Contents lists available at MID Publisher International

Technology Sciences Insights Journal

Journal homepage: https://journal.midpublisher.com/index.php/tsij

Analisis penerapan Trust Network Access (ZTNA) dengan penggunaan CAPTCHA pada website umum

Hafizhah Najwa

Prodi Sistem Informasi, Fakultas Sains, Institut Teknologi Bacharuddin Jusuf Habibie, Parepare, Indonesia

INFORMASI ARTIKEL

Sejarah Artikel:
Diterima: Juli 2024
Revisi: September 2024
Diterima: September 2024
Dipublikasi: November 20204

Kata Kunci:
Zero Trust Network Access (ZTNA), Keamanan Jaringan, Otentikasi Multifaktor (MFA), Segmentasi Mikro, Kebijakan Akses Kontekstual. Ancaman Siber, Strategi Implementasi Keamanan

*Penulis Korespondensi:
Hafizhahnajwa4@gmail.com

ABSTRAK

Model keamanan konvensional yang berpusat pada perimeter jaringan tidak lagi memadai mengingat ancaman siber yang semakin kompleks dan peningkatan penggunaan teknologi digital. Metode keamanan Zero Trust Network Access (ZTNA) muncul sebagai solusi yang lebih efektif untuk mengatasi ancaman tersebut. Menurut ZTNA, tidak ada entitas yang dapat dipercaya secara otomatis, baik di dalam maupun di luar jaringan, jadi setiap akses harus divalidasi terlebih dahulu. Dalam penelitian ini, konsep ZTNA, prinsip-prinsipnya, dan tahapan implementasinya di situs web dipelajari. Studi menunjukkan bahwa ZTNA meningkatkan keamanan melalui verifikasi ketat setiap pengguna dan perangkat melalui otentikasi multifaktor (MFA) dan pemantauan aktivitas pengguna yang berkelanjutan. Meskipun implementasi ZTNA menghadirkan masalah seperti biaya awal yang tinggi dan kompleksitas integrasi, metode ini menawarkan fleksibilitas, mobilitas kerja yang lebih baik, dan pengurangan permukaan. serangan melalui kebijakan akses berbasis kontekstual dan segmentasi mikro. Studi ini memberikan pedoman praktis untuk organisasi yang ingin menggunakan ZTNA untuk meningkatkan keamanan jaringan mereka.

ABSTRACT

The conventional security model centered on network perimeter is no longer adequate given the increasingly complex cyber threats and the rise in digital technology usage. The Zero Trust Network Access (ZTNA) security method emerges as a more effective solution to address these threats. According to ZTNA, no entity can be automatically trusted, whether inside or outside the network, so every access must be validated first. This study examines the concept of ZTNA, its principles, and its implementation stages on a website. The study shows that ZTNA enhances security through strict verification of each user and device via multifactor authentication (MFA) and continuous monitoring of user activity. Although implementing ZTNA presents challenges such as high initial costs and integration complexity, this method offers flexibility, better work mobility, and reduced attack surfaces through contextual access policies and micro-segmentation. This study provides practical guidelines for organizations looking to adopt ZTNA to improve their network security.

PENDAHULUAN

Dengan semakin kompleksnya ancaman siber dan meningkatnya penggunaan teknologi digital, model keamanan tradisional yang berfokus pada perimeter jaringan tidak lagi memadai. Konsep Zero Trust Network Access (ZTNA) muncul sebagai pendekatan keamanan yang lebih adaptif dan efisien dalam mengatasi ancaman tersebut. ZTNA mengasumsikan bahwa tidak ada

Copyright © 2024 Authors. This is an open-access article distributed under the terms of the Creative Commons Attribution-ShareAlike 4.0 International License (http://creativecommons.org/licences/by-sa/4.0/)

entitas yang dapat dipercaya secara default, baik dari dalam maupun luar jaringan, sehingga setiap akses harus divalidasi terlebih dahulu. [1]

