Article

Zero Trust VPN (ZT-VPN): A Cybersecurity Framework for Modern Enterprises to Enhance IT Security and Privacy in Remote Work Environments

Syed Muhammad Zohaib , Syed Muhammad Sajjad , Zafar Iqbal , Muhammad Yousaf , Muhammad Haseeb , Zia Muhammad *

Posted Date: 4 October 2024

doi: 10.20944/preprints202410.0301.v1

Keywords: Zero Trust VPN; Zero Trust Network Access (ZTNA); Enterprise Security Framework; Zero Trust Architecture; Latency and Throughput in VPNs; Secure Remote Access; Zero Trust Security Model; Enterprise VPN Solutions; ZT and VPN Integration

Article

Zero Trust VPN (ZTVPN): A Cybersecurity Framework for Modern Enterprises to Enhance IT Security and Privacy in Remote Work Environments

Syed Muhammad Zohaib [1], Syed Muhammad Sajjad [2], Zafar Iqbal [3], Muhammad Yousaf [4], Muhammad Haseeb [5] and Zia Muhammad [6,7,*]

[1] Department of Cyber Security, Air University, Islamabad, Pakistan
[2] Department of Computer Science and Cyber Security, Air University, Kharian, Pakistan
[3] Department of Cyber Security, National University of Computer & Emerging Sciences, Islamabad, Pakistan
[4] Director National Cert, Islamabad, Pakistan
[5] Department of Computer Science, University of North Dakota, Grand Forks, ND 58202, USA
[6] Department of Computer Science, North Dakota State University, Fargo, ND 58102, USA
[7] Department of Computer Science and Technology, University of Jamestown, ND 58405, USA
* Correspondence: zia.muhammad@ndsu.edu

Abstract: Modern organizations have migrated from localized physical offices to work-from-home environments. This surge in remote work culture has exponentially increased the demand and usage of Virtual Private Network (VPN), which permits remote employees to access corporate offices effectively. However, the technology raise concerns including security threats, latency, throughput, and scalability, among others. These Newer generation threats are more complex and frequent, which makes the legacy approach to security ineffective. The research paper gives an overview of contemporary technologies used across enterprises including VPN and Zero Trust Network Access (ZTNA), Proxy Servers, Secure Shell (SSH) Tunnels, Software-defined wide area network (SD-WAN), and Secure Access Service Edge (SASE). This paper also presents a comprehensive cybersecurity framework named Zero Trust VPN (ZTVPN), which is a VPN solution based on Zero Trust principles. The proposed framework is aimed to enhance IT security and privacy for modern enterprises in remote work environments and addresses concerns of latency, throughput, scalability, and security. Finally, the paper demonstrates the effectiveness of the proposed framework in various enterprise scenarios, highlighting its ability to prevent data leaks, manage access permissions, and provide seamless security transitions. The findings underscore the importance of adopting ZTVPN to fortify cybersecurity frameworks, offering an effective protection tool against contemporary cyber threats. This research serves as a valuable reference for organizations aiming to enhance their security posture in an increasingly hostile threat landscape.

Keywords: zero trust VPN; zero trust network access (ZTNA); enterprise security framework; zero trust architecture; latency and throughput in VPNs; secure remote access; zero trust security model; enterprise VPN solutions; ZT and VPN integration

1. Introduction

Network infrastructures serve as the backbone of communication and information exchange. They facilitate the seamless flow of data, enabling organizations and individuals to access resources, collaborate, and conduct business efficiently [1,2]. However, the increasing reliance on networks has also attracted malicious actors who seek to exploit vulnerabilities and disrupt operations for various purposes, ranging from financial gain to espionage or activism [3]. As a result, understanding network attacks and developing effective defense mechanisms has become paramount in maintaining the security and integrity of network infrastructures [4].

Even with advancements in technology, there are many scams targeting businesses, for example, phishing remains the most common form of cyber-attack, accounting for 90% of data breaches [5]. In 2023, 343,338,964 people were the targets of 2,365 cyberattacks. Data breaches increased by 72% in 2023 compared to the previous record-holder, 2021 [6,7]. Surprisingly, 96% of these phishing attacks are delivered via email. In 2023, a staggering 72.7% of organizations experienced a ransomware attack [8]. Similarly, another major cyber attack is ransomware [9]. The costs associated with ransomware are expected to climb to USD 265 billion annually by 2031. In 2023, the average cost of a data breach saw a 15% rise over the previous three years, reaching $4.45 million on a worldwide scale [10,11]. Pay-outs were greatest in the US, at $5.09 million per breach [12–14].

Cyber insurance premiums in the US saw a 50% hike in 2022, with premiums collected amounting to USD 7.2 billion [15]. Over 75% of targeted attacks initiate from an email, with 94% of malware being delivered through this channel.C ybercrime costs are on a steep rise, expected to reach USD 10.5 trillion annually by 2025, marking a 15% yearly increase [16,17]. In the past, cybercrime rates increased by 600% during the COVID-19 pandemic, illustrating how dangers have adjusted to new global circumstances [18]. On average, a data breach would cost about $4.45 million. Approximately 35% of malware in 2023 was sent by email, making it the most frequent vector for malware [19,20]. Protecting an organization and understanding the motives behind these attacks is important, it helps in assessing the potential impact on network security and identifying appropriate mitigation strategies [21]. It is also equally important to access the network devices and perform security assessment of IT products [22]. Attacks like Denial of Service (DoS) try to block legitimate users from accessing resources or services on a network by overwhelming them [23,24]. These attacks can sabotage an organization and affect network availability [25].

Nowadays, organizations are relying on remote work technology and using a variety of technologies to access their organizational networks [26]. For example VPN is one of them, that allows for the safe transfer of data and other types of information between remote locations. One or more VPN devices that the user connects to via their web browser make up an SSL VPN [27]. It uses encryption for data transfer and operates at the application layer [28]. Cryptography ensures transport-level secrecy, whereas SSL offers encrypted public keys for key management and authentication [29]. By encrypting data in transit, it protects the connection between the client and the resource. No data is sent over the Internet or internal networks in plain text when end-to-end security is used. Every step, from the customer to the vendor, is encrypted and verified for security [30].

Despite this enormous and ubiquitous usage, VPNs come with various security challanges, and performance-related issues, thereby hindering users from taking maximum advantage of this technology [31,32]. One potential downside of relying only on VPNs is that they treat all users as trustworthy and give them unrestricted access to the network. To address this concern, VPN users must choose the most secure and perfect VPN solution for the smooth functioning of daily activities [33,34]. Similary, the traditional 'castle and moat approach' of security is insufficient in light of the new age and evolving attacks along with the growing trend of the workplace from home [35]. Therefore, VPNs are becoming fundamental in defending today's Network architectures and allowing remote access [36,37].

For a long time, VPNs have been employed to create safe and exclusive communications in the generally accessible network. VPNs compromise encryption and tunneling protocols, therefore forming a more secure Virtual Network overlaying an insecure Network Infrastructure [38,39]. VPN can be used for access privilege, confidential data integrity, and authentication when connecting remote and geographically disjointed networks [40,41]. On the other hand, conventional telecom architecture and, particularly, physically configured and hard-wired networks, accompanied by typical perimeters of protection, have failed to cope with the ever-changing cyber threats.

Nonetheless, the old paradigm of perimetral security has been replaced with the Zero Trust Network Access (ZTNA) due to the dynamics of threat and the necessity of a more accurate and dynamic security model [42,43]. It is a security model that verifies users and devices before granting access to applications or resources. ZTNA is based on the principle of "never trust, always verify" and is designed to reduce the attack surface area and improve security posture [44]. Some assumptions are made by pneumonic; firstly, it narrows down its view in networks and regards each user and device both within and outside the network as hostile and, therefore, has to be and should be authentically and authoritatively authorized by the network each time they want to access the network's products [45–47]. This shift in mentality is important in combating newer and more advanced attacks that use vulnerabilities and lateral movement in the network. The use of both VPNs and ZTNA could provide a robust solution for the remote access problem and the protection of networks [48,49].

The posibiiltiy to murge VPN and ZTNA technology can give promising solution to industrial secuity accorded by end device identity, context, and, most importantly, the principle of least privilege to use the network resources. This integration allows organizations to apply tighter security measures to limit the attack vector and safeguard the data.

