAN: PENDEKATAN BERBASIS SIMULASI

**Yudhi Kusnanto[1)], Muhammad Agung Nugroho[2)], Rikie Kartadie*[3)]**
1. Teknologi Komputer, Universitas Teknologi Digital Indonesia
2. Informatika, Universitas Teknologi Digital Indonesia
3. Teknik Komputer, Universitas Teknologi Digital Indonesia

**Article Info**
**Kata Kunci:** DDoS; least privilege access; man-in-the-middle; micro-segmentation; Zero Trust Architecture

**Keywords:** DDoS; least privilege access; man-in-the-middle; micro-segmentation; Zero Trust Architecture

**Article history:**
Received 11 September 2024
Revised 5 Oktober 2024
Accepted 10 November 2024
Available online 1 December 2024

**DOI :**
https://doi.org/10.29100/jipi.v4i1.6943

* Corresponding author.
Corresponding Author
E-mail address:
rikie@utdi.ac.id

**ABSTRAK**
Penelitian ini mengeksplorasi penerapan Zero Trust Architecture (ZTA) sebagai pendekatan keamanan untuk mengatasi tantangan keamanan jaringan yang dihadapi oleh perusahaan modern, terutama dengan meningkatnya jumlah perangkat Internet of Things (IoT) yang terhubung. Simulasi dilakukan dengan menggunakan alat iperf dan Wireshark untuk mengukur performa jaringan sebelum dan sesudah penerapan ZTA, khususnya dalam menguji efektivitasnya dalam menghadapi serangan man-in-the-middle, DDoS, dan insider threats. Hasil pengujian menunjukkan bahwa penerapan ZTA mampu mengurangi risiko serangan siber secara signifikan, meskipun terdapat sedikit kompromi pada performa jaringan, dengan penurunan throughput sebesar 5% dan peningkatan latency sebesar 5 ms. Kebijakan micro-segmentation, multi-factor authentication (MFA), dan least privilege access terbukti efektif dalam meningkatkan stabilitas jaringan dan mencegah akses tidak sah. Meskipun demikian, penelitian ini menekankan pentingnya optimalisasi ZTA untuk memastikan keseimbangan antara keamanan dan kinerja jaringan di masa depan.

**ABSTRACT**
This research explores the application of Zero Trust Architecture (ZTA) as a security approach to address network security challenges faced by modern enterprises, especially with the increasing number of connected Internet of Things (IoT) devices. Simulations were conducted using iperf and Wireshark tools to measure network performance before and after the implementation of ZTA, specifically in testing its effectiveness in dealing with man-in-the-middle, DDoS, and insider threats. The test results show that the implementation of ZTA is able to significantly reduce the risk of cyberattacks, although there is a slight compromise on network performance, with a 5% decrease in throughput and a 5 ms increase in latency. Micro-segmentation, multi-factor authentication (MFA), and least privilege access policies proved effective in improving network stability and preventing unauthorized access. Nonetheless, this study emphasizes the importance of ZTA optimization to ensure a balance between network security and performance in the future.

.

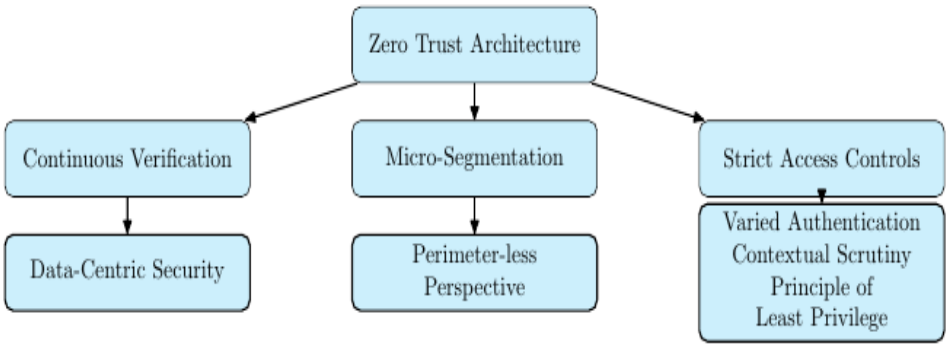
## I. PENDAHULUAN

KEAMANAN jaringan telah menjadi tantangan utama bagi organisasi di era digital. Peningkatan jumlah perangkat yang terhubung ke jaringan, termasuk perangkat *Internet of Things* (IoT) [1], serta ancaman siber yang semakin canggih, telah mendorong para peneliti dan praktisi untuk mencari pendekatan keamanan baru yang lebih efektif [2,3]. Model keamanan tradisional, yang mengandalkan *perimeter-based defens*, telah terbukti tidak mampu melindungi jaringan dari serangan yang datang dari dalam, seperti serangan yang dilakukan oleh pihak dalam (*insider threats*), maupun serangan eksternal yang berhasil menembus perimeter [4] .

