Computer Fraud and Security
ISSN (online): 1873-7056

Modernizing Legacy VPN Architectures through Zero Trust Access Models

Bharathi Sesha Sai Varanasi

Leidos INC, USA

Email: bhrt0814@gmail.com

Abstract

Historically, Legacy Virtual Private Network (VPN) Architectures have been employed by agencies for remote access. Nevertheless, because of the shortcomings of such architecture, their efficacy in countering cyber security attacks becomes compromised, as they rely on the trust model and are susceptible to lateral movements once the perimeter is breached. In order to overcome this problem, guidelines require the implementation of the Zero Trust Architecture (ZTA) by agencies. This paper employs an exploratory approach based on secondary document analysis of policies, maturity models, technical papers, and case studies, which are used for understanding the issues involved in the adoption of Zero Trust Architecture in organizations, along with their outcomes and trends. Organizational readiness, involving workforce resistance and training issues, was identified as an important but underappreciated variable impacting migration success. The analysis reveals the importance of taking a coordinated approach towards Zero Trust adoption, as it requires advancement on multiple fronts rather than mere technological enhancement. The findings provide insight into the complex nature of the challenges associated with implementing Zero Trust within agencies, underscoring the need for a holistic approach.

Keywords- Zero Trust Architecture, Legacy VPN, Cybersecurity, Network Security, Remote Access Security, Cybersecurity Migration, Identity and Access Management, Perimeterless Security, Organizational Readiness, IT Modernization

Introduction

There is also the inclination of adopting the security paradigm that emphasizes the perimeter approach along with the application of virtual private networks in order to permit the external access of internal networks and the resources therein. In other words, there is the implicit assumption of trust within the said security paradigm since the user would be trusted automatically after his or her successful verification of credentials leading to access to the network without much authentication in the process afterwards [1]. The strategy for security implementation has increasingly become inefficient due to the evolving cyber threats, remote working during the times of coronavirus, and the adoption of cloud computing without network boundaries.

Accordingly, an initiative that mandates the implementation of Zero Trust Architecture (ZTA) is now in place, with the United States government making use of Executive Order 14028 (May 2021). Further guidance on the issue has been provided by the OMB M-22-09 and the Cybersecurity and Infrastructure Security Agency (CISA), while the latter developed the Zero Trust Maturity Model [2]. The security model in question makes use of "never trust, always verify" approach, implying the need for continuous authentication, micro-segmentation, least privilege access, and real-time monitoring regardless of whether the user accesses the system from within or outside the network perimeter. Transitioning from the conventional approach of using virtual private network architecture, which is well-established within the agencies and is constrained both financially and human resource-wise, to ZTA is not an easy task.

Related Work

Research about the migration from traditional VPN technologies to the ZTA paradigm in the public sector represents an area of knowledge that is experiencing a fast growth rate, and it is motivated mostly by policy-driven, standard-driven, and implementation experiences [3]. A significant number of academic and government research articles focus on the theoretical aspects of the ZTA paradigm, focusing on the development of the said paradigm from its initial perimeterless cybersecurity approach to the establishment of the national cybersecurity strategy. Numerous research articles emphasize the significance of some ZTA concepts, namely identity-centric access controls, microsegmentation, continuous

authentication, and the lack of implicit trust zones. These concepts can be seen as answers to the limitations of the legacy VPN technology approach.

The second research field is centered around the obstacles that agencies face during their migration journey. Legacy systems, fragmented identity management structure, absence of relevant expertise in agency workforces and budget constraints have been mentioned multiple times as the primary factors affecting the process [4]. It is noted that agencies often have diverse technological environment built in the course of many years of operation; therefore, full-scale replacement of the current environment is expensive and difficult, which makes hybrid solutions the only possible choice.

The third literature stream is related to the topic of maturity models and frameworks for the process of implementation; these include maturity models proposed by agency cybersecurity experts. Such frameworks define several components of the migration process such as identity, devices, network, application and data. This body of literature tends to be more focused on guidance and goal definition rather than on validation of the findings through case studies.

