Contents lists available at MID Publisher International

Technology Sciences Insights Journal

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

Penerapan Zero Trust Network Access (ZTNA) dengan penggunaan CAPTCHA pada website umum

Rakhmadi Rahman, Aldi Fatur Rahman

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, CAPTCHA, Keamanan Siber, Website Umum, Verifikasi Pengguna, Serangan DDoS, Perlindungan Data.

*Penulis Korespondensi:
aldifatur463@gmail.com

ABSTRAK

Metode keamanan yang mengutamakan prinsip "tidak ada yang dipercaya secara default" untuk mengakses sumber daya jaringan dikenal sebagai Zero Trust Network Access (ZTNA). ZTNA dapat memperkuat sistem informasi, terutama situs web umum yang rentan terhadap serangan siber. Studi ini membahas penerapan ZTNA dengan menambahkan CAPTCHA sebagai metode verifikasi untuk memastikan bahwa pengguna yang mengakses website adalah manusia dan bukan bot. Dengan menganalisis berbagai studi kasus dan implementasi nyata, penelitian ini menunjukkan bahwa penerapan CAPTCHA dalam konteks ZTNA meningkatkan keamanan dan juga mengurangi risiko serangan DDoS dan penyalahgunaan akses. Hasil penelitian menunjukkan bahwa kombinasi ZTNA dan CAPTCHA dapat meningkatkan keamanan web dengan menambahkan lapisan perlindungan tambahan.

ABSTRACT

A security method that prioritizes the principle of "no one is trusted by default" to access network resources is known as Zero Trust Network Access (ZTNA). ZTNA can strengthen information systems, especially public websites that are vulnerable to cyber attacks. This study discusses the application of ZTNA by adding CAPTCHA as a verification method to ensure that users accessing the website are humans and not bots. By analyzing various case studies and real implementations, this research shows that implementing CAPTCHA in the context of ZTNA improves security and also reduces the risk of DDoS attacks and misuse of access. The research results show that the combination of ZTNA and CAPTCHA can improve web security by adding an additional layer of protection.

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

Dalam era digital saat ini, perlindungan infrastruktur jaringan menjadi prioritas utama perusahaan di seluruh dunia. ZTNA bekerja bersama Secure Access Service Edge (SASE) untuk membentuk jaringan yang lebih aman dan responsif. ZTNA memungkinkan pemantauan yang ketat dan sebagai komponen pembangunan SASE, memberikan akses informasi yang sebelumnya sulit diakses seperti data lalu lintas dan tindakan. Implementasi ZTNA sangat penting untuk mengatasi perbedaan dalam teknologi dan metode akses yang aman, memastikan pengguna dapat mengakses aplikasi dari berbagai perangkat dan lokasi, serta menghasilkan

jaringan yang lebih aman, fleksibel, dan berpotensi mengurangi biaya dengan mengurangi kebutuhan akan infrastruktur kompleks dan mahal.

Rumusan Masalah

1. Apa itu Zero Trust Network Access (ZTNA) dan bagaimana prinsip-prinsipnya diterapkan dalam keamanan jaringan?
2. Bagaimana tahapan impelemntasi ZTNA pada sebuah website?

Tujuan

Tujuan dari penelitian ini adalah untuk menganalisis konsep dan prinsip-prinsip Zero Trust Network Access (ZTNA) serta mengidentifikasi langkah-langkah implementasi ZTNA pada sebuah website. Penelitian ini akan menggali lebih dalam mengenai bagaimana ZTNA dapat meningkatkan keamanan jaringan dengan verifikasi ketat setiap pengguna dan perangkat. Selain itu, penelitian ini bertujuan untuk mengembangkan panduan praktis bagi implementasi ZTNA, termasuk kebijakan akses yang ketat, penggunaan otentikasi multifaktor, dan pemantauan aktivitas pengguna secara berkelanjutan, sehingga dapat melindungi website dari akses tidak sah dan berbagai ancaman keamanan.

HASIL DAN PEMBAHASAN

Tujuan implementasi Zero Trust Network Access (ZTNA) adalah untuk mencapai sejumlah hasil penting dalam manajemen keamanan akses jaringan. Pertama, dengan menggunakan prinsip "tidak pernah percaya, selalu verifikasi", ZTNA memastikan bahwa setiap permintaan akses pengguna atau perangkat harus melalui proses verifikasi yang ketat sebelum diizinkan untuk mengakses sumber daya jaringan. Ini secara efektif mengurangi risiko dari ancaman internal maupun eksternal karena memungkinkan akses hanya untuk entitas yang terverifikasi, melindungi sumber daya jaringan dari akses yang tidak sah. Dengan memungkinkan karyawan mengakses aplikasi dan data perusahaan dari mana saja, ZTNA meningkatkan mobilitas dan fleksibilitas kerja. Ini sangat penting dalam lingkungan kerja modern yang memungkinkan produktivitas yang tinggi tetapi tetap aman.

