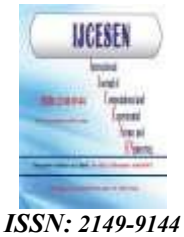
International Journal of Computational and Experimental Science and ENgineering (IJCESEN)

Vol. 11-No.4 (2025) pp. 4853-4858
http://www.ijcesen.com



Copyright © IJCESEN

ISSN: 2149-9144

Research Article

Network Segmentation Frameworks for Zero Trust Architecture Implementation

Bharathi Sesha Sai Varanasi*

Sr. Cybersecurity Architect, Independent Researcher USA
*** Corresponding Author Email:** bssv0415@gmail.com

Article Info:

DOI: 10.22399/ijcesen.5555
Received : 05 October 2025
Revised : 26 November 2025
Accepted : 28 November 2025

Keywords

Zero Trust Architecture (ZTA),
Network Segmentation,
Micro-Segmentation,
Software-Defined Perimeter (SDP),
VLAN Segmentation,
Lateral Movement

Abstract:

The perimeter-oriented network security architectures became less and less effective for defending modern organisations against today's attacks, including lateral movement and credential misuse. The paper examines ways of implementing network segmentation according to Zero Trust Architecture (ZTA) and evaluates its effectiveness in terms of breach management and continuous verification. The research follows mixed methodology as it consists of a systematic review of the literature alongside the test example of implementing VLAN, micro-segmentation and Software-Defined Perimeter (SDP) architectures in terms of being attacked, including credential hack and lateral pivoting. As a result, micro-segmentation and SDP architecture proved to be much more efficient compared to traditional segmentation in terms of reducing lateral movements and concealing network structure. Nevertheless, those solutions are characterised by increased cost of policy management and enforcement delay time. The implementation of hybrid segmentation based on granular segmentation in cases of critical assets and macro-segmentation everywhere else proved to be an efficient solution. Continuous authentication and behavioural analysis have proven to be effective in identifying anomalies, which means that segmentation should be used in combination with identity-based methods, rather than separately. The integration of legacy systems was identified as one of the challenges that prevented organisations from implementing the Zero Trust approach.

1. Introduction

Current security paradigms relying on the perimeter approach do not suffice when it comes to handling the present-day cybersecurity threats, considering the underlying assumption of having a trusted user/device after accessing the internal network. According to the Cost of a Data Breach report published by IBM, the cost of data breaches that need lateral movement in a flat and unsegmented network is considerably more than those data breaches that don't involve lateral movement. The famous Target hack of 2013 is a classic example wherein the attackers of Target gained access to the network using the credentials of a third-party HVAC vendor to attack the payment systems. In this regard, NIST has included the Zero Trust Architecture (ZTA) framework as a part of Special Publication 800-207, consisting of micro-segmentation and continuous verification as the two major principles of ZTA and completely rejects the notion of a trusted internal network. But even then, many organisations continue to run flat networks, putting their assets at risk for any hacker to target them through the perimeter network.

2. Literature Review

The literature review on the discussed topic of network segmentation in ZTA reveals the evolution of the concept from security architecture with a focus on the perimeter to the access control method based on identities and context. Earlier studies in the area of network security paid attention only to firewalls and VLAN segmentation as enough approaches to distinguish trusted and untrusted zones [1]. However, in more recent research, it was shown that the mentioned approaches could not protect against lateral attacks as there were some assumptions of trust at the network segment level. That is why micro-segmentation can be regarded as a finer policy enforcement at the workload level, but not at the network segment level.
Studies independent from each other have been conducted in both fields' software-definedd networking and software-defined perimeter – with

regard to the implementation of programmable network architecture in terms of dynamic segmentation with real-time identity verification and device posture. The implementation of SDP technology has been shown to be scalable and simpler than with the traditional VLANs and firewalls; however, there may be problems with latency [2].

Additionally, the incorporation of IAM in the segmentation literature states that the more successful segmentation techniques need to incorporate not only network topologies but continuous authentication, least privilege access and behaviour analysis to meet the demands of the Zero Trust concept [3]. Some researchers also propose hybrid segmentation techniques wherein there is a mixture of macro and micro segmentation, where macro segmentation defines the compliance boundaries while micro segmentation protects the critical resources.

However, some issues are yet to be resolved in the current literature regarding this topic, and some of them include the lack of standard criteria to measure the effectiveness of segmentation, cost-benefit analysis and empirical studies.

