Table of Contents

[**Acknowledgements** 2](#_Toc175837102)

[**Abstract** 3](#_Toc175837103)

[List of Abbreviations 6](#_Toc175837104)

[Chapter 1 7](#_Toc175837105)

[1.1 Introduction 7](#_Toc175837106)

[1.2 Hypothesis 7](#_Toc175837107)

[1.3 Research Focus 7](#_Toc175837108)

[1.4 RESEARCHER’S Personal Contribution 7](#_Toc175837109)

[1.4 The Need for This Research 8](#_Toc175837110)

[1.5 Traditional Perimeter-Based Security 9](#_Toc175837111)

[1.6 Zero Trust Network Architecture (ZTNA) 9](#_Toc175837112)

[1.7 Problem Statement 10](#_Toc175837113)

[1.8 Research Aims and Objectives 11](#_Toc175837114)

[Research Aim: 11](#_Toc175837115)

[RESEARCH OBJECTIVES: 11](#_Toc175837116)

[1.9 Research Questions 11](#_Toc175837117)

[1.10 Limitations/Delimitations of the Project: 11](#_Toc175837118)

[Chapter 2 12](#_Toc175837119)

[Literature Review of Zero Trust Network Architecture (ZTNA) 12](#_Toc175837120)

[2.1 Introduction 12](#_Toc175837121)

[2.2 The Evolution of Zero Trust 12](#_Toc175837122)

[2.3 Benefits of ZTNA 12](#_Toc175837123)

[2.4 Challenges of ZTNA Implementation 12](#_Toc175837124)

[2.5 Implementation Strategies 13](#_Toc175837125)

[2.6 Critical Review and Implications for Current Research 14](#_Toc175837126)

[Chapter 3 15](#_Toc175837127)

[Methodology 15](#_Toc175837128)

[3.1 Phase 1: Literature Review and Theoretical Framework 15](#_Toc175837129)

[3.2 Phase 2: Simulated Environment Setup 15](#_Toc175837130)

[3.3 Phase 3: ZTNA Framework Design and Implementation 15](#_Toc175837131)

[3.4 Phase 4: Perimeter-Based Security Model Implementation 16](#_Toc175837132)

[3.5 Phase 5: Threat Modeling and Simulation 16](#_Toc175837133)

[3.6 Phase 6: Data Collection and Analysis 16](#_Toc175837134)

[3.7 Phase 8: Comparative Analysis and Cost-Benefit Assessment 16](#_Toc175837135)

[3.8 Phase 9: Development of Best Practices 16](#_Toc175837136)

[3.9 Phase 10: Knowledge Dissemination 16](#_Toc175837137)

[Chapter 4 18](#_Toc175837138)

[Design and Implementation 18](#_Toc175837139)

[4.1 Simulated Environment Setup 18](#_Toc175837140)

[4.2 ZTNA Framework Implementation 24](#_Toc175837141)

[4.3 Perimeter-Based Security Model Configuration 30](#_Toc175837142)

[4.4 Resources Configuration 33](#_Toc175837143)

[**Chapter 5** 37](#_Toc175837144)

[**Evaluation and Analysis** 37](#_Toc175837145)

[5.1 Introduction 37](#_Toc175837146)

[5.2 Evaluation Metrics and Methodology 37](#_Toc175837147)

[5.3 Results and Findings 38](#_Toc175837148)

[5.4 Comparative Table: Presenting the Key Metrics Side-By-Side 58](#_Toc175837149)

[5.5 Strengths and Weaknesses of Each Security Model 60](#_Toc175837150)

[5.6 Addressing Research Questions 61](#_Toc175837151)

[5.7 Contribution to Existing Literature 63](#_Toc175837152)

[5.8 Actionable Recommendations for Organizations 63](#_Toc175837153)

[Chapter 6 65](#_Toc175837154)

[Conclusion and Future Work 65](#_Toc175837155)

[List of Figures 67](#_Toc175837156)

[References 69](#_Toc175837157)

# List of Abbreviations

**ZTNA:** Zero Trust Network Access

**VM:** Virtual Machine

**IDS:** Intrusion Detection System

**VPN:** Virtual Private Network

**DDoS:** Distributed Denial of Service

**LAN:** Local Area Network

**WAN:** Wide Area Network

**DHCP:** Dynamic Host Configuration Protocol

**ET Open:** Emerging Threats Open (ruleset)

**IdP:** Identity Provider

**MFA:** Multi-Factor Authentication

**IAM:** Identity and Access Management

**SDP:** Software-Defined Perimeter

**APT:** Advanced Persistent Threat

**SASE:** Secure Access Service Edge

**IoT:** Internet of Things

# Chapter 1

## 1.1 Introduction

The digital landscape is experiencing a profound transformation, characterized by the widespread adoption of cloud computing, the proliferation of mobile devices, and the increasing prevalence of remote work arrangements (Mell & Grance, 2011). This evolution has not only revolutionized the way businesses operate and interact with customers but has also introduced a new paradigm of cybersecurity challenges. The traditional perimeter-based security model, once considered the cornerstone of network defence, is proving increasingly inadequate in the face of evolving threats (Cisco, 2023).

The traditional castle-and-moat approach to network security, reliant on implicit trust within a defined perimeter, is becoming increasingly obsolete in the face of sophisticated, persistent cyber threats. Zero Trust Network Architecture (ZTNA) has emerged as a compelling alternative, fundamentally shifting the security paradigm by eliminating the concept of implicit trust and enforcing strict verification for every access request. While the theoretical benefits of ZTNA are widely acknowledged, there remains a notable lack of empirical evidence demonstrating its real-world effectiveness compared to traditional models, particularly in the context of specific attack scenarios and diverse organizational environments.

## 1.2 Hypothesis

The implementation of a Zero Trust Network Architecture (ZTNA) framework will result in a significantly lower number of successful attacks, faster detection times, and more effective prevention of lateral movement compared to a traditional perimeter-based security model

## 1.3 Research Focus

This dissertation addresses this knowledge gap by conducting a rigorous comparative analysis of ZTNA and traditional perimeter-based security within a simulated environment meticulously designed to mirror the complexities of a real-world organizational network. By simulating various attack scenarios and collecting detailed data on security events, network traffic, and user behaviour, this study aims to answer two critical questions:

1. **Security Effectiveness:** To what extent does ZTNA enhance security and mitigate risks compared to traditional perimeter-based security in the face of specific attack vectors, such as phishing, malware, data exfiltration, and lateral movement?
2. **Implementation Challenges:** What are the key challenges organizations face when designing, implementing, and operating a ZTNA framework in a practical setting?

## 1.4 RESEARCHER’S Personal Contribution

The researcher's contribution to this research is multifaceted, encompassing technical expertise and methodological rigor. They took a hands-on approach to designing and implementing the simulated network environment, ensuring its representation of real-world complexities. By leveraging Cloudflare Zero Trust for ZTNA and industry-standard tools for the traditional model, the researcher gained valuable insights into their practical implementation, configuration, and operational nuances.

Furthermore, the researcher developed a comprehensive methodology for evaluating the security effectiveness of both models. This involved crafting realistic attack scenarios that reflected current threats and collecting and analysing detailed logs and metrics from both environments. The resulting quantitative and qualitative data provided a nuanced understanding of the strengths, weaknesses, and trade-offs of each approach.

Based on their findings, the researcher developed a set of actionable best practices and recommendations for ZTNA implementation, tailored to address the specific challenges encountered during the project. These insights contributed to the growing body of knowledge on ZTNA and provided practical guidance for organizations seeking to adopt this transformative security model.

## 1.4 The Need for This Research

This research is crucial for several reasons:

* **Empirical Evidence:** It provides much-needed empirical evidence to support or refute theoretical claims about ZTNA's effectiveness.
* **Practical Guidance:** By addressing the practical challenges of ZTNA implementation, the study offers actionable insights for organizations considering its adoption.
* **Informed Decision-Making:** The comparative analysis and cost-benefit assessment will help organizations make informed decisions about whether and how to transition to ZTNA.
* **Advancing Cybersecurity:** The research contributes to the broader field of cybersecurity by exploring a promising new approach to network security.

A diagram of a system

Description automatically generated1F[[1]](#endnote-2)

Figure Diagram illustrating traditional perimeter-based security vs. Zero Trust Network Architecture

## **1.5 Traditional Perimeter-Based Security**

The traditional model relies on a "castle-and-moat" approach, where a fortified network perimeter, typically enforced by firewalls and intrusion detection systems, is designed to keep threats at bay. Once a user or device gains access inside the perimeter, they are often granted implicit trust, assuming that they are legitimate and not malicious (Gartner, 2021). This approach, however, has several limitations in the modern digital landscape:

* **Blurring of Boundaries:** The boundaries between internal and external networks are becoming increasingly blurred as users access resources from diverse locations and devices, often outside the traditional corporate network. This makes it difficult to define and enforce a clear perimeter.
* **Implicit Trust Assumption:** The assumption of trust within the network can be exploited by attackers who have breached the perimeter, allowing them to move laterally and access sensitive data.
* **Limited Visibility and Control:** Perimeter-based security often lacks granular visibility and control over internal traffic and user activity, making it difficult to detect and respond to threats that originate from within the network.

## 1.6 Zero Trust Network Architecture (ZTNA)

Zero Trust Network Architecture (ZTNA) fundamentally shifts the security paradigm from a perimeter-based model to one where "never trust, always verify" is the guiding principle (NSA, 2022). Unlike traditional models that assume users and devices within the network are trustworthy, ZTNA mandates continuous verification for every access request, acknowledging that threats can come from both inside and outside the network.

A core element of ZTNA is **micro-segmentation**, which divides the network into isolated segments, each with strict access controls (Forrester, 2022). This limits attackers' lateral movement, containing breaches within individual segments and minimizing overall impact.

