IMPLEMENTASI GLOBALPROTECT PRISMA ACCESS BERBASIS ZERO TRUST

Nasrullah, Tomi Loveri, Akmal Budi Yulianto
Program Studi Teknik Informatika, STMIK Jayakarta, Indonesia
Jl. Salemba Raya No.24, RT.4/RW.6, Kenari, Kec. Senen, Kota Jakarta Pusat, DKI Jakarta 10430)
nasrul_bucos@yahoo.com

ABSTRAK

Perkembangan teknologi informasi yang pesat, disertai meningkatnya ancaman siber, menuntut institusi perbankan untuk menerapkan sistem keamanan jaringan yang lebih robust, khususnya dalam menyediakan akses jarak jauh yang aman guna melindungi data sensitif dan menjaga integritas sistem. Penelitian ini bertujuan mengimplementasikan dan mengevaluasi sistem keamanan jaringan berbasis Zero Trust Network Access (ZTNA) menggunakan GlobalProtect Prisma Access serta menganalisis efektivitasnya dalam meningkatkan keamanan akses jarak jauh, efisiensi operasional, dan perlindungan data.Metode penelitian yang digunakan adalah deskriptif dengan pendekatan eksperimental, menerapkan kerangka Network Development Life Cycle (NDLC) yang meliputi tahapan analisis kebutuhan, perancangan, pembuatan prototipe, implementasi, pemantauan dan evaluasi, serta pemeliharaan. Implementasi sistem mencakup konfigurasi portal dan gateway GlobalProtect, integrasi autentikasi Two-Factor Authentication (2FA) melalui Okta, penerapan security profiles, serta konfigurasi captive portal.Hasil pengujian menunjukkan keberhasilan sistem pada sembilan skenario uji, antara lain koneksi Always-On, Internal Host Detection (IHD), pemilihan gateway optimal, Host Information Profile (HIP) checking, dekripsi SSL, autentikasi pengguna, akses aplikasi internal, URL filtering, serta deteksi dan pencegahan ancaman. Sistem mampu menerapkan kontrol akses berbasis identitas, inspeksi trafik tingkat lanjut, pencegahan ancaman secara real-time, dan logging terpusat untuk monitoring aktivitas jaringan. Implementasi GlobalProtect Prisma Access berbasis Zero Trust terbukti efektif dalam meningkatkan keamanan akses jaringan, mencegah akses tidak sah, serta memberikan visibilitas menyeluruh terhadap aktivitas jaringan perbankan.

***Kata kunci**: Zero Trust; GlobalProtect; Prisma Access; Keamanan Jaringan; Remote Access; Two-Factor Authentication; Perbankan.*

1. PENDAHULUAN

Perkembangan teknologi informasi yang pesat dan meningkatnya adopsi pola kerja jarak jauh telah mendorong organisasi, khususnya sektor perbankan, untuk menyediakan akses jaringan yang aman, fleksibel, dan andal. Transformasi digital menyebabkan data dan aplikasi perusahaan tidak lagi terbatas pada jaringan internal, melainkan dapat diakses dari berbagai lokasi dan perangkat, sehingga memperluas permukaan serangan siber. Ancaman seperti data breach, malware, phishing, dan eksploitasi autentikasi yang lemah menjadi risiko serius, terutama bagi institusi yang mengelola data sensitif dan tunduk pada regulasi ketat.

Teknologi Virtual Private Network (VPN) tradisional yang selama ini digunakan untuk mendukung akses jarak jauh memiliki keterbatasan mendasar karena hanya melakukan autentikasi di awal koneksi dan memberikan kepercayaan penuh kepada pengguna setelah terhubung. Pendekatan ini tidak lagi relevan dengan lanskap ancaman modern. Oleh karena itu, paradigma Zero Trust Network Access (ZTNA) hadir dengan prinsip never trust, always verify, yang mewajibkan verifikasi berlapis berbasis identitas, konteks, dan kondisi perangkat. Prisma Access dari Palo Alto Networks, dengan GlobalProtect sebagai agen endpoint, merupakan solusi berbasis cloud-native yang menerapkan konsep Zero Trust dan diharapkan mampu menutup celah keamanan VPN tradisional sekaligus meningkatkan kinerja dan pengalaman pengguna.