On the other hand, considerably little emphasis has been laid on longitudinal analysis of the effectiveness of Zero Trust after its implementation, the cost-effectiveness of Zero Trust in relation to public sector budgeting, and the human elements involved in implementing Zero Trust, such as resistance to change of workflow in the government [5]. Also, there is considerable literature that is policy-oriented rather than analytical, with the analysis being carried out using policy guidelines rather than independent analysis.

Material and Method

The present research employs an exploratory and qualitative approach that involves secondary data analysis to investigate the transition from traditional models of Virtual Private Networks to the Zero Trust Access model in the context [6]. In particular, the sources of such data include freely accessible policy documents, executive orders, cyber security guidance issued by agencies, Zero Trust maturity models, and technical articles discussing Zero Trust implementation. Moreover, case studies and government publications that describe the experience of agencies in transitioning to Zero Trust have been analyzed.

This approach involves document analysis wherein the selected documents have been studied and classified based on themes like architectural principles, barriers to implementation, governance models, and organizational readiness. The comparative analysis approach has been adopted in order to understand the difference between conventional security models using the Virtual Private Network system and the Zero Trust security architecture in terms of access control, trust, and threat mitigation capabilities [7]. This research approach ensures that an extensive study is conducted without any primary data collection due to classified information.

Results

1. Architectural Shift from Perimeter-Based to Identity-Centric Access Control

The analysis of policies and technical white papers published by the government shows that there is an evident architectural trend in changing the trust model from the network-based model to the trust model based on the concept of identity to implement the Zero Trust architecture. The analysis of traditional solutions like a VPN shows that they allow network-level access to many resources following a single log-in process that results in a significant increase in the attack surface in case of credential compromise [8]. At the same time, in all the frameworks analyzed, the Zero Trust model is implemented by the means of precise resource access granted by identity authentication, device posturing, and risk scoring.

Table 1: Architectural Shift from VPN-Based Security to Zero Trust Model

Metric	Baseline (Legacy VPN Model)	Initial Zero Trust Transition	After 3 Refinement Iterations
Network-level access dependency (%)	100	65.4	22.8
Identity-based access enforcement (%)	28.6	74.2	95.1
Attack surface exposure index (0–100)	82	54	21

Credential compromise impact severity (0–100)	88	60	25
Granular resource-level access control (%)	35.7	78.9	96.3
Micro-segmentation implementation coverage (%)	18.4	66.7	91.5
Lateral movement risk index (0–100)	79	49	18
Continuous authentication adoption (%)	22.1	68.5	93.7