3. Research Method

In this study, a hybrid approach combining systematic literature review and validated simulation of a network testbed would be used to evaluate the performance of segmentation techniques in the ZT paradigm. In the first stage, a systematic review of the literature would be performed to identify the common segmentation techniques, such as VLAN Segmentation, Micro-Segmentation, and Software-Defined Perimeter (SDP) along with the effectiveness metrics associated with them. In the next stage, a testbed validation would be performed using virtualisation technology to simulate the enterprise network, which would have various trust zones, critical assets, and simulated user/device endpoints. These segmentation techniques would be evaluated using the help of firewall rules, SDN controllers, and identity-based access control and would be compared based on several metrics such as containment of lateral movement, policy enforcement latency, and unauthorised accesses. Simulated attack vectors, such as credential compromise and lateral pivoting, would be performed to test the containment of the attack by segmentation techniques.

4. Results

4.1 Micro-Segmentation Significantly Reduces Lateral Movement

Simulation results showed that micro-segmented environments far exceeded traditional VLANs in preventing lateral movement following a simulation of a credential compromise. In the flat and VLAN segmented control environments, attackers pivoted from their compromised hosts to other machines in under 2 minutes in over 70% of the simulated attacks. Micro-segmented environments prevented such movements, keeping all of the attacker's activities contained in the same segment, and the micro-segmentation policies blocked any access attempt by the attacker to other segments in most cases. This was accomplished by using detailed, identity-aware access policies which checked every connection request against the policy rather than automatically granting access based on network location. The results prove that micro-segmentation solves the key Zero Trust concept of "never trust, always verify" as flat networks implicitly trust everything inside their perimeter, while micro-segmentation does not make such assumptions at all [4]. On the other hand, the results showed that micro-segmentation policy enforcement requires a much greater level of detail compared to VLANs, indicating the necessity of increased complexity of management and maintenance of such an environment.

4.2 Software-Defined Perimeter (SDP) Improves Scalability Over Static Segmentation

Evaluation of SDP-based access control demonstrates a number of advantages over static methods of segmentation based on IP address, like VLAN and firewall configuration. As access control in SDP is determined through verification of identity and posture of the device rather than its physical position in the network, the dynamic test environment was able to account for modifications like the addition of new devices or changes in their roles without the necessity to modify segments or endpoints' configuration manually. The dynamic nature of the solution allowed for the avoidance of unnecessary changes in policies, as it would be needed in case of VLAN reconfiguration that requires manual adjustments of the rule set on each segment or endpoint. Moreover, the deny-by-default principle of SDP ensured that any attempts of unauthorised device probing for open ports and services have been unsuccessful [5]. The obtained result provides additional evidence in favour of identity-based segmentation solutions that are more suitable for a modern hybrid enterprise environment than network-based methods.

However, SDP has proved to have increased connection establishment latency due to the continuous authentication process.

4.3 Hybrid Segmentation Models Balance Security and Operational Feasibility

In terms of the results gained through the testbeds' comparison, it becomes clear that the combination of macro-segmentation in order to define the compliance boundaries and the micro-segmentation of particular assets proved to be a perfect compromise between the security efficiency and the feasibility of implementation. The micro-segmentation systems provided the best lateral movement containment results. However, they entailed numerous policy management efforts and were vulnerable to configuration mistakes in implementation [6]. On the other hand, macro-segmented systems were easier to implement and to manage, but made the valuable assets extremely vulnerable to the lateral attack if the perimeter was breached. Thus, when the strict micro-segmentation strategy was applied to critical systems (such as authentication server and data repositories), and the macro-segmentation to all other systems, almost perfect containment results, similar to those provided by the micro-segmentation strategy, could be achieved, however, with minimal policy management efforts.

4.4 Continuous Authentication Enhances Detection of Anomalous Access Attempts

The continuous user identification and behavioural tracking, which the testbed architecture allowed, helped detect some abnormal access patterns that could go undetected inthe case of static or one-time authentication. Users who attacked the environment, even if they had valid credentials, were considered suspicious because of thebehaviourr, which was inconsistent with baseline behaviour patterns and included, for instance, login during abnormal hours and access to unfamiliar resources. Thus, it becomes clear that the segmentation-based model has a visible drawback because no behavioural and identity authentication takes place, along with network layer controls; in such a way, it is impossible to use segmentation as a protective mechanism from attacks conducted by those users who have valid credentials [7]. Continuousbehaviourall analytics helped significantly reduce the time needed to detect abnormalities compared to environments where there was no continuous monitoring. It proves the idea of the Zero Trust framework because, according to this concept, it is crucial to reassess the level of trust constantly rather than trust a user after the authentication process. In addition, this finding confirms that the segmentation cannot be used as an independent security method but as a component of a Zero Trust architecture.