Berdasarkan kondisi tersebut, permasalahan yang diangkat dalam penelitian ini meliputi bagaimana meningkatkan keamanan akses jarak jauh, memperku at autentikasi pengguna, meningkatkan visibilitas dan kontrol jaringan, serta mengurangi ketergantungan pada infrastruktur keamanan tradisional yang kompleks dan kurang adaptif terhadap kebutuhan kerja jarak jauh.

Penelitian ini bertujuan untuk mengimplementas ikan dan mengevaluasi sistem keamanan jaringan berbasis Zero Trust Network Access menggunakan GlobalProtect Prisma Access. Tujuan khusus penelitian adalah menganalisis peningkatan keamanan akses jarak jauh, mengevaluasi efektivitas konfigurasi komponen utama sistem Zero Trust, menilai peran autentikasi berlapis melalui Two-Factor Authentication (2FA), serta mengkaji dampaknya terhadap efisiensi operasional dan kenyamanan pengguna.

Penyelesaian masalah dilakukan melalui pendekatan Network Development Life Cycle (NDLC) yang mencakup analisis kebutuhan, perancangan, implementasi, pengujian, serta evaluasi sistem. Implementasi meliputi konfigurasi GlobalProtect portal dan gateway, integrasi autentikasi 2FA berbasis Okta, penerapan security profiles, dan captive portal. Pengujian dilakukan pada berbagai skenario akses jarak jauh untuk menilai efektivitas

keamanan, performa sistem, dan visibilitas aktivitas jaringan.

2. TINJAUAN PUSTAKA

2.1. Penelitian Terdahulu

Kajian penelitian terdahulu menunjukkan bahwa pendekatan keamanan jaringan berbasis perimeter tradisional tidak lagi efektif dalam menghadapi ancaman siber modern. Kusnanto et al. [1] membuktikan bahwa penerapan Zero Trust Architecture (ZTA) melalui simulasi mampu meningkatkan keamanan jaringan secara signifikan, meskipun berdampak pada penurunan performa ringan. Namun, penelitian tersebut masih terbatas pada lingkungan simulasi dan belum merepresentasikan kompleksitas jaringan nyata.

Mukhlisin dan Firmansyah [2] melalui systematic literature review menegaskan bahwa ZTA efektif meningkatkan keamanan dan privasi data, khususnya pada institusi pendidikan. Kendati demikian, penelitian ini bersifat konseptual dan belum menyertakan implementasi teknis di lingkungan operasional. Rahman et al. [3] mengkaji implementasi Zero Trust Security pada UMKM dan menunjukkan penurunan insiden keamanan hingga 50%, tetapi masih menghadapi kendala biaya dan kesiapan sumber daya manusia.

Pendekatan integratif ZTA dengan teknologi lain juga diteliti. Fitrian et al. [4] mengombinasikan ZTA dan blockchain untuk meningkatkan keamanan cloud, sementara Darmawan et al. [5] mengintegrasikan ZTA dengan machine learning untuk deteksi intrusi IoT dengan akurasi tinggi. Walaupun inovatif, kedua penelitian tersebut belum mengkaji penerapan ZTA secara langsung pada sistem akses jarak jauh berbasis enterprise cloud security.

Berdasarkan penelitian-penelitian tersebut, dapat disimpulkan bahwa masih terdapat research gap pada implementasi Zero Trust Network Access (ZTNA) secara nyata untuk akses jarak jauh di lingkungan perbankan menggunakan solusi cloud-native terintegrasi seperti Prisma Access GlobalProtect.