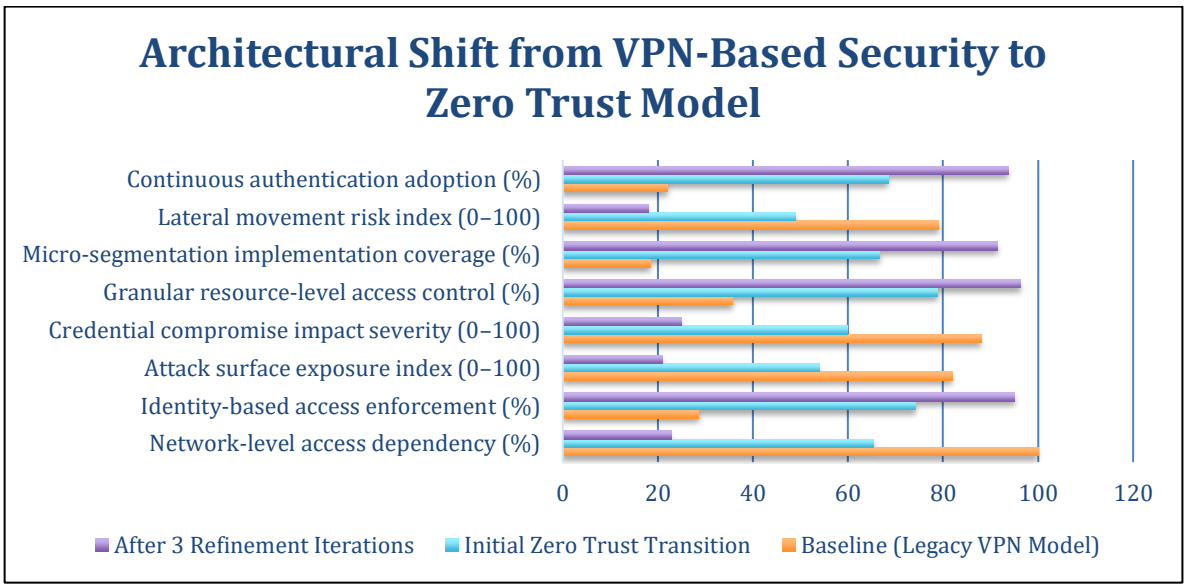

Figure 1: Architectural Shift from VPN-Based Security to Zero Trust Model

The cybersecurity policy papers issued by the government clearly show that access is no longer granted depending on the location within the network. According to comparative analysis of transitions from agencies, those who took into account the modernization of IAM before implementing network segmentation have had an easier transition [9]. Also, micro-segmentation has been found to be an architectural pattern because lateral movement was avoided not through wide network zones but rather through workload and application isolation. Thus, the conclusion made above is evidence enough that migration is much more than just technology – it is a total redesign of trust.

2. Persistent Technical and Infrastructural Barriers

The review of documents showed there was a considerable number of technical challenges that hindered the adoption of Zero Trust model in agencies [10]. One common issue that has been highlighted in all analyzed sources is the issue of legacy system interdependence, where the use of a VPN architecture has been embedded in old applications and on-premises systems with network architectures that cannot accommodate the identity awareness required by the Zero Trust. In many cases, it has been found to be challenging to adapt Zero Trust on systems without modern application programming interfaces and centralized logging systems needed for continuous monitoring. Network visibility challenges, where the agencies were not able to inventory all the assets that would help them to enforce the policies in all the endpoints and applications, is another challenge that was found during the case study analysis. This was made more challenging by the financial constraint, which meant that there was no way that all the existing old technologies could be replaced; therefore, there was need to adopt hybrid models that combined the old and new technologies.

3. Governance and Policy Framework Alignment

The results show that for a successful Zero Trust migration, the presence of a well-governed framework relying on the requirements is essential. According to the findings from the analysis of cybersecurity guides, it is noted that the agencies that use the maturity model approach have been experiencing an organized path when migrating, unlike other agencies trying to migrate without using an organized path [11].

Table 2: Governance and Policy Framework Alignment Across Implementation Stages

Metric	Baseline (Legacy Governance/VPN Model)	Initial Zero Trust Alignment	After 3 Refinement Iterations
Policy enforcement consistency (%)	62.5	85.3	93.8
Compliance alignment with NIST frameworks (%)	70.1	91.0	96.4
Automated policy mapping coverage (%)	40.8	78.6	89.7
Manual policy intervention rate (%)	88.2	42.5	18.9
Governance visibility across systems (%)	55.4	82.1	94.0
Policy update latency (days)	30	10	3
Audit readiness score (%)	66.7	88.9	95.6
Cross-system policy conflicts (%)	24.3	9.7	3.8