Hence, the purpose of this article is to discuss and identify how to use VPNs to establish zero-trust network access. Thus, the goal of familiarising ourselves with the ZTVPNconcepts and principles is to create patterns, standards, and recommendations for organizations that are trying to implement a safe and efficient remote access solution. Furthermore, we will discuss the issues, implications, and possible drawbacks of combining and offering case-study analyses. Taken in its entirety, these two approaches present a clear promise, in terms of conceptual development, of effectively conquering the security vulnerabilities that threaten organizations at present. Hence, this article endeavours offers some insights and real-life best practices for organizations that are aspiring to have strong and fortified network security that incorporates the use of VPNs and ZTNA for the attainment of secure remote access. This article discusses and analyzes various categories of network attacks, their features, and the impact they could have on current networks. We hope that by the end of this research, we will be in a position to add to the body of knowledge on how VPN and ZTNA can complement each other, thus reinforcing network security and offering secure access to remote resources. The key contributions of the research are as follows:

1. The research paper gives an overview of contemporary technologies used across enterprises including VPN and ZTNA, Proxy Servers, Secure Shell (SSH) Tunnels, Software-defined wide area network (SD-WAN), and Secure Access Service Edge (SASE), among others.
2. The paper identifies critical concerns associated with traditional technologies, such as latency, throughput, scalability, and cyber threats, and identifies the gap to overcome these challenges.
3. The paper presents a novel Zero Trust VPN (ZTVPN) framework that integrates zero trust network access with virtual private networks to create a robust cybersecurity framework for remote work environments, aiming to fortify modern enterprises' cybersecurity and privacy.
4. Finally, the paper demonstrates the effectiveness of the ZTVPN framework through various enterprise scenarios, highlighting its ability to prevent data leaks, manage access permissions, and provide seamless security transitions, thereby fortifying cybersecurity frameworks against contemporary cyber threats.

The organization of this paper is structured as follows: The Introduction section (1) provides an overview of the shift to remote work environments and the associated cybersecurity challenges. The Background - Related Work section (2) reviews contemporary technologies and existing research in the field. The Proposed Framework section (3) details the design and architecture of the Zero Trust VPN (ZTVPN) framework, including examples of implementation case studies. The Results and Evaluation section (4) presents the findings from various enterprise scenarios, accompanied by a discussion of the results and acknowledgment of limitations. Finally, the Conclusion and Future Work section (5) summarizes the key contributions of the research and outlines potential directions for future studies.

2. Background - Related Work

The purpose of this Section is to provide a comprehensive review of existing technologies and research relevant to the topic of the paper. This section sets the context for the proposed framework by discussing contemporary technologies It also highlights the limitations and challenges of current approaches, thereby establishing the need for the proposed ZTVPN framework. By reviewing related work, this section helps to position the research within the broader field of cybersecurity and demonstrates how the proposed framework builds upon and advances existing knowledge.

2.1. Virtual Private Network (VPN)

It is a technology that creates a secure and encrypted connection over a less secure network, such as the internet. It allows users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network [50].

VPNs are commonly used by businesses to allow employees to securely access the company's internal network from remote locations. This is particularly useful for remote work, enabling employees to access files, applications, and other resources as if they were in the office. VPNs provide a secure connection, protecting your data from hackers and cybercriminals, especially when using public Wi-Fi networks. The encryption ensures that even if the data is intercepted, it cannot be read [51]. By masking your IP address, a VPN helps protect your online privacy. It prevents websites, advertisers, and even your internet service provider (ISP) from tracking your online activities. VPNs allow you to bypass geographic restrictions and access content that may be blocked in your region. For example, you can access streaming services, websites, and online services that are only available in certain countries.

Figure 1 provides a detailed explanation of how a VPN works. It shows that, on a border level, when a person connects to a VPN, it encrypts your internet traffic. This means that the data you send and receive is converted into a secure code that is difficult for unauthorized parties to decipher. This encryption ensures that sensitive information, such as passwords and personal data, is protected from eavesdropping. The internet traffic is routed through a VPN server.

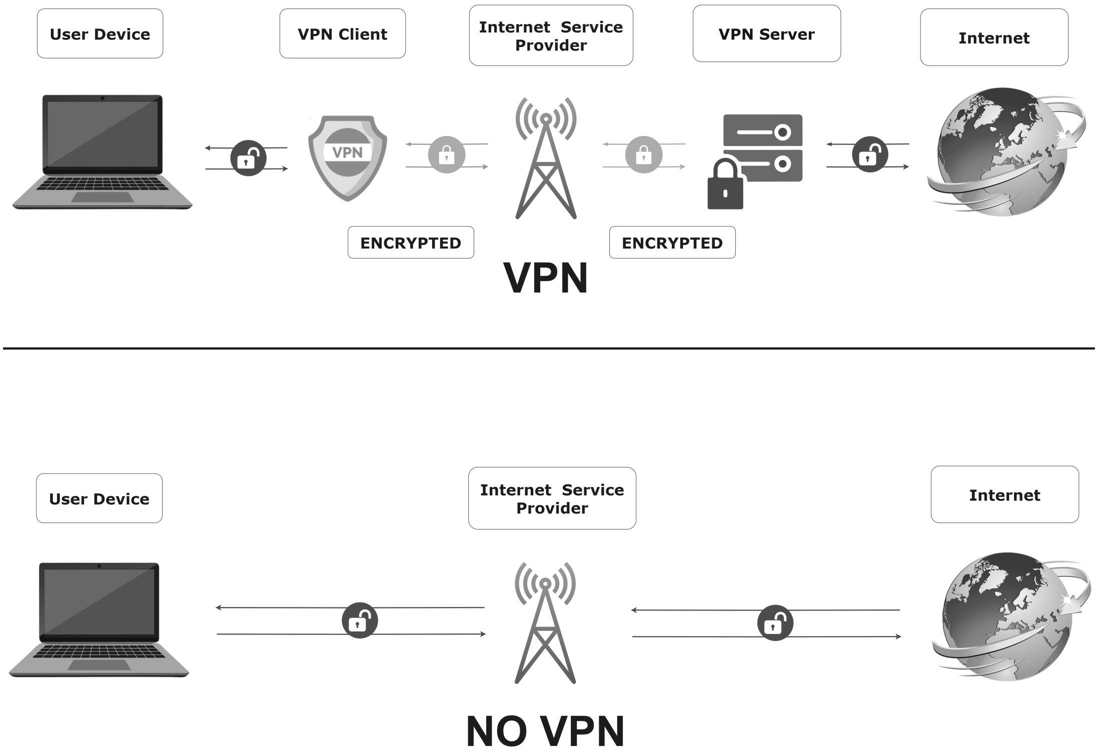

Figure 1. Visual representation of how how a VPN works. The image show how the status of traffic with and without VPN usage.

This server acts as an intermediary between your device and the internet. When a person accesses a website or online service, your request is first sent to the VPN server, which then forwards it to the destination. The response from the website is sent back to the VPN server, which then forwards it to your device. Importantly, By routing the traffic through a VPN server, your real IP address is hidden, and this appears to be accessing the internet from the location of the VPN server. This helps protect to identity and location, providing a layer of anonymity.

doi:10.20944/preprints202410.0301.v1

2.2. Zero Trust Network Access (ZTNA)

Zero Trust Network Access (ZTNA) is a security framework that operates on the principle of "never trust, always verify." Unlike traditional security models that assume everything inside an organization's network can be trusted, ZTNA assumes that threats can exist both inside and outside the network [52]. Therefore, it requires strict verification for every user and device attempting to access resources. Figure 2 provides detailed explanation of how a ZTNA works. The figure shows that, it is a security framework that assumes no inherent trust in any user or device seeking access to network resources. It emphasises the verification of user identities, strict access control and continuous monitoring. ZTNA relies on technologies such as multifactor authentication (MFA), identity and access management (IAM), network segmentation and micro-segmentation to enforce security controls [53].

Table 1 provides an overview and differences between VPN and ZTNA. As we can see from table that, ZTNA is well-suited for modern, dynamic environments, including remote work and cloud-based applications. It can easily scale to accommodate growing and changing organizational needs. ZTNA's micro-segmentation and least-privilege access policies help contain potential breaches, preventing attackers from moving laterally within the network and accessing sensitive data [54]. By requiring continuous verification and limiting access based on identity and context, ZTNA significantly reduces the attack surface and improves overall security posture. ZTNA provides detailed insights into user and device activity, allowing organizations to detect and respond to threats more effectively. This visibility also helps in compliance with regulatory requirements.

