INTISARI

PENGAMANAN REMOTE ACCESS INFRASTRUKTUR HYBRID CLOUD BERBASIS PRIVILEGED ACCESS MANAGEMENT DAN ZERO TRUST NETWORK ACCESS

Rafif Dzakwan Nur Azhari
20/464276/SV/18595

Adopsi infrastruktur *Hybrid Cloud* menghadirkan tantangan pengamanan *Remote Access*, dimana metode tradisional gagal mengatasi risiko akses terlalu luas, kerentanan kredensial, kurangnya audit, dan hambatan konektivitas NAT atau *firewall*. Implementasi arsitektur terintegrasi *Privileged Access Management* menggunakan Jumpserver dengan *Zero Trust Network Access* melalui Netbird, Zitadel, dan Cloudflare Access. Pengujian fungsionalitas menggunakan metode *Black Box Testing* memvalidasi keberhasilan sistem dalam menyediakan *Remote Access* pada SSH, VNC, dan MariaDB yang aman, terkontrol, dan teraudit pada kedua lingkungan infrastruktur, termasuk yang berada dalam jaringan NAT dengan koneksi untuk salah satu *protocol* memiliki latency yang sedikit lebih besar sekitar 0.1 ms dibandingkan menggunakan sistem metode tradisional. Hasilnya sistem PAM dan ZTNA menunjukkan peningkatan postur keamanan, sentralisasi manajemen, serta latency yang minim pada infrastruktur *Hybrid Cloud*. Dengan sistem *Secure Remote Access* ini, organisasi dapat mengamankan infrastruktur Hybrid Cloud secara aman pada lingkungan *production*.

Kata kunci : *Secure Remote Access*, *Privileged Access Management*, *Zero Trust Network Access, Hybrid Cloud*

ABSTRACT

SECURE REMOTE ACCESS HYBRID CLOUD INFRASTRUCTURE BASED ON PRIVILEGED ACCESS MANAGEMENT AND ZERO TRUST NETWORK ACCESS

Rafif Dzakwan Nur Azhari
20/464276/SV/18595

The adoption of Hybrid Cloud infrastructure presents significant challenges in securing Remote Access, where traditional methods fail to address risks such as excessive access privileges, credential vulnerabilities, lack of audit capabilities, and connectivity barriers caused by NAT or firewalls. This research implements an integrated architecture combining Privileged Access Management using Jumpserver with Zero Trust Network Access through Netbird, Zitadel, and Cloudflare Access. Functional testing using the Black Box Testing method validates the system's success in providing secure, controlled, and audited Remote Access for SSH, VNC, and MariaDB protocols across both infrastructure environments, including those behind NAT networks, with one protocol showing slightly higher latency of 0.1 ms compared to traditional methods. The results demonstrate that the PAM and ZTNA system achieves improved security posture, centralized management, and minimal latency in Hybrid Cloud infrastructure. With this Secure Remote Access system, organizations can securely protect their Hybrid Cloud infrastructure in production environments.

Keyword: Secure Remote Access, Privileged Access Management, Zero Trust Network Access, Hybrid Cloud