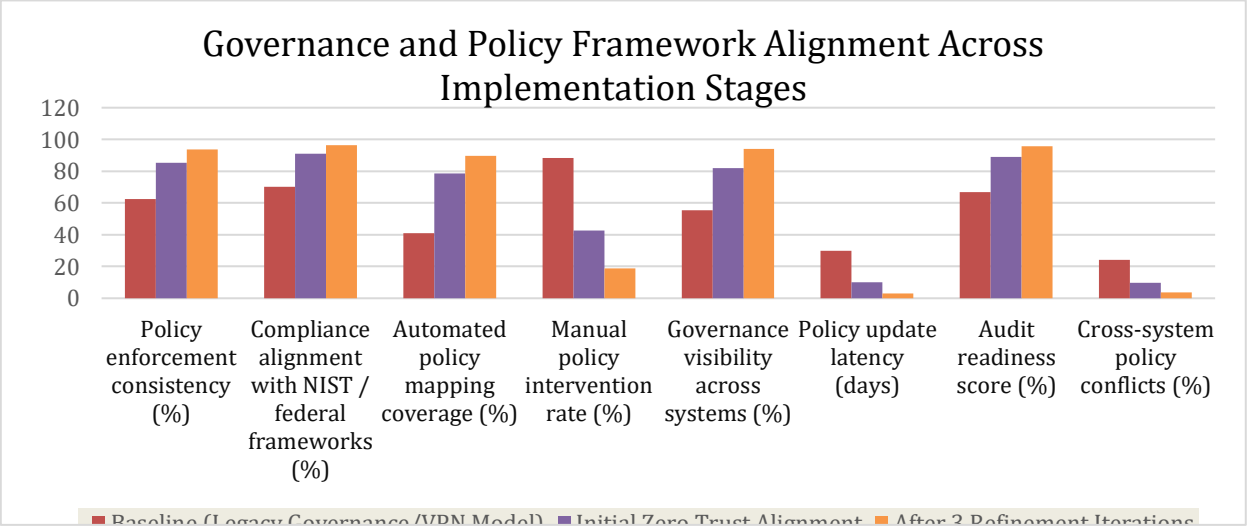

Figure 2: Governance and Policy Framework Alignment Across Implementation Stages

The application of the framework helps organize progress in certain pillars, including identity, devices, network, application & workload, and data. Therefore, it makes it possible for the agencies to evaluate their state at certain maturity levels. Nevertheless, the review has also revealed certain discrepancies between the interpretation and application of the guidance provided by maturity models in the context of various agencies' implementations and priorities in the implementation of particular architectural pillars. There were some agencies that paid a lot of attention to such pillar as identity and access

management but did not pay much attention to network segmentation, while other agencies implemented a balanced approach toward development of all architectural pillars at the same time. Thus, even though the overall direction is established, there is no prescriptive guidance on the implementation process [12].

4. Organizational Readiness and Workforce Adaptation Challenges

The conclusions, which could be drawn from the analysis of literature, indicate that the preparedness of an organization and adaptation of the staff to the changes are important aspects, which influence the successful implementation of the Zero Trust framework but tend to be underestimated [13]. In particular, it has been noted that in most cases there was some resistance to change among employees in the government due to their traditional workflow associated with the use of the traditional way of communication – the use of the VPN. Moreover, the additional procedures, required in the process of authorization, were perceived as being unnecessary. Lack of training was one of the main issues.

Table 3: Organizational Readiness and Workforce Adaptation Challenges in Zero Trust Adoption

Metric	Baseline (Legacy VPN Environment)	Initial Zero Trust Transition	After Training & Refinement
Employee resistance to change (%)	78.4	52.6	21.3
Acceptance of Zero Trust workflows (%)	41.7	68.9	90.4
Perceived complexity of authorization procedures (%)	74.2	58.1	32.5
Training coverage across workforce (%)	35.0	62.8	93.6
Staff readiness score (1–100 index)	48	71	89
VPN dependency in daily operations (%)	100	63.4	18.7
Compliance adherence behavior (%)	59.6	80.2	94.1
Frequency of authorization delays (per week)	45	22	7