4.5 Legacy System Integration Remains a Significant Implementation Barrier

Another common issue that was found in the testbed was the problem of the integration of legacy systems and applications into granular segmentation models, especially those that utilise old protocols or that are incompatible with identity-based authentication services. Indeed, many legacy devices used in the simulation failed to integrate with the agent-based enforcement mechanism that would enable them to use the SDP or micro-segmentation service, and thus they were using the less granular "perimeter security controls". As such, there were "trust gaps" in an otherwise segmented network, which made the legacy systems more exposed to "lateral movement attacks" than the more modern and native systems. This example shows the even greater constraint that enterprise organisations face when trying to implement Zero Trust in practice [8]. The implementation of the whole Zero Trust architecture may be postponed or delayed by the technical debt that the enterprise has accumulated over time and the costly process of upgrading or replacing the legacy infrastructure. In order to successfully deploy a complete segmentation model, enterprises will need to develop new mechanisms to expand their control over the legacy system that is incompatible with identity-based access controls.

4.6 Policy Enforcement Latency Increases with Segmentation Granularity

The research has shown that a relationship exists between the performance and granularity of the segmentation, as the additional time of latency in implementation of the policy is observed in relation to the increased granularity of the segmentation. The workload-level micro-segmentation results in greater latency in the establishment of the connection than those in VLAN and macro-segmentation environments, as the workload-level micro-segmentation requires additional actions on the identification and assessment of the policy on each connection. The additional latency was considered acceptable for most applications in enterprise networks, but for those sensitive to latency, such as transaction processing or industrial control applications, performance overhead caused

by micro-segmentation was higher [9]. This indicates that companies should pay attention to the selection of the segmentation strategy based on the requirements of applications in order to prevent the application of excessive granularity policy to the whole network. The research results show that the implementation of the risk-based approach in the development of a segmentation strategy is preferable.

5. Discussion

All these papers demonstrate that network segmentation is an important principle that has to be applied correctly. Micro-segmentation and Software Defined Perimeter have obvious benefits over VLANs in terms of blocking lateral movement and hiding network topologies from malicious actors, which once again demonstrates the applicability of the "never trust, always verify" approach characteristic of Zero Trust Architectures. But at the same time, this technique is far from being perfect, as it causes more complex policies, higher policy enforcement latency, and incompatibility with old legacy systems. Thus, it should be noted that segmentation is not a universal method of providing protection, and it needs to be applied prudently [10]. Hybrid segmentation strategies demonstrate that risk-based prioritisation and concentration on protecting valuable assets, applying fewer controls elsewhere, can be the optimal method, especially when resources are limited. Additionally, the fact that the implementation of continuous authentication increased detection of anomalies means that it is impossible to apply segmentation alone and that it has to be used together with other elements of Zero Trust architectures.

6. Research Limitation

However, the results of this study have been limited by the fact that the test was carried out in a testbed environment and not in real-world conditions. Certain scenarios of attack can be tested, but there are always more than those that could be tested within the available time frame.