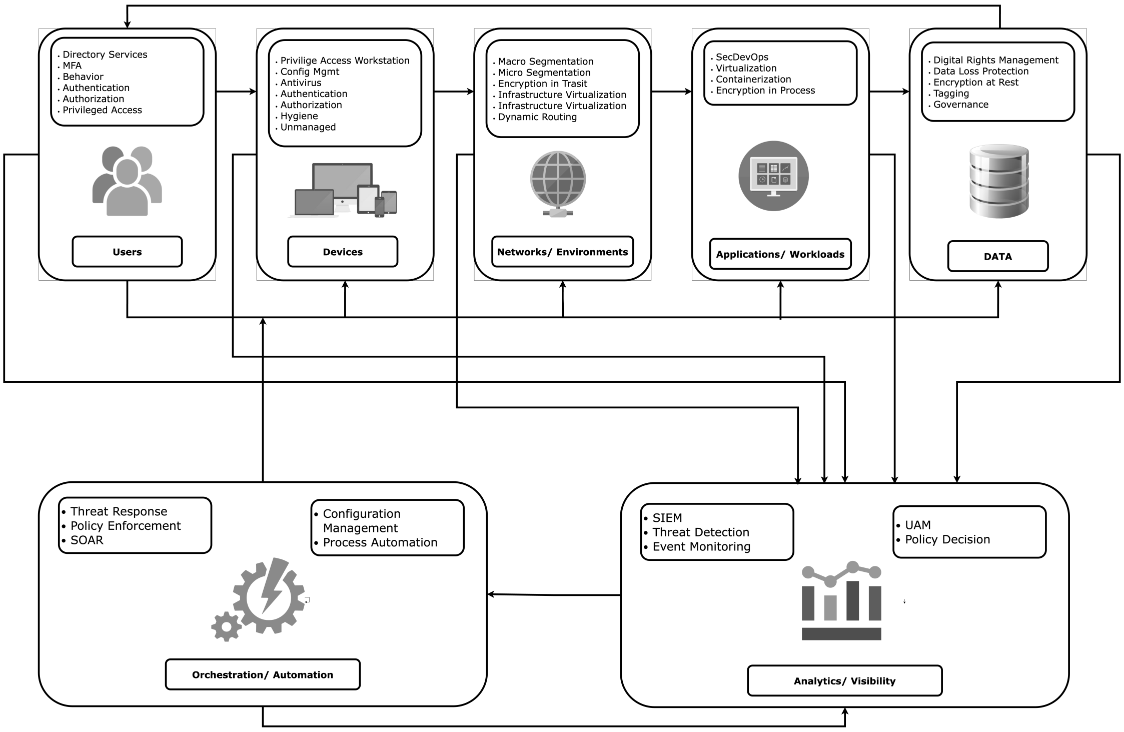

Figure 2. Visual representation of how ZTNA works.

2.3. Proxy Servers

A proxy server is an intermediary server that sits between a client (such as a computer or mobile device) and the internet. It acts as a gateway, handling requests from clients seeking resources from other servers. Proxy servers can provide an additional layer of security by filtering out malicious content and blocking access to harmful websites [55]. They can also protect against certain types of cyberattacks. proxy servers help protect the client's privacy and prevent tracking by websites and advertisers. Proxy servers can bypass geographic restrictions and allow clients to access content that

doi:10.20944/preprints202410.0301.v1

may be blocked in their region [56]. Proxy servers can cache frequently accessed content, reducing the load on the target servers and improving response times for clients. Proxy Servers Work as follows:

1. When a client makes a request for a resource (such as a web page), the request is first sent to the proxy server. The proxy server then forwards the request to the target server on behalf of the client. Once the target server responds, the proxy server sends the response back to the client. This process adds a layer of separation between the client and the target server.
2. Proxy servers can hide the client's IP address by replacing it with their own. This helps protect the client's identity and location, providing a layer of anonymity.
3. Proxy servers can cache frequently requested resources. When a client requests a resource that is already cached, the proxy server can deliver it directly from its cache, reducing the time and bandwidth required to retrieve the resource from the target server.

doi:10.20944/preprints202410.0301.v1

Table 1. Comprehensive Comparison of VPN and ZTNA

Checklist	VPN	ZTNA
Security Features	Creates an encrypted tunnel for data transfer between the user's device and the company's network. However, it may be vulnerable to attacks if misconfigured or if outdated encryption standards are used.	Provides customizable access control settings with a more granular security approach, including micro-segmentation and adaptive trust, which minimizes lateral movement within the network.
Trust Model	Trust is established once when the user connects to the network, after which they have access to all resources.	Employs a zero-trust model, verifying identity and access permissions continuously, ensuring that only authorized users can access specific resources.
Access Security Model	After authentication, users have broad access to the network, potentially increasing the risk if credentials are compromised.	Users can only access specific applications or data as defined by granular policies. Access is determined based on factors such as user identity, device posture, and application sensitivity.
Performance	Can introduce latency as all traffic is routed through a central server, creating a single point of congestion, especially under heavy load. Performance can degrade with increased distance from the server.	Traffic is routed directly to the application or service, reducing latency and avoiding bottlenecks. It also allows local breakout, which improves user experience.
Authent- ication	Typically uses basic methods like username and password. Additional security layers like MFA (Multi-Factor Authentication) are optional and may not be consistently enforced.	Enforces robust authentication methods, including MFA, device identity verification, and contextual factors like geolocation and time of access.
Deployment Complexity	Generally straightforward to deploy, especially for small to medium-sized networks. Requires configuration of VPN servers and client software on user devices.	Deployment can be complex, requiring integration with identity providers, defining granular policies, and ensuring compatibility with existing applications and network infrastructure.
Scalability	Scalability can be challenging as VPN servers need to handle all traffic, which may require significant infrastructure investment as the user base grows.	Designed for scalability, as it does not route all traffic through a central point. Easily supports a growing user base and can integrate with cloud services seamlessly.
Use Cases	Suitable for remote access to internal resources, secure communication over public networks, and when centralized control over network traffic is needed.	Ideal for secure access to cloud applications, enforcing least privilege principles, and protecting against insider threats by restricting lateral movement.

2.4. Secure Shell (SSH) Tunnels

SSH Tunnels, also known as SSH port forwarding, are a method of transporting data over an encrypted SSH connection. This technique allows secure communication between a client and a server, even over an unsecured network [57].

SSH tunneling begins with establishing an SSH connection between a client and an SSH server. This connection is encrypted, ensuring that any data transmitted between the client and the server is secure and protected from eavesdropping. It uses strong encryption algorithms to secure the data transmitted through the tunnel [58]. It also employs authentication mechanisms, such as passwords, public keys, or multi-factor authentication, to verify the identity of the client and the server.

SSH tunnels can be used to bypass firewalls and network restrictions. For example, if a firewall blocks access to a specific service, an SSH tunnel can be used to route the traffic through an allowed port. SSH tunnels enable secure remote access to services and applications. This is particularly useful for system administrators who need to manage servers and devices from remote locations.

2.5. Software-Defined Wide Area Network (SD-WAN)

A Software-Defined Wide Area Network (SD-WAN) is a virtual WAN architecture that leverages software-defined networking (SDN) technology to manage and optimize the performance of a wide area network (WAN) [59]. It allows enterprises to use a combination of transport services, such as MPLS, LTE, and broadband internet, to securely connect users to applications.

SD-WAN separates the control plane from the data plane. The control plane is responsible for making decisions about where traffic should be sent, while the data plane is responsible for forwarding the traffic [60,61]. This separation allows for centralized management and control of the network. SD-WAN provides a centralized management interface that allows network administrators to configure and manage the entire WAN from a single location. This simplifies network operations and reduces the complexity associated with traditional WAN architectures.

SD-WAN can dynamically select the best path for traffic based on real-time network conditions. It can route traffic over multiple transport links, such as MPLS, LTE, and broadband, to optimize performance and ensure high availability. SD-WAN is application-aware, meaning it can identify and prioritize traffic based on the application. This ensures that critical applications receive the necessary bandwidth and low latency, while less critical applications are given lower priority.SD-WAN includes built-in security features such as encryption, firewall, and intrusion prevention. It can also integrate with existing security solutions to provide end-to-end protection for the network.

2.6. Secure Access Service Edge (SASE)

It is a cloud-based architecture model that combines wide area networking (WAN) and network security services into a single, unified framework. It is designed to securely connect users, systems, endpoints, and remote networks to applications and resources, regardless of their location [62]. Here's a detailed explanation of how SASE works:

1. SASE integrates networking functions, such as Software-Defined Wide Area Network (SD-WAN), with security services, including Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Firewall as a Service (FWaaS), and Zero Trust Network Access (ZTNA). This convergence allows for a more streamlined and efficient approach to managing and securing network traffic [63].
2. SASE is built on a cloud-native architecture, meaning that both the networking and security functions are delivered as cloud services. This allows for greater scalability, flexibility, and ease of deployment compared to traditional on-premises solutions.
3. SASE grants access based on the identity of users and devices, rather than relying on the traditional perimeter-based security model. This ensures that only authenticated and authorized users can access specific applications and resources, enhancing security.
4. SASE solutions are globally distributed, meaning that they have points of presence (PoPs) around the world. This ensures that users can securely access applications and resources with low latency, regardless of their geographic location.

Table 2 provides a comparison of Different Network Security and Access Technologies. We can see that, VPN creates a secure and encrypted connection over the internet, allowing users to access corporate networks remotely. However, traditional VPNs grant broad access to the entire network once authenticated, which can pose security risks. In contrast, ZTNA operates on the principle of "never trust, always verify," continuously verifying every user and device attempting to access resources. ZTNA provides granular access control, granting users access only to specific applications and resources based on their identity and context, thereby reducing the attack surface and enhancing security.