Perubahan paradigma ini didorong oleh berbagai faktor, termasuk peningkatan jumlah perangkat yang terhubung ke jaringan, adopsi cloud computing, dan semakin canggihnya metode serangan siber. Model keamanan tradisional yang berasumsi bahwa segala sesuatu di dalam perimeter jaringan dapat dipercaya telah terbukti tidak efektif dalam menghadapi ancaman-ancaman modern. Dengan ZTNA, setiap akses ke sumber daya jaringan diperlakukan sebagai potensi risiko, yang memerlukan verifikasi dan otorisasi yang ketat. [1]

Namun, implementasi ZTNA bukan tanpa tantangan. Organisasi harus memahami konsep dan prinsip-prinsip ZTNA secara mendalam, serta memiliki strategi yang jelas untuk mengintegrasikan teknologi dan proses yang diperlukan. Oleh karena itu, penelitian ini bertujuan untuk menganalisis konsep ZTNA dan langkah-langkah implementasinya, sehingga dapat memberikan panduan praktis bagi organisasi dalam meningkatkan keamanan jaringan mereka. [2]

METODE

Analisis deskriptif digunakan dalam jurnal ini untuk mendapatkan pemahaman dan evaluasi konsep Zero Trust Network Access (ZTNA), prinsip-prinsipnya, dan prosedur implementasinya pada sebuah website. Metode ini terdiri dari beberapa langkah. Pertama, penelitian literatur dilakukan dengan mengumpulkan informasi dari berbagai sumber, termasuk jurnal, artikel, dan penelitian sebelumnya terkait ZTNA. Berbagai studi dan artikel yang menjelaskan implementasi ZTNA dan teknologi yang terkait juga digunakan. Prinsip "never trust, always verify", yang merupakan ide dasar dari ZTNA, dipelajari secara menyeluruh setelah itu. Ketiga, tahapan implementasi ZTNA diidentifikasi. Tahapan ini mencakup verifikasi perangkat, verifikasi pengguna melalui CAPTCHA, dan penggunaan otentikasi multifaktor (MFA). Keempat, keunggulan ZTNA dalam meningkatkan keamanan jaringan serta kelemahan dan tantangan yang mungkin dihadapi selama implementasi, seperti biaya tinggi dan kompleksitas integrasi. Terakhir, upaya untuk membantu organisasi mengadopsi ZTNA termasuk perencanaan yang matang, pelatihan karyawan, evaluasi infrastruktur, dan penerapan kebijakan akses dinamis. Panduan praktis dibuat untuk membantu ini. Dengan analisis deskriptif ini, jurnal ini memberikan pemahaman yang luas tentang ZTNA dan saran praktis untuk pelaksanaannya di dunia nyata.

Zero Trust Network Access (ZTNA)

Zero Trust Network Access (ZTNA) merupakan sebuah model keamanan jaringan yang beroperasi berdasarkan prinsip "never trust, always verify." Pendekatan ini menggantikan model keamanan tradisional yang mengandalkan perimeter jaringan yang dianggap dapat dipercaya. ZTNA memperlakukan setiap entitas, baik pengguna, perangkat, maupun aplikasi, sebagai potensi risiko dan memerlukan proses autentikasi dan otorisasi yang ketat sebelum memberikan akses ke sumber daya jaringan.

Implementasi ZTNA di sebuah website, melibatkan beberapa langkah utama: pengguna mencoba mengakses website dari perangkat mereka, menyelesaikan CAPTCHA untuk verifikasi sebagai manusia, memasukkan kode verifikasi dari aplikasi autentikasi di ponsel, dan sistem memverifikasi bahwa perangkat memenuhi kebijakan keamanan. Meskipun ZTNA menawarkan peningkatan signifikan dalam keamanan jaringan, penelitian menunjukkan bahwa tantangan yang dihadapi termasuk biaya implementasi awal yang tinggi dan kompleksitas integrasi dengan sistem yang sudah ada.[3]

