International Journal on Perceptive and Cognitive Computing (IJPCC) Vol 11, Issue 1 (2025)
https://doi.org/10.31436/ijpcc.v11i1.494

A Comprehensive Review of Zero Trust Network Architecture (ZTNA) and Deployment Frameworks

Zainab Senan Mahmod Attar Bashi[1]*, Shayma Senan[2]

[1]Department of Computer Science, International Islamic University Malaysia, Gombak, Malaysia.
[2]Electrical and Computer Engineering Department, International Islamic University Malaysia, Gombak, Malaysia.

*Corresponding author Zainab_senan@iium.edu.my
(Received: 30th July 2024; Accepted: 7th December, 2024; Published on-line: 30th January, 2025)

Abstract— – The zero trust (ZT) approach has initiated significant advancements in network security, addressing the limitations of traditional security models. Traditional network security approaches have faced challenges adapting to modern trends such as bring your own device (BYOD) and cloud computing, resulting in increased complexity in meeting new security requirements. The zero trust security model operates on the principle that no entity within the network, whether internal or external, is inherently trusted. Therefore, all users and devices must undergo strict authentication and authorization processes prior to accessing organizational resources. This review paper provides a comprehensive analysis of zero trust network architecture (ZTNA) and outlines a general deployment framework model, highlighting the critical role of zero trust in modern network security.

Keywords— Zero Trust, Network Security, Identity and Access Management.

I. Introduction

Zero Trust, a groundbreaking network security strategy introduced by [1], represents a shift from the conventional "trust but verify" approach to a more determined "never trust, always verify" approach. This paradigm challenges the traditional belief that devices inside the network are inherently trustworthy while those outsides are suspicious. In the Zero Trust model, every user and device, regardless of their location or prior access history, is treated with skepticism until their identity and authorization are thoroughly verified. This departure from the historical perimeter-based security concept is especially related in the contemporary landscape of remote work and cloud computing, where the traditional network perimeter has become increasingly vulnerable. Zero Trust stands as a robust response to this evolution, emphasizing the continuous connectivity and access, limiting the potential security breaches, and acknowledging that the threat landscape demands continuous monitoring.

Prior to the emergence of the Zero Trust security model, companies typically granted network access exclusively to users deemed inherently trustworthy. The assumption was that internal employees and collaborators were inherently reliable. However, the rapid development of the internet, cloud computing, and the Internet of Things (IoT) has necessitated the integration of different technologies and systems within organizational operations, consequently making data more accessible to both internal and external actors. This shift has increased vulnerabilities, leading to a higher risk of data breaches and cyber-attacks.

In response to these challenges, the Zero Trust security model was proposed to mitigate the risks associated with implicit trust. The model requests that all users, devices, and systems must authenticate and authorize their identities before accessing network resources.

In 2018, the Zero Trust model by introducing the Zero Trust eXtended (ZTX) framework was introduced [2], which encompasses seven core pillars: workforce security, device security, workload security, network security, data security, visibility and analytics, and automation and orchestration as shown in table (1). These pillars assist organizations in constructing a security architecture that denys implicit trust in favor of continuous authentication and authorization of identities, devices, and network activities.

TABLE I
SUMMARY OF THE PILLARS OF ZERO TRUST EXTENDED (ZTX) FRAMEWORK [2]

Zero Trust Pillar	**Actions**
Users	- Flag excessive access - Limit and enforce data access - Alert on abnormal behavior - Assign data owners based on activity
Devices	- Assess device trustworthiness - Pair users to devices for detecting suspicious behavior
Network	- Fix misconfigurations - Analyze VPN, DNS, and web activity - Report on network threats
Applications	- Monitor and manage application access

https://doi.org/10.31436/ijpcc.v11i1.494

	- Track and alert on configuration changes - Alert on access from unsanctioned locations
Automation	- Classify sensitive data - Detect threats - Remediate overexposed files - Enforce privacy policies
Analytics	- Monitor and analyze events - Perform risk assessments - Run data classification scans - Maintain an audit trail