Proxy Servers act as intermediaries between clients and the internet, masking the client's IP address and providing anonymity. They can cache frequently requested content to improve performance but do not offer the same level of encryption and security as VPNs or ZTNA. SSH Tunnels provide secure communication for specific applications by transporting data over an encrypted SSH connection, ensuring data protection even over unsecured networks. SD-WAN optimizes network performance by dynamically selecting the best path for traffic and providing centralized management. Each technology has its unique strengths and use cases, making them suitable for different network and security requirements. VPNs and ZTNA focus on secure remote access, with ZTNA providing more granular control. Proxy servers offer anonymity and content filtering, while SSH tunnels secure specific application communications. SD-WAN enhances network performance and scalability, and SASE provides a comprehensive, cloud-based solution for modern enterprises.

Table 2. Comparison of Different Network Security and Access Technologies

Technology	Security	Trust Model	Performance	Use Case	Scalability
VPN	Encrypted tunnel, risk of broad access	Trust established once	Latency due to centralized routing	Secure remote access to internal resources	Limited scalability due to server capacity
ZTNA	Granular access, continuous verification	Zero-trust, continuous	Direct routing, low latency	Securing cloud and hybrid environments	Highly scalable, supports cloud integration
Proxy Servers	Basic anonymity, web filtering	Basic credentials, no internal security	May introduce latency	Content filtering, anonymity	Scales for web traffic, not for internal security
SSH Tunnels	Strong encryption, secure remote access	Single-session access	Minimal impact	Secure remote management, tunneling	Not scalable for large user bases
SD-WAN	Integrated security options, optimized routing	Secure site-to-site	Dynamic routing, optimized traffic	Connecting branches, performance optimization	Scales for large networks, complex deployment
SASE	Comprehensive security, zero-trust	Zero-trust, granular	Optimized, low latency	Cloud-native, remote workforce security	Highly scalable, complex implementation

2.7. Literature Review

Zero-Trust is a security architecture that safeguards on-premises resources by eradicating unidentified users and uncontrolled devices and restricting any lateral movement [64]. Research work by Cherrueau et al. [65] discusses the potential risks and mitigations, emphasising the importance of secure configuration, encryption and identity-based access controls. The study identifies the challenges of scaling ZTNA VPN solutions and provides recommendations for addressing security concerns.

Research work S et al.'s study [66]," Security issues with Virtual Private Network (VPN) and proxy services: Performance and Usability: Usability and performance are crucial factors when implementing ZTNA and VPN solutions. The study also suggests that bad VPN configuration and execution, rather than, say, inadequate cryptography, are the key issues. Research work Wang et al. [67] evaluate the performance of ZTNA VPN solutions: Considering factors such as latency, throughput and scalability. The study emphasises the need for efficient protocols and optimised configurations to maintain a balance between security and performance. According to Da Silva et al., [68,69], smart home security should include zero trust access control that takes context into account and uses behaviour-based continuous authentication. There is a proposal for a zero-aware smart home system that would regulate access to the smart home system by continually verifying the user's authenticity using zero trust continuous identity verification. Powering it up is edge computing, which gets rid of unreliable service providers and any access. The correctness is not guaranteed, and there has been no testing of the effect of latency and concurrency in a real context.

Research work Hunt et al. [70] propose a ZTNA VPN model. The research highlights the benefits of this integration, such as enhanced visibility and control over network traffic. This states that incoming requests from users or devices should be accepted after authentication. Running both ZTNA and VPN simultaneously may introduce additional latency and performance overhead. This can impact the user experience, particularly for latency-sensitive applications. He et al. [71] conduct research comparing common trust assessment techniques and outlining the benefits and drawbacks of various access control regimes and authentication procedures. The emphasis of this study is also on protocols for network authentication and access control. Syed et al. [29] broadened the design's scope to include software-defined perimeters and micro-segmentation and talked about the difficulties of such an architecture. Research work Data objects, rather than user-accessible paths, are subject to the zero-trust concepts and tenets surveyed by Pittman et al. [72]. Trust computation in a dynamic system like a network is, according to their findings, an issue of categorisation and regression. In their research, Buck et al.[73] used a search model to distinguish between academic material and grey literature while evaluating articles published on ZTNA. Any piece of writing that does not originate from an academic setting, such as a private or commercial enterprise, is considered grey literature.

To some extent, the methods outlined here are comparable to Google's ZTN approach to access control [74,75]. However, the execution of decision continuity, risk management, and policy wording have been vague. NIST [76] provides a vendor-agnostic framework for ZT implementation. It focuses on the continuous verification of user and device identities. Policy enforcement is based on context, such as user identity, device health, and location. Micro-segmentation and least privilege access. Comprehensive and detailed guidance applicable to a wide range of organisations. Encourages continuous monitoring and verification, allowing for flexible implementation.

It may be seen as overly complex due to detailed and broad guidelines. Implementation requires a thorough understanding and careful planning. Forrester Model [77] Popularised by Forrester Research, this model emphasises the need to eliminate trust from the network. Continuous monitoring and validation of all users and devices. Micro-segmentation to limit lateral movement within networks. Data-centric security, ensuring data protection regardless of its location. Strong focus on data protection and reducing attack surfaces. A practical approach that can be adapted to various environments. Significant changes may be required to the existing network and security infrastructure. The broad approach might be challenging for smaller organisations to implement fully. Research work Some of the concepts presented here are similar to Dynfire, an AC policy management framework for ZTN put into practice on a college campus, as described by Vensmer et al. [78]. Problematically, neither risk management nor decision continuity are part of it. A ZTN AC solution for cloud computing, AL-SAFE, is described by Giannoku et al. [79]. However, it is missing policy language, risk management, and decision continuity features.

From Table 3, we can see that Scaling both ZTNA and VPN solutions to accommodate the increased number of users and devices can be effective. Ensuring seamless scalability while maintaining security can be a complex task. In today's computing and mobile device settings, when dynamic characteristics make the idea of a conventional DMZ [80] outdated, this comparatively static approach to security, focused on physical or virtual perimeters, fails. As the new network edge, an implicit trust strategy cannot sufficiently protect the cloud. The idea of protecting information systems [70]. Changes were made to accomplish the required IP security based on a review of the company's policy, the SSL encryption technique and the software utilised in the business. These steps will enable the information system for manufacturing locations to reach appropriate security. Given the context of prior research and the underlying hypotheses, the author delves into the data and their potential interpretation. Conversations on the results and their implications need to have a wide view. It is also possible to emphasise potential avenues for future science. Table

Table 3. Comparison of Models and scholarly contributions.

Criteria	Google BeyondCorp [74,75]	NIST Zero Trust Architecture (SP 800-207) [76]	Forrester Zero Trust Model [77]
Primary Focus	Device and user authentication	Continuous verification and micro-segmentation	Data-centric security and continuous monitoring
Implementation Complexity	High, complex outside of Google ecosystem	High, due to comprehensive guidelines	Moderate, adaptable but requires significant changes
Flexibility	Limited, tailored to Google infrastructure	High, vendor-neutral	Moderate, adaptable to various environments
Device Management	Centralized control, strong device verification	Device posture checks	Focus on endpoint security
User Authentication	Strong emphasis on SSO and MFA	Multi-factor authentication	Continuous identity verification
Network Access	No inherent trust, direct access to applications	Micro-segmentation, network isolation	Micro-segmentation, no trust within network
Data Protection	Focus on securing access to data through identity and device state	Policy-based data protection	Strong emphasis on data protection
Monitoring and Logging	Centralized monitoring, comprehensive logging	Continuous monitoring	Continuous monitoring and incident response
Maturity	High, well-established in large-scale environments	High, comprehensive and widely accepted	High, influential in industry standards
Support and Documentation	Extensive support and documentation from Google	Detailed guidelines and government backing	Extensive industry literature and best practices
Best Suited For	Large enterprises, especially those using Google infrastructure	Government agencies, large enterprises	Enterprises prioritizing data security and adaptable solutions

The manner in which companies work has changed over the last many years. Working remotely and other trends like bring your device (BYOD) [81] are driving the demand for flexible access to company data and apps from devices outside of the company's internal network. This tendency is being exacerbated by the rising number of remote workers and the coronavirus epidemic. Additionally, problems arise for the organisation's network architecture due to external connections, such as the incorporation of partners and service providers or the mutual sharing of assets. So far, the majority of companies have provided external users or services with encrypted connections to their internal networks so that they may access internal resources. When a user or service is considered trustworthy, they are granted access to the network's resources. The problem is that most existing solutions rely on inflexible components like subnetworks, firewalls, and rule sets, making it impossible to adapt to these kinds of ever-changing conditions. Because of this design, there are major security holes. One issue is that the internal network is not segmented or controlled. Once an outsider or malevolent employee breaches an organisation's network defence, they may access almost every part of the system. A large number of organisational resources are, therefore, vulnerable to reading, modification and harm.

According to zero-trust techniques, which aim to fix the problems with existing networking solutions, the fundamental premise is that no one on the network can be trusted and that any access to company resources might be a security risk. This means that all accesses are checked and confirmed.