Dengan demikian, ZTNA merupakan pendekatan keamanan yang lebih adaptif dan efisien dalam menghadapi ancaman siber modern, meskipun memerlukan perencanaan dan pelaksanaan yang cermat untuk mengatasi berbagai tantangan yang mungkin timbul.[4]

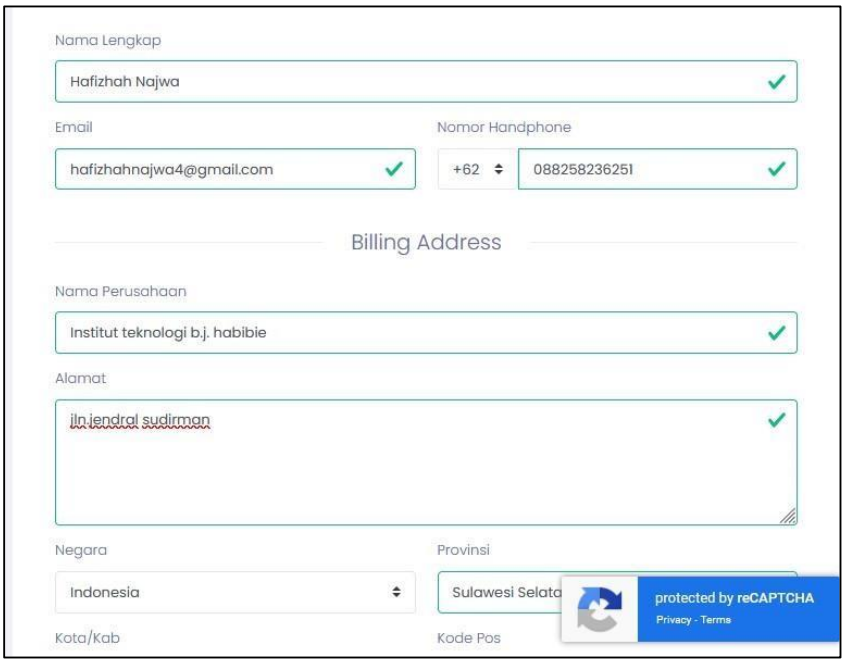
HASIL DAN PEMBAHASAN

Dalam menghadapi semakin kompleksnya ancaman siber dan meningkatnya penggunaan teknologi digital, model keamanan tradisional yang berfokus pada perimeter jaringan tidak lagi memadai. Konsep Zero Trust Network Access (ZTNA) muncul sebagai pendekatan keamanan yang lebih adaptif dan efisien dalam mengatasi ancaman tersebut dengan asumsi bahwa tidak ada entitas yang dapat dipercaya secara default, baik dari dalam maupun luar jaringan, sehingga setiap akses harus divalidasi terlebih dahulu. ZTNA menggantikan pendekatan keamanan perimeter tradisional dengan prinsip "never trust, always verify," yang berarti setiap pengguna, perangkat, atau aplikasi harus melalui proses autentikasi dan otorisasi yang ketat, sering kali melalui multifactor authentication (MFA), sebelum diberikan akses.