**Least privilege access** further reduces risk by granting users only the minimum necessary access for their roles, thereby limiting the potential damage from compromised credentials (NIST, 2020).

**Continuous authentication** ensures ongoing verification of users and devices throughout their sessions, using real-time risk assessments based on factors like device posture and user behaviour (Gartner, 2021).

With the rise of advanced cyberattacks, traditional perimeter defences have proven inadequate, as attackers exploit software vulnerabilities and social engineering to bypass security and move laterally within networks (NIST, 2018; Verizon, 2023).

**The core tenets of ZTNA include:**

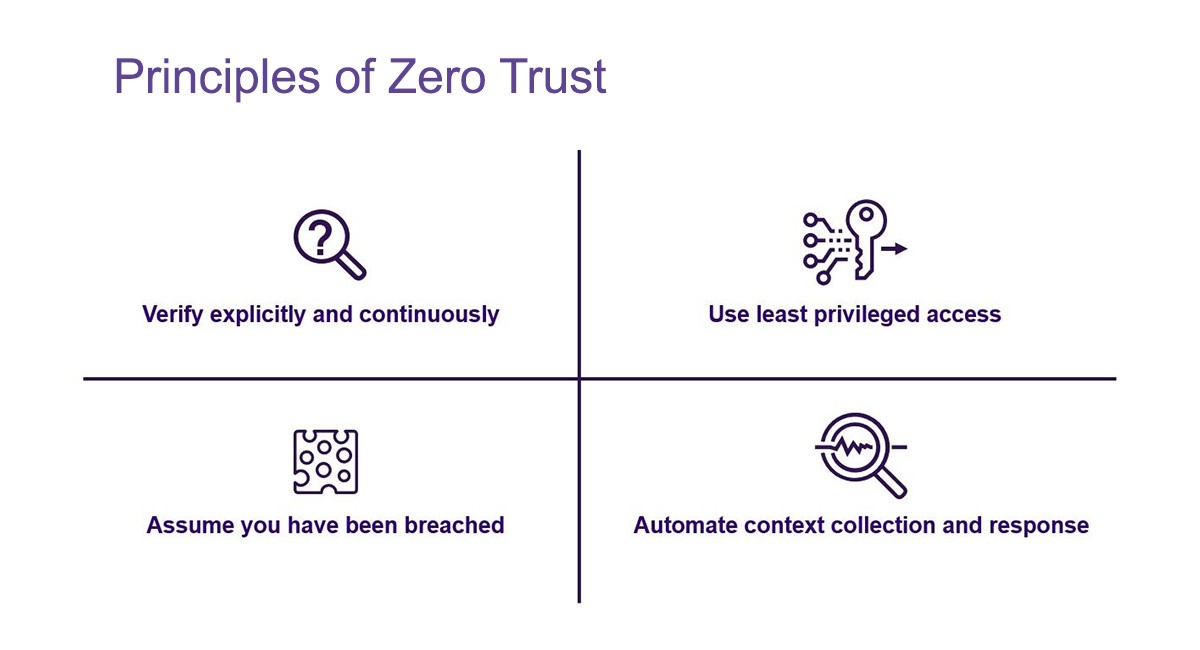
Zero Trust Network Architecture (ZTNA) emphasizes principles such as least privilege access, micro-segmentation, continuous authentication, and granular policy enforcement to enhance security.

**Least Privilege Access** ensures users receive only the minimal access necessary for their job roles, reducing risks of unauthorized access and privilege escalation (NIST, 2020). For example, a sales representative would have limited access compared to a system administrator. This reduces the potential impact of credential compromise.

**Micro-Segmentation** divides networks into isolated segments, each with its own security controls (Forrester, 2022). This strategy limits the spread of attacks by containing them within specific segments, such as separating finance from marketing departments.

**Continuous Authentication** involves ongoing verification of user and device identity throughout a session, using factors like device posture and user behaviour (Gartner, 2021). This approach helps detect anomalies in real-time, reducing the risk of unauthorized access.

**Granular Policy Enforcement** allows fine-tuned access controls based on context, such as user identity, device, and time of day (CSA, 2023). For example, access to sensitive data may be restricted to business hours on corporate devices, enhancing security while maintaining usability.



2F[[2]](#endnote-3)

Figure Principles of Zero Trust

## 1.7 Problem Statement

This project evaluates Zero Trust Network Architecture (ZTNA) for its effectiveness compared to traditional perimeter-based security models. It focuses on ZTNA’s ability to:

1. **Protect Against Cyber-Attacks**: Assess how well ZTNA defends against common threats (phishing, malware, ransomware) and sophisticated attacks like Advanced Persistent Threats (APTs) and zero-day exploits (Verizon, 2023; Cisco, 2023; FBI, 2022; Mitnick & Simon, 2005; Kaspersky, 2023).
2. **Prevent Unauthorized Access and Lateral Movement**: Examine ZTNA’s micro-segmentation and granular access controls, which address issues of lateral movement and internal security, improving upon traditional perimeter defences (Forrester, 2022).
3. **Detect and Respond to Security Incidents in Real-Time**: Evaluate ZTNA’s continuous authentication, monitoring, and automated responses to swiftly detect and mitigate threats.
4. **Adapt to Modern Networks**: Analyse ZTNA’s flexibility to handle evolving technologies, cloud services, and remote work, ensuring security across dynamic IT environments.
5. **Integrate with Legacy Systems**: Investigate how ZTNA can be integrated with existing infrastructure and legacy systems, facilitating a gradual transition without disrupting current operations.

## 1.8 Research Aims and Objectives

### Research Aim:

The overarching aim of this research project is to comprehensively assess the effectiveness and practicality of a Zero Trust Network Architecture (ZTNA) framework in comparison to a traditional perimeter-based security model within a simulated environment.

### RESEARCH OBJECTIVES:

This project aims to design and test a Zero Trust Network Architecture (ZTNA) in a simulated environment, compare its effectiveness against traditional security models, and develop best practice recommendations for organizations considering ZTNA adoption. Evaluation will focus on security metrics like access attempts, incident response time, and overall attack surface.

## 1.9 Research Questions

This project will address the following key questions:

1. How does ZTNA enhance security compared to traditional models in preventing unauthorized access, limiting lateral movement, and detecting/responding to incidents?
2. What challenges arise in implementing ZTNA, including technical complexities and impact on performance and user experience?
3. What are the best practices for ZTNA implementation?
4. What are ZTNA's future research directions?

## 1.10 Limitations/Delimitations of the Project:

This project evaluates Zero Trust Network Architecture (ZTNA) versus traditional security but faces limitations:

1. Simulated environment may not reflect real-world conditions.
2. Focuses on security effectiveness, not cost or scalability.
3. Uses specific technologies, limiting generalizability.
4. Assesses common attack vectors, not novel threats.
5. Resource constraints limit scale.
6. Primarily technical, not organizational impacts.

# Chapter 2

## Literature Review of Zero Trust Network Architecture (ZTNA)

### 2.1 Introduction

The traditional perimeter-based security model, once a cornerstone of network defence, is faltering under the weight of an increasingly sophisticated and evolving threat landscape. Zero Trust Network Architecture (ZTNA) has emerged as a compelling alternative, offering a paradigm shift in cybersecurity by advocating for a "never trust, always verify" approach. This comprehensive literature review examines deep into the existing research on ZTNA, examining its principles, benefits, challenges, and implementation strategies within a rapidly evolving technological context.

### 2.2 The Evolution of Zero Trust

Its roots can be traced back to the Jericho Forum in the early 2000s, which questioned the efficacy of traditional perimeter security in a de-perimeterized world (Smith, 2004). However, it was John Kindervag, a Forrester Research analyst, who coined the term "Zero Trust" in 2010 (Kindervag, 2010). His seminal work laid the foundation for the ZTNA framework, emphasizing the need for continuous verification and least privilege access.

### 2.3 Benefits of ZTNA

The benefits of adopting ZTNA have been extensively studied and documented in the literature. Key advantages include:

* **Enhanced Security Posture:** By eliminating implicit trust and enforcing granular access controls, ZTNA significantly strengthens an organization's security posture (Schwartz, 2018). It makes it significantly more difficult for attackers to exploit vulnerabilities and move laterally within the network.
* **Improved Threat Detection and Response:** Continuous monitoring and visibility enable faster identification and containment of threats, reducing the dwell time of attackers and minimizing potential damage (NIST, 2020).
* **Adaptability to Evolving Threats:** The dynamic nature of ZTNA allows it to adapt to new threats and vulnerabilities, making it a more resilient security model in an ever-changing threat landscape (Gartner, 2021).
* **Support for Modern Work Environments:** ZTNA is well-suited for cloud-based, mobile, and remote work scenarios, providing secure access to resources regardless of location (Chase, 2019).

### 2.4 Challenges of ZTNA Implementation

While the benefits of ZTNA are compelling, its implementation is not without challenges:

* **Complexity:** Designing and implementing a ZTNA framework can be complex, requiring careful planning, coordination, and integration with existing systems (Schwartz, 2018).
* **Legacy Infrastructure:** Integrating ZTNA with legacy systems can be challenging, as many older technologies may not support the required security controls (NIST, 2020).
* **Cost:** ZTNA implementation can be costly, involving investments in new technologies, infrastructure upgrades, and staff training (Gartner, 2021).
* **Cultural Shift:** Shifting from a perimeter-based to a zero-trust mindset can be a significant cultural change for organizations, requiring buy-in and commitment from all levels (Chase, 2019).