*Zero Trust Architecture* (ZTA) merupakan salah satu pendekatan yang berkembang pesat dalam beberapa tahun terakhir. Berbeda dengan model tradisional, ZTA menghilangkan kepercayaan bawaan pada perangkat atau pengguna di dalam jaringan. Sebaliknya, ZTA menerapkan autentikasi dan otorisasi berkelanjutan, di mana setiap permintaan akses harus diverifikasi, baik yang berasal dari dalam maupun luar jaringan [5], Gambar 1

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 9, No. 4, Desember 2024, Pp. 2357-2364

menggambarkan peta konsep dari Arsitektur *Zero Trust*. Penelitian sebelumnya menunjukkan bahwa ZTA dapat mengurangi risiko serangan siber dengan signifikan, terutama dalam konteks organisasi besar dengan infrastruktur jaringan yang kompleks [6]. Namun, meskipun banyak penelitian telah dilakukan mengenai konsep ZTA, implementasi praktis dan dampaknya pada kinerja jaringan secara menyeluruh masih memerlukan penelitian lebih lanjut [1].




Gambar 1. Peta Konsep Arsitektur Zero Trush, Sumber: [3]

Beberapa penelitian yang ada fokus pada penggunaan ZTA untuk melindungi data di *cloud* atau untuk mendeteksi ancaman *insider* secara *real-time* [7]. Namun, gap penelitian yang belum banyak dieksplorasi adalah penerapan ZTA dalam konteks jaringan komputer berskala besar, khususnya bagaimana arsitektur ini dapat diintegrasikan dengan sistem keamanan jaringan yang sudah ada, tanpa menurunkan performa jaringan [5, 8]. Selain itu, penelitian mengenai simulasi *Zero Trust* dalam menghadapi serangan siber yang bervariasi, seperti serangan *man-in-the-middle* dan *Distributed Denial of Service* (DDoS), masih sangat terbatas [9] . Sejumlah alat simulasi telah digunakan secara luas dalam penelitian untuk mengevaluasi efektivitas arsitektur keamanan, termasuk simulasi berbasis perangkat lunak seperti GNS3 dan Cisco Packet Tracer [10][11]. Masih terdapat kekurangan dalam studi yang secara spesifik menguji implementasi ZTA dalam lingkungan jaringan berskala besar dan bagaimana arsitektur ini dapat diadaptasi untuk mengelola serangan siber yang lebih beragam, seperti serangan DDoS dan man-in-the-middle.

Penelitian ini unik karena fokus pada penerapan ZTA dalam jaringan berskala besar menggunakan alat simulas. Penelitian sebelumnya seringkali terbatas pada skenario yang lebih kecil atau pada komponen tertentu dari arsitektur ZTA. Selain itu, penelitian ini juga menyelidiki dampak ZTA terhadap kinerja jaringan secara menyeluruh, bukan hanya pada aspek keamanan. Selain itu, penelitian ini memberikan kontribusi unik dengan menggunakan alat simulasi GNS3 dan Cisco Packet Tracer untuk menilai performa jaringan dalam konteks penerapan ZTA di jaringan besar, yang jarang dilakukan dalam penelitian sebelumnya. Pendekatan ini menawarkan pemahaman praktis bagi organisasi mengenai efektivitas ZTA dalam menangani ancaman keamanan, tanpa mengorbankan performa jaringan secara signifikan.

Hasil dari penelitian ini diharapkan dapat memberikan kontribusi yang signifikan dalam pengembangan pedoman implementasi ZTA yang praktis bagi organisasi. Dengan mengetahui kelebihan dan kekurangan ZTA dalam berbagai skenario, organisasi dapat membuat keputusan yang lebih informatif terkait investasi dalam teknologi keamanan jaringan. Selain itu, hasil simulasi ini dapat digunakan untuk mengembangkan sistem deteksi intrusi yang lebih efektif berdasarkan prinsip-prinsip ZTA.

## II. METODE PENELITIAN

Penelitian ini dilakukan dengan pendekatan berbasis simulasi untuk menguji efektivitas *Zero Trust Architecture* (ZTA) dalam meningkatkan keamanan jaringan. Simulasi dilakukan menggunakan perangkat lunak GNS3 dan Cisco Packet Tracer sebagai alat utama untuk membangun dan memvisualisasikan jaringan [12]. Langkah-langkah penelitian meliputi pembangunan infrastruktur jaringan, penerapan kebijakan Zero Trust, simulasi serangan siber, dan pengukuran kinerja jaringan.