The approval of a request is contingent upon its verification. Either complete access to the service or access to just the allowed operations or data may be provided. When verifying a user's identity, it's important to take into account not only their password but also their device, location, time and access rights. In addition, resource access is limited to what is necessary for carrying out tasks in accordance with the concept of least privilege. This highlights the need to establish and rigorously follow access rules. The access regulations in question, however, are dynamic. It is possible to include the behaviour patterns of the network participants in the verification process by continuously monitoring and recording network traffic. Zero-trust is more of a strategy than a technology; it is an umbrella term for a set of guiding principles. his article discusses and analyzes various categories of network attacks, their features, and the impact they could have on current networks. We hope that by the end of this research, we will be in a position to add to the body of knowledge on how VPN and ZTNA can complement each other, thus reinforcing network security and offering secure access to remote resources. The key contributions of the research are as follows:

3. Proposed Framework - Design and Architecture

The detailed architecture of the Zero Trust VPN (ZTVPN) is illustrated in the provided diagram, comprising three main modules: Policy Enforcement Point (PEP), Identity Enforcement Point (IEP), and Security Enforcement Point (SEP). The PEP module handles the initial access flow, encrypting traffic and validating interactions between the subject and the resource. This involves certificate-based authentication, where both the client and server use SSL/TLS certificates to establish a secure connection, and username/password authentication, which adds an additional layer of security by requiring clients to provide valid credentials. The combination of these authentication methods ensures that only authorized clients can establish a VPN tunnel with the server.

Once connected to the VPN, the IEP module validates the user's identity through login credentials and a one-time password (OTP) sent to the registered device. It also verifies the device's health, operating system settings, and the user's location before granting role-based access to organizational resources. The SEP module monitors session time and grants time-bound access, logging user activities and monitoring access to organizational resources. This comprehensive approach enhances the overall security and access control of the organization's network, ensuring that only authenticated and authorized users can access sensitive resources.

A detailed architecture diagram of the ZTVPN is illustrated in Figure 3. It has three modules, namely Policy Enforcement Point (PEP), Identity Enforcement Point (IEP), and Security Enforcement Point (SEP). In the first form, the subject or person uses the resource on behalf of a requester or as a requester. The access flow is blocked by the PEP, which encrypts the traffic once the subject interacts with the resource and validation is successful, which is shown in Algorithm 1. Details are provided below:

- **Certificate-Based Authentication:** OpenVPN creates an encrypted connection between the client and server based on SSL/TLS. Certificates are employed to ensure that both the client and the server are genuine. The process is as follows: The process is as follows:
  - The VPN server has an independent SSL/TLS certificate and private key.
  - Every client gives out a distinct SSL/TLS certificate and a private key.
  - During the SSL/TLS negotiation, when a client connects to the server, it has to send its certificate to the server.
  - The server checks the client's certificate against the list of the trusted certificates the server possesses. If the client's certificate is valid and recognised as trustworthy by the server, then the SSL/TLS negotiation is accomplished, and the connection is established.
- **Username/Password Authentication:** Apart from the certificate, the VPN can also use the names and secret codes for other recognition in addition to the use of certificates. This is particularly useful when multiple clients use the same certificate, for instance, in road warrior configurations.

  - Every client has a username and a password created on the VPN server.
  - If the client attempts a connection, it presents a certificate as mentioned above, and then the server is asked for a username and password.
  - It then has to verify the username and the password of the client against the list of clients and the password with which it has been configured.
  - If the credentials match those of the authenticated client, the client will be logged in and connected to the VPN.

- **Combining Certificate and Username/Password Authentication:** Besides the certificates, OpenVPN also has options for the username and password in the second level of the authentication. This is especially useful when several clients have the same certificate (for example, for the road warriors).

  - Users get an account on the VPN server, which has their unique username and password.
  - When a client attempts to connect, it sends its certificate, as mentioned above, and the VPN server then asks for a username and password.
  - The server compares the given username and password with the client list and the necessary password.
  - If the username and password are correct, the client is authorised, and Phase 2 of the VPN connection is initiated.

- **Combining Certificate and Username/Password Authentication:** In practice, VPN can be configured to require both certificate-based authentication and username/password authentication for enhanced security. This ensures that clients possess the correct certificate and valid credentials to connect to the VPN server. In this, the clients go through both certificate-based authentication and username/password authentication before being granted access to the VPN server.

The server verifies the certificates and then checks the provided username and password against its client credentials database. Only after successful validation are the clients allowed to establish the VPN tunnel with the server. After successful validation of credentials, the IP address has been assigned to the client from a predefined IP pool managed by the VPN server. Each time a client connects, it receives an available IP address from the pool. This approach is more scalable and useful when you have a large number of clients connecting intermittently. If a client disconnects, its assigned IP address becomes available for future connections. This allows efficient use of the address space as clients come and go.

In the second module, After the user connects to the VPN, IEP will act and validate its identity through user login credentials. OTP is sent to the given device through which the device is verified. Afterwards, the device health, OS settings, and person location will be verified. Then, role-based access is granted to that person for organisational resources, as can be seen in Algorithm 2 from lines 1 to 22. In the SEP module, session time is monitored, and limited time-based access is granted to every user. It is a time-bound session; once the user logs in, the session time is collected from the log's server, and the counter starts with it. Then, the user profile and activities are also monitored through server logs. Once the user tries to access any organisational resources or tries to access any link, it can be logged and monitored as well, which can be seen in Algorithm **??** and 2 from lines 24 to 49.

This implementation can enhance the overall security and access control of an organisation's network. In VPN, client credentials are typically validated through a combination of certificate-based authentication and username/password authentication. Let's explore how this validation process works along with a Diagram:

doi:10.20944/preprints202410.0301.v1

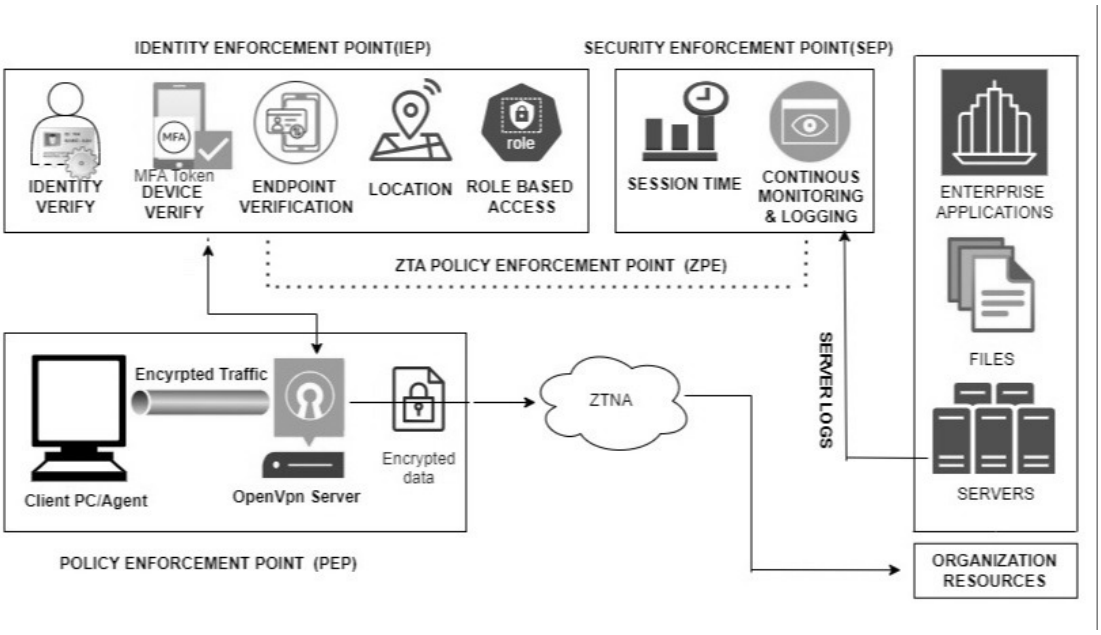

Figure 3. Architecture diagram of ZTV

These are the steps through which we can achieve our goal are described below:

- The user has to put his credentials of the VPN Client, and then it will validate with the server, and then traffic goes to the Internet.
- Then the person can access the Web application; if VPN credentials aren't validated, then it will not permit access to the Web application.
- Now, the user has to put his credentials in the web app; at this point, the user is validated with a password, and it also receives the OTP on its registered mobile number.
- In the next step, the user device OS, settings, and device health are monitored, and user logs are generated every time it performs any activity.
- There is also access management; the user is restricted to the privileges that are allowed by the admin.