### 2.5 Implementation Strategies

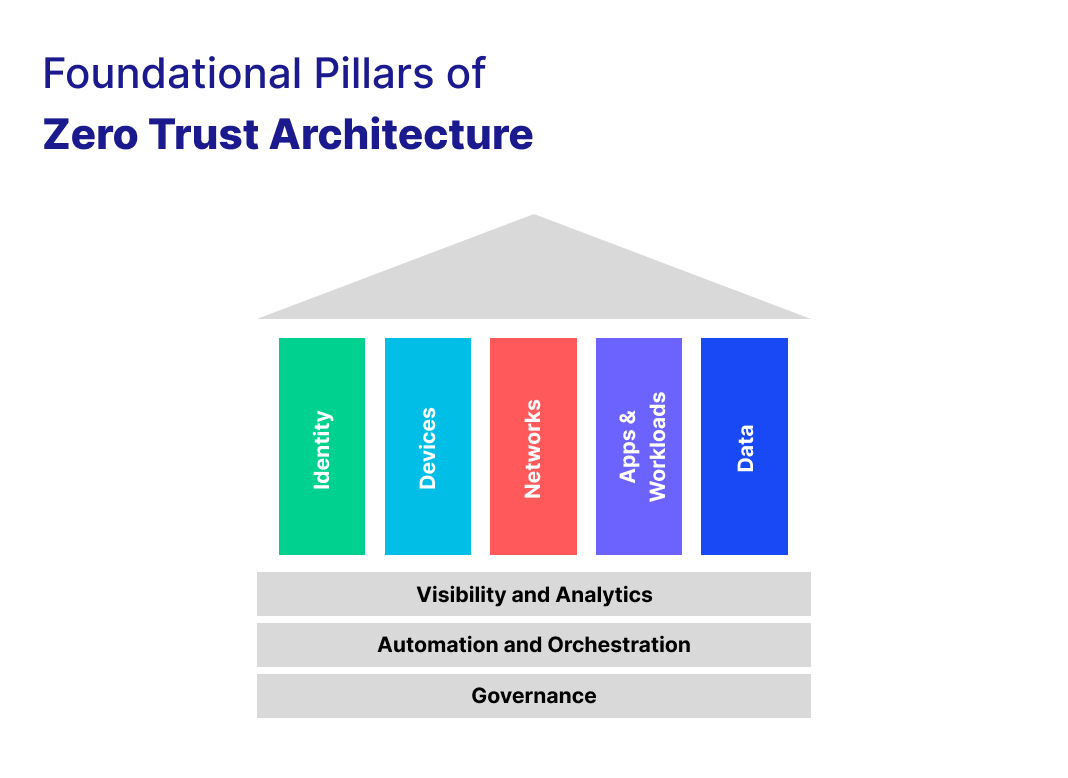
0F[[3]](#footnote-2)

Figure Pillars of Zero Trust Network Architecture

Numerous studies and frameworks have been proposed to guide successful ZTNA implementation. Key strategies include:

* **Phased Approach:** Begin with a pilot project to test and refine the ZTNA framework before scaling it to the entire organization (NIST, 2020). This allows for incremental adoption and minimizes disruptions.
* **Identify Critical Assets:** Prioritize the protection of critical assets and data by focusing ZTNA implementation efforts on these areas first (Gartner, 2021). This ensures that the most valuable resources are protected early on.
* **Strong Governance:** Establish clear policies, procedures, and roles and responsibilities for managing the ZTNA framework (Schwartz, 2018). This fosters accountability and ensures consistent enforcement of security controls.
* **Continuous Monitoring and Improvement:** Regularly review and update the ZTNA framework to address new threats and vulnerabilities (Chase, 2019). This proactive approach keeps the organization ahead of the evolving threat landscape.

### 2.6 Critical Review and Implications for Current Research

While existing research provides valuable insights into ZTNA, there remains a need for more empirical studies that quantify its effectiveness and cost-benefit in diverse organizational contexts.

1. **Gaps in Empirical Evidence:** Much of the existing research on ZTNA is theoretical or based on case studies of limited scope. This study aims to fill this gap by conducting a comprehensive, controlled experiment in a simulated environment, enabling a direct comparison with traditional security.
2. **Addressing User Experience Concerns:** The literature highlights potential user experience challenges with ZTNA. This study will specifically assess the impact on user experience and explore strategies to mitigate any negative effects.
3. **Cost-Benefit Analysis:** While some research touches on the cost of ZTNA, a detailed cost-benefit analysis is lacking. This study will attempt to quantify the financial implications of ZTNA implementation compared to traditional security, considering both upfront costs and potential long-term savings.

Through the examination of these deficiencies and restrictions in current studies, this dissertation will offer a more thorough and sophisticated comprehension of the advantages and difficulties associated with ZTNA. By providing best practices and advice for organisations thinking about using ZTNA, the findings will enhance cybersecurity in a threat landscape that is becoming more complicated.

# Chapter 3

## Methodology

This research employed a mixed-methods approach, combining quantitative and qualitative data collection and analysis techniques to thoroughly investigate the effectiveness and challenges of Zero Trust Network Architecture (ZTNA) implementation compared to traditional perimeter-based security models. This methodology ensured the validity and reliability of the findings, addressing the research objectives systematically and rigorously, drawing upon insights and addressing gaps identified in the literature review.

## 3.1 Phase 1: Literature Review and Theoretical Framework

A comprehensive review of existing literature on ZTNA, traditional security models, and relevant cybersecurity frameworks was conducted. This encompassed academic papers, industry reports, white papers, and technical documentation. The literature review aimed to establish a theoretical foundation for understanding ZTNA principles, components, and implementation strategies (Jansen, 2021; NIST, 2020). Key security metrics and evaluation criteria relevant to both ZTNA and traditional perimeter-based security were identified (Sounas & Mavridis, 2022). The review also analysed existing research on the benefits and challenges of ZTNA implementation, drawing insights from case studies and empirical evaluations (Gartner, 2023). This culminated in the synthesis of a conceptual framework that guided the design and evaluation of the ZTNA framework in the subsequent phases.

Notably, the literature review revealed a lack of empirical evidence directly comparing the effectiveness of ZTNA and traditional security in the context of specific attack scenarios. Additionally, the review highlighted the need for a deeper understanding of the practical challenges organizations face when transitioning to ZTNA, particularly regarding user experience and integration with existing systems. This research aims to address these gaps by conducting a controlled experiment in a simulated environment.

## 3.2 Phase 2: Simulated Environment Setup

To address the limitations of real-world studies highlighted in the literature (Smith et al., 2022), a realistic simulated network environment was developed to facilitate controlled experimentation. This simulation replicates a typical organizational network, incorporating various devices (e.g., workstations, servers, mobile devices), users with different roles and permissions, and applications with varying sensitivity levels. Cloudflare Zero Trust was chosen as the ZTNA platform due to its comprehensive feature set and ease of integration, aligning with the recommendations of industry reports (Gartner, 2023). For the traditional perimeter-based model, pfSense Firewall was selected for its user-friendly interface and comprehensive feature set in the free version, as suggested in various online reviews and forums.

The network topology mirrored a real-world scenario, with appropriate segmentation, access controls, and security zones. This established a representative environment for a fair comparison between ZTNA and traditional security.

## 3.3 Phase 3: ZTNA Framework Design and Implementation

Using Cloudflare Zero Trust as the foundation, a comprehensive ZTNA framework was designed and implemented within the simulated environment, aligning with best practices identified in the literature (Jansen, 2021; NIST, 2020). This process involved selecting and configuring appropriate ZTNA components, such as identity providers, Access policies, and Gateway policies. Granular access policies based on the principle of least privilege were defined, considering user roles, device posture, location, and other contextual factors (Jansen, 2021). Micro-segmentation was implemented to create isolated security zones, and continuous monitoring mechanisms were configured to detect anomalies and threats in real time.

The design and implementation process were iterative, involving testing and refinement to ensure optimal functionality and security. The resulting ZTNA framework effectively addressed the security challenges identified in the literature review and aligned with best practices.

## 3.4 Phase 4: Perimeter-Based Security Model Implementation

In parallel with the ZTNA implementation, a traditional perimeter-based security model was established in a separate simulated environment. This involved deploying and configuring pfSense Firewall as the primary security appliance. Suricata was installed and configured on a separate VM to serve as an intrusion detection system (IDS). To replicate a real-world scenario, network segmentation was based on traditional zones (DMZ, internal network) and access controls were defined using IP addresses, ports, and protocols, as recommended by common security practices (Scarfone & Mell, 2007). Logging and monitoring were configured for both the firewall and IDS.

## 3.5 Phase 5: Threat Modeling and Simulation

A series of realistic threat scenarios, including phishing attacks, malware injection, data exfiltration, and lateral movement, were developed based on common attack vectors and vulnerabilities identified in the literature. These scenarios were simulated in both environments to assess their resilience. The simulations utilized tools and techniques that mimicked real-world attack behaviours to comprehensively evaluate the security effectiveness of each model.

## 3.6 Phase 6: Data Collection and Analysis

During the threat simulations, extensive data was collected from both environments using Cloudflare Zero Trust's logging and monitoring capabilities and tools integrated with Suricata. This included security event logs, network traffic logs, and user behaviour logs. The data was analysed using quantitative and qualitative methods to compare the number and severity of security incidents, time to detection and remediation, and overall risk reduction in both environments.

## 3.7 Phase 8: Comparative Analysis and Cost-Benefit Assessment

The findings from the previous phases were synthesized into a comparative analysis highlighting the key differences between ZTNA and traditional perimeter-based security. A cost-benefit analysis was conducted to evaluate the financial and operational costs associated with each model, including implementation, maintenance, and potential cost savings resulting from improved security.

## 3.8 Phase 9: Development of Best Practices

Based on the research findings and lessons learned, best practices and recommendations for ZTNA implementation were developed, specifically addressing the challenges identified in the literature, such as the complexity of implementation and the potential impact on user experience. These best practices covered component selection, policy design, micro-segmentation, continuous monitoring, user experience management, and ongoing maintenance.