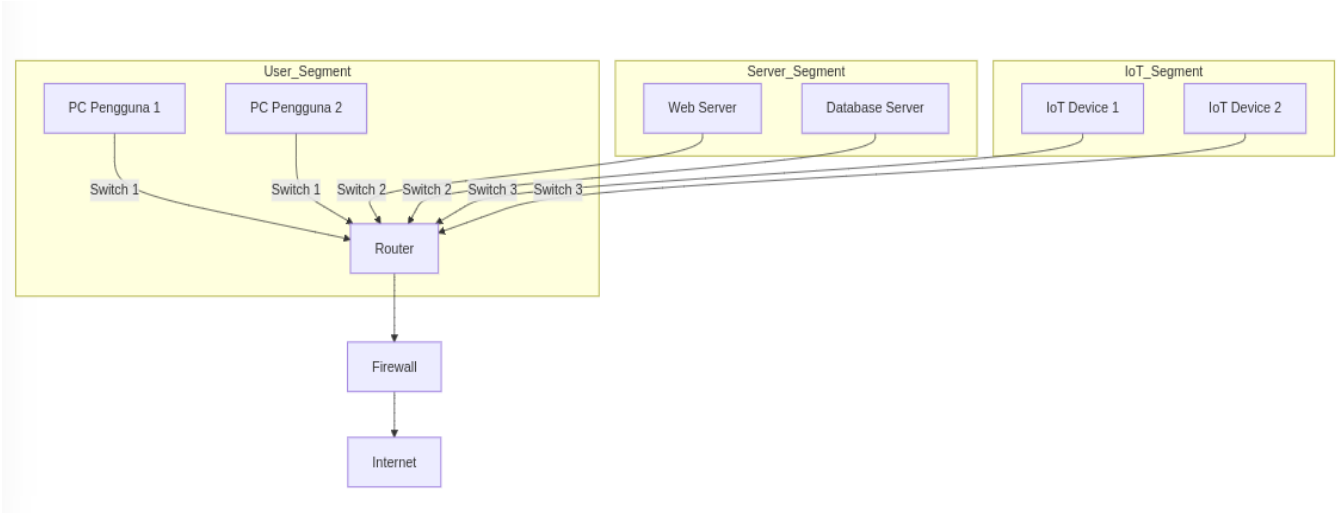
Dalam penelitian ini, kami memilih menggunakan GNS3 dan Cisco Packet Tracer sebagai alat simulasi utama. GNS3 dipilih karena fleksibilitasnya dalam mensimulasikan jaringan yang kompleks dan realistis, serta

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 9, No. 4, Desember 2024, Pp. 2357-2364

dukungannya terhadap berbagai protokol jaringan [13]. Cisco Packet Tracer digunakan untuk memvalidasi konfigurasi perangkat individu dan menganalisis lalu lintas jaringan secara lebih detail [14, 15, 16, 17]. Kombinasi kedua alat ini, seperti yang disarankan oleh sejumlah penelitian sebelumnya, memungkinkan kami untuk membangun lingkungan simulasi yang komprehensif dan realistis, yang dapat mensimulasikan program perangkat lunak yang memodelkan perilaku jaringan yang mungkin sulit dibuat ulang di dunia nyata [18, 19].

### *A. Pembangunan Infrastruktur Jaringan*

Infrastruktur jaringan dibangun dengan beberapa segmen terpisah, yaitu segmen pengguna, segmen server, dan segmen IoT. Setiap segmen dihubungkan oleh *router*, dan lalu lintas antar segmen diatur oleh kebijakan keamanan yang diterapkan melalui *firewall*. Segmen Pengguna adalah bagian jaringan yang terdiri dari perangkat-perangkat pengguna akhir, seperti komputer desktop atau laptop yang digunakan oleh karyawan atau pengguna jaringan. Pada segmen ini, akses ke sumber daya jaringan sangat dibatasi melalui kebijakan *least privilege access*. Topologi jaringan yang digunakan dalam simulasi ini digambarkan dalam Gambar 2 berikut:



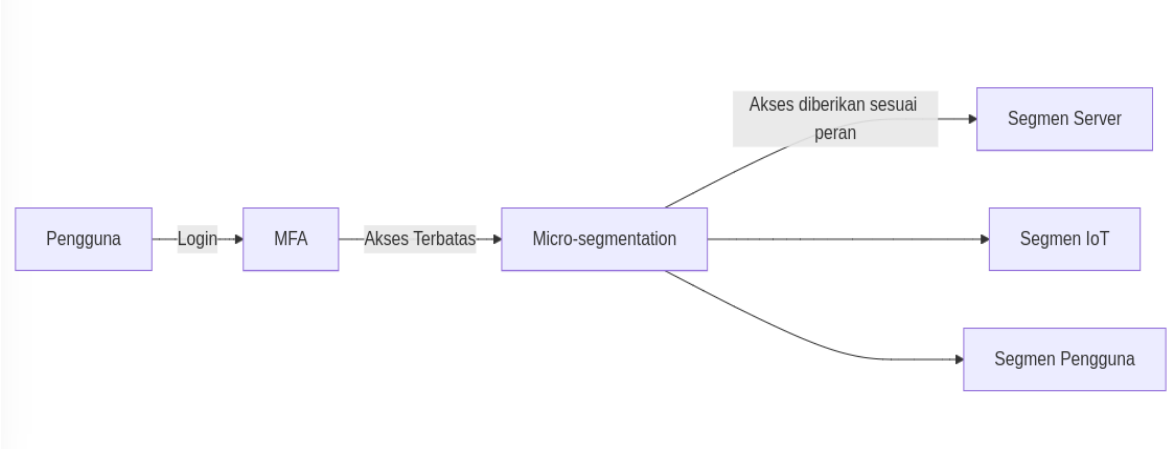

Gambar 2. Topologi Jaringan Simulasi Zero Trust

*User Segment*: Terhubung ke jaringan melalui Switch 1, pengguna akhir (PC Pengguna 1 dan 2) melakukan akses ke server atau perangkat IoT yang tersedia di jaringan melalui Router; *Server Segment*: Server, termasuk Web Server dan Database Server, terhubung ke Switch 2, yang juga terhubung ke Router. Ini memungkinkan server mengakses atau diakses oleh perangkat di segmen lain; *IoT Segmen*t: Perangkat IoT (misalnya sensor atau perangkat pintar) terhubung melalui Switch 3, memberikan layanan atau menerima data dari server dan pengguna; dan *Firewall*: Semua komunikasi yang keluar dari jaringan menuju internet melalui firewall, yang bertanggung jawab untuk memfilter lalu lintas masuk dan keluar berdasarkan kebijakan keamanan yang diterapkan.

### *B. Penerapan Kebijakan Zero Trust*

*Zero Trust* diterapkan di seluruh jaringan dengan tiga kebijakan utama: *Micro-segmentation, Multi-Factor Authentication* (MFA), dan *Least Privilege Access. Micro-segmentation* memisahkan setiap segmen secara logis, memastikan bahwa akses di antara segmen-segmen tersebut terbatas dan hanya diizinkan melalui proses verifikasi. MFA memastikan bahwa setiap pengguna atau perangkat yang ingin mengakses sumber daya jaringan harus melewati autentikasi berlapis. *Least Privilege Access* membatasi hak akses setiap pengguna atau perangkat hanya untuk sumber daya yang diperlukan sesuai dengan tugasnya, terilhat pada Gambar 3.

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 9, No. 4, Desember 2024, Pp. 2357-2364




Gambar 3. Diagram Alur Kebijakan Zero Trust

Pada Gambar 3, pengguna atau perangkat yang mencoba mengakses jaringan harus melewati proses MFA terlebih dahulu untuk diverifikasi. Setelah diverifikasi, akses dibatasi melalui kebijakan *micro-segmentation*, di mana hanya segmen atau sumber daya yang relevan yang dapat diakses. Misalnya, pengguna dengan hak akses tertentu hanya dapat mengakses server yang diperlukan atau perangkat IoT yang terkait dengan tugasnya, sesuai dengan kebijakan *Least Privilege Access*.

### *C. Simulasi Serangan Siber*

Setelah penerapan *Zero Trust*, beberapa simulasi serangan siber dilakukan untuk menguji ketahanan jaringan. Serangan yang disimulasikan meliputi:

- *Man-in-the-middle Attack*: Penyerang mencoba menyadap komunikasi antara pengguna dan server.
- *Distributed Denial of Service* (DDoS): Penyerang mencoba membanjiri jaringan dengan permintaan yang berlebihan untuk mengganggu layanan.
- *Insider Threat*: Pengguna dengan akses internal mencoba melakukan tindakan yang melanggar aturan, seperti mencuri data sensitif atau merusak sistem.

Simulasi ini dilakukan menggunakan perangkat lunak seperti Wireshark untuk menganalisis lalu lintas jaringan, dan iperf untuk mengukur dampak serangan terhadap performa jaringan.

### *D. Pengukuran Kinerja Jaringan*

Setelah simulasi serangan dilakukan, kinerja jaringan diukur untuk melihat dampak penerapan Zero Trust terhadap performa. Pengukuran yang dilakukan meliputi:

*Throughput*: Mengukur jumlah data yang berhasil dikirimkan dalam periode waktu tertentu, menggunakan rumus (1), melalui alat iperf, throughput jaringan diukur sebelum dan setelah penerapan ZTA untuk melihat pengaruhnya terhadap kecepatan transmisi data.

$$\text{Throughput} = \frac{\text{TotalData}}{\text{WaktuTransfer}} \quad (1)$$

*Latency*: Mengukur waktu yang dibutuhkan untuk mengirimkan permintaan dan menerima respons, menggunakan rumus (2).

$$\text{Latency} = \frac{\text{TotalWaktuRespon}}{\text{JumlahPermintaan}} \quad (2)$$

*Packet Loss*: Mengukur persentase paket yang hilang selama transmisi data, menggunakan rumus (3).

$$\text{PacketLoss} = \frac{\text{JumlahPaketHilang}}{\text{TotalPaketDikirim}} \times 100 \quad (3)$$

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 9, No. 4, Desember 2024, Pp. 2357-2364

*Jitter*: Mengukur variasi dalam waktu pengiriman paket, dengan menggunakan rumus (4).

$$\text{Jitter} = \text{RerataWaktuPengirimanPaket} - \text{WaktuPengirimanIdeal} \quad (4)$$

Semua hasil pengukuran dibandingkan sebelum dan setelah penerapan *Zero Trust* untuk menilai dampak kebijakan ini terhadap performa jaringan.