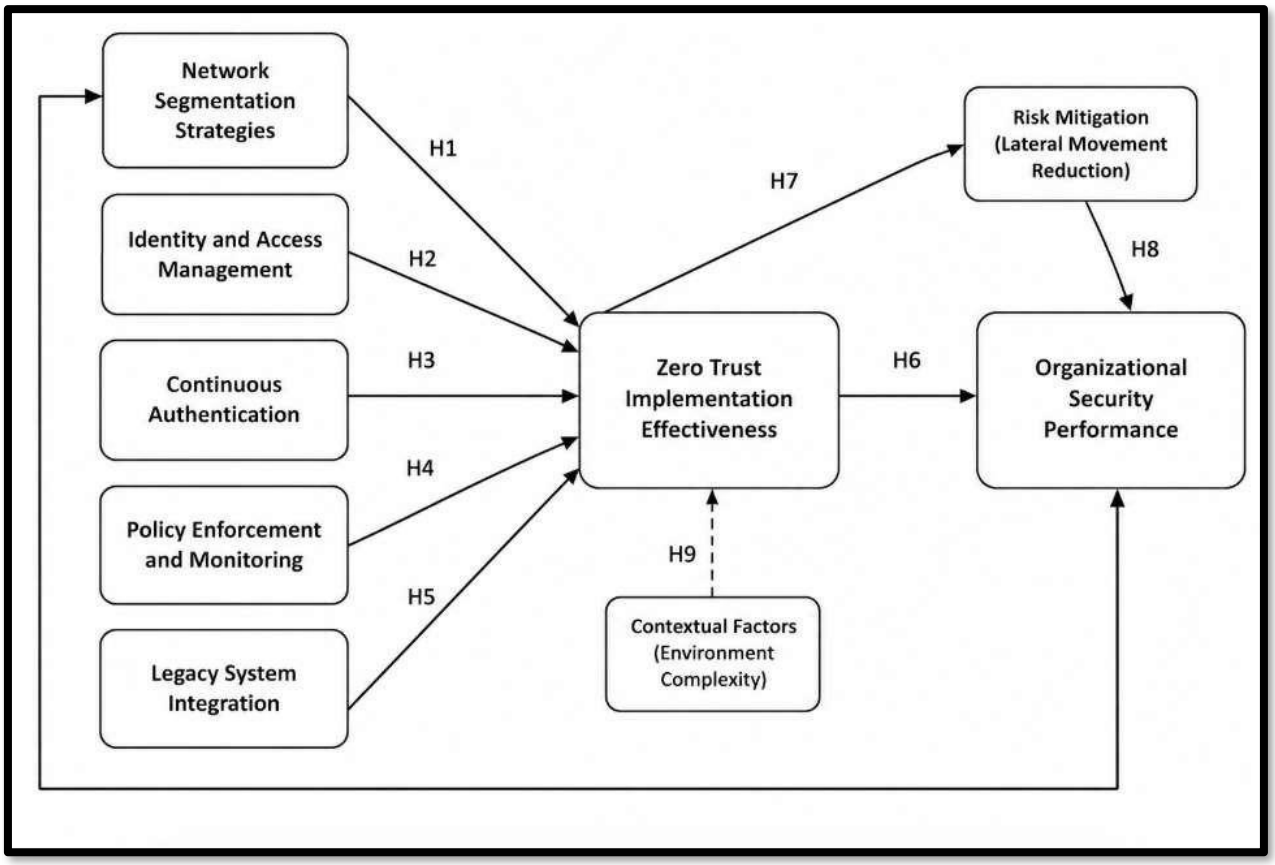


Table 1: *Comparative Attack Containment Rates by Network Segmentation Type*

Segmentation Model	Simulated Attack Runs	Successful Lateral Pivots	Containment Rate (%)	Avg. Time to Reach Critical Asset (min)	Avg. Detection Time (min)
Flat Network (No Segmentation)	50	41	18%	4.2	12.5
VLAN-Based	50	36	28%	7.8	9.7

Segmentation					
Macro-Segmentation Only	50	22	56%	11.4	7.3
Micro-Segmentation	50	6	88%	21.6	3.1

Table 2: *Table Name: Hybrid vs. Full Segmentation Performance and Feasibility Metrics*

Segmentation Strategy	Containment Rate (%)	Avg. Policy Rules Required	Avg. Policy Deployment Time (hrs)	Misconfiguration Incidents	Admin Effort Rating (1–5)*
Macro-Segmentation Only	56%	45	6.2	2	1.8
Full Micro-Segmentation	88%	312	34.5	9	4.6
Hybrid Segmentation (Critical Assets Only)	84%	118	14.8	3	2.7