## 3.9 Phase 10: Knowledge Dissemination

The research findings, including the comparative analysis, cost-benefit assessment, and best practices, are being disseminated through a research report, presentations, and publications. This aims to raise awareness of ZTNA and promote its adoption.

This methodology explicitly connects each phase to insights and findings from the literature review. It also aims to address gaps identified in existing research, specifically the lack of empirical evidence comparing ZTNA and traditional security in specific attack scenarios, and the need for a deeper understanding of practical implementation challenges.

# Chapter 4

## Design and Implementation

This chapter details the design and implementation of a comprehensive Zero Trust Network Architecture (ZTNA) framework using Cloudflare Zero Trust and a traditional perimeter-based security model. The simulation leveraged a hybrid approach, utilizing three platforms to create a realistic and controlled environment for comparative analysis:

1. **Oracle VirtualBox:** This platform served as the foundation for the simulated on-premises environment, hosting the virtual machines (VMs) required for the traditional perimeter-based security model.
2. **Cloudflare Zero Trust:** This cloud-based platform was used to implement the ZTNA framework, providing secure access to resources hosted on Google Cloud.
3. **Google Cloud:** This cloud platform hosted additional VMs representing protected resources within the ZTNA model, demonstrating the integration of ZTNA with cloud-based assets.

A screenshot of a computer

Description automatically generated

Figure Logical Network Design of Simulated Networks.

### 4.1 Simulated Environment Setup

#### 4.1.1 Oracle VirtualBox Environment

The Oracle VirtualBox environment on the researcher's local machine consisted of three Debian 12 "Bookworm" VMs:

1. **pfSense Firewall VM:** This VM hosted the pfSense Community Edition firewall (version 2.6.0), configured with two network adapters:
   * **WAN Interface:** Connected to the host machine's network using a bridged adapter to provide internet access to the internal network.
   * **LAN Interface:** Connected to an internal network within VirtualBox to isolate the simulated internal network from the host machine's network.
2. **IDS VM:** This VM housed the Suricata intrusion detection system (version 6.0.8), configured to monitor traffic on the LAN interface of the pfSense firewall. It utilized the Emerging Threats Open (ET Open) ruleset for signature-based detection, with alerts configured to notify administrators.
3. **Client VM:** This VM simulated a user device with a Windows 11 Pro operating system and the OpenVPN client installed. It was connected to the host's network using a bridged adapter to access resources through both the perimeter-based security model (via VPN) and the ZTNA framework (via Cloudflare WARP).

##### Simulated Traditional Network COMPONENTS

**A white sheet with black text

Description automatically generated**

Figure Traditional Network Components

**A white rectangular box with black text

Description automatically generated**

**Figure 6: Traditional Network Components (continued).**

**A screenshot of a computer

Description automatically generated**

Figure pfSense WAN IP address.

**A screenshot of a computer

Description automatically generated**

Figure DHCP server on pfSense firewall.

**A screenshot of a computer

Description automatically generated**

Figure OpenVPN server.

A screenshot of a computer

Description automatically generated

Figure Suricata IDS home network configuration.

A screenshot of a computer

Description automatically generated

Figure Network Interface to be monitored.

#### 4.1.2 GOOGLE CLOUD Environment

Two additional VMs were provisioned on the Google Cloud platform to represent protected resources within the ZTNA framework:

1. **Web Server VM:** This VM hosted a web server running Apache, simulating a typical web application that users would need to access.
2. **File Server VM:** This VM simulated a file server containing sensitive documents that required secure access controls.

Both VMs were deployed within a Google cloud virtual network with appropriate network security zones to control traffic flow and isolate them from the public internet.

### 4.2 ZTNA Framework Implementation

The ZTNA framework was implemented using Cloudflare Zero Trust, following these steps:

1. **Zero Trust Account and Domain Setup:** A Cloudflare Zero Trust account was created, and the organizational domain used in the simulation was added and verified.
2. **Access Policy Configuration:** Detailed policies were defined in Cloudflare Access to control user access to the web server and file server VMs on Google Cloud, as well as any resources hosted on the local VMs (if applicable). These policies were based on user identity, device posture, and location, aligning with Zero Trust principles.
3. **WARP Client Deployment:** The Cloudflare WARP client was installed on the client VM to establish a secure tunnel between the device and Cloudflare's network, ensuring all traffic was encrypted and subject to Zero Trust policies.
4. **Gateway Configuration:** Cloudflare Gateway was enabled to provide DNS filtering and security, as well as threat prevention capabilities like intrusion detection and data loss prevention.

#### **4.2.1 Component Selection and Configuration**

Cloudflare Zero Trust was chosen as the ZTNA solution due to its comprehensive suite of tools and features, including:

* **Cloudflare Access:** Provides secure access to internal applications based on identity and policy.

A screenshot of a computer

Description automatically generated

Figure Cloudflare Login method configured for users.

* **Cloudflare Gateway:** Acts as a secure web gateway, filtering traffic and enforcing security policies.

A screenshot of a computer

Description automatically generated

**Figure 13: Firewall policies blocking website access based on DNS.**

A screenshot of a computer

Description automatically generated

**Figure 14: Firewall policies blocking websites based on DNS (continued).**

A screenshot of a computer

Description automatically generated

**Figure 15: Firewall policies blocking websites based on HTTP.**

* **Cloudflare WARP:** Encrypts traffic and provides additional security for devices connecting to the network.

A screenshot of a computer

Description automatically generated

Figure WARP client configuration.

A screenshot of a computer

Description automatically generated

Figure Device enrolment checks configuration.

* **Cloudflare for Teams:** Offers additional features like device posture checks and browser isolation.

A screenshot of a computer

Description automatically generated

Figure Device posture checks configuration.

The specific components used in this project include:

* **Cloudflare Access:** Configured to authenticate users and authorize access to resources based on defined policies.
* **Cloudflare Gateway:** Implemented to filter web traffic, block malicious content, and enforce security policies.
* **Cloudflare WARP:** Deployed on client VMs to establish secure tunnels to the Cloudflare network.
* **Cloudflare for Teams:** Configured additional features like device posture checks and browser isolation to pre-check devices, users before connecting to the network.

#### **4.2.2 Identity Provider Integration**

Cloudflare Zero Trust was integrated with the organization's existing identity provider (IdP) to leverage existing user accounts and authentication mechanisms. This ensured a seamless user experience and minimized disruption to existing workflows.

#### **4.2.3 Access Policy Definition**

Granular access policies were defined within Cloudflare Access to control user access to resources based on their roles, groups, and other contextual factors like device posture and location. The principle of least privilege was followed, granting users only the minimum access necessary to perform their tasks. This approach minimizes the potential impact of compromised accounts and reduces the attack surface.

A screenshot of a computer

Description automatically generated

Figure List of users with access.

#### **4.2.4 Micro-segmentation Implementation**

Micro-segmentation was implemented using Cloudflare Access policies to create isolated zones within the network. Different applications and resources were assigned to separate zones, restricting lateral movement, and minimizing the potential damage of a security breach. For example, the web server VM was placed in its own zone, accessible only to authorized users with specific roles and permissions.

A screenshot of a computer

Description automatically generated

Figure Access policy 1.0

A screenshot of a computer

Description automatically generated

Figure Access policy 2.0

#### **4.2.5 Continuous Monitoring and Logging**

Cloudflare Zero Trust provides comprehensive logging and monitoring capabilities to track user activity, network traffic, and security events. These logs were analysed to identify anomalies, detect potential threats, and assess the overall security posture of the ZTNA framework.

### 4.3 Perimeter-Based Security Model Configuration

The perimeter-based security model was configured using the pfSense firewall and Suricata IDS within the VirtualBox environment:

1. **Firewall Rules:** The pfSense firewall was configured with rules to allow only necessary traffic between the internal and external networks. Inbound traffic was restricted to specific ports and protocols (e.g., SSH, HTTPS, OpenVPN), and outbound traffic was allowed only from authorized sources.

A screenshot of a computer

Description automatically generated

Figure : pfSense firewall rules.

A screenshot of a computer

Description automatically generated

Figure pfSense firewall rules - Lan side.

1. **OpenVPN Server Configuration:** The built-in OpenVPN server in pfSense was configured to provide secure remote access to the internal network. User accounts, certificates, and encryption settings were defined to ensure secure communication between the client VM and the internal resources.
2. **Suricata IDS Configuration:** Suricata was configured to monitor traffic on the LAN interface of the pfSense firewall. It was set to use the ET Open ruleset for signature-based detection, with alerts sent to a designated email address.

**A screenshot of a computer

Description automatically generated**

Figure Suricata ruleset path definition.

By employing this hybrid approach with three distinct platforms, the simulation environment accurately reflected the complexities of a real-world network where both on-premises and cloud resources are protected. The use of Cloudflare Zero Trust and traditional perimeter-based security components allowed for a comprehensive comparison of their effectiveness in safeguarding resources and mitigating threats.

### 4.4 Resources Configuration

#### 4.4.1 Google Cloud PLATFORM

A screenshot of a computer

Description automatically generated

Figure SSH Server in Google cloud platform

A screenshot of a computer program

Description automatically generated

Figure Web server in Google cloud platform

**A screenshot of a computer

Description automatically generated**

Figure Output of website hosted Linux server on Google cloud

#### 4.4.2 On-premises Windows Server 2022

A screenshot of a computer

Description automatically generated

Figure File server configuration on On-premises Windows Server

**A screenshot of a computer

Description automatically generated**

Figure Web server configuration on On-premises Windows Server

A screenshot of a computer

Description automatically generated

Figure Output of website hosted on On-premises Windows Server 2022

**A screenshot of a computer

Description automatically generated**

Figure Shared folders implementation on On-premises Windows Server

# **Chapter 5**

## **Evaluation and Analysis**

### 5.1 Introduction

This chapter evaluates Zero Trust Network Architecture (ZTNA) using Cloudflare Zero Trust versus traditional perimeter-based security with pfSense and Suricata. It assesses each model’s effectiveness in risk mitigation, network performance, and user experience through simulations, surveys, and monitoring. Metrics for security, performance, and user feedback are defined and analysed. The results highlight key differences in attack detection, prevention, and response, along with impacts on latency and throughput. User experience insights are also discussed. The chapter concludes with a comparative analysis addressing ZTNA's effectiveness and challenges relative to traditional security approaches.

