Enhancing the Flexibility of Cross Domain Solutions through a Zero Trust Overlay Approach*

SangKyu Ham[1] and Jungsoo Park[2]

[1] Department of Computer Engineering, Kangnam University (Undergraduate Student)
[2] Department of Computer Engineering, Kangnam University (Professor, Corresponding Author)

Abstract

The COVID-19 pandemic revealed the security limitations of VPNs, and Zero Trust Architecture (ZTA) has emerged as an alternative. ZTA complements the limitations of conventional session-based access control by applying request-level verification. This paper proposes a converged model that combines the principles of ZTA with the Access Cross Domain Solution (Access CDS) concept, viewing external-to-internal network access in a similar context.

Keywords: Zero Trust Architecture, Cross Domain Solution, Network Security, Risk-based Access Control

1 Introduction

The COVID-19 pandemic rapidly expanded remote work environments, exposing the security limitations of VPNs, such as credential theft and lack of scalability [1]. As an alternative, the Zero Trust Architecture (ZTA) has emerged, proposing a security model that continuously verifies every access request based on the principle of "Never Trust, Always Verify."

Remote access from an external network to an internal network is essentially an access between different security domains, which is functionally similar to an Access Cross Domain Solution (CDS). However, Access CDS relies on session-based authentication and authorization, making it difficult to reflect dynamic security attributes [2]. To address this limitation, this paper proposes a converged model that applies ZTA principles to Access CDS.

2 Related Work

A Cross Domain Solution (CDS) is a structural security framework designed to safely enable information exchange between domains with different security policies or classification levels. CDS fulfills the requirements of high-assurance environments by providing not only path control but also content filtering, data transformation, and audit logging. CDS is generally classified into Access, Transfer, and Multi-Level Security (MLS) types. In particular, Access CDS serves as a gateway that allows session-based access between physically or logically separated networks. However, existing CDS implementations rely on static policy-based control, making it difficult to reflect dynamic security attributes such as session context, user behavior, and device status [3].

Zero Trust Architecture (ZTA) is a security model that can complement these limitations by performing continuous identity verification and context-based access control for all entities, including users, devices, and networks. Under the principle of "Never Trust, Always Verify," it repeatedly verifies each request instead of trusting an entire session. This approach supplements the static policy structure of existing CDS and enables active response to evolving threat environments [4].

*Proceedings of the 9th International Conference on Mobile Internet Security (MobiSec'25), Article No. P-35, December 16-18, 2025, Sapporo, Japan.

3 Proposed Model

In this study, to overcome the session-based control limitations of Access CDS, we propose a Portal-Resource based hybrid structure that applies Zero Trust Architecture. The proposed model aggregates all access requests from external users through a Policy Enforcement Point (PEP), and the portal performs TLS termination and OIDC/JWT-based authentication.

The PEP in the external zone enforces access policies, while the internal PDP performs policy decisions and risk evaluation. This structure keeps policy logic and audit data in the trusted domain and routes all requests through the portal, reducing the external attack surface.

Through this approach, the proposed model retains the conventional CDS structure while realizing request-level verification and context-based access control. When a user connects to the portal, the PEP verifies the device certificate and token, and transmits contextual information (user, device, location, etc.) to the PDP. The PDP calculates a risk score based on this data and determines whether to allow, reauthenticate, or block access. The risk score is derived from factors such as device integrity, user reputation, location anomalies, and behavioral deviation. If the score exceeds a threshold, additional authentication (MFA) or session termination is triggered.

The portal continuously reevaluates RiskScore and triggers reauthentication when anomalies occur. The proposed architecture preserves network separation while overlaying existing CDS, mitigating threats like credential theft and session hijacking.

4 Conclusion

This paper proposed a Portal-Resource based hybrid model applying Zero Trust Architecture (ZTA) to address the session-based control limitations of Access CDS in separated network environments. The proposed model verifies every access request at a single portal and performs dynamic request-level access control through TLS/OIDC-based authentication and risk score evaluation. This approach maintains the security advantages of network separation while actively responding to threats such as credential theft and session hijacking.

Acknowledgments

This work was supported by the IITP (Institute of Information & Communications Technology Planning & Evaluation) - ITRC (Information Technology Research Center) grant funded by the Korea government (Ministry of Science and ICT) (IITP-2025-RS-2020-II201602).

References

[1] Velayutham, A. (2023). *Secure Access Service Edge (SASE) Framework in Enhancing Security for Remote Workers and Its Adaptability to Hybrid Workforces in the Post-Pandemic Workplace Environment*. Nobislab.

[2] U.S. Department of Defense. (2021). *Cross Domain Solution (CDS) Overview*. National Security Agency (NSA).

[3] Sundaravarathan, V., Siddiqui, A., Alqalaf, H., Kim, K., Lee, S., Reisslein, M., Thyagaturu, A. S., Ross, N., Howard, J., & Tayal, S. (2024). *Cross-Domain Solutions (CDS): A Comprehensive Survey*. IEEE Access.

[4] Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero Trust Architecture* (NIST Special Publication 800-207). National Institute of Standards and Technology.