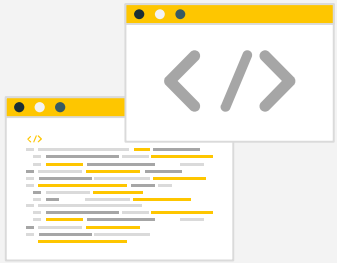
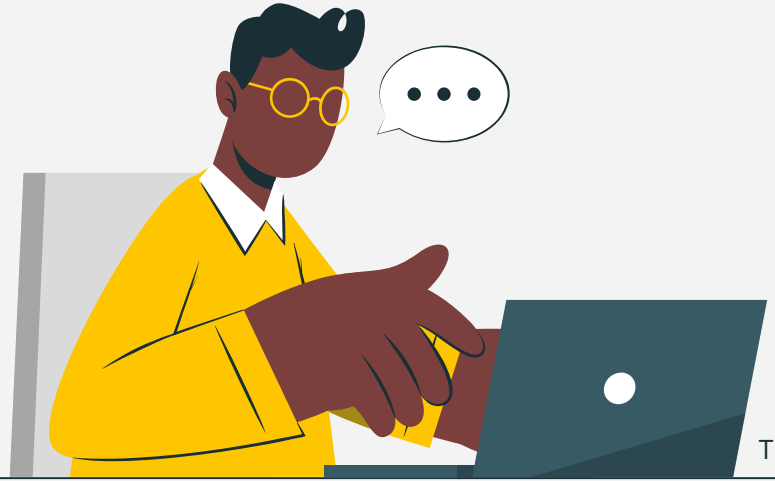
Komputasi Berbasis Jaringan (P)
KELOMPOK 5



Proposal Paper :

Analisis Dampak Penerapan Zero Trust Network Access (ZTNA) pada Aplikasi Website terhadap Waktu Respons dan Penggunaan Sumber Daya Sesuai ISO 25023. Studi Kasus : PT. XYZ



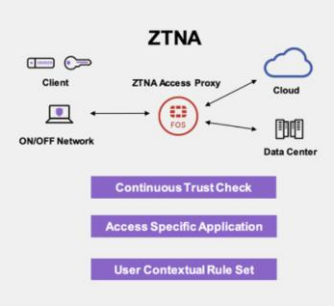
Anggota :

1. [6025241052] Devita Dwitama Putri Baron
2. [6025241009] Iqbal Fadhil
3. [6025241031] Zain Maulana Azmi

Daftar Isi

Overview

ZTNA



Keamanan Siber yang **mengeliminasi konsep trust (kepercayaan) pada jaringan secara otomatis. User melakukan verifikasi secara kontinu dalam akses ke aplikasi**

Selalu verifikasi

User diberikan akses minimal atau sesuai dengan Role Access Matrix

Terus memantau ancaman

ZTNA vs VPN

Aspek	ZTNA	VPN
Security	• Memberikan akses hanya kepada pengguna dan perangkat yang didaftarkan • Setiap trafik akan tetap diinspeksi/dicek walaupun telah berhasil login	• Perangkat apa pun yang akses VPN dapat dipercaya • Setelah berhasil login trafik tidak akan diinspeksi/dicek
Scope	Menyediakan akses sesuai User Access Role Matrix	Menyediakan akses jaringan penuh
Scalability	Cloud-based (Easy to Scale)	On Premise (Difficult to Scale)

Rekomendasi BSSN

Overview

Aplikasi Public vs Private

Public	Private
Aplikasi yang **dapat diakses oleh siapa saja tanpa pembatasan khusus** dan ditujukan untuk penggunaan umum oleh masyarakat luas. Sehingga tidak diperlukan Akses ZTNA	Aplikasi yang **diakses terbatas**, biasanya dalam lingkungan organisasi saja. Akses ke aplikasi ini dikontrol ketat melalui sistem login atau jaringan internal untuk memastikan bahwa hanya pengguna yang berwenang yang dapat mengakses. Keamanan yang diterapkan ini salah satunya menggunakan ZTNA sebagai Next Gen dari VPN

01 Latar Belakang

Permasalahan

- Meningkatnya ancaman dalam security system, seperti ransomware, phising, dan serangan APT
- Perubahan pola bekerja saat ini mulai mengadopsi model kerja jarak jauh atau hybrid sehingga perlu ditingkatkannya akses security jaringan untuk dapat diakses jarak jauh seperti menggunakan VPN dll.
- Penggunaan akses ke seluruh jaringan berpotensi menjadi resiko jika kredensial pengguna bocor.

Tujuan

- Mengimplementasikan ZTNA pada suatu sistem perusahaan kemudian dilanjutkan dengan menguji dampak penggunaan ZTNA terhadap kinerja dalam waktu respons pada device yang digunakan, penggunaan memory dan CPU.