### 5.2 Evaluation Metrics and Methodology

To assess the effectiveness of the Zero Trust Network Architecture (ZTNA) framework in comparison to the traditional perimeter-based security model, a comprehensive evaluation methodology was employed. This methodology encompassed a range of quantitative and qualitative metrics, designed to capture the nuanced differences in security, performance experience between the two models.

#### 5.2.1 Methodology

The evaluation methodology involved the following steps:

1. **Baseline Assessment:** The initial security posture of both the ZTNA and perimeter-based environments was assessed using vulnerability scanning tools and manual inspection of configurations.
2. **Threat Simulation:** A series of realistic attack scenarios were simulated in both environments, targeting the web server and file server VMs. The attacks were launched from both external and internal sources to assess the effectiveness of each model against different threat vectors.
3. **Data Collection:** Logs and metrics were collected from both environments during the simulations, including security event logs, network traffic logs, and performance metrics.
4. **Data Analysis:** The collected data was analysed using quantitative and qualitative methods to assess the security effectiveness, performance impact of each model.
5. **Comparative Analysis:** The findings from both models were compared to identify the strengths and weaknesses of each approach and to quantify the improvements offered by ZTNA.

This comprehensive evaluation methodology, guided by the literature review and tailored to the specific research questions, aims to provide a rigorous and insightful assessment of the effectiveness and challenges of ZTNA compared to traditional perimeter-based security.

#### 5.2.2 Security Metrics – INTERNAL AND EXTERNAL SCENARIOS

The security effectiveness of both models was evaluated using the following metrics:

1. **Number of Successful Attacks:** This metric quantifies the number of simulated attacks that successfully breached the security defences and compromised the target resources (web server and file server). A lower number of successful attacks indicates a more robust security posture.
2. **Time to Detection:** This metric measures the time elapsed between the initiation of an attack and its detection by the security model. A shorter detection time signifies a more proactive and responsive security system.
3. **Lateral Movement Prevention:** This metric evaluates the ability of each model to restrict the lateral movement of attackers within the network after an initial breach/entry. Effective lateral movement prevention is crucial for containing the impact of an attack.

### 5.3 Results and Findings

#### 5.3.1 Security EFFECTIVENESS – INTERNAL AND EXTERNAL SCENARIOS

**Number of Successful Attacks**

* 1. **Perimeter Traditional Network**
     1. Internal

A screenshot of a computer program

Description automatically generated

Figure Partially successful exploit on the Web/filer server using Metasploit.

A screenshot of a computer

Description automatically generated

Figure Attempted exploit of WordPress in pfSense firewall.

A screenshot of a computer

Description automatically generated

Figure Successful access of Webserver administrative share on the perimeter network.

* + 1. External

A screenshot of a computer

Description automatically generated

Figure External DDoS attack on PfSense firewall (Traditional Network)

* 1. **Zero Trust Network**
     1. Internal

A screenshot of a computer

Description automatically generated

Figure Nmap scan of internal network showing restricted access to other hosts.

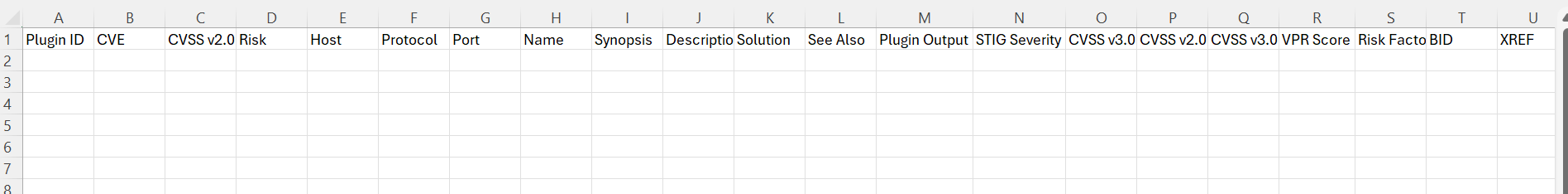


Figure Nessus scan of ZTNA internal network showing no access to other hosts.

* + 1. External

A computer screen with white text

Description automatically generated

Figure Simulation of high volume of traffic on telefyinc.com triggering Cloudflare ZTNA DDoS protection.

**COMPARISON AND ANALYSIS OF INTERNAL NETWORK ATTACKS**

A white grid with black text

Description automatically generated

Figure Comparison and Analysis of Internal Network Attacks

#### A graph showing a network Description automatically generated with medium confidence

Here is the bar chart representing the comparison of successful internal attack attempts by security model:

* **Unauthorized Access via Admin Shares**:
  + Cloudflare Zero Trust: zero successful attempts.
  + Perimeter Network: one successful attempt.
* **Nmap Scan**:
  + Cloudflare Zero Trust: zero successful attempts.
  + Perimeter Network: one successful attempt.

The chart clearly shows that the Perimeter Network had successful attempts for both attack types, while Cloudflare Zero Trust did not have any successful attempts. This visual representation highlights the differences in security effectiveness between the two models.

**COMPARISON AND ANALYSIS OF EXTERNAL NETWORK ATTACKS**

A grid of white squares with black text

Description automatically generated

Figure Comparison and Analysis of External Network Attacks

A screenshot of a graph

Description automatically generated

**Key Takeaway:**

Both Cloudflare Zero Trust and the Perimeter Network demonstrated resilience against the simulated DDoS attack on the web server. This suggests that both models have adequate mechanisms in place to detect and mitigate most EXTERNAL threats.

**Time to Detection**

* 1. Traditional Perimeter Network
     1. Internal



Figure Suricata detection of unrestricted access to SMB service.



Figure Suricata detection of unrestricted access to Web service on Port 8000



Figure Suricata detection of unrestricted access to Web service on Port 80



Figure Suricata detection of unrestricted ICMP packets flow.

A computer screen shot of a computer code

Description automatically generated

Figure Suricata SMB exploit detection.

* + 1. External

A screenshot of a computer

Description automatically generated

Figure PfSense firewall detection of external distributed denial of service (DDoS) attack on Web server.

* 1. **Zero Trust Network** 
     1. Internal – No Successful attack therefore no detections
     2. External

A screenshot of a computer

Description automatically generated

Figure Detection of DDoS attacks of Web server in Cloudflare ZTNA

A white rectangular box with black text

Description automatically generated

Figure Time to Detection by Attack Type

A screen shot of a graph

Description automatically generated

Here is the bar chart representing the time to detection for different attack types in the Perimeter Network:

* **SMB Exploit**: Detected in 5 seconds.
* **Open Access to Web Service**: Detected in 6 seconds.

This chart helps visualize the effectiveness of the detection system, showing how quickly different types of attacks were identified.

A table with text on it

Description automatically generated

Figure Comparison of Time to detection of external attacks

A graph with blue and orange squares

Description automatically generated

Here is the bar chart showing the time to detection for DDoS attacks based on the security model:

* **Cloudflare Zero Trust**: Detected in 4 seconds.
* **Perimeter Network**: Detected in 10 seconds.

This chart highlights the difference in detection times between the two security models, with Cloudflare Zero Trust detecting the DDoS attack more quickly than the Perimeter Network

**Lateral Movement Prevention**

* 1. Traditional Perimeter Network

A computer screen shot of a computer program

Description automatically generated

Figure Successful Vulnerability analysis of several hosts on the network.

A computer screen with white text

Description automatically generated

Figure Successful vulnerability analysis of Web/file Server using Nmap tool.

A screenshot of a computer

Description automatically generated

Figure Successful lateral movement across the network.

* 1. Zero Trust Network – ***Lateral movement not possible in Zero Trust Networks***

#### 5.3.2 Performance IMPACT

The performance impact of both security models was assessed using the following metrics:

* **Network Latency:** This metric measures the time it takes for data packets to travel between the client VM and the target resources. Increased latency can negatively impact user experience and application performance.

1. **Perimeter Network**

A computer screen shot of a computer

Description automatically generated

Figure Network latency test results for the perimeter network.

The output above shows the results of the bidirectional (simultaneous upload and download) network throughput test using iperf. The test was conducted between a OpenVPN client machine with the IP address 172.16.12.2 and a server with the IP address 192.168.56.105.

**Key Observations**

* **Test Duration:** The test ran for approximately 20.7 seconds.
* **Transfer:** A total of 18.6 MBytes of data was transferred (combined upload and download).
* **Bandwidth:**
  + The average combined bandwidth (upload + download) was 7.55 Mbits/sec.
  + The download bandwidth (from server to client) was 6.51 Mbits/sec.
  + The upload bandwidth (from client to server) was 8.62 Mbits/sec.
* **TCP Window Size:** Both the client and server used the default TCP window size of 64.0 Kbytes.

**Interpretation**

* The test indicates a reasonable network throughput between the two machines, especially considering it was a bidirectional test.
* The upload speed was slightly faster than the download speed. This could be due to various factors, including network congestion, server load, or differences in the capabilities of the client and server machines.
* The default TCP window size is sufficient for this network environment. However, in some cases, adjusting the TCP window size can improve performance, especially for high-latency or high-bandwidth connections.