## III. HASIL DAN PEMBAHASAN

### A. *Pengukuran Throughput Jaringan*

Pengukuran throughput dilakukan menggunakan iperf dalam mode client-server. Server dikonfigurasi pada alamat IP 192.168.1.10, sementara klien terhubung dari alamat IP 192.168.1.20. Pengujian dijalankan selama 10 detik untuk mengukur kecepatan transfer data antara klien dan server, sebelum dan setelah penerapan *Zero Trust Architecture* (ZTA).

Pada pengujian sebelum penerapan ZTA, throughput tercatat sebesar 100 Mbps, sedangkan setelah penerapan ZTA, throughput turun menjadi 95 Mbps. Berikut hasil lengkap dari pengujian throughput menggunakan iperf:

```
Connecting to host 192.168.1.10, port 5201
[  5] local 192.168.1.20 port 53520 connected to 192.168.1.10 port 5201
[ ID] Interval           Transfer     Bandwidth
[  5]   0.00-10.00 sec   112 MBytes   95.0 Mbits/sec
```

Penurunan throughput ini dapat dijelaskan oleh penambahan lapisan autentikasi dan segmentasi yang diterapkan melalui kebijakan Zero Trust, yang menambah *overhead* dalam aliran data.

### B. *Pengukuran Jitter dan Packet Loss*

Selain throughput, pengujian *jitter* dan *packet loss* dilakukan menggunakan iperf dalam mode UDP untuk menguji stabilitas transmisi paket. Hasil pengukuran jitter dan packet loss setelah penerapan ZTA disajikan di bawah ini:

```
[ ID] Interval           Transfer     Bandwidth       Jitter   Lost/Total Datagrams
[  5]   0.00-10.00 sec  1.25 MBytes  1.05 Mbits/sec   0.185 ms  0/900 (0%)
```

Dari hasil tersebut, jitter tercatat sebesar 0.185 ms, menandakan bahwa stabilitas waktu pengiriman paket relatif baik setelah penerapan ZTA. Tidak ada packet loss yang tercatat selama pengujian, menunjukkan bahwa semua paket berhasil diterima dengan baik, yang menunjukkan kestabilan jaringan.

### C. *Hasil Pengukuran Kinerja Jaringan*

Pengukuran kinerja jaringan dilakukan sebelum dan setelah penerapan Zero Trust Architecture (ZTA). Hasil pengukuran kinerja jaringan untuk parameter throughput, latency, packet loss, dan jitter disajikan dalam Tabel 1 di bawah ini.

Penurunan throughput sebesar 5% dan peningkatan latency setelah penerapan ZTA dapat dijelaskan oleh adanya lapisan autentikasi tambahan yang menjadi bagian dari arsitektur ini. Dalam ZTA, setiap permintaan akses ke sumber daya jaringan harus melewati proses autentikasi dan otorisasi yang berkelanjutan, baik untuk akses internal maupun eksternal. Proses ini meningkatkan waktu yang dibutuhkan untuk pengiriman data karena verifikasi berlapis dilakukan di setiap titik akses. Selain itu, micro-segmentation pada ZTA membagi jaringan menjadi segmen-segmen kecil, sehingga setiap aliran data antar segmen perlu melewati firewall dan kebijakan akses tambahan yang memperlambat kecepatan transmisi.

Sementara itu, peningkatan latency juga disebabkan oleh overhead yang ditambahkan oleh kebijakan multi-factor authentication (MFA) dan least privilege access, di mana setiap akses divalidasi untuk memastikan pengguna atau perangkat hanya dapat mengakses sumber daya yang relevan. Penambahan verifikasi ini, meskipun efektif dalam

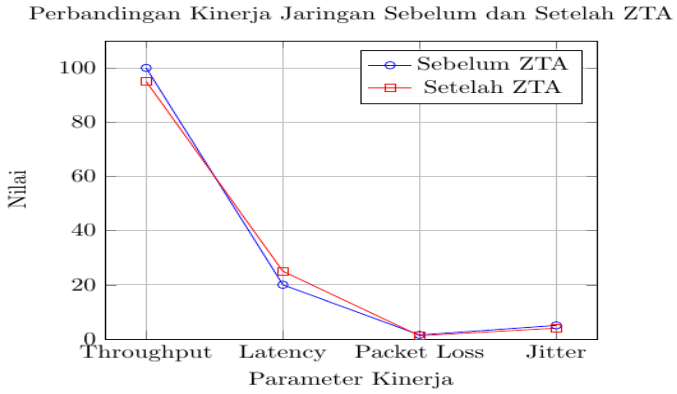
JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 9, No. 4, Desember 2024, Pp. 2357-2364

meningkatkan keamanan, menambah waktu respons dari sistem secara keseluruhan.