2.2. Zero Trust Network Access (ZTNA)

Zero Trust Network Access (ZTNA) merupakan paradigma keamanan jaringan yang menerapkan prinsip never trust, always verify, di mana setiap permintaan akses diverifikasi berdasarkan identitas pengguna, kondisi perangkat, dan konteks koneksi [6]. Berbeda dengan VPN tradisional yang memberikan akses tingkat jaringan, ZTNA hanya memberikan akses ke aplikasi tertentu sesuai kebijakan (least privilege access).

ZTNA bekerja melalui mekanisme autentikasi berlapis, evaluasi endpoint posture, serta segmentasi mikro yang mencegah pergerakan lateral ancaman [7]. Pendekatan ini terbukti lebih adaptif terhadap lingkungan kerja jarak jauh dan adopsi cloud dibandingkan model keamanan konvensional.

Arsitektur Zero Trust Network Access (ZTNA)
(User → Identity Provider → Policy Engine → Application)

2.3. GlobalProtect dan Prisma Access

GlobalProtect merupakan agen endpoint dari Palo Alto Networks yang berfungsi mengamankan koneksi pengguna ke jaringan organisasi dengan menerapkan prinsip ZTNA [8]. GlobalProtect memastikan setiap koneksi diverifikasi secara berkelanjutan melalui autentikasi pengguna, pemeriksaan Host Information Profile (HIP), serta penerapan kebijakan keamanan berbasis identitas.

Prisma Access adalah layanan keamanan berbasis cloud yang mengadopsi arsitektur Secure Access Service Edge (SASE) dengan mengintegrasikan NGFW, ZTNA, dan Secure Web Gateway [9]. Dengan pendekatan application-level access, Prisma Access menghilangkan ketergantungan pada VPN tradisional dan meningkatkan visibilitas serta kontrol lalu lintas jaringan secara terpusat.

Tabel 1. Perbandingan VPN Tradisional dan ZTNA

Aspek	VPN Tradisional	ZTNA
Model Akses	Network-level	Application-level
Trust Model	Trusted after login	Continuous verification
Segmentasi	Tidak granular	Mikro-segmentasi
Risiko Lateral Movement	Tinggi	Rendah

2.4. Two-Factor Authentication (2FA) dan Okta

Two-Factor Authentication (2FA) merupakan mekanisme autentikasi berlapis yang mengombinasikan dua faktor verifikasi untuk meningkatkan keamanan akses sistem [10]. Penerapan 2FA terbukti efektif dalam menurunkan risiko phishing dan pencurian kredensial [11].

Okta sebagai platform Identity and Access Management (IAM) berbasis cloud mendukung implementasi 2FA, Single Sign-On (SSO), dan manajemen identitas terpusat [12]. Integrasi Okta dengan Prisma Access GlobalProtect memperkuat kontrol akses berbasis identitas dan selaras dengan prinsip Zero Trust.

2.5. Posisi Penelitian

Berdasarkan tinjauan pustaka, penelitian ini memposisikan diri sebagai studi implementatif yang mengisi celah antara kajian konseptual ZTA dan penerapan teknis di lingkungan perbankan. Berbeda dengan penelitian sebelumnya yang dominan berbasis simulasi atau kajian literatur, penelitian ini mengimplementasikan Prisma Access GlobalProtect berbasis ZTNA dengan autentikasi 2FA Okta pada lingkungan uji yang merepresentasikan sistem

perbankan, serta mengevaluasi keamanan, performa, dan efisiensi operasional akses jarak jauh.

3. METODE PENELITIAN

Penelitian ini menggunakan jenis penelitian terapan (applied research) dengan pendekatan studi kasus. Pendekatan ini dipilih karena penelitian berfokus pada penerapan dan evaluasi arsitektur keamanan jaringan berbasis Zero Trust Network Access (ZTNA) dalam lingkungan organisasi nyata, bukan pada pengembangan teori murni. Penelitian terapan memungkinkan pengujian langsung efektivitas solusi keamanan terhadap permasalahan akses jarak jauh yang dihadapi organisasi.