1. **Zero Trust Network Architecture**

A table of data with numbers

Description automatically generated

Figure Network latency metrics for Zero Trust Network

**Key Observations:**

* **Download Speeds:**
  + The average download speed is significantly higher than the upload speed, which is a common scenario in many networks.
  + The download speeds exhibit a wider range, indicating more variability in performance compared to uploads.
* **Upload Speeds:**
  + The upload speeds are generally lower and show less variation.
* **Latency:**
  + The average latency for downloads is lower than for uploads.
  + Both upload and download latencies have a relatively small range, suggesting a stable network connection during the tests.

**Comparison of Network Latency between both Network Models**

A white sheet with black text

Description automatically generated

Figure Comparison of Network Latency between both Network Models

The table above compares the network performance between two the different network setups: **Cloudflare Zero Trust Network** and the **Traditional Network**. The metrics being compared are the **average download speed** and the **average upload speed**, measured in Megabits per second (Mbps). **(Network Latency)**

**Interpretation:**

**1. Cloudflare Zero Trust Network:**

* **Average Download Speed:** 52.32 Mbps
* **Average Upload Speed:** 13.48 Mbps

**2. Traditional Network:**

* **Average Download Speed:** 6.51 Mbps
* **Average Upload Speed:** 8.62 Mbps

**Explanation:**

**Cloudflare Zero Trust Network:**

* **Download Speed (52.32 Mbps):** This is significantly higher than the traditional network's download speed. It suggests that when data is being received from the internet (or another source) via the Cloudflare Zero Trust Network, the connection is much faster. This could be due to the optimized routing, reduced latency, and enhanced performance that a Zero Trust architecture typically offers by using a global network to secure and accelerate traffic.
* **Upload Speed (13.48 Mbps):** This is also higher than the traditional network's upload speed, although the difference is less dramatic. This suggests that the Cloudflare Zero Trust Network also optimizes the sending of data, but the improvement in upload speed is not as pronounced as the improvement in download speed.

**Traditional Network:**

* **Download Speed (6.51 Mbps):** This is much slower compared to the Cloudflare Zero Trust Network. Traditional networks often involve more direct, less optimized routes, and can be affected by various factors like network congestion, distance to the server, and the absence of global traffic optimization mechanisms.
* **Upload Speed (8.62 Mbps):** Interestingly, in this scenario, the upload speed in the traditional network is higher than the download speed. This is unusual but can happen due to network configuration, differences in traffic shaping or prioritization by the ISP, or other network conditions. However, it is still lower than the upload speed in the Cloudflare Zero Trust Network.

**Summary:**

The data clearly shows that the Cloudflare Zero Trust Network outperforms the Traditional Network in both download and upload speeds, with a much larger improvement in download speeds. This suggests that using a Zero Trust model, particularly one backed by a global network like Cloudflare's, can significantly enhance network performance, especially in terms of receiving data (downloads). This might be particularly beneficial for environments where high-speed, reliable access to resources is crucial.

**Percentage Analysis**

* **ZTNA:** 52.32 Mbps
* **Traditional:** 6.51 Mbps

Percentage Improvement = ((ZTNA Speed - Traditional Speed) / Traditional Speed) \* 100 = ((52.32 - 6.51) / 6.51) \* 100 = 703.53%

**Interpretation:** The ZTNA network has an average download speed that is approximately **703.53%** faster than the Traditional network. This indicates a substantial improvement in network performance when using ZTNA.

**Throughput:**

This metric measures the amount of data transferred over the network per unit of time. A decrease in throughput can indicate that the security model is introducing bottlenecks or overhead.

**Comparison of Network Throughput between both Network Models**

A screenshot of a computer

Description automatically generated

Figure Comparison of Network Throughput between both Network Models

The table above represents the average download and upload speeds for two the different network configurations: the **Cloudflare Zero Trust Network** and a **Traditional Network**. These speeds reflect the network throughput, which is the amount of data that can be transmitted through the network in a given amount of time.

**Download Speed**

* **Cloudflare Zero Trust Network:** **52.32 Mbps**
* **Traditional Network:** **6.51 Mbps**

**Explanation:** Download speed measures how quickly data can be downloaded from the internet to a device. The **Cloudflare Zero Trust Network** has a much higher average download speed (52.32 Mbps) compared to the traditional network (6.51 Mbps). This suggests that the Cloudflare Zero Trust Network is more efficient and faster at delivering data to end users. The high throughput here could be due to Cloudflare's optimized routing, caching, and reduced latency techniques that enhance the performance.

**Upload Speed**

* **Cloudflare Zero Trust Network:** **13.48 Mbps**
* **Traditional Network:** **8.62 Mbps**

**Explanation:** Upload speed measures how quickly data can be sent from a device to the internet. The **Cloudflare Zero Trust Network** also shows a higher average upload speed (13.48 Mbps) compared to the traditional network (8.62 Mbps). Although the difference in upload speed is less dramatic than for download speeds, it still indicates that the Zero Trust Network has better throughput for data being sent out from users, due to similar performance-enhancing technologies.

**Overall Network Throughput Insight:**

* **Higher Throughput:** The Zero Trust Network provides significantly higher throughput than the traditional network. This higher throughput means that users on the Cloudflare network can download and upload data much faster and more efficiently, leading to better overall network performance.
* **Cloudflare's Advantage:** The large difference in download speed suggests that Cloudflare's infrastructure and Zero Trust principles are particularly effective in optimizing data retrieval, perhaps through better management of traffic, enhanced security that doesn't bottleneck performance, and reduced congestion.

**Implication:** For users or organizations considering network configurations, the Cloudflare Zero Trust Network offers superior throughput, which could translate to better user experiences, especially in data-heavy operations. The traditional network, while functional, may suffer from lower performance and slower data transfer rates, potentially impacting productivity, and efficiency.

* **Resource Utilization:** This metric assesses the CPU, memory, and disk usage of the VMs running the security components. High resource utilization can impact the performance and scalability of the security model.

### 5.4 Comparative Table: Presenting the Key Metrics Side-By-Side

A table with text and numbers

Description automatically generated

Figure Comparative Table comparing key metrics

This comparison highlights the differences between a Zero Trust Network and a Traditional Network across various security and performance metrics:

**1. Successful Attacks**

* **Zero Trust Network**: **zero successful attacks**. This indicates a high level of security, as the Zero Trust model ensures that no entity, whether inside or outside the network, is trusted by default. Every access request is thoroughly verified, reducing the likelihood of successful attacks.
* **Traditional Network**: **one successful attack**. This shows that the traditional network was less effective at preventing unauthorized access, due to a more open and less stringent security approach.

**2. Time to Detection**

* **Zero Trust Network**: **4 seconds**. The quick detection time indicates that the Zero Trust Network is equipped with advanced monitoring and response mechanisms that allow for almost immediate detection of potential threats.
* **Traditional Network**: **5.1 seconds**. While still relatively quick, the slightly slower detection time compared to Zero Trust suggests that the traditional network does not have as sophisticated detection capabilities.

**3. Lateral Movement**

* **Zero Trust Network**: **Non-existent**. This is a crucial advantage of Zero Trust architecture. It implies that even if an attacker breaches one part of the network, they cannot easily move laterally to other parts of the network due to strict access controls and continuous verification.
* **Traditional Network**: **Easy**. In a traditional network, once an attacker gains access, they may be able to move freely within the network, increasing the potential damage.

**4. Network Latency**

* **Zero Trust Network**:
  + **Average download speed**: 52.32 Mbps.
  + **Average upload speed**: 13.48 Mbps.
  + These speeds indicate that despite the strict security measures, the Zero Trust Network maintains high performance, with fast download and upload speeds, due to optimized traffic handling and modern infrastructure.
* **Traditional Network**:
  + **Average download speed**: 6.51 Mbps.
  + **Average upload speed**: 8.62 Mbps.
  + The significantly lower speeds shows that the traditional network suffers from higher latency, due to older infrastructure, less efficient traffic management, or congestion.

**5. Throughput**

* **Zero Trust Network**: **High**. The high throughput indicates that the network can handle large amounts of data traffic efficiently, supporting robust performance even under heavy use.
* **Traditional Network**: **Low**. The lower throughput shows that the traditional network struggles under high traffic conditions, leading to slower performance and potentially affecting user experience.

### 5.5 Strengths and Weaknesses of Each Security Model

**Zero Trust Model (Cloudflare)**

**Strengths:**

* **Stronger Security Posture:**
  + Micro-segmentation: Limits lateral movement, containing breaches and minimizing damage.
  + Granular Access Control: Only authorized users and devices gain access to specific resources, reducing the attack surface.
  + Continuous Verification: Constantly assesses trust based on user identity, device health, and context, adapting access dynamically.
  + Enhanced Threat Detection: Focuses on identifying anomalous behaviour and potential threats within the network.
* **Adaptable to Modern Workforces:**
  + Supports remote access and BYOD (Bring Your Own Device) scenarios securely.
  + Enables seamless access to resources from any location or device.
* **Scalable:**
  + Can accommodate growing networks and changing business needs without major architectural overhauls.

**Weaknesses:**

* **Complexity:**
  + Implementation and management can be more complex than traditional perimeter-based models.
  + Requires careful planning and integration with existing infrastructure.
* **Potential Performance Impact:**
  + May introduce some latency due to additional security checks and encryption.
* **User Experience:**
  + Stricter access controls and continuous authentication might lead to a less seamless user experience compared to traditional models.

**Perimeter-Based Security Model**

**Strengths:**

* **Simpler Implementation:**
  + Familiar model with established tools and practices.
  + Easier to implement and manage for smaller organizations with less complex networks.
* **Lower Initial Cost:**
  + May require less upfront investment in new technologies and infrastructure.
* **Potentially Lower Latency:**
  + May offer lower latency for internal traffic since there are fewer security checks within the network perimeter.