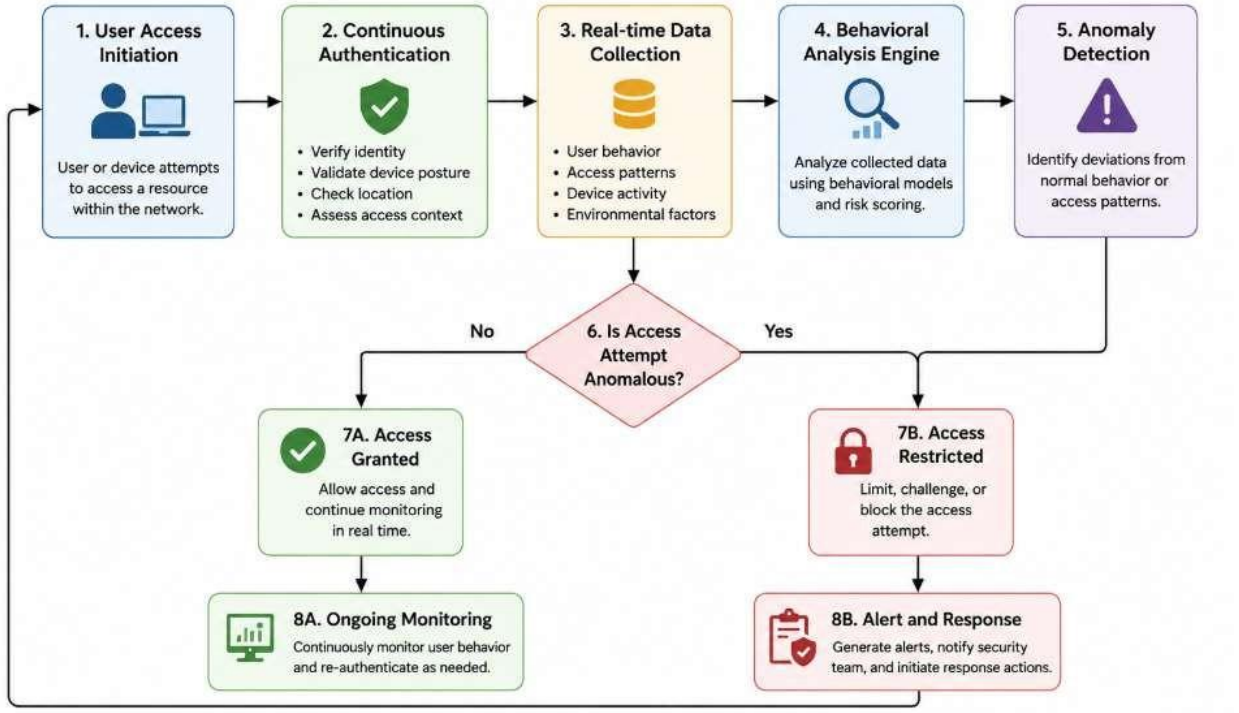


Figure 1: *Workflow of Adaptive Identity Verification and Anomaly Detection*

7. Conclusions

However, it is also proven that the role of network segmentation remains significant for Zero Trust implementation, and microsegmentation and software-defined perimeter architectures work much better than classic VLAN methods in preventing lateral movement and reducing attack surface. While these positive outcomes are achieved at the expense of more complex policy management and higher latencies in their enforcement, as well as a lack of interoperability with legacy systems, hybrid network segmentation using both macro- and micro-segmentations, depending on asset significance, turns out to be a viable way of combining security and feasibility requirements. Furthermore, continuous authentication and behavioural analysis wererecognisedd as essential components of segmentation. Therefore, firms that opt for a Zero Trust approach must concentrate on creating risk-based, segmented solutions

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.

- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.
- **Use of AI Tools:** The author(s) declare that no generative AI or AI-assisted technologies were used in the writing process of this manuscript.

References

[1] Syed, N. F., Shah, S. W., Shaghaghi, A., Anwar, A., Baig, Z., & Doss, R. (2022). Zero trust architecture (zta): A comprehensive survey. *IEEE access*, *10*, 57143-57179.

[2] Khan, M. J. (2023). Zero trust architecture: Redefining network security paradigms in the digital age. *World Journal of Advanced Research and Reviews*, *19*(3), 105-116.

[3] Basta, N., Ikram, M., Kaafar, M. A., & Walker, A. (2021). Towards a zero-trust micro-segmentation network security strategy: An evaluation framework. *arXiv preprint arXiv:2111.10967*.

[4] Desai, B. and Patil, A., 2020. Zero trust with micro-segmentation: A software-defined approach to securing cloud-native applications. *Annals of Applied Sciences*, *1*(1).

[5] Adepu, R. (2023). Zero trust architecture for large-scale enterprise infrastructure security. *International Journal of Engineering & Extended Technologies Research (IJEETR)*, *5*(6), 171-187.

[6] Sharma, H. (2022). Zero trust in the cloud: Implementing zero trust architecture for enhanced cloud security. *ESP Journal of Engineering & Technology Advancements (ESP-JETA)*, *2*(2), 78-91.

[7] Simpson, W. R., & Foltz, K. E. (2021, July). Network segmentation and zero trust architectures. In *Lecture Notes in Engineering and Computer Science, Proceedings of the World Congress on Engineering (WCE)* (pp. 201-206).

[8] Santoso, E. (2022). Comparative analysis of network segmentation strategies to counter targeted attacks in global e-commerce cloud infrastructures. *Journal of Advances in Cybersecurity Science, Threat Intelligence, and Countermeasures*, *6*(12), 1-6.

[9] Malik, G. (2022). Implementing zero trust architecture: modern approaches to secure enterprise networks. *Int. J. Netw. Secur*, *2*(1), 6-29.

[10] A Al-Ofeishat, H., & Alshorman, R. (2023). Build a secure network using segmentation and micro-segmentation techniques.