The same year, Google advanced the practical implementation of Zero Trust by developing its own Zero Trust architecture. This framework is defined as a set of concepts and ideas designed to minimize uncertainty in enforcing accurate, on-demand access decisions within network-facing information systems and services. The Zero Trust Architecture (ZTA) serves as an enterprise cybersecurity blueprint that integrates Zero Trust principles into component relationships, workflow planning, and access policies. Full implementation of a Zero Trust Architecture solution involves three key elements: enhanced identity governance and policy-based access control, micro-segmentation, and software-defined perimeter and overlay networks. These elements collectively ensure a comprehensive and resilient security posture, capable of addressing the dynamic threats faced by modern organizations. Figure (2) shows the logical components of Zero Trust Architecture (ZTA).

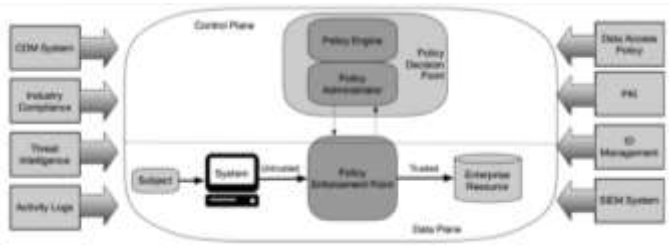

Fig 1. Logical Components of Zero Trust Architecture [3]

This paper is organized into several key sections. The following section highlights related works and presents a detailed examination of traditional network security models, highlighting their limitations and the need for a paradigm shift. Subsequently, the core principles and components of Zero Trust Network Architecture (ZTNA) are discussed, including authentication mechanisms, micro-segmentation, and policy enforcement points. The paper then explores some case studies and real-world implementations, showcasing the impact of Zero Trust in various organizational settings. Finally, the review concludes with a discussion on the future directions of Zero Trust, emphasizing ongoing research, emerging trends, and potential challenges in widespread adoption.

II. Related Works

The field of network security has seen significant advancements over the years, with traditional security models evolving to address emerging threats and challenges. However, these traditional approaches have faced limitations in coping with the dynamic and complex nature of modern network environments. This section explores various traditional security models, highlighting their key features, limitations, and the challenges they encounter in today's context.

Perimeter-Based Security has long been a foundational approach in network defense. This model focuses on protecting the network boundary using firewalls and intrusion detection systems (IDS) [4]. The underlying assumption is that internal network traffic can be trusted, while external traffic is potentially harmful. While effective in its early days, perimeter-based security struggles to address insider threats and manage the complexities introduced by Bring Your Own Device (BYOD) policies and remote access. Additionally, it offers limited protection against advanced persistent threats (APTs) [5], which can intrude into the network.

Virtual Private Networks (VPNs) are another traditional method aimed at securing data transmitted over public networks and providing secure remote access [6]. VPNs encrypt data, ensuring its confidentiality and integrity. However, this approach can introduce performance issues due to encryption overhead, and managing VPNs at scale can be complex and challenging. Furthermore, if endpoints are compromised, VPNs become vulnerable, undermining the security they are meant to provide.

Endpoint Security focuses on securing individual devices using antivirus software, firewalls, and endpoint detection and response (EDR) systems [7]. While this method is essential for protecting devices, its scope is limited to the endpoints themselves and does not encompass the entire network. This high dependency on user behavior makes it ineffective against zero-day threats [8] and sophisticated attacks that can bypass endpoint defenses.

Network Access Control (NAC) [9] solutions aim to control access to network resources based on device compliance and user credentials, providing visibility and control over devices on the network. Despite these advantages, NAC implementation and management can be complex and may not scale well with the increasing number of devices. Additionally, NAC systems can struggle to effectively counter sophisticated attacks that exploit network vulnerabilities.