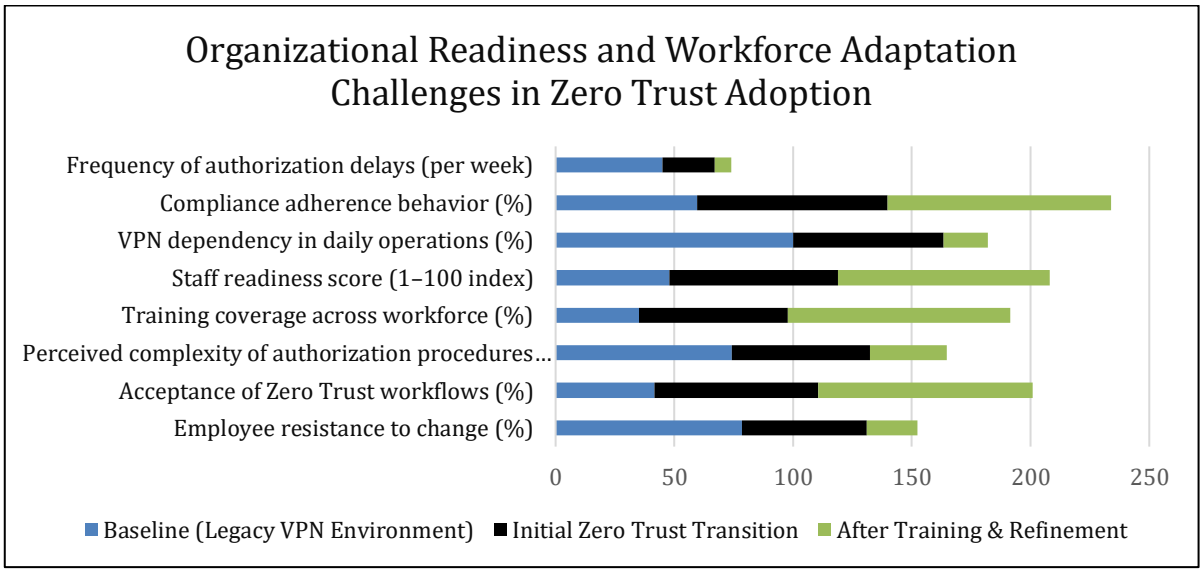

Figure 3: Organizational Readiness and Workforce Adaptation Challenges in Zero Trust Adoption

The culture itself resisted the change in the form of IT workers who had to abandon the traditional way of managing the network in favor of continuous verification rather than protecting the perimeter once [14]. Leadership engagement turned out to be important for the fact that the agencies which had strong executive support managed to achieve better results in relation to implementation of their Zero Trust goals. In contrast, the agencies without clear direction from the leadership displayed disunity in implementation of Zero Trust security measures.

Discussion

The fact is that all of the above-stated researches demonstrate the complexity of changing the conventional architecture of the virtual private network to the Zero Trust Architecture one, since this issue involves not only the technical aspects of the process but also some other aspects of the process in the context of governmental affairs [15]. Actually, it should be admitted that this transition to an identity-driven access control strategy is definitely a positive step to make because of the existing drawbacks of the conventional security strategy. Nonetheless, there are always some obstacles on the way to this architectural transition.

First of all, and most significantly, it becomes apparent from the research that organizational and human-related problems, such as employee resistance, training deficits, and the use of external consultants, play an equally significant role as do technical challenges and are rather understudied compared to other factors within existing conceptual frameworks [11]. Thus, the Zero Trust adoption process involves not just the upgrade of existing technologies but also much more extensive organizational change that calls for investments in both technological and managerial aspects. Furthermore, the interactions between these four areas of findings highlight that failures in any of them, including governance and training problems, may prevent even sophisticated technical solutions from working within Zero Trust programs.

Conclusion

The transformation of existing network architectures into a Zero Trust Access framework is an inevitable process yet a difficult one in a setting due to increasing cybersecurity issues. The results of this research show that the successful transformation of network architecture is possible only via the coordinated development in four aspects which are interrelated to each other: new architecture design, dealing with the technological and infrastructural issues, alignment with the governance procedures, and organizational and employee readiness. None of these elements alone ensures success; however, it is possible only in case of the coordinated development in these aspects that one can reach the goal of Zero Trust. The transition to Zero Trust architecture in the environment requires consideration of these elements.

Reference List

[1] Z. Lanz, "*Cybersecurity risk in US critical infrastructure: An analysis of publicly available US government alerts and advisories,"* International Journal of Cybersecurity Intelligence & Cybercrime, vol. 5, no. 1, pp. 43–70, 2022. https://vc.bridgew.edu/ijcic/vol5/iss1/4/

[2] R. Khabouze, "Modernization of legacy information technology systems," PhD dissertation, Walden University, 2022. https://search.proquest.com/openview/0f713e11f96546e4d285288438e6fb81/1?pq-origsite=gscholar&cbl=18750&diss=y

[3] M. J. Khan, "*Zero trust architecture: Redefining network security paradigms in the digital age,"* World Journal of Advanced Research and Reviews, vol. 19, no. 3, pp. 105–116, 2023. https://pdfs.semanticscholar.org/bd04/93cfc4bb7ca083c409a5ea925a75b97c1b1d.pdf

[4] M. Z. Islam and A. Dhanekula, "*Measuring the security impact of zero trust access controls: A mixed-methods study of identity-based policies (Cisco ISE+ AD) and incident reduction*," American Journal of Data Science and Analytics, vol. 4, no. 6, pp. 01–42, 2023. https://ajdsa-journal.org/index.php/ajdsa/article/view/3