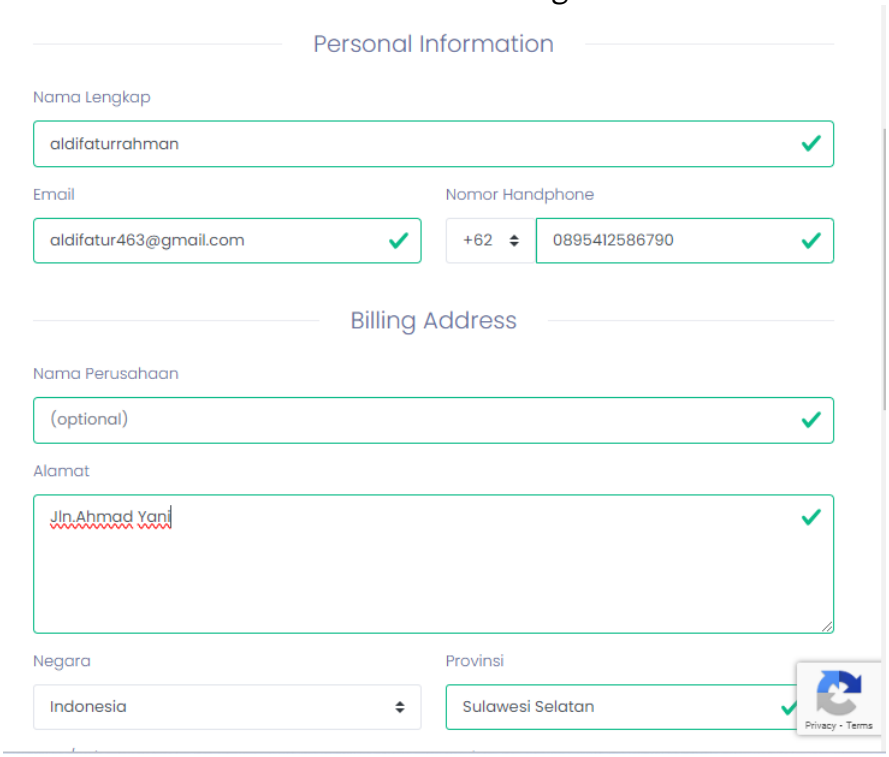
ZTNA memungkinkan organisasi untuk memberikan tingkat akses yang sesuai dengan konteks pengguna, seperti lokasi, perangkat, dan lainnya, dengan memantau dan mengelola setiap sesi akses. Selain itu, dengan menggunakan akses berbasis kontekstual, ZTNA segmentasi jaringan mikro dan memungkinkan pengaturan kebijakan akses yang sangat spesifik untuk setiap pengguna atau perangkat. Ini membatasi dampak potensial dari pelanggaran keamanan, sehingga upaya untuk menyebar ke bagian lain jaringan dapat dikurangi atau dicegah sepenuhnya jika suatu bagian jaringan mengalami pelanggaran keamanan. Sangat penting untuk melakukan analisis menyeluruh tentang hasil peningkatan keamanan yang dicapai, fleksibilitas kerja yang lebih besar, dan efisiensi segmentasi jaringan mikro dalam mengurangi risiko keamanan secara keseluruhan saat berbicara tentang hasil implementasi ZTNA.

Selain itu, monitoring dan evaluasi berkala terhadap kinerja ZTNA diperlukan untuk memastikan bahwa sistem tetap berfungsi dengan baik saat menghadapi ancaman keamanan yang terus muncul dan untuk menemukan area yang memerlukan penyesuaian atau perbaikan kebijakan. Metode ini memungkinkan perusahaan untuk membangun dan mempertahankan lingkungan IT yang lebih aman dan responsif terhadap masalah keamanan kontemporer. 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