Algorithm 1 : Policy Enforcement Point (PEP)

```
Require: VPN client, VPN configuration file (.ovpn), credentials (username and password)
Module 1: Enforcement Point (EP)
Submodule 1: Install VPN Client
1.1 Download the appropriate OpenVPN client for your operating system.
1.2 Follow the installation instructions to install the OpenVPN client on your device.

Submodule 2: Obtain OpenVPN Configuration File
2.1 Obtain the .ovpn configuration file from your network administrator or VPN service provider.
2.2 Ensure you have the necessary credentials (username and password), if required.

Submodule 3: Configure OpenVPN Client
3.1 Place the .ovpn configuration file in the appropriate directory:
    Windows: C:\Program Files\OpenVPN\config\
3.2 If needed, open the .ovpn file in a text editor and modify any settings as per your requirements.

Submodule 4: Connect to OpenVPN Server
4.1 Launch the OpenVPN client application.
4.2 Select the appropriate .ovpn configuration file.
4.3 Enter your credentials (username and password) if prompted.
4.4 Click on the Connect button to establish the VPN connection.

Submodule 5: Verify the Connection
5.1 Once connected, verify the VPN connection:
    5.1.1 Check the OpenVPN client status window for connection details.
    5.1.2 Verify your IP address has changed to the VPN server's IP address using an online service like whatismyip.com.
    5.1.3 Ensure you can access network resources that require a VPN connection.
```

Algorithm 2 : ZTNA Policy Enforcement Point (ZPE)

```
Require: resources, userRoles, accessPolicies, ztnaConfig
Module 2: Identity Enforcement Point (IEP)
Submodule 1: Define Access Policies
defineResources(resources)
defineUserRoles(userRoles)
createAccessPolicies(accessPolicies)
Submodule 2: Set Up ZTNA Infrastructure
selectZTNASolution(ztnaConfig.solution)
deployZTNAController(ztnaConfig.controller)
installZTNAAgents(ztnaConfig.agents)
Submodule 3: Implement Authentication Mechanisms configureAuthentication(ztnaConfig.authMechanisms)
Submodule 4: Enforce Zero Trust Principles
for user in users do
    if authenticate(user, ztnaConfig.auth) then
        session = establishZTNASession(user)
        if assessAccess(session, ztnaConfig.policies) then
            grantAccess(session, user)
        else
            denyAccess(session, user)
        end if
    else
        denyAccess(user)
    end if
end for
Module 3: Security Enforcement Point (SEP)
Submodule 1: Monitoring and Logging
setupActivityLogging()
enableRealTimeMonitoring()
configureAlertsAndReports()
Submodule 2: Continuous Improvement
while True do
    updateZTNASoftware(ztnaConfig)
    reviewPolicies(accessPolicies)
    conductUserTraining()
end while
function grantAccess(session, user)
function allowAccess(session, user)
    allowAccess(session, user)
end function
function denyAccess(session, user)
    blockAccess(session, user)
end function
function setupActivityLogging()
    configureLogging()
end function
function enableRealTimeMonitoring()
    startMonitoring()
end function
function configureAlertsAndReports()
    setupAlerts()
    generateReports()
end function
```

3.1. Impliementation Case Study

Enterprises can vary widely in size, structure, and scope, from small businesses to multinational corporations. Within an enterprise, there are various roles that individuals may assume, each with distinct responsibilities and contributions to the organisation's success. The structure and specific roles can vary depending on the assigned tasks and skills, and giving role-based access and monitoring the activity is the need of the hour right now due to the increasing number of security breach incidents. As network infrastructures become more complex and the threat landscape evolves, traditional security models and perimeter-based approaches are no longer enough to secure delicate data and resources. The emergence of ZTNA has gained attention as a security framework that focuses on substantiating every access request, irrespective of the user's place or network context. However, there is a need to explore our integration of ZTNA principles with VPNs, which have long been used to secure network communications. The problem lies in understanding how VPNs can be effectively employed to achieve ZTNA, addressing challenges such as trust boundaries, user authentication, access control mechanisms, and data protection. This research aims to investigate the design, implementation, and evaluation of ZTVPN to provide a comprehensive understanding of the potential benefits; through this, how can an organisational network be secure from insider and outside attacks and the limitations of this integration, as well as to propose recommendations for successful deployments.

4. Results and Evaluation

he proposed ZTVPN framework has been evaluated in various enterprise scenarios to assess its effectiveness and advantages over traditional VPNs, ZTNA), and other security solutions. The results demonstrate that ZTVPN offers significant improvements in terms of security, performance, and scalability. When integrating VPN and ZTNA, the result is a comprehensive remote access solution that combines the benefits of both technologies to enhance security and access control. Here's a discussion regarding the integration:

- **Improved Security:** VPNs traditionally provide a secure tunnel for remote users to access corporate resources.
- **Enhanced User Experience:** Integrating VPN and ZTNA allows organisations to strike a balance between security and user experience.
- **Scalability and Flexibility:** VPNs are typically designed to accommodate a fixed number of concurrent connections, which can be a limitation for organisations with dynamic workforces or fluctuating access demands.
- **Granular Access Control:** This solutions enable organisations to implement granular access controls based on user roles, device types, and other contextual factors.
- **Centralized Management and Visibility:** ZTNA solutions often provide centralised management consoles and comprehensive visibility into user access and activity.

Table 4 shows that, the proposed framework, "ZTVPN", remedies all of the problems listed above. ZTVPN allows enterprises to implement robust access controls that consider several contextual aspects, such as device health, identification, and more, through enforcement policy. This greatly decreases the likelihood of illegal access and data breaches. Making sure people have safe access to resources with little hassle. Because of this solution's inherent scalability and flexibility, enterprises may more readily adjust to changing access needs. With centralised access control, organisations can monitor user activity in both on-premises and remote locations more effectively.

doi:10.20944/preprints202410.0301.v1

Table 4. Comparison of surveys and assessments that have been done in the past. Some of them have been examined, while others have been ignored. A: The Approach Used to Categorise the Works Reviewed, B: Comparing individual statistics across several works C: Analysing Models with Variable Features, D: Data pertaining to hybrid network problems

Author(s)	Principal Remark	A	B	C	D
He et al. [71]	The technologies forming the framework of Zero Trust are investigated and reviewed.	Y	Y	Y	X
Syed et al. [29]	Discussion as to how ZT interferes with access control and authentication in distinct situations.	Y	Y	P	P
Pittman et al. [72]	ZT tenets as a methodology implemented on data objects rather than data access avenues	Y	X	X	P
Buck et al.[73]	Analysis of industrial and academic knowledge gaps, as well as a compilation of works based on the Zero Trust principle	Y	X	X	P
This Article	ZTV/VPN-based ZTNA, OpenSource and ZTNA-based evaluation. ZTNA vendor-assisted adoption.	Y	Y	Y	Y

4.1. Discussion and Limitations

The ZTVPN is a complete solution for enterprises as it secures the network as well as organisational resources. The framework combines the strengths of both VPN and ZTNA by integrating certificate-based authentication, username/password authentication, and continuous monitoring of user and device credentials. This multi-layered approach ensures that only authenticated and authorized users can access organizational resources. Unlike traditional VPNs, which grant broad access to the entire network once authenticated, ZTVPN provides granular access control, reducing the attack surface and preventing unauthorized lateral movement within the network. Additionally, the continuous verification of user and device health, operating system settings, and location further enhances security, making it more robust than standalone ZTNA solutions.

The ZTVPN framework addresses common performance issues associated with traditional VPNs, such as latency and throughput. By dynamically selecting the best path for traffic and optimizing network performance, ZTVPN ensures that critical applications receive the necessary bandwidth and low latency. This results in a better user experience and increased productivity. The integration of Software-Defined Wide Area Network (SD-WAN) technology within the ZTVPN framework further enhances performance by providing centralized management and dynamic path selection based on real-time network conditions.

The cloud-native architecture of the ZTVPN framework allows for easy scalability and flexibility. Organizations can quickly adapt to changing business needs and deploy new services without the need for extensive hardware investments. The framework's ability to integrate with existing security solutions, such as Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), and Firewall as a Service (FWaaS), ensures comprehensive protection and seamless security transitions. This makes ZTVPN a more scalable and adaptable solution compared to traditional VPNs and standalone ZTNA implementations.

The framework provides a unified approach to access control by combining the principles of Zero Trust with the secure connectivity of VPNs. This ensures that users are granted access based on their identity, role, and context, rather than relying on the traditional perimeter-based security model. The role-based access control and time-bound sessions further enhance security by limiting access to only the necessary resources for a specific duration. This comprehensive access control mechanism is more effective than the broad access granted by traditional VPNs and the application-specific access provided by ZTNA.

5. Conclusion and Future Work

The rapid shift to remote work environments has necessitated the development of robust cybersecurity frameworks to protect organizational resources and ensure seamless operations. This paper has presented a comprehensive overview of contemporary technologies employed in enterprises. Among these, the proposed ZTVPN framework stands out as a highly effective solution for enhancing IT security and privacy in modern enterprises. The ZTVPN framework integrates zero trust principles with VPN technology, addressing critical concerns such as security threats, latency, throughput, and scalability. By continuously verifying every user and device attempting to access corporate resources, ZTVPN ensures a robust security posture, preventing data leaks, managing access permissions, and providing seamless security transitions. The effectiveness of the ZTVPN framework has been demonstrated through various enterprise scenarios, highlighting its potential to fortify cybersecurity frameworks against contemporary cyber threats.