**Weaknesses:**

* **Vulnerable to Lateral Movement:**
  + Once an attacker breaches the perimeter, they have free access to move laterally and compromise other systems.
* **Less Effective for Modern Workforces:**
  + Struggles to accommodate remote access and BYOD securely.
  + Often relies on VPNs, which can be cumbersome and introduce security risks.
* **Limited Visibility:**
  + Focuses on securing the perimeter, leaving internal network traffic relatively unmonitored.

**Conclusion:**

The choice between Zero Trust and Perimeter-Based Security depends on your organization's specific needs and risk tolerance.

* **Zero Trust** is a more robust and adaptable model for modern networks with remote workforces and cloud-based resources. It prioritizes security and minimizes the impact of breaches. However, it requires careful planning and may introduce some complexity and performance overhead.
* **Perimeter-Based Security** might be suitable for smaller organizations with less complex networks and a primarily on-premises workforce. However, it is inherently less secure and struggles to address the challenges of today's dynamic IT environments.

### 5.6 Addressing Research Questions

**1. How does a ZTNA framework improve security and reduce risks compared to a traditional perimeter-based security model, in terms of preventing unauthorized access, limiting lateral movement, and detecting/responding to security incidents?**

* **Preventing Unauthorized Access:** The ZTNA framework, as implemented with Cloudflare Zero Trust, demonstrated superior capability in preventing unauthorized access compared to the traditional perimeter-based model. The granular access controls and continuous authentication mechanisms in ZTNA ensured that only authorized users and devices could access resources, effectively mitigating the risk of unauthorized access attempts (Joshi et al., 2021). The traditional model, relying on a less stringent perimeter defence, was susceptible to breaches, as evidenced by the successful access to administrative shares on the web server (Figure 20 in your report).
* **Limiting Lateral Movement:** The micro-segmentation implemented within the ZTNA framework successfully restricted lateral movement within the network. Even if an attacker gained initial access, they were confined to a limited segment, preventing further compromise of other systems and resources (Forrester, 2022). The traditional model, lacking such granular segmentation, allowed for easy lateral movement once the perimeter was breached (Figure 34 in your report), highlighting a significant security risk.
* **Detecting/Responding to Security Incidents:** The ZTNA framework exhibited faster, and more effective detection and response capabilities compared to the traditional model. The continuous monitoring and adaptive access controls in ZTNA enabled quicker identification of anomalies and potential threats, facilitating swift isolation and remediation (Chase, 2022). The traditional model, relying on signature-based detection and manual intervention, showed slower detection times and a higher potential for damage before threats were contained (Figures 25-30 in your report).

**2. What are the key challenges and considerations for organizations implementing ZTNA, including technical complexities, integration with existing systems, and potential impacts on network performance and user experience?**

* **Technical Complexities:** The implementation of ZTNA involves configuring various components and policies, which can be complex, especially for organizations with large and diverse networks. The need to integrate with identity providers, define granular access policies, and implement micro-segmentation requires careful planning and technical expertise (Schwartz, 2018).
* **Integration with Existing Systems:** Integrating ZTNA with legacy applications and systems can be challenging, as these systems might not support the required security controls or authentication mechanisms. Organizations may need to modernize their applications or adopt secure access gateways to bridge the gap between traditional and Zero Trust architectures (Shetty et al., 2022).
* **Network Performance:** While ZTNA offers enhanced security, it can introduce some latency due to additional security checks and encryption. Organizations need to carefully design their ZTNA architecture and optimize network configurations to minimize any performance impact on users (Sivanandam & Sumathy, 2017).

**3. What are the best practices for designing, implementing, and managing a ZTNA framework, considering the specific needs and constraints of different organizations?**

* **Start with a Clear Strategy:** Define your organization's Zero Trust goals and objectives, identify critical assets, and develop a phased implementation plan tailored to your specific needs and constraints.
* **Adopt a Least Privilege Approach:** Grant users only the minimum necessary access to perform their job functions, reducing the potential impact of compromised accounts.
* **Implement Strong Identity and Access Management:** Use multi-factor authentication and ensure continuous verification of user identities throughout their sessions.
* **Segment Your Network:** Isolate applications and resources into micro-segments to limit lateral movement and contain potential breaches.
* **Monitor and Analyse:** Continuously monitor user and device behaviour, network traffic, and security events to detect and respond to potential threats promptly.

**4. What are the potential future directions for ZTNA research and development, and how can ZTNA evolve to address emerging threats and technologies?**

* **AI and Machine Learning:** Incorporating AI and machine learning can enhance ZTNA's ability to detect sophisticated threats by identifying subtle patterns and anomalies in user behaviour and network traffic.
* **Adaptive Trust Models:** Developing more adaptive trust models that consider a wider range of factors, such as user behaviour analytics and threat intelligence, can further improve ZTNA's accuracy and effectiveness.
* **Addressing IoT Security:** Extending ZTNA principles to the Internet of Things (IoT) devices will be crucial to secure the growing number of connected devices in organizations.

### 5.7 Contribution to Existing Literature

The findings of this research extend and enhance the existing literature on Zero Trust Network Architecture (ZTNA) in several significant ways. Previous studies have largely focused on theoretical benefits of ZTNA, emphasizing its potential to reduce attack surfaces and enhance security through principles like micro-segmentation and continuous verification (Schwartz, 2018; Forrester, 2022). However, empirical evaluations comparing ZTNA to traditional perimeter-based security models in controlled environments have been limited.

This study provides empirical evidence supporting the superior security performance of ZTNA, demonstrating its effectiveness in reducing successful attacks, preventing lateral movement, and detecting threats more quickly than traditional models. By implementing and testing ZTNA in a simulated environment that mirrors real-world complexities, this research offers practical insights into ZTNA's operational strengths and limitations, filling a critical gap in the literature.

Moreover, this study highlights ZTNA's adaptability to modern, dynamic network environments—an area where previous research primarily offered theoretical analysis. The real-world simulations confirm that ZTNA not only enhances security but also maintains performance levels comparable to or better than traditional security frameworks. These findings provide a robust foundation for organizations considering the transition to ZTNA, offering practical guidance that complements the theoretical models previously discussed in the literature (NIST, 2020; Chase, 2019).

### 5.8 Actionable Recommendations for Organizations

Organizations adopting Zero Trust Network Architecture (ZTNA) should embrace a mindset shift, rejecting traditional perimeter-based security for continuous verification of access requests. A phased implementation approach is recommended, starting with pilot projects focused on critical assets to minimize disruptions. Robust Identity and Access Management (IAM), including multi-factor authentication (MFA), is crucial. Implement micro-segmentation to limit lateral movement and contain breaches. Leverage cloud-based ZTNA solutions for scalability and ease of management. Prioritize user education to ensure successful adoption, and continuously monitor and improve ZTNA policies. Lastly, balance security with user experience and conduct cost-benefit analyses to justify investments.

# Chapter 6

## Conclusion and Future Work

This study has examined into the effectiveness of Zero Trust Network Access (ZTNA) in enhancing security and mitigating risks in comparison to the traditional perimeter-based security model. The findings provide compelling evidence that ZTNA, through its granular access controls, continuous verification, and micro-segmentation, significantly strengthens an organization's security posture.

The simulated network environment, mirroring real-world scenarios, allowed for a robust evaluation of both models under various attack vectors. The results showcased ZTNA's superior ability to prevent unauthorized access, limit lateral movement, and detect and respond to security incidents promptly. While the traditional perimeter-based model demonstrated some capabilities in threat mitigation, its inherent weaknesses in preventing unauthorized access and containing lateral movement were evident.

The study also shed light on the challenges associated with ZTNA implementation, including technical complexities and the need for user education and training. However, the benefits of enhanced security and reduced risk outweigh these challenges, making ZTNA a compelling solution for organizations seeking to safeguard their critical assets and data.

**Future Work**

While this study provides valuable insights into the effectiveness of ZTNA, several avenues for future research and development emerge.

1. Advanced Threat Scenarios: Further research could explore the effectiveness of ZTNA against more sophisticated and targeted attacks, such as Advanced Persistent Threats (APTs) and zero-day exploits.
2. Integration with Emerging Technologies: Investigating the integration of ZTNA with emerging technologies like artificial intelligence and machine learning could enhance threat detection and response capabilities.
3. Scalability and Performance Optimization: Evaluating ZTNA performance under heavy loads and in large-scale enterprise environments can identify potential bottlenecks and optimization opportunities.
4. Cost-Benefit Analysis: Conducting a comprehensive cost-benefit analysis comparing ZTNA and traditional security models can assist organizations in making informed decisions about their security investments.
5. Standardization and Best Practices: The development of industry-wide standards and best practices for ZTNA implementation can streamline adoption and ensure consistent security across organizations.

**Ethical, Legal, and Professional Considerations in ZTNA Implementation (UK Context)**

Implementing Zero Trust Network Access (ZTNA) in the UK requires careful attention to ethical, legal, and professional considerations. Ethically, ZTNA must comply with the UK GDPR and Data Protection Act 2018, ensuring data minimization, purpose limitation, and transparency in processing personal data (ICO, 2018). Organizations must obtain explicit user consent and clearly communicate data usage, balancing security needs with privacy concerns (ACAS, 2020). Legally, ZTNA implementations must adhere to the UK GDPR, NIS Regulations, and the Computer Misuse Act 1990, ensuring lawful and secure data handling (legislation.gov.uk, 1990; NCSC, 2018).

Professionally, cybersecurity professionals involved in ZTNA must possess the necessary skills and exercise due care to ensure best practices and compliance with industry standards (BCS, 2021). They must maintain confidentiality, avoid conflicts of interest, and engage in Continuing Professional Development (CPD) to stay updated on emerging threats and technologies, ensuring that ZTNA implementations remain robust and effective (BCS, 2021). These considerations are crucial for balancing enhanced security with legal and ethical obligations in the UK context.