TABEL I
HASIL PENGUKURAN KINERJA

| Parameter | Sebelum ZTA | Setelah ZTA |
|---|---|---|
| *Throughput* | 100 Mbps | 95 Mbps |
| *Latency* | 20 ms | 25 ms |
| *Packet Loss* | 1.5% | 1.2% |
| *Jitter* | 5 ms | 4 ms |

Dari Tabel 1, terlihat bahwa ada penurunan *throughput* sebesar 5% setelah penerapan ZTA. Peningkatan *latency* dari 20 ms menjadi 25 ms juga tercatat. Namun, hasil menunjukkan bahwa *packet loss* dan *jitter* sedikit menurun setelah penerapan *Zero Trust*, yang mengindikasikan peningkatan stabilitas jaringan. Untuk memvisualisasikan perubahan kinerja jaringan secara lebih jelas, berikut disajikan grafik perbandingan kinerja jaringan sebelum dan setelah penerapan ZTA pada Gambar 4 berikut.




Gambar 4. Perbandingan Kinerja Jaringan Sebelum dan Setelah Peneraoan ZTA

Dari grafik tersebut, dapat dilihat bahwa meskipun *throughput* dan *latency* mengalami perubahan negatif, parameter seperti *packet loss* dan *jitter* menunjukkan peningkatan performa setelah penerapan ZTA

Penerapan Zero Trust Architecture (ZTA) dalam jaringan terbukti meningkatkan stabilitas jaringan, yang tercermin dari penurunan jitter menjadi 0.185 ms dan hilangnya packet loss selama pengujian. Kebijakan micro-segmentation yang diterapkan dalam ZTA memungkinkan setiap segmen jaringan beroperasi secara terisolasi dengan akses yang dibatasi, sehingga mengurangi jumlah lalu lintas antar segmen. Segmentasi ini meminimalisir kemungkinan kemacetan di segmen-segmen yang lebih kecil dan menjaga konsistensi waktu pengiriman paket, yang berkontribusi pada rendahnya jitter [20].

## *D. Hasil Simulasi Serangan Siber*

Selain pengukuran kinerja, simulasi serangan siber seperti *man-in-the-middle* dan *DDoS* juga dilakukan untuk menguji efektivitas ZTA dalam mencegah ancaman keamanan. Hasil dari simulasi ini ditunjukkan pada Tabel 2.

TABEL II
HASIL SIMULASI SERANGAN SIBER SEBELUM DAN SESUDAH ZTA

| Jenis Serangan | Sebelum ZTA | Setelah ZTA |
|---|---|---|
| *Man-in-the-middle* | Serangan berhasil | Serangan terdeteksi dan diblokir |
| *DDoS* | Layanan Terganggu | Layanan tetap berjalan meskipun ada penurunan throughput |
| *Insider Threat* | Akses tidak sah berhasil | Akses dibatasi melalui MFA dan least privilege |

Serangan *man-in-the-middle* dan *insider threats* berhasil dicegah setelah penerapan ZTA. Selain itu, meskipun serangan DDoS meningkatkan penggunaan *bandwidth*, layanan tetap berjalan dengan stabil tanpa gangguan besar. Dari hasil pengukuran dan simulasi, penerapan *Zero Trust Architecture* terbukti memberikan peningkatan signifikan dalam hal keamanan jaringan, meskipun ada sedikit kompromi pada kinerja.

- *Throughput* menurun sekitar 5%, yang diharapkan karena adanya peningkatan overhead dari proses autentikasi tambahan.
- *Latency* mengalami sedikit peningkatan, namun masih dalam batas yang dapat diterima.

- *Packet loss* dan *jitter* menurun, menunjukkan bahwa stabilitas jaringan meningkat setelah penerapan ZTA.

Hasil simulasi menunjukkan bahwa Zero Trust Architecture (ZTA) secara efektif mendeteksi dan mencegah serangan man-in-the-middle (MITM) dengan menggunakan pendekatan autentikasi berlapis. Dalam ZTA, setiap permintaan akses, baik internal maupun eksternal, harus melewati proses autentikasi dan otorisasi yang ketat. Autentikasi berlapis ini memungkinkan sistem untuk mendeteksi aktivitas mencurigakan saat terjadi upaya penyadapan komunikasi. Setiap upaya untuk menyusup atau menyadap jaringan tanpa autentikasi yang sah langsung diblokir oleh sistem, mengurangi risiko keberhasilan serangan MITM

Pada serangan DDoS, ZTA terbukti mampu menjaga stabilitas layanan melalui kebijakan pembatasan akses (rate-limiting) dan micro-segmentation. Rate-limiting membantu mengontrol lalu lintas yang berlebihan dengan membatasi jumlah permintaan akses yang diizinkan dalam satu waktu, sementara micro-segmentation memastikan bahwa setiap segmen jaringan beroperasi secara independen dan terisolasi. Kombinasi strategi ini membantu membatasi dampak serangan DDoS pada segmen-segmen tertentu, memungkinkan layanan tetap berjalan dan jaringan tidak terganggu meskipun terdapat lonjakan lalu lintas.