3.1. Teknik Pengumpulan Data

Teknik pengumpulan data dalam penelitian ini meliputi:

a. Observasi Teknis
Observasi dilakukan terhadap proses akses jaringan sebelum dan sesudah penerapan ZTNA untuk mengidentifikasi perubahan pola akses dan potensi risiko keamanan.

b. Studi Dokumentasi
Dokumentasi teknis berupa konfigurasi sistem, kebijakan keamanan, dan log akses digunakan untuk mendukung analisis implementasi.

c. Pengujian Sistem
Pengujian dilakukan dengan mensimulasikan skenario akses pengguna untuk mengevaluasi efektivitas kontrol akses, autentikasi berlapis, dan pembatasan hak akses.

3.2. Teknik Analisis Data

Analisis data dilakukan secara deskriptif-kualitatif dengan membandingkan kondisi sistem sebelum dan sesudah implementasi ZTNA. Parameter analisis meliputi:

a. Tingkat pembatasan akses jaringan
b. Mekanisme autentikasi dan otorisasi
c. Visibilitas dan kontrol keamanan

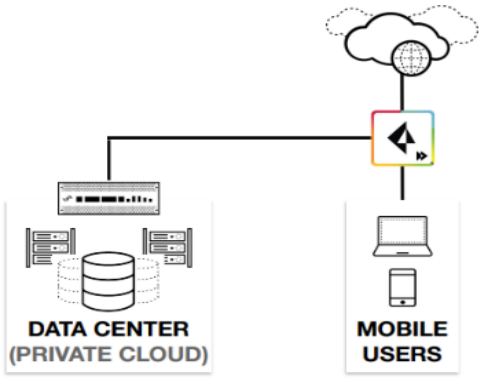
Hasil analisis disajikan dalam bentuk tabel perbandingan dan deskripsi teknis untuk memudahkan interpretasi.

Table 2. Parameter Analisis Implementasi ZTNA

Parameter	Sebelum Implementasi	Sesudah Implementasi
Model Akses	Berbasis jaringan	Berbasis jaringan
Autentikasi	Single factor	Two-factor
Visibilitas Keamanan	Terbatas	Terpusat
Risiko Lateral Movement	Tinggi	Rendah

3.3. Merancang Desain

Dari hasil analisis kebutuhan, akan dibangun sebuah topologi jaringan sederhana untuk validasi konsep yang terdiri dari mobile user, data center dan satu instance GlobalProtect (Prisma Access) sebagai gateway/cloud security.



Gambar 1. Topology Jaringan

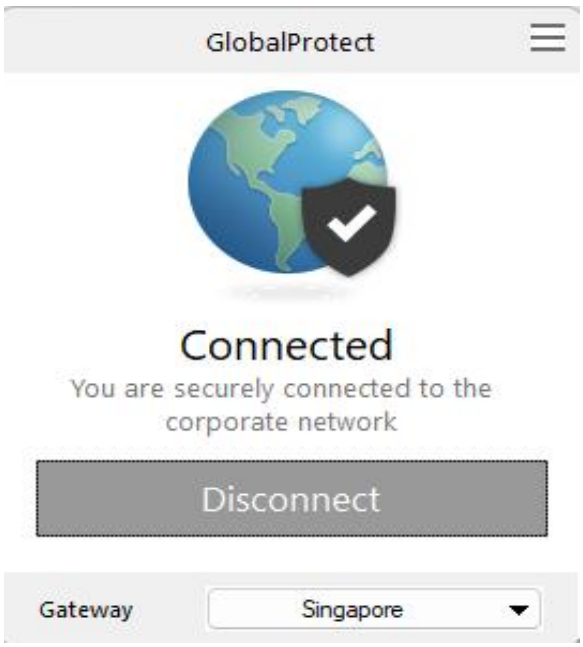
4. HASIL DAN PEMBAHASAN

Pengujian dilakukan dengan mensimulasikan beberapa skenario akses pengguna, baik dari jaringan internal maupun eksternal.