Despite the promising results, there are several areas for future research and development. One potential direction is the exploration of advanced cryptographic techniques to further enhance the security and performance of the ZTVPN framework so it can resist post-quantum cryptography cyber-attacks. Additionally, the integration of artificial intelligence can provide real-time threat detection and response capabilities, further strengthening the security posture of enterprises. Another possible future work is the evaluation of the ZTVPN framework in diverse organizational contexts, including small and medium-sized enterprises (SMEs) and large multinational corporations. This would provide valuable insights into the scalability and adaptability of the framework across different environments.

List of Abbreviations

Table 5. List of Abbreviations and Full Forms

Abbreviation	Full Form
ZTVPN	Zero Trust VPN
ZTNA	Zero Trust Network Access
VPN	Virtual Private Network
SSH	Secure Shell
SD-WAN	Software-defined Wide Area Network
SASE	Secure Access Service Edge
DoS	Denial of Service
MFA	Multi-Factor Authentication
IAM	Identity and Access Management
PEP	Policy Enforcement Point
IEP	Identity Enforcement Point
SEP	Security Enforcement Point
TLS	Transport Layer Security
SSL	Secure Sockets Layer
DHCP	Dynamic Host Configuration Protocol
IP	Internet Protocol
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
PoP	Point of Presence
BYOD	Bring Your Own Device

References

1. Hodge, R. VPN use surges during the coronavirus lockdown, but so do security risks. *CNET, April* **2020**, *23*.
2. Singer, P.W.; Friedman, A. *Cybersecurity: What everyone needs to know*; oup usa, 2014.
3. Deibert, R.J. Subversion Inc: the age of private espionage. *Journal of Democracy* **2022**, *33*, 28–44.

4. Zhang, Z.; Zhang, Y.Q.; Chu, X.; Li, B. An overview of virtual private network (VPN): IP VPN and optical VPN. *Photonic network communications* **2004**, *7*, 213–225.
5. Baykara, M.; Gürel, Z.Z. Detection of phishing attacks. 2018 6th International Symposium on Digital Forensic and Security (ISDFS). IEEE, 2018, pp. 1–5.
6. Kaur, J.; Ramkumar, K. The recent trends in cyber security: A review. *Journal of King Saud University-Computer and Information Sciences* **2022**, *34*, 5766–5781.
7. Ghelani, D. Cyber security, cyber threats, implications and future perspectives: A Review. *Authorea Preprints* **2022**.
8. Alkhalil, Z.; Hewage, C.; Nawaf, L.; Khan, I. Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science* **2021**, *3*, 563060.
9. O'Kane, P.; Sezer, S.; Carlin, D. Evolution of ransomware. *Iet Networks* **2018**, *7*, 321–327.
10. McIntosh, T.; Kayes, A.; Chen, Y.P.P.; Ng, A.; Watters, P. Ransomware mitigation in the modern era: A comprehensive review, research challenges, and future directions. *ACM Computing Surveys (CSUR)* **2021**, *54*, 1–36.
11. Dutkowska-Zuk, A.; Hounsel, A.; Xiong, A.; Roberts, M.; Stewart, B.; Chetty, M.; Feamster, N. Understanding how and why university students use virtual private networks. *arXiv preprint arXiv:2002.11834* **2020**.
12. Jegede, A.; Fadele, A.; Onoja, M.; Aimufua, G.; Mazadu, I.J. Trends and future directions in automated ransomware detection. *Journal of Computing and Social Informatics* **2022**, *1*, 17–41.
13. Khan, E.; Sperotto, A.; van der Ham, J.; van Rijswijk-Deij, R. Stranger VPNs: Investigating the Geo-Unblocking Capabilities of Commercial VPN Providers. International Conference on Passive and Active Network Measurement. Springer, 2023, pp. 46–68.
14. Santhanamahalingam, S.; Alagarsamy, S.; Subramanian, K. A study of cloud-based VPN establishment using network function virtualization technique. 2022 3rd International Conference on Smart Electronics and Communication (ICOSEC). IEEE, 2022, pp. 627–631.
15. Li, Y.; Liu, Q. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports* **2021**, *7*, 8176–8186.
16. Zhang, Z.; Al Hamadi, H.; Damiani, E.; Yeun, C.Y.; Taher, F. Explainable artificial intelligence applications in cyber security: State-of-the-art in research. *IEEE Access* **2022**, *10*, 93104–93139.
17. Furnell, S. The cybersecurity workforce and skills. *Computers & Security* **2021**, *100*, 102080.
18. Rajasekharaiah, K.; Dule, C.S.; Sudarshan, E. Cyber security challenges and its emerging trends on latest technologies. IOP Conference Series: Materials Science and Engineering. IOP Publishing, 2020, Vol. 981, p. 022062.
19. AL-Hawamleh, A.M. Predictions of cybersecurity experts on future cyber-attacks and related cybersecurity measures. *momentum* **2023**, *3*, 15.
20. Shaukat, K.; Luo, S.; Varadharajan, V.; Hameed, I.A.; Xu, M. A survey on machine learning techniques for cyber security in the last decade. *IEEE access* **2020**, *8*, 222310–222354.
21. Secure Remote Access Best Practices - Check Point Software — checkpoint.com. https://www.checkpoint.com/cyber-hub/network-security/what-is-vpn/covid-19-and-secure-remote-access-best-practices/. [Accessed 26-08-2024].
22. Fatima, M.; Abbas, H.; Yaqoob, T.; Shafqat, N.; Ahmad, Z.; Zeeshan, R.; Muhammad, Z.; Rana, T.; Mussiraliyeva, S. A survey on common criteria (CC) evaluating schemes for security assessment of IT products. *PeerJ Computer Science* **2021**, *7*, e701.
23. Streun, F.; Wanner, J.; Perrig, A. Evaluating susceptibility of VPN implementations to DoS attacks using adversarial testing. Network and Distributed Systems Security Symposium 2022 (NDSS'22). Internet Society, 2022.
24. Zhou, Y.; Zhang, K. Dos vulnerability verification of ipsec vpn. 2020 IEEE International Conference on Artificial Intelligence and Computer Applications (ICAICA). IEEE, 2020, pp. 698–702.
25. Ginty, S. Discover the anatomy of an external cyberattack surface with new RiskIQ report | Microsoft Security Blog — microsoft.com. https://www.microsoft.com/en-us/security/blog/2022/04/21/discover-the-anatomy-of-an-external-cyberattack-surface-with-new-riskiq-report/?msockid=355668c01f696b823ed97c6f1e6f6a0f. [Accessed 26-08-2024].
26. Singh, K.K.V.; Gupta, H. A New Approach for the Security of VPN. Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies, 2016, pp. 1–5.