Signature-Based Detection [10] involves using known signatures of malware and threats to detect and prevent attacks. Common tools in this category include antivirus software and IDS. However, signature-based approaches

https://doi.org/10.31436/ijpcc.v11i1.494

are inherently limited in their ability to detect new, unknown threats, and they often require constant updates to maintain their effectiveness. High false positive rates and the need for regular updates to signature databases further complicate their use.

Behavior-Based Detection [11] shifts the focus to monitoring network and user behavior to identify anomalies and potential threats. Using machine learning and analytics, this method offers a more dynamic defense mechanism. Nonetheless, it is resource-intensive, complex to manage, and can produce false positives. Effective deployment of behavior-based detection requires advanced expertise to interpret results and manage the systems.

Role-Based Access Control (RBAC) [12] grants access to resources based on users' roles within an organization, simplifying permission management. However, RBAC can become complex in large organizations with dynamic access needs. The static nature of roles may not adapt well to evolving threats, making it challenging to maintain an up-to-date and effective access control framework.

Security Information and Event Management (SIEM) [13] systems collect and analyze security data from various sources, offering real-time monitoring and incident response capabilities. While SIEM provides comprehensive security visibility, it comes with high costs and complexity. Effective use of SIEM systems requires skilled personnel, and there is a risk of data overload and false positives, which can hinder efficient threat detection and response. Table (2) summarizes these traditional security approaches, their key features, and their limitations.

TABLE III
SUMMARY OF RELATED WORKS

Security Model	**Key Features**	**Limitations**
Perimeter-Based Security	- Focuses on protecting the network boundary with firewalls and intrusion detection systems (IDS). - Assumes all internal network traffic is trusted.	- Ineffective against insider threats. - Difficulty in managing BYOD and remote access. - Limited protection against advanced persistent threats (APTs).
VPN (Virtual Private Network)	- Encrypts data transmitted over public networks. - Provides secure remote access.	- Performance issues due to encryption overhead. - Complex management and scalability challenges. - Vulnerable to attacks if endpoints are compromised.
Endpoint Security	- Focuses on securing individual devices using antivirus software, firewalls, and endpoint detection and response (EDR).	- Limited scope, does not protect the entire network. - High dependency on user behavior. - Ineffective against zero-day threats and sophisticated attacks.
Network Access Control (NAC)	- Controls access to network resources based on device compliance and user credentials. - Provides visibility and control over devices on the network.	- Complex implementation and management. - Scalability issues with increasing number of devices. - Limited effectiveness against sophisticated attacks.
Signature-Based Detection	- Uses known signatures of malware and threats to detect and prevent attacks. - Includes antivirus and intrusion detection systems (IDS).	- Ineffective against new, unknown threats. - High false positive rates. - Requires constant updates to signature databases.
Behavior-Based Detection	- Monitors network and user behavior to detect anomalies and potential threats. - Utilizes machine learning and analytics.	- High complexity and resource-intensive. - May produce false positives. - Requires advanced expertise to manage and interpret results.
Role-Based Access Control (RBAC)	- Grants access to resources based on user roles within the organization. - Simplifies management of permissions and access control.	- Can become complex with large organizations. - Difficult to manage dynamic access needs. - Static roles may not adapt well to changing threats.
Security Information and Event Management (SIEM)	- Collects and analyzes security data from various sources. - Provides real-time monitoring and incident response.	- High cost and complexity. - Requires skilled personnel for effective use. - Potential for data overload and false positives.

III. DEPLOYMENT FRAMEWORKS FOR ZTNA

The deployment of Zero Trust Network Architecture (ZTNA) requires a systematic and comprehensive framework to ensure its effective implementation and operation. The following subsections detail the key

https://doi.org/10.31436/ijpcc.v11i1.494

components and methodologies involved in deploying ZTNA, focusing on main steps, tools, and best practices.