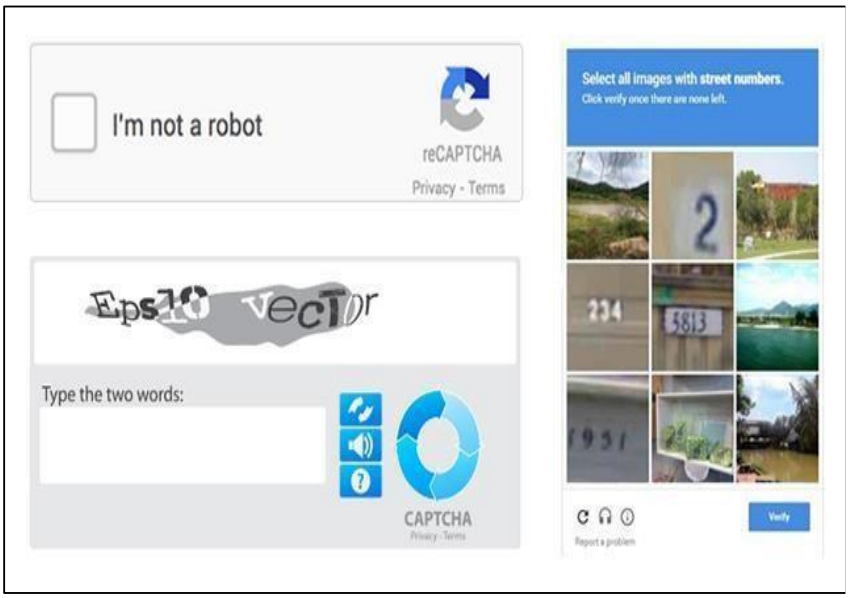
Kebijakan akses ZTNA bersifat dinamis dan kontekstual, menyesuaikan izin berdasarkan berbagai faktor seperti lokasi pengguna, jenis perangkat, waktu akses, dan perilaku pengguna sebelumnya. Selain itu, segmentasi mikro membantu membatasi dampak potensi pelanggaran keamanan dengan membatasi pergerakan lateral di dalam jaringan, dan pemantauan serta analitik berkelanjutan digunakan untuk mendeteksi dan merespons aktivitas mencurigakan. Semua komunikasi dalam arsitektur ZTNA dienkripsi untuk memastikan kerahasiaan dan integritas data.

Implementasi ZTNA pada sebuah website melibatkan beberapa langkah utama: pengguna mencoba mengakses website dari perangkat mereka, menyelesaikan CAPTCHA untuk verifikasi sebagai manusia, memasukkan kode verifikasi dari aplikasi autentikasi di ponsel, dan sistem memverifikasi bahwa perangkat memenuhi kebijakan keamanan. Keunggulan ZTNA termasuk peningkatan keamanan, fleksibilitas dan mobilitas kerja, serta pengurangan permukaan serangan melalui segmentasi mikro dan akses berbasis kontekstual. Namun, implementasi ZTNA juga memiliki beberapa kelemahan seperti kompleksitas integrasi dengan sistem yang ada, biaya implementasi awal yang tinggi, dan ketergantungan pada konektivitas internet yang andal. Kesimpulannya, meskipun ZTNA menawarkan peningkatan signifikan dalam keamanan jaringan dan manajemen risiko, organisasi harus siap menghadapi tantangan dalam implementasi dan pemeliharaan sistem ini. Berikut tahapan ZTNA pada sebuah website:

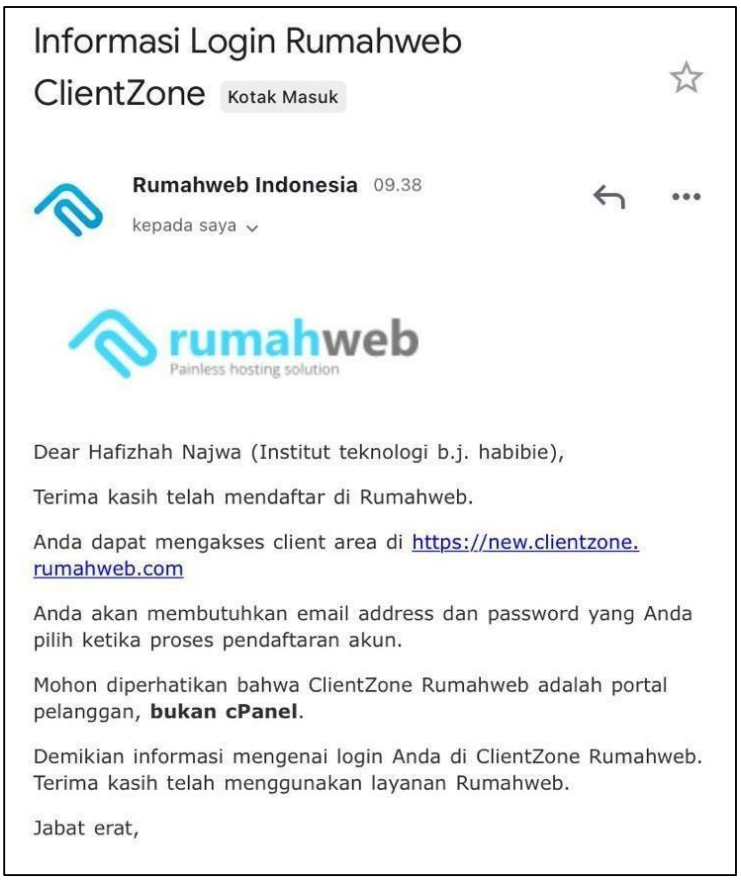
1. Mahasiswa Akses website: Mahasiswa mencoba mengakses sebuah web dari laptop di rumah.