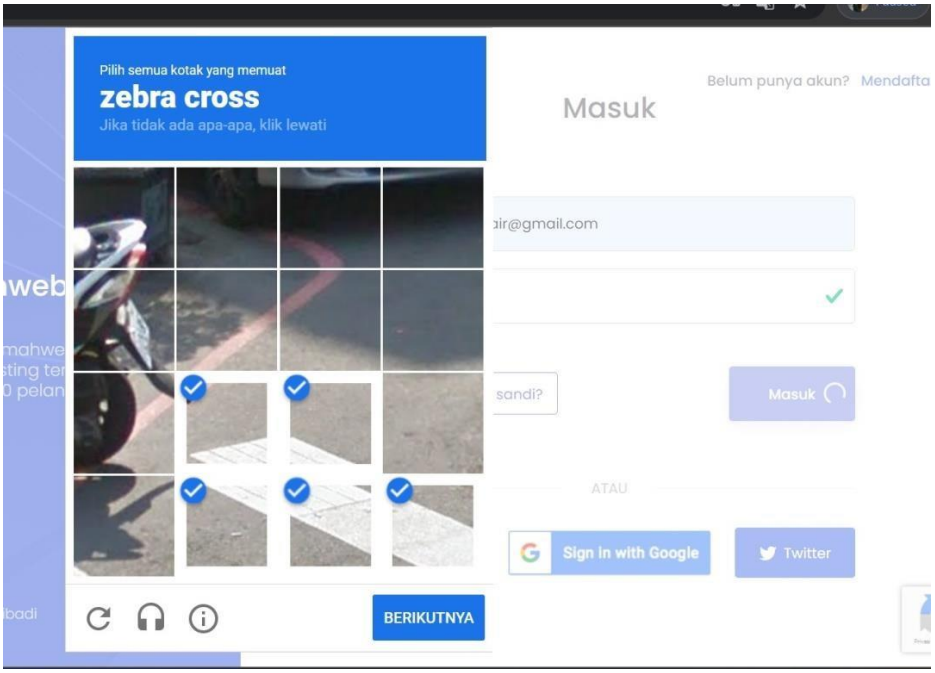
serangan melalui segmentasi mikro dan akses berbasis kontekstual. Namun, implementasi ZTNA juga memiliki beberapa kelemahan seperti kompleksitas integrasi dengan sistem yang ada, biaya implementasi awal yang tinggi, dan ketergantungan pada konektivitas internet yang andal. Kesimpulannya, meskipun ZTNA menawarkan peningkatan signifikan dalam keamanan jaringan dan manajemen risiko, organisasi harus siap menghadapi tantangan dalamimplementasi dan pemeliharaan sistem ini.

Berikut tahapan ZTNA pada sebuah website:

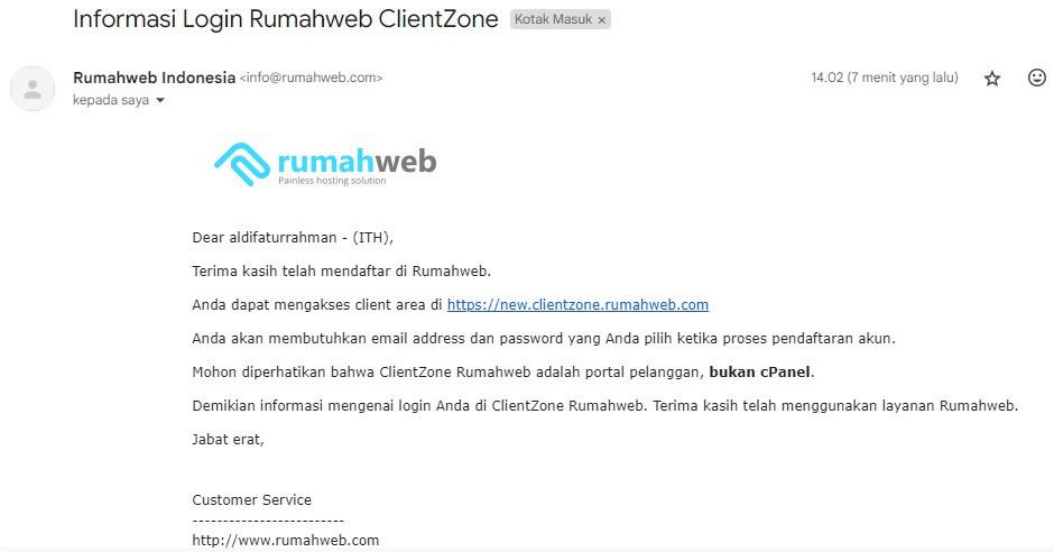
1. Mahasiswa Akses website: Mahasiswa mencoba mengakses sebuah web dari laptop di rumah



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.

REFERENSI

Adhar, S., & Saprudin, U. (2023). Implementasi Cloudflare Zero Trust Dalam Mendeteksi Aktivitas Cryptojcking Pada Jaringan Komputer. *JTKSI (Jurnal Teknologi Komputer dan Sistem Informasi)*, *6*(1), 23-28.

Hardiyanto sari, (2023). Bagaimana cara kerja Chapca dan tombol Im not robot?. (https://www.kompas.com/tren/read/2023/05/02/120000265/bagaimana-cara-kerja- tes-captcha-atau-tombol-i-m-not-a-robot-?page=all) di akses pada tanggal 15 juni 2023.

Yulianto, B. T., Quraisy, M., Daulay, A., Daulay, A., & Sari, A. P. (2023). JURNAL ILMU KOMPUTER. *Jurnal Ilmu Komputer| Vol*, *1*(2), 195-207.

Innovations Advance, (2023). Mengenal zero trus security, konsep dan manfaatnya dalam keamanan IT Bisnis. (https://www.ad-ins.com/id/our-story/kisah-adins/mengenal-zero-

trust- security-konsep-dan-manfaatnya-dalam-keamanan-it-bisnis/) di akses pada tanggal 15 juni 2023.

Mediana, S. D., & Fadhli, M. (2023). Implementing Zero Trust Model for SSH Security with kerberos and OpenLDAP. *S*