A. Defining the Zero Trust Security Policy

The first step in deploying ZTNA involves defining a robust security policy that aligns with the Zero Trust principles of "never trust, always verify." This policy should encompass the following elements:

- *Identity Verification:* Establishing strict identity verification processes for users, devices, and applications. This includes multi-factor authentication (MFA) and continuous monitoring of identity attributes.

- *Access Control:* Implementing access control policies that grant the least privilege necessary for users and devices to perform their tasks. Role-based access control (RBAC) and attribute-based access control (ABAC) can be utilized to enforce these policies.

- *Data Protection:* Ensuring that sensitive data is encrypted both in transit and at rest. Data loss prevention (DLP) tools should be deployed to monitor and control data access and movement.

B. Network Segmentation

Network segmentation is a critical component of ZTNA, aimed at limiting the potential threats within the network. This involves dividing the network into smaller, isolated segments, each with its own security controls. Key practices include:

- *Micro-Segmentation:* Using software-defined networking (SDN) and network virtualization techniques to create isolated segments. This limits access to resources based on predefined policies and real-time context.

- *Firewalls and Gateways:* Deploying next-generation firewalls (NGFW) and secure web gateways (SWG) to monitor and control traffic between segments. These tools help enforce security policies and detect anomalous behavior.

C. Continuous Monitoring and Analytics

ZTNA relies heavily on continuous monitoring and real-time analytics to detect and respond to security incidents promptly. This involves:

- *Security Information and Event Management (SIEM):* Implementing SIEM systems to collect, analyze, and correlate security events from various sources. SIEM provides real-time visibility into network activities and helps identify potential threats.

- *User and Entity Behavior Analytics (UEBA):* Using UEBA to monitor user and device behavior, detect anomalies, and identify malicious activities. Machine learning algorithms can be used to analyze behavior patterns and generate alerts for suspicious actions.

- *Endpoint Detection and Response (EDR):* Deploying EDR solutions to continuously monitor endpoints for signs of compromise and to enable rapid incident response. EDR tools provide detailed visibility into endpoint activities and facilitate threat hunting.

D. Secure Access Service Edge (SASE)

Secure Access Service Edge (SASE) is an emerging framework that integrates networking and security services into a single cloud-delivered solution [14]. SASE provides a scalable and flexible approach to implementing ZTNA by combining the following components:

- *SD-WAN:* Software-defined wide area networking (SD-WAN) optimizes network performance and ensures secure connectivity for remote users and branch offices. SD-WAN enables dynamic traffic routing based on application requirements and security policies.

- *Cloud Access Security Broker (CASB):* CASBs provide visibility and control over cloud applications and data. They enforce security policies, protect against data breaches, and ensure compliance with regulatory requirements [15].

E. Automation and Orchestration

Automation and orchestration play a crucial role in the effective deployment and management of ZTNA. Key strategies include:

- *Policy Automation:* Automating the creation, enforcement, and updating of security policies based on predefined criteria and real-time context. This reduces the risk of human error and ensures consistent policy application.

- *Incident Response Automation:* Using automated workflows to respond to security incidents promptly. This includes automated threat detection, containment, and remediation processes.

- *Orchestration Tools:* Deploying orchestration tools to integrate and manage security solutions across the network. These tools provide a unified interface for configuring, monitoring, and controlling security policies and operations.

Table 3 is summarizing the key components of the ZTNA implementation framework:

TABLE IIIII
KEY COMPONENTS OF THE ZTNA IMPLEMENTATION FRAMEWORK

Component	Key Actions
Identity Verification	Implement MFA, continuous monitoring of identity attributes.
Access Control	Use RBAC/ABAC, enforce least privilege access.
Data Protection	Encrypt data in transit and at rest, deploy DLP tools.
Micro-Segmentation	Utilize SDN, network virtualization for granular segmentation.

https://doi.org/10.31436/ijpcc.v11i1.494

Firewalls and Gateways	Deploy NGFW and SWG to monitor and control inter-segment traffic.
SIEM	Implement SIEM for real-time security event analysis.
UEBA	Use machine learning for behavior analytics and anomaly detection.
EDR	Deploy EDR solutions for continuous endpoint monitoring and incident response.
SD-WAN	Use SD-WAN for optimized, secure remote connectivity.
CASB	Deploy CASB for cloud application visibility and control.
ZTNA Solutions	Implement ZTNA solutions for secure, identity-based access.
Policy Automation	Automate policy creation, enforcement, and updates.
Incident Response	Use automated workflows for threat detection and remediation.
Orchestration Tools	Deploy orchestration tools for unified security management.
Training and Awareness	Conduct regular security training and simulations.