(User → Autentikasi IAM → Verifikasi 2FA → GlobalProtect → Prisma Access → Aplikasi)

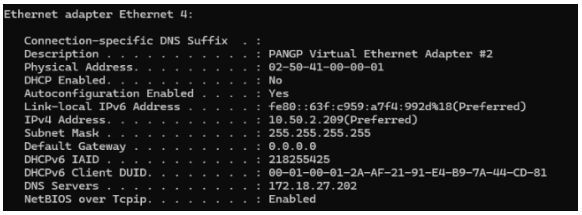
4.1. Jaringan External.

Melakukan koneksi ke GlobalProtect menggunakan jaringan external dan tunnel vpn terbentuk secara otomatis setelah user berhasil konek ke global protect.

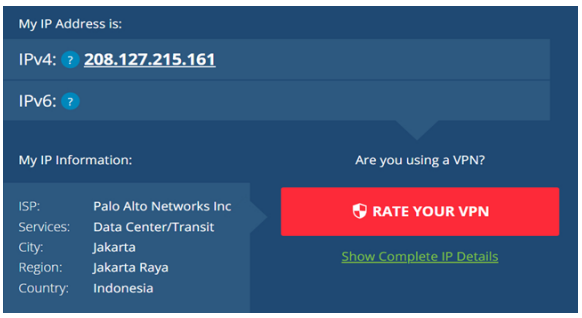


Gambar 2. GlobalProtect-external network

Setelah berhasil konek endpoint akan memperoleh ip address dari pool vpn sesuai configurasi dan semua traffic akan melewati prisma access.



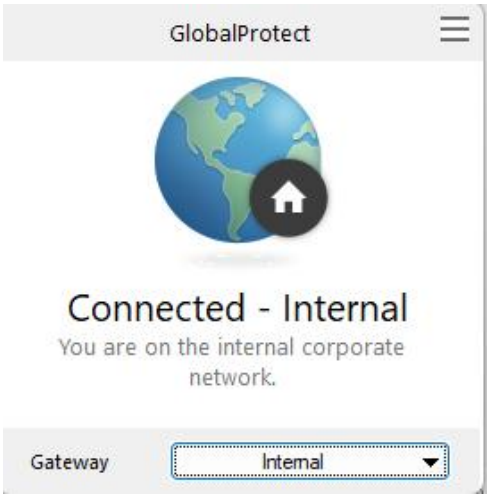
Gambar 3. Ip Address



Gambar 4. Ip Prisma Access

4.2. Jaringan Internal

Saat endpoint berada di jaringan internal status globalprotect connected tanpa membentuk tunnel yang berdampak meningkatkan efisiensi trafik internal.



Gambar 5. GlobalProtect-internal network

Hasil pengujian menunjukkan bahwa sistem secara konsisten menerapkan autentikasi berlapis sebelum memberikan akses ke aplikasi internal. pergeseran dari kontrol berbasis jaringan ke kontrol berbasis identitas secara langsung menjawab permasalahan keamanan akses jarak jauh yang menjadi fokus penelitian.

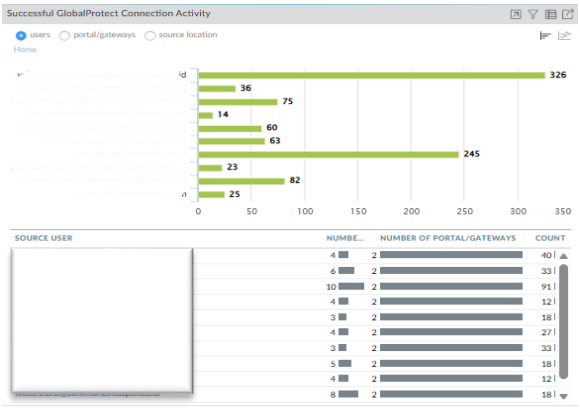
Tabel 3. Hasil Pengujian Akses Pengguna 1