02 What is Known & Unknown ?

Known

- Penelitian sebelumnya dalam penggunaan ZTNA sudah dilakukan pada 2 penelitian berikut:
- **Online Laboratory Access Control With Zero Trust Approach: Twingate Use Case**
- **Study of Zero Trust Architecture for Applications and Network Security**

Unknown

- Pengukuran kuantitatif perbedaan kinerja dalam hal waktu respons antara Aplikasi dengan ZTNA dan tanpa ZTNA belum banyak dilakukan
- Pengukuran kuantitatif perbedaan perbedaan kinerja dalam hal penggunaan sumber daya antara Aplikasi dengan ZTNA dan tanpa ZTNA belum banyak dilakukan

Institut Teknologi Sepuluh Nopember

03 Studi Kasus

Perbandingan dari 2 Aplikasi Identik

Terdapat 2 (dua) aplikasi identik pada PT. XYZ seperti berikut:

1. Aplikasi Sistem Informasi dan Administrasi Legal di Environment Development yang dilindungi ZTNA
2. Aplikasi Sistem Informasi dan Administrasi Legal di Environment Production tanpa ZTNA

04 Rencana Hipotesis

How and Why *Fill the Gap*

1. Membandingkan dengan dua aplikasi yang sama yaitu Aplikasi Sistem Informasi dan Administrasi Legal pada Environment Development (menggunakan ZTNA) dan Environment Production (tidak menggunakan ZTNA)
2. Melakukan perbandingan metrik kinerja untuk mengetahui seberapa besar perbedaan pada aspek Waktu Respons dan Penggunaan Sumber Daya untuk fungsi yang sama di kedua aplikasi tersebut

05 Rencana Metodologi

1. Menentukan skenario fitur yang akan dilakukan pengujian perbandingan
2. Analisis Kuantitatif Hitung waktu respons dan Penggunaan Sumber Daya (resource) untuk setiap skenario fitur.
   a. Analisis efisiensi kinerja dalam aspek waktu respons dan kapasitas akses menggunakan tools JMeter.
   b. Analisis efisiensi kinerja dalam aspek penggunaan sumber daya menggunakan tools Monitoring Server yaitu OpManager
3. Evaluasi aspek waktu respons dan penggunaan sumber daya di setiap skenario fitur pada kedua aplikasi

06 Kesimpulan

1. Penelitian ini diharapkan menghasilkan informasi terkait penggunaan ZTNA pada aplikasi website. Mengacu pada teknologi lain yang serupa untuk pengamanan data, hasil penggunaan ZTNA diharapkan tidak banyak mengurangi kinerja sesuai dengan ISO 25023.
2. Informasi yang diharapkan didapat dari penelitian ini adalah sebagai berikut
   - Waktu respon
   - Penggunaan *resources*: memori dan CPU

07 Referensi

- E. Tuyishime, F. Radu, P. Cotfas, D. Cotfas, T. Balan and A. Rekeraho, "Online Laboratory Access Control With Zero Trust Approach: Twingate Use Case," 2024 16th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Iasi, Romania, 2024, pp. 1-7
- F. A. Qazi, "Study of Zero Trust Architecture for Applications and Network Security," 2022 IEEE 19th International Conference on Smart Communities: Improving Quality of Life Using ICT, IoT and AI (HONET), Marietta, GA, USA, 2022, pp. 111-116
- Zulfa, F., Munawaroh, H., & Rochimah, S. (2020). Portability Characteristics Evaluation of MyITS Mobile using ISO/IEC 25010 Quality Standard. 2020 International Seminar on Application for Technology of Information and Communication (ISemantic), 537–542
- Indrianto. (2023). PERFORMANCE TESTING ON WEB INFORMATION SYSTEM USING APACHE JMETER AND BLAZEMETER. Jurnal Ilmiah Ilmu Terapan Universitas Jambi, 7(2), 138–149

07 Referensi

- T. Sajid, "Securing 5G Cloud Native NFV Architecture with Zero Trust Security," 2023 IEEE Future Networks World Forum (FNWF), Baltimore, MD, USA, 2023, pp. 1-5
- J. Lin, Q. Jiang, W. Zhang, Z. Lin and X. Du, "Quantum-Enhanced Zero Trust Security: Evolution, Implementation, and Application," 2024 International Conference on Quantum Communications, Networking, and Computing (QCNC), Kanazawa, Japan, 2024, pp. 211-215
- ISO/IEC 25023:2016 - Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Measurement of system and software product quality
- S. Juneja, Arshdeep, S. Maiti, S. Raweri, B. S. Bhati and H. Sharma, "Comprehensive Evaluation of Network Performance Monitoring Solutions," 2024 International Conference on Intelligent Systems for Cybersecurity (ISCS), Gurugram, India, 2024, pp. 1-6

ITS
Institut
Teknologi
Sepuluh Nopember

Thank You!