Penelitian ini memberikan kontribusi yang signifikan dalam studi Zero Trust Architecture (ZTA) pada jaringan berskala besar, yang menjadi pembeda utama dibandingkan penelitian sebelumnya. Sebagai contoh, penelitian Rose [2] dan Wood [3] terutama berfokus pada penerapan ZTA di lingkungan berbasis cloud dan hanya meneliti dampak keamanan tanpa mengukur performa jaringan secara mendetail. Penelitian kami tidak hanya mengevaluasi efektivitas ZTA dalam mendeteksi dan mencegah serangan seperti MITM dan DDoS tetapi juga menganalisis dampak pada parameter performa jaringan seperti throughput, latency, jitter, dan packet loss dalam jaringan berskala besar.

Selain itu, penggunaan alat simulasi GNS3 dan Cisco Packet Tracer memungkinkan penelitian ini untuk memodelkan lingkungan jaringan yang lebih realistis dengan infrastruktur kompleks. Studi ini menunjukkan bahwa meskipun ZTA memperkenalkan sedikit kompromi pada performa jaringan, manfaat keamanan yang diberikan jauh lebih besar, terutama dalam lingkungan yang memprioritaskan keamanan data. Dengan demikian, penelitian ini memberikan panduan praktis yang lebih komprehensif bagi organisasi yang mempertimbangkan penerapan ZTA pada infrastruktur jaringan yang kompleks.

## IV. SIMPULAN

Penerapan *Zero Trust Architecture* (ZTA) pada jaringan komputer terbukti meningkatkan keamanan jaringan secara signifikan, terutama dalam mendeteksi dan mencegah berbagai ancaman siber seperti *man-in-the-middle*, *Distributed Denial of Service* (DDoS), dan *insider threats*. Penelitian ini menunjukkan bahwa meskipun terdapat sedikit penurunan performa, khususnya pada *throughput* dan *latency*, penurunan tersebut masih dalam batas yang dapat diterima dalam skenario jaringan yang memprioritaskan keamanan. Penurunan *throughput* sebesar 5% yang diamati setelah penerapan ZTA dapat dijelaskan oleh proses tambahan autentikasi dan verifikasi yang dibutuhkan dalam setiap interaksi jaringan. Meskipun *latency* meningkat sebesar 5 ms, kebijakan seperti *multi-factor authentication* (MFA) dan *micro-segmentation* memberikan perlindungan yang kuat terhadap akses tidak sah dan potensi serangan internal. Dari hasil simulasi serangan, ZTA berhasil memblokir serangan *man-in-the-middle* dan membatasi dampak serangan DDoS melalui kebijakan *rate-limiting* yang diterapkan pada *firewall*. *Insider threats* juga dapat dikendalikan dengan membatasi akses melalui kebijakan least privilege access, memastikan bahwa setiap pengguna hanya memiliki akses ke sumber daya yang dibutuhkan. Secara keseluruhan, hasil penelitian ini menggarisbawahi pentingnya penerapan ZTA dalam lingkungan jaringan yang kompleks, terutama di organisasi yang memiliki kebutuhan tinggi akan keamanan data. Meskipun ada sedikit kompromi pada kinerja jaringan, manfaat yang diperoleh dari peningkatan keamanan lebih dari cukup untuk menjustifikasi penerapannya. Penelitian lebih lanjut dapat dilakukan untuk mengoptimalkan penerapan *Zero Trust* tanpa menurunkan performa jaringan secara signifikan, serta mengkaji bagaimana arsitektur ini dapat diterapkan dalam lingkungan yang lebih luas dengan infrastruktur jaringan yang lebih kompleks.

## UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Universitas Teknologi Digital Indonesia atas dukungan yang diberikan selama penelitian ini. Ucapan terima kasih juga ditujukan kepada tim IT dan staf laboratorium jaringan yang telah menyediakan infrastruktur dan alat simulasi yang diperlukan untuk menjalankan eksperimen ini. Selain itu, terima kasih kepada rekan-rekan peneliti yang telah memberikan masukan berharga dalam penyusunan artikel ini.