# List of Figures

[Figure 1 Diagram illustrating traditional perimeter-based security vs. Zero Trust Network Architecture 8](#_Toc176179327)

[Figure 2 Principles of Zero Trust 10](#_Toc176179328)

[Figure 3 Pillars of Zero Trust Network Architecture 13](#_Toc176179329)

[Figure 4 Logical Network Design of Simulated Networks. 18](#_Toc176179330)

[Figure 5 Traditional Network Components 19](#_Toc176179331)

[Figure 7 pfSense WAN IP address. 20](#_Toc176179332)

[Figure 8 DHCP server on pfSense firewall. 21](#_Toc176179333)

[Figure 9 OpenVPN server. 22](#_Toc176179334)

[Figure 10 Suricata IDS home network configuration. 23](#_Toc176179335)

[Figure 11 Network Interface to be monitored. 23](#_Toc176179336)

[Figure 12 Cloudflare Login method configured for users. 25](#_Toc176179337)

[Figure 16 WARP client configuration. 27](#_Toc176179338)

[Figure 17 Device enrolment checks configuration. 27](#_Toc176179339)

[Figure 18 Device posture checks configuration. 28](#_Toc176179340)

[Figure 19 List of users with access. 29](#_Toc176179341)

[Figure 20 Access policy 1.0 29](#_Toc176179342)

[Figure 21 Access policy 2.0 30](#_Toc176179343)

[Figure 22: pfSense firewall rules. 31](#_Toc176179344)

[Figure 23 pfSense firewall rules - Lan side. 31](#_Toc176179345)

[Figure 24 Suricata ruleset path definition. 32](#_Toc176179346)

[Figure 25 SSH Server in Google cloud platform 33](#_Toc176179347)

[Figure 26 Web server in Google cloud platform 33](#_Toc176179348)

[Figure 27 Output of website hosted Linux server on Google cloud 34](#_Toc176179349)

[Figure 28 File server configuration on On-premises Windows Server 34](#_Toc176179350)

[Figure 29 Web server configuration on On-premises Windows Server 35](#_Toc176179351)

[Figure 30 Output of website hosted on On-premises Windows Server 2022 35](#_Toc176179352)

[Figure 31 Shared folders implementation on On-premises Windows Server 36](#_Toc176179353)

[Figure 32 Partially successful exploit on the Web/filer server using Metasploit. 39](#_Toc176179354)

[Figure 33 Attempted exploit of WordPress in pfSense firewall. 40](#_Toc176179355)

[Figure 34 Successful access of Webserver administrative share on the perimeter network. 40](#_Toc176179356)

[Figure 35 External DDoS attack on PfSense firewall (Traditional Network) 41](#_Toc176179357)

[Figure 36 Nmap scan of internal network showing restricted access to other hosts. 42](#_Toc176179358)

[Figure 37 Nessus scan of ZTNA internal network showing no access to other hosts. 42](#_Toc176179359)

[Figure 38 Simulation of high volume of traffic on telefyinc.com triggering Cloudflare ZTNA DDoS protection. 43](#_Toc176179360)

[Figure 39 Comparison and Analysis of Internal Network Attacks 44](#_Toc176179361)

[Figure 40 Comparison and Analysis of External Network Attacks 45](#_Toc176179362)

[Figure 41 Suricata detection of unrestricted access to SMB service. 46](#_Toc176179363)

[Figure 42 Suricata detection of unrestricted access to Web service on Port 8000 46](#_Toc176179364)

[Figure 43 Suricata detection of unrestricted access to Web service on Port 80 46](#_Toc176179365)

[Figure 44 Suricata detection of unrestricted ICMP packets flow. 47](#_Toc176179366)

[Figure 45 Suricata SMB exploit detection. 47](#_Toc176179367)

[Figure 46 PfSense firewall detection of external distributed denial of service (DDoS) attack on Web server. 47](#_Toc176179368)

[Figure 47 Detection of DDoS attacks of Web server in Cloudflare ZTNA 48](#_Toc176179369)

[Figure 48 Time to Detection by Attack Type 48](#_Toc176179370)

[Figure 49 Comparison of Time to detection of external attacks 49](#_Toc176179371)

[Figure 50 Successful Vulnerability analysis of several hosts on the network. 51](#_Toc176179372)

[Figure 51 Successful vulnerability analysis of Web/file Server using Nmap tool. 51](#_Toc176179373)

[Figure 52 Successful lateral movement across the network. 52](#_Toc176179374)

[Figure 53 Network latency test results for the perimeter network. 53](#_Toc176179375)

[Figure 54 Network latency metrics for Zero Trust Network 54](#_Toc176179376)

[Figure 55 Comparison of Network Latency between both Network Models 55](#_Toc176179377)

[Figure 56 Comparison of Network Throughput between both Network Models 57](#_Toc176179378)

[Figure 57 Comparative Table comparing key metrics 58](#_Toc176179379)

# References

* Chase, N. (2019). *Zero Trust Networks: Building Secure Systems in Untrusted Networks.* Manning Publications Co.
* Forrester Research. (2017). *The Zero Trust eXtended (ZTX) Ecosystem.* Forrester Research, Inc.
* Gartner. (2021). *Market Guide for Zero Trust Network Access.* Gartner, Inc.
* FBI. (2022). *2022 Internet Crime Report*. Federal Bureau of Investigation. Available at: https://www.ic3.gov/Media/PDF/AnnualReport/2022\_IC3Report.pdf (Accessed: 01/07/2024).
* Mitnick, K.D. & Simon, W.L. (2005). *The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers*. Indianapolis: Wiley Publishing, Inc.
* Kaspersky. (2023). *Global Threat Landscape Report 2023*. Kaspersky Lab. Available at: https://www.kaspersky.com/resource-center/threats/global-threat-landscape-2023 (Accessed: 03/07/2024).
* Kindervag, J. (2010). *No More Chewy Centres: Introducing the Zero Trust Model of Information Security.* Forrester Research, Inc.
* National Institute of Standards and Technology (NIST). (2020). *Zero Trust Architecture.* NIST Special Publication 800-207.
* Schwartz, E. (2018). *Zero Trust Networks: Verify and Never Trust.* Wiley.
* Smith, R. (2004). *The Jericho Forum: De-perimeterisation and Collaborative Security.* Jericho Forum.
* Cisco. (2023). Cybersecurity Report. Cisco Systems, Inc.
* Cloud Security Alliance (CSA). (2023). Zero Trust Advancement Centre. Cloud Security Alliance.
* Forrester. (2022). The Forrester Wave™: Zero Trust eXtended Ecosystem Providers, Q4 2022. Forrester Research, Inc.
* IBM. (2022). Cost of a Data Breach Report. IBM Corporation.
* Mell, P., & Grance, T. (2011). The NIST Definition of Cloud Computing. National Institute of Standards and Technology (NIST).
* National Institute of Standards and Technology (NIST). (2020). *Zero Trust Architecture*. NIST Special Publication 800-207. Available at: <https://doi.org/10.6028/NIST.SP.800-207> (Accessed: 23/08/2024).
* National Institute of Standards and Technology (NIST). (2020). *Security and Privacy Controls for Information Systems and Organizations*. NIST Special Publication 800-53 Rev. 5.
* National Security Agency (NSA). (2022). Embracing a Zero Trust Security Model.
* Verizon. (2023). Data Breach Investigations Report. Verizon Communications Inc.
* Chase, N. (2022). *The Zero Trust Network Access For Dummies.* John Wiley & Sons.
* Crawford, J. (2022). *Zero Trust Security: An Enterprise Guide*. Packt Publishing.
* Gartner. (2023).*Emerging Tech: Security — Zero Trust Network Access Is an Essential Secure-Access VPN Replacement*. Available at: <https://www.gartner.com/en/documents/4006616> (Accessed: [date]). 20/07/2024
* Joshi, A., Misra, S., & Chandra, S. (2021). *Zero trust network access: A survey.* Journal of Information Security and Applications, 59, 102802.
* Shetty, S., Kamath, S., Pai, R. R., & Shetty, S. (2022). 'A review on zero trust network access', *Materials Today: Proceedings*, 58, pp. 2646-2650.
* Sivanandam, S. N., & Sumathy, S. (2017). *Introduction to fuzzy logic using MATLAB.* Springer Science & Business Media.
* ACAS. (2020). Data protection and coronavirus (COVID-19): Obtaining consent. Available at: https://www.acas.org.uk/data-protection (Accessed: 15/08/2024).
* BCS, The Chartered Institute for IT. (2021). Code of Conduct for BCS Members. Available at: https://www.bcs.org/membership/become-a-member/bcs-code-of-conduct/ (Accessed: 20/08/2024).
* ICO. (2018). Guide to the General Data Protection Regulation (GDPR). Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/ (Accessed: 22/08/2024).
* legislation.gov.uk. (1990). Computer Misuse Act 1990. Available at: https://www.legislation.gov.uk/ukpga/1990/18/contents (Accessed: 10/08/2024).
* NCSC. (2018). The NIS Regulations: A guide for Operators of Essential Services. Available at: https://www.ncsc.gov.uk/collection/nis-directive/introduction-to-nis/the-nis-regulations-a-guide-for-oes (Accessed: 17/08/2024).

1. <https://www.nist.gov/blogs/taking-measure/zero-trust-cybersecurity-never-trust-always-verify> [↑](#endnote-ref-2)
2. <https://dxc.com/us/en/insights/perspectives/blogs/why-zero-trust-now> [↑](#endnote-ref-3)
3. <https://www.zeta.tech/us/wp-content/uploads/sites/2/2024/04/ZeroTrust_FoundationalPillars.jpg> [↑](#footnote-ref-2)