IV. AUTHENTICATION AND AUTHORIZATION IN ZTNA

Identity and Access Management (IAM) plays an importnt role in the Zero Trust Network Architecture (ZTNA) by ensuring that only authorized users and devices gain access to critical resources. The IAM framework encompasses policies, processes, and technologies that facilitate the management of digital identities, enforce access controls, and monitor user activities. This section presents the key aspects of IAM in the context of ZTNA, focusing on Multi-Factor Authentication (MFA) and Continuous Authentication and Monitoring.

A. Multi-Factor Authentication (MFA)

Multi-Factor Authentication (MFA) is a security mechanism that requires users to provide multiple forms of verification before granting access to a system. Unlike traditional single-factor authentication, which relies solely on a password, MFA combines two or more independent credentials: something the user knows (password), something the user has (smartphone or hardware token), and something the user is (biometric verification). This layered approach significantly enhances security by making it more challenging for attackers to gain unauthorized access.

By requiring multiple forms of verification, MFA reduces the risk of credential theft and unauthorized access. Even if one factor is compromised, the attacker would still need to bypass additional security layers. Modern MFA solutions often incorporate user-friendly methods such as push notifications and biometric authentication, minimizing friction for legitimate users while enhancing security.

To implement MFA effectively, organizations should adopt a risk-based approach, ensuring that MFA is applied consistently across all access points without hindering user productivity. This involves integrating MFA with Single Sign-On (SSO) solutions, using adaptive authentication that adjusts the level of verification based on the context (e.g., location, device, behavior), and ensuring that MFA is part of a broader IAM strategy that aligns with the organization's security objectives.

B. Continuous Authentication and Monitoring

In the Zero Trust paradigm, the assumption that no user or device should be implicitly trusted necessitates continuous authentication and monitoring. Continuous authentication goes beyond the initial login, regularly verifying the user's identity throughout their session based on contextual and behavioral data. This approach ensures that access remains secure even if the user's credentials are compromised after initial authentication.

That can be done by evaluating contextual factors such as the user's location, device, and network to determine the legitimacy of the access request. Monitoring user behavior, such as typing patterns, mouse movements, and interaction habits, can also be used to detect anomalies that may indicate compromised credentials. Another key component is to continuously assessing the risk associated with each access request and adjusting authentication requirements accordingly.

Effective implementation of continuous authentication involves integrating advanced analytics and machine learning algorithms to analyze user behavior and detect anomalies. Organizations should use Identity and Access Management (IAM) solutions that support adaptive authentication, enabling dynamic responses to potential threats. Additionally, establishing clear policies and procedures for incident response and user verification is crucial to ensure that continuous authentication operates smoothly and effectively.

V. CONCLUSION

This article presented a significant discussion of the details about the zero trust security model along with their background and implementation of this model. Zero trust is essentially an initiative from a cybersecurity plan to provide more secure networking and safeguarding resources such as assets, workflow planning, and services. By adopting the zero trust model, organizations can improve their security posture and fortify themselves against cyber threats. The foundation of zero trust is changing to a dynamic, identity-centric, and policy-based approach that makes it reliable to cope with the complexity of enterprise environments.

Therefore, optimize the technology and security architecture for future adaptability.