# DAFTAR PUSTAKA

[1] Tao Chuan et al 2020 J. Phys.: Conf. Ser. 1651 012010, DOI 10.1088/1742-6596/1651/1/012010
[2] M. Rose, "Zero Trust Architecture for Enhanced Network Security," *IEEE Communications Magazine*, vol. 58, no. 10, pp. 112-119, 2020.
[3] S. Wood, "Evaluating the Performance Impact of Zero Trust Models on Network Security," *Journal of Network Security*, vol. 22, no. 3, pp. 45-53, 2021.
[4] A. Pourghorban, M. Dorothy, D. Shishika, A. Von Moll and D. Maity, "Target Defense against Sequentially Arriving Intruders," 2022 IEEE 61st Conference on Decision and Control (CDC), Cancun, Mexico, 2022, pp. 6594-6601, doi: 10.1109/CDC51059.2022.9992425.
[5] Khan, N. M. J. (2023). Zero trust architecture: Redefining network security paradigms in the digital age. World Journal of Advanced Research and Reviews, 19(3), 105–116. https://doi.org/10.30574/wjarr.2023.19.3.1785
[6] Chandramouli, R., & Butcher, Z. (2023). A zero trust architecture model for access control in cloud-native applications in multi-location environments. https://doi.org/10.6028/nist.sp.800-207a
[7] Ahmed, I., Nahar, T., Urmi, S. S., & Taher, K. A. (2020). Protection of Sensitive Data in Zero Trust Model. Protection of Sensitive Data in Zero Trust Model. https://doi.org/10.1145/3377049.3377114
[8] Ramezanpour, K., & Jagannath, J. (2022). Intelligent zero trust architecture for 5G/6G networks: Principles, challenges, and the role of machine learning in the context of O-RAN. Computer Networks, 217, 109358. https://doi.org/10.1016/j.comnet.2022.109358
[9] Hassan, H. U., Nor, R. M., Amiruzzaman, M., Wani, S., & Islam, M. R. (2021). DNS attack mitigation Using OpenStack Isolation. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2106.04575.
[10] J. Smith, "Network Simulation Tools for Evaluating Security Architectures," International Journal of Cybersecurity, vol. 15, no. 2, pp. 89-98, 2019.
[11] B. C. Asman, M. H. Kim, R. A. Moschitto, J. C. Stauffer and S. H. Huddleston, "Methodology for analyzing the compromise of a deployed tactical network," 2011 IEEE Systems and Information Engineering Design Symposium, Charlottesville, VA, USA, 2011, pp. 164-169, doi: 10.1109/SIEDS.2011.5876871.
[12] Kurniawan, D. E., Arif, H., Nelmiawati, N., Tohari, A. H., & Fani, M. (2019). Implementation and analysis ipsec-vpn on cisco asa firewall using gns3 network simulator. Journal of Physics Conference Series, 1175, 012031. https://doi.org/10.1088/1742-6596/1175/1/012031
[13] Helali, Saida. (2020). Simulating Network Architectures with GNS3. 9-25. 10.1002/9781119779964.ch2.
[14] Cisco. (2023). Cisco Packet Tracer documentation. https://www.netacad.com/cisco-packet-tracer
[15] Eka Putra, Fauzan & Ubaidi, Ubaidi & Tamam, Alief & Efendi, Reynal. (2024). Implementation And Simulation Of Dynamic Arp Inspection In Cisco Packet Tracer For Network Security. Brilliance: Research of Artificial Intelligence. 4. 340-347. 10.47709/brilliance.v4i1.4199.
[16] Hashimi, S. M., & Güneş, A. (2017). Performance Evaluation of a Network Using Simulation Tools or Packet Tracer. IOSR Journal of Computer Engineering, 19(01), 01–05. https://doi.org/10.9790/0661-1901010105
[17] P. Srikanth Reddy, P. Saleem Akram, T. V. Ramana, P. Aditya Sai Ram, R. Pruthvi Raj and M. Adarsh Sharma, "Configuration of Firewalls in Educational Organisation LAB setup by using Cisco Packet Tracer," 2020 IEEE International Symposium on Sustainable Energy, Signal Processing and Cyber Security (iSSSC), Gunupur Odisha, India, 2020, pp. 1-6, doi: 10.1109/iSSSC50941.2020.9358818. keywords: {Training;Firewalls (computing);Information security;Organizations;Tools;Signal processing;Safety;Cisco Packet Tracer;Firewall;LAN;Virtual research},
[18] S. Sharma, A. N. Mahajan, and R. C. Poonia, "An Inclusive survey of Network Simulators," SSRN Electronic Journal, Jan. 2019, doi: 10.2139/ssrn.3363025. Available: https://doi.org/10.2139/ssrn.3363025
[19] L. Campanile, M. Gribaudo, M. Iacono, F. Marulli, and M. Mastroianni, "Computer Network Simulation with ns-3: A Systematic Literature Review," Electronics, vol. 9, no. 2, p. 272, Feb. 2020, doi: 10.3390/electronics9020272. Available: https://doi.org/10.3390/electronics9020272
[20] S. Thomas, R. McGuinness, G. M. Voelker, and G. Porter, *Dark packets and the end of network scaling*. 2018. doi: 10.1145/3230718.3230727. Available: https://doi.org/10.1145/3230718.3230727