2. CAPTCHA: Mahasiswa menyelesaikan CAPTCHA untuk memastikan bahwa mereka adalah manusia.



3. Multi-Factor Authentication (MFA): Mahasiswa memasukkan kode verifikasi dari aplikasi autentikasi di ponsel.



4. Verifikasi Perangkat: Sistem memverifikasi bahwa laptop memenuhi kebijakan keamanan.

Zero Trust Network Access (ZTNA) adalah pendekatan keamanan yang menegaskan prinsip "never trust, always verify". Setiap pengguna dan perangkat harus melalui proses autentikasi yang kuat sebelum diberikan akses, berdasarkan kebijakan yang dinamis dan kontekstual. Meskipun menawarkan peningkatan keamanan, implementasi ZTNA bisa kompleks dan memerlukan biaya tinggi. Namun, dengan mengurangi permukaan serangan dan menyederhanakan pengalaman pengguna, ZTNA menjadi langkah signifikan dalam menghadapi ancaman keamanan modern dan meningkatkan manajemen risiko secara keseluruhan.

KESIMPULAN DAN SARAN

Zero Trust Network Access (ZTNA) adalah pendekatan keamanan yang menggantikan model tradisional dengan prinsip "never trust, always verify," memastikan setiap akses ke sumber daya jaringan melalui autentikasi dan otorisasi ketat. Meskipun implementasinya bisa kompleks dan mahal, ZTNA menawarkan peningkatan keamanan signifikan, fleksibilitas, dan pengurangan risiko. Untuk mengoptimalkan implementasi ZTNA, organisasi harus melakukan perencanaan matang, memberikan pelatihan kepada staf IT, melakukan evaluasi infrastruktur, menerapkan kebijakan akses dinamis secara bertahap, serta memastikan pemantauan dan respons cepat terhadap ancaman. Kolaborasi dengan vendor teknologi terpercaya juga penting untuk mengatasi tantangan teknis dan menyesuaikan solusi dengan kebutuhan keamanan.

DAFTAR PUSTAKA

A. Nuryasa and I. Suharjo, "Implementasi Traefik sebagai Reverse Proxy dengan Prinsip Zero Trust".

P. García-Teodoro, J. Camacho, G. Maciá-Fernández, J. A. Gómez-Hernández, and V. J. López-Marín, "A Novel Zero-Trust Network Access Control Scheme based on the Security Profile of Devices and Users." [Online]. Available: https://nesg.ugr.es

R. Sahtyawan, "Penerapan Zero Entry Hacking Didalam Security Misconfiguration Pada Vapt (Vulnerability Assessment and Penetration Testing)," 2019.

B. T. Yulianto *et al.*, "Rancang Bangun Private Server Menggunakan Platform Proxmox dan Penerapan Zero Trust Model dengan Cloudflare," Desember.