Kondisi User	Captive Portal	HIP Posture	Akses Internet	Akses Internal
user login	✗	-	✓	✗
Sudah login	✓	Non-Compliant	✓	✗ (restricted)
Sudah login	✓	Compliant	✓	✓ sesuai policy

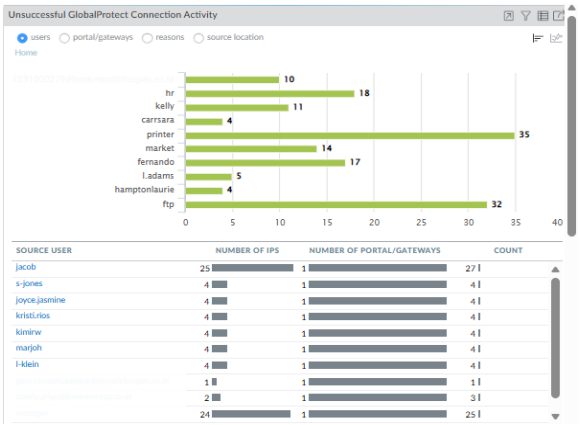
Data pada Tabel 3 menunjukkan bahwa mekanisme ZTNA mampu membatasi akses sesuai kebijakan dan mencegah akses tidak sah.

4.3. Hasil Monitoring

Sistem mampu mencatat setiap percobaan akses, baik yang berhasil maupun yang ditolak, sehingga memudahkan proses audit dan evaluasi keamanan.



Gambar 6. user sukses login



Gambar 7. User Gagal Login

5. KESIMPULAN DAN SARAN

Berdasarkan hasil penelitian dan pengujian yang telah dilakukan, dapat disimpulkan bahwa implementasi GlobalProtect Prisma Access berbasis Zero Trust Network Access (ZTNA) berhasil meningkatkan tingkat keamanan akses jaringan. Mekanisme autentikasi berlapis yang mengintegrasikan Active Directory, Two-Factor Authentication (2FA) melalui Okta, serta Captive Portal menunjukkan efektivitas yang tinggi dalam memastikan bahwa hanya pengguna yang terverifikasi yang dapat mengakses sumber daya internal. Selain itu, penerapan Host Information Profile (HIP) sebagai bagian dari evaluasi posture keamanan perangkat memungkinkan sistem melakukan kontrol akses yang tidak hanya berbasis identitas pengguna, tetapi juga kondisi keamanan endpoint yang digunakan.

DAFTAR PUSTAKA

[1] Y. Kusnanto et al., "Implementasi Zero Trust Architecture untuk Meningkatkan Keamanan Jaringan," JIPI, vol. 9, no. 4, pp. 2357–2364, 2024.
[2] M. Mukhlisin dan R. A. Firmansyah, "Zero Trust Architecture: Systematic Literature Review," JATI, vol. 9, no. 4, pp. 6926–6935, 2025.
[3] A. Rahman et al., "Implementation of Zero Trust Security in MSME," Sinkron, vol. 8, no. 3, pp. 2077–2087, 2024.
[4] H. P. Fitrian et al., "Analisis Keamanan Cloud dengan Zero Trust dan Blockchain," JGTC, vol. 4, no. 1, pp. 36–43, 2024.
[5] R. W. Darmawan et al., "Adaptive Zero Trust Architecture for IoT," RIGGS, vol. 3, no. 4, pp. 36–45, 2025.
[6] R. Dhiman et al., "Zero Trust Network Access: Concepts and Challenges," 2024.
[7] Skyhigh Security, Zero Trust Network Access Overview, 2025.
[8] Palo Alto Networks, GlobalProtect Administrator's Guide, 2022.
[9] Palo Alto Networks, Prisma Access Technical Overview, 2022.
[10] R. Herdiantoro et al., "Implementasi Two-Factor Authentication," 2023.
[11] I. Saputra et al., "2FA and Firewall Policy for Web Security," 2021.
[12] Okta Inc., Identity and Access Management Platform, 2024.