27. Frahim, J.; Huang, Q. *Ssl remote access vpns (network security)*; Cisco Press, 2008.
28. Shut the Front Door: Analyzing VPN Vulnerability Exploits — mandiant.com. https://www.mandiant.com/resources/webinars/mandiant-intelligence-briefing-stories-directly-frontline. [Accessed 26-08-2024].
29. Syed, N.F.; Shah, S.W.; Shaghaghi, A.; Anwar, A.; Baig, Z.; Doss, R. Zero trust architecture (zta): A comprehensive survey. *IEEE access* **2022**, *10*, 57143–57179.
30. Nagmote, S.U. An Overview Of Network Security Model Using Cryptography, Firewall And Vpn For Social Organization With There Benifits. *International Journal of Engineering* **2013**, *2*.
31. Adeyinka, O. Analysis of problems associated with IPSec VPN Technology. 2008 Canadian Conference on Electrical and Computer Engineering. IEEE, 2008, pp. 001903–001908.
32. Sombatruang, N.; Omiya, T.; Miyamoto, D.; Sasse, M.A.; Kadobayashi, Y.; Baddeley, M. Attributes affecting user decision to adopt a Virtual Private Network (VPN) app. Information and Communications Security: 22nd International Conference, ICICS 2020, Copenhagen, Denmark, August 24–26, 2020, Proceedings 22. Springer, 2020, pp. 223–242.
33. Rothvoß, T.; Sanita, L. On the complexity of the asymmetric VPN problem. International Workshop on Approximation Algorithms for Combinatorial Optimization. Springer, 2009, pp. 326–338.
34. Dutkowska-Zuk, A.; Hounsel, A.; Morrill, A.; Xiong, A.; Chetty, M.; Feamster, N. How and why people use virtual private networks. 31st USENIX Security Symposium (USENIX Security 22), 2022, pp. 3451–3465.
35. Sawalmeh, H.; Malayshi, M.; Ahmad, S.; Awad, A. VPN remote access OSPF-based VPN security vulnerabilities and counter measurements. 2021 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT). IEEE, 2021, pp. 236–241.
36. Cheung, K.H.; Mišić, J. On virtual private networks security design issues. *Computer Networks* **2002**, *38*, 165–179.
37. Bansode, R.; Girdhar, A. Common vulnerabilities exposed in VPN–A survey. Journal of Physics: Conference Series. IOP Publishing, 2021, Vol. 1714, p. 012045.
38. With everyone working from home, VPN security is now paramount — zdnet.com. https://www.zdnet.com/article/covid-19-with-everyone-working-from-home-vpn-security-has-now-become-paramount/. [Accessed 26-08-2024].
39. Einler Larsson, L.; Qollakaj, K. Cybersecurity of remote work migration: A study on the VPN security landscape post covid-19 outbreak, 2023.
40. VPN Access and Activity Monitoring," Sans, 2020. - Bing — bing.com. https://www.bing.com/search?q=VPN+Access+and+Activity+Monitoring%2C"+Sans%2C+2020.&qs=n&form=QBRE&sp=-1&lq=1&pq=vpn+access+and+activity+monitoring%2C"+sans%2C+2020.&sc=1-48&sk=&cvid=167E379FC8C341CCB182FAC4A95D10D3&ghsh=0&ghacc=0&ghpl=. [Accessed 26-08-2024].
41. Ikram, M.; Vallina-Rodriguez, N.; Seneviratne, S.; Kaafar, M.A.; Paxson, V. An analysis of the privacy and security risks of android vpn permission-enabled apps. Proceedings of the 2016 internet measurement conference, 2016, pp. 349–364.
42. Yoo, S.J. A Study on the Improvement of Security Enhancement for ZTNA. *Convergence Security Journal* **2024**, *24*, 21–26.
43. Nazir, A.; Iqbal, Z.; Muhammad, Z. ZTA: A Novel Zero Trust Framework for Detection and Prevention of Malicious Android Applications **2024**.
44. Stafford, V. Zero trust architecture. *NIST special publication* **2020**, *800*, 207.
45. Developing a framework to improve critical infrastructure cybersecurity. https://www.nist.gov/system/files/documents/2017/06/01/040513_cgi.pdf. [Accessed 26-08-2024].
46. Cybersecurity, C.I. Framework for improving critical infrastructure cybersecurity. *URL: https://nvlpubs. nist. gov/nistpubs/CSWP/NIST. CSWP* **2018**, *4162018*, 7.
47. Malatji, M.; Marnewick, A.L.; Von Solms, S. Cybersecurity capabilities for critical infrastructure resilience. *Information & Computer Security* **2022**, *30*, 255–279.
48. Zscaler's 2022 VPN Report: As VPN Exploits Grow, 80 Percent of Organizations Shift Towards Zero Trust Security — zscaler.com. https://www.zscaler.com/press/. [Accessed 26-08-2024].
49. amzetta.com. https://amzetta.com/wp-content/uploads/2021/05/AmZetta-Remote-AccessSecurity-Going-Beyond-VPN-Security-Brief.pdf. [Accessed 26-08-2024].

50. Pavlicek, A.; Sudzina, F. Use of virtual private networks (VPN) and proxy servers: Impact of personality and demographics. 2018 Thirteenth International Conference on Digital Information Management (ICDIM). IEEE, 2018, pp. 108–111.
51. Hurkens, C.A.; Keijsper, J.C.M.; Stougie, L. Virtual private network design: A proof of the tree routing conjecture on ring networks. *SIAM Journal on Discrete Mathematics* **2007**, *21*, 482–503.
52. Talan, A. Zero Trust Network Access with Cybersecurity Challenges and Potential Solutions. PhD thesis, Dublin, National College of Ireland, 2022.
53. Campbell, M. Beyond zero trust: Trust is a vulnerability. *Computer* **2020**, *53*, 110–113.
54. Sood, A.K. Empirical Cloud Security: Practical Intelligence to Evaluate Risks and Attacks **2023**.
55. Jeffery, C.L.; Das, S.R.; Bernal, G.S. Proxy-sharing proxy servers. Proceedings of COM'96. First Annual Conference on Emerging Technologies and Applications in Communications. IEEE, 1996, pp. 116–119.
56. Saini, K. *Squid Proxy Server 3.1: beginner's guide*; Packt Publishing Ltd, 2011.
57. Xu, V. MAZE: a secure cloud storage service using Moving Target Defense and Secure Shell Protocol (SSH) tunneling. PhD thesis, University of Pittsburgh, 2020.
58. Dusi, M.; Gringoli, F.; Salgarelli, L. A preliminary look at the privacy of SSH tunnels. 2008 Proceedings of 17th International Conference on Computer Communications and Networks. IEEE, 2008, pp. 1–7.
59. Yang, Z.; Cui, Y.; Li, B.; Liu, Y.; Xu, Y. Software-defined wide area network (SD-WAN): Architecture, advances and opportunities. 2019 28th International Conference on Computer Communication and Networks (ICCCN). IEEE, 2019, pp. 1–9.
60. Yalda, K.G.; Hamad, D.J.; Ţăpuş, N. A survey on Software-defined Wide Area Network (SD-WAN) architectures. 2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA). IEEE, 2022, pp. 1–5.
61. Iesar, H.; Iqbal, W.; Abbas, Y.; Umair, M.Y.; Wakeel, A.; Illahi, F.; Saleem, B.; Muhammad, Z. Revolutionizing Data Center Networks: Dynamic Load Balancing via Floodlight in SDN Environment. 2024 5th International Conference on Advancements in Computational Sciences (ICACS). IEEE, 2024, pp. 1–8.
62. Islam, M.N.; Colomo-Palacios, R.; Chockalingam, S. Secure access service edge: A multivocal literature review. 2021 21st International Conference on Computational Science and Its Applications (ICCSA). IEEE, 2021, pp. 188–194.
63. Yiliyaer, S.; Kim, Y. Secure access service edge: A zero trust based framework for accessing data securely. 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC). IEEE, 2022, pp. 0586–0591.
64. Awale, V.; Gaikwad, S. Zero Trust Architecture Using Hyperledger Fabric. 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT). IEEE, 2023, pp. 1–4.
65. Abbas, H.; Emmanuel, N.; Amjad, M.F.; Yaqoob, T.; Atiquzzaman, M.; Iqbal, Z.; Shafqat, N.; Shahid, W.B.; Tanveer, A.; Ashfaq, U. Security assessment and evaluation of VPNs: a comprehensive survey. *ACM Computing Surveys* **2023**, *55*, 1–47.
66. Security issues with Virtual Private Network (VPN) and proxy services - Bing — bing.com. https://www.bing.com/search? [Accessed 26-08-2024].
67. Cybersecurity After COVID-19: 10 Ways to Protect Your Business and Refocus on Resilience. https://www.marshmclennan.com/assets/insights/publications/2020/june/cybersecurity_after_covid_19.pdf. [Accessed 26-08-2024].
68. Fuchs, J. Vishing: New Threat to VPNs — avanan.com. https://www.avanan.com/blog/vishing-new-threat-vpn. [Accessed 26-08-2024].
69. Odokuma, E.; Musa, M. Internet Threats and Mitigation Methods in Electronic Businesses Post Covid-19. *Int. J. Comput. Appl* **2022**, *184*, 1–4.
70. Purchina, O.; Poluyan, A.; Fugarov, D. Securing an Information System via the SSL Protocol. *International Journal of Safety & Security Engineering* **2022**, *12*.
71. He, Y.; Huang, D.; Chen, L.; Ni, Y.; Ma, X. A survey on zero trust architecture: Challenges and future trends. *Wireless Communications and Mobile Computing* **2022**, *2022*, 6476274.
72. Pittman, J.M.; Alaee, S.; Crosby, C.; Honey, T.; Schaefer, G.M. Towards a model for zero trust data. *American Journal of Science & Engineering* **2022**, *3*, 18–24.

73. Buck, C.; Olenberger, C.; Schweizer, A.; Völter, F.; Eymann, T. Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust. *Computers & Security* **2021**, *110*, 102436.
74. Ward, R.; Beyer, B. Beyondcorp: A new approach to enterprise security. *; login:: the magazine of USENIX & SAGE* **2014**, *39*, 6–11.
75. Osborn, B. Beyondcorp: Design to deployment at google. Usenix, 2016, Vol. 41, p. 28.
76. Stafford, V. Zero trust architecture. *NIST special publication* **2020**, *800*, 207.
77. Cunningham, C. Zero Trust: what, why and how **2018**.
78. Vensmer, A.; Kiesel, S. Dynfire: Dynamic firewalling in heterogeneous environments. World Congress on Internet Security (WorldCIS-2012). IEEE, 2012, pp. 57–58.
79. Giannakou, A.; Rilling, L.; Pazat, J.L.; Morin, C. AL-SAFE: a secure self-adaptable application-level firewall for IaaS clouds. 2016 IEEE International Conference on Cloud Computing Technology and Science (CloudCom). IEEE, 2016, pp. 383–390.
80. Crichigno, J.; Bou-Harb, E.; Ghani, N. A comprehensive tutorial on science DMZ. *IEEE Communications Surveys & Tutorials* **2018**, *21*, 2041–2078.
81. French, A.M.; Guo, C.; Shim, J.P. Current status, issues, and future of bring your own device (BYOD). *Communications of the Association for Information Systems* **2014**, *35*, 10.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.