ACKNOWLEDGMENT

The authors hereby acknowledge the review support offered by the IJPCC reviewers who took their time to study the manuscript and find it acceptable for publishing.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest

REFERENCES

[1] J. Kindervag, "No More Chewy Centers: Introducing The Zero Trust Model of Information Security," Forrester Research, USA, Sep. 14, 2010. [Online]. Available: https://media.paloaltonetworks.com/documents/Forrester-No-More-Chewy-Centers.pdf

[2] C. Cunningham, "The Zero Trust eXtended (ZTX) Ecosystem, Strategic Plan: The Zero Trust Security Playbook," Forrester Research, Jul. 11, 2019.

[3] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, Zero Trust Architecture, NIST Special Publication 800-207, 2020

[4] Z. Sun, D. Huang, S. Li, H. Yang, and C. Zhao, "High Efficiency Positioning of Vibration Intrusions for Long Distance Perimeter Security Monitoring Based on Time-Frequency Variation Envelopes," IEEE Transactions on Instrumentation and Measurement, vol. PP, pp. 1–1, 2024, doi: 10.1109/TIM.2023.3348889.

[5] N. Wagh and Y. Jadhav, "Eclipsing Security: An In-Depth Analysis of Advanced Persistent Threats," International Journal of Scientific Research in Engineering and Management, vol. 7, pp. 1–11, 2023, doi: 10.55041/IJSREM27653.

[6] B. Mixon-Baca, J. Knockel, D. Xue, T. Ayyagari, D. Kapur, R. Ensafi, and J. Crandall, "Attacking Connection Tracking Frameworks as Used by Virtual Private Networks," Proceedings on Privacy Enhancing Technologies, vol. 2024, pp. 109–126, 2024, doi: 10.56553/popets-2024-0070.

[7] S.-J. Lee, S.-E. Jeon, and I.-G. Lee, "A machine learning-enhanced endpoint detection and response framework for fast and proactive defense against advanced cyber attacks," Soft Computing, pp. 1–15, 2024, doi: 10.1007/s00500-024-09727-7.

[8] M. Wa Nkongolo and M. Tokmak, "Zero-Day Threats Detection for Critical Infrastructures," arXiv preprint, 2023. doi: 10.48550/arXiv.2306.06366.

[9] M. Xu, B. Chen, Z. Tan, S. Chen, L. Wang, Y. Liu, T. San, S. Fong, W. Wang, and J. Feng, "AHAC: Advanced Network-Hiding Access Control Framework," Applied Sciences, vol. 14, no. 5593, 2024, doi: 10.3390/app14135593.

[10] M. Schroetter, A. Niemann, and B. Schnor, "A Comparison of Neural-Network-Based Intrusion Detection against Signature-Based Detection in IoT Networks," Information, vol. 15, no. 164, 2024, doi: 10.3390/info15030164.

[11] A. Badea, V. Croitoru, and D. Gheorghica, "Computer networks security based on the detection of user's behavior," in Proceedings of the International Symposium on Advanced Topics in Electrical Engineering (ATEE), 2015, pp. 55–60, doi: 10.1109/ATEE.2015.7133679.

[12] S. Ramakrishnan, "Revolutionizing Role-Based Access Control: The Impact of AI and Machine Learning in Identity and Access Management," Journal of Artificial Intelligence & Cloud Computing, vol. 2, pp. 1–7, 2023, doi: 10.47363/JAICC/2023(2)236.

[13] M. Jhaveri and V. Parmar, "CLOUD Security Information and Event Management," GIS-Zeitschrift fü Geoinformatik, vol. 10, pp. 13, 2023.

[14] A. Ragula, "Emerging Trends in Cloud Security: Zero Trust and SASE," International Journal for Research in Applied Science and Engineering Technology, vol. 12, pp. 10–17, 2024, doi: 10.22214/ijraset.2024.62457.

[15] P. Selvam, "Secure Cloud Services by Integrating CASB Based Approach," International Journal of Scientific Research in Engineering and Management, vol. 4, 2022, doi: 10.55041/IJSREM15210.