

COMP8260 Advanced System and Network Security

**Zero Trust Network Architecture:**

**Strategies for Enhanced Network Security and Access Control**

Reza Pakravan

Abhijith Ajith Nair

Omavinash Bangale

# 

# 

[**Introduction**](#_uxa37khc61xy) **2**

[**Traditional Network Security Models and Challenges**](#_m1ckidozqx9s) **3**

[Castle-and-Moat Model](#_ifwklbbp27im) 3

[VPN-Based Remote Access](#_ba58oqzhom4) 3

[Network Segmentation only](#_v5oji8lhtdwh) 4

[Insider Threats](#_cf6zoefwhons) 5

[Over-reliance on Firewalls and VPNs](#_cgbdiibc6hxm) 5

[**Real world scenarios with data breach**](#_kef8zo69p4lw) **5**

[**Introduction to Zero Trust Networking**](#_tdywaosuf6pk) **6**

[Core Components of Zero Trust Architecture](#_8jzew1wdks4g) 6

[Zero Trust for Cloud and Hybrid Environments](#_eweo95oi2ul9) 8

[Implementation and Case Studies](#_qd5bbojk32dn) 9

[Case Studies of ZTNA](#_mjqr05dx9o) 9

[Challenges and Future Trends](#_qtxyry90gbn8) 9

[Future Trends of Zero Trust](#_hr233ho0n154) 9

[Challenges in Implementing ZTNA](#_i3wgbrwsdl9q) 10

[**Appendix**](#_3et30gtbaaus) **11**

# 

# 

# Introduction

Nowadays Cloud Computing is becoming dominant in the real-world digital landscape, and the traditional networking models cannot provide the best solutions for the cybersecurity concerns and challenges.

In traditional networking, it relies on edge network devices like Firewalls and VPN. The assumption is we keep the indoor secure and all the threats are sitting outside of our network.

In the world of Cloud Computing with users working remotely, connecting to the network with mobile devices, we don’t have clear boundaries in place. There is no inside or outside network.

The Zero Trust concept is based on not trusting anyone or any device in or outside of the network. Always do the verification regardless of the user or device’s location. This project will provide some details about what the Zero Trust Network is and what sections must be taken care of.

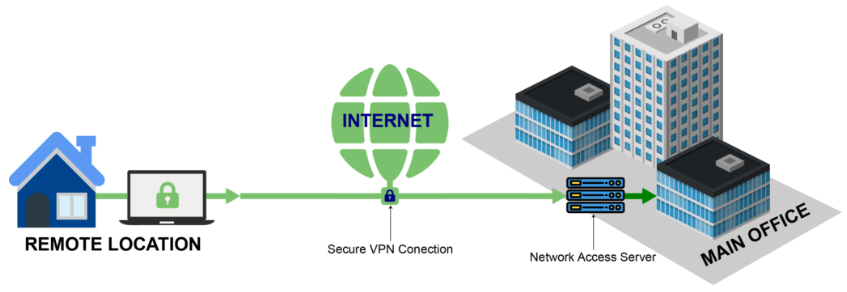
# Traditional Network Security Models and Challenges

## Castle-and-Moat Model

The "castle-and-moat" model is a traditional network security framework where external entities are restricted from accessing internal data, while those within the network are granted broad access. In this analogy, the organisation's network is represented as a castle, with the network perimeter acting as a protective moat, preventing unauthorised external access but allowing unrestricted internal movement.[1]

## VPN-Based Remote Access

A Remote Access Virtual Private Network (VPN) allows individual users to connect to an organisation's network securely from a remote location. This connection is established via the Internet using a computer or other compatible devices, such as those running iOS or Android operating systems.[3]



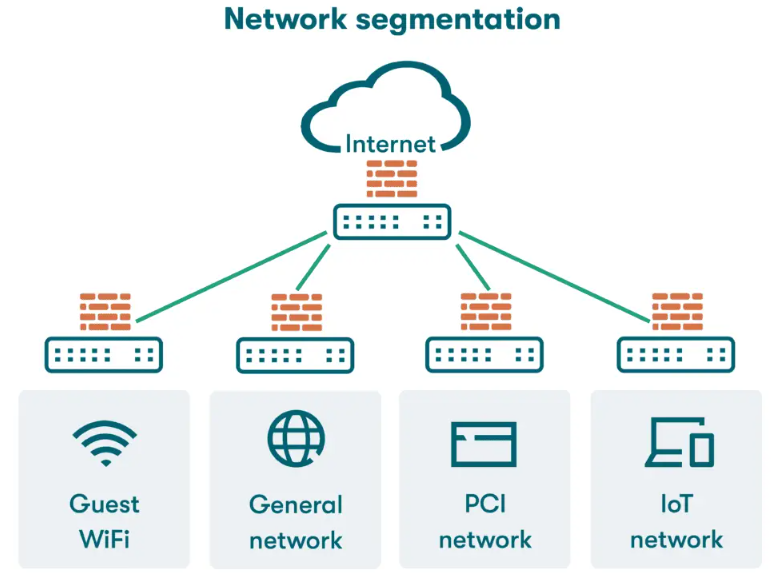
Secure VPN connection

There are a few drawbacks to such an approach:

* **Vulnerability to attack:** A VPN acts as a potential single point of failure for the applications and data it protects. If a device or account is compromised, an attacker could exploit this vulnerability to access the resources secured by the VPN.[1]
* **Slower performance:** Encryption of data is performed in VPN technology, which may introduce latency to the network. The extent of this latency depends on the type of encryption protocol in use, such as IPsec or SSL.[1]
* **Scalability:** VPN servers have finite capacity to handle traffic. As the number of users increases, the server may need to be upgraded to accommodate the additional demand. [1]

## Network Segmentation only

Network segmentation is a design strategy that partitions a larger network range into smaller subnets and each subnet functioning as an independent network. Hence allowing network administrators to regulate the flow of traffic between these subnets through the implementation of granular access control policies.



Network Segmentation

Organisations use segmentation to improve monitoring, boost performance, localise technical issues and most importantly enhance security.[2]

Network segmentation is to control access and stop attacks from spreading. This improves security by reducing the areas attackers can reach.

## Insider Threats

Insider threats are a big challenge for traditional network security because they come from within the organisation. These threats can be caused by malicious employees or careless users who accidentally put the network at risk.[2]



Types of Insider Threats

## Over-reliance on Firewalls and VPNs

Many traditional security models rely a lot on firewalls and VPNs for protection. While these tools are good at controlling access and securing data, they often can't stop modern threats like phishing, social engineering, or new types of attacks.

# Real world scenarios with data breach

While several data breaches have made the news in recent years, a few stand out due to their severity and size:

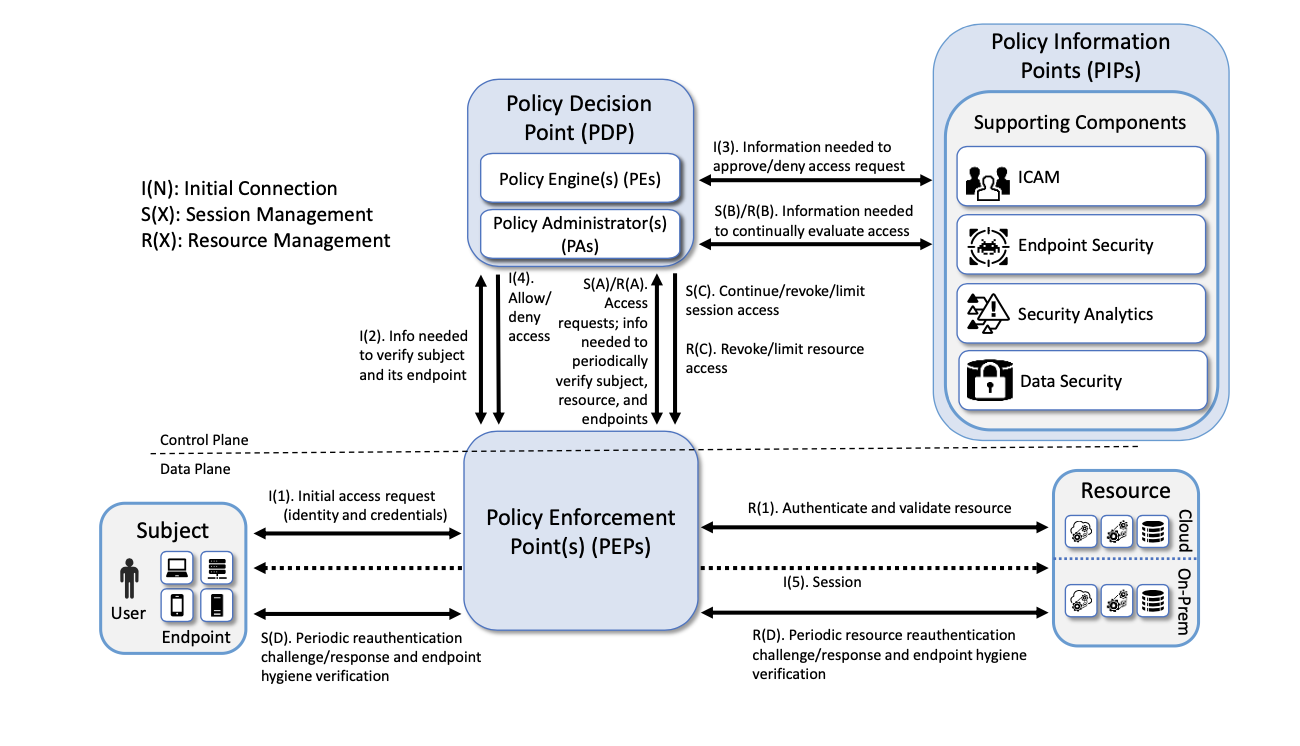
1. **Equifax**: A server vulnerability resulted in the breach of credit reports for over 140 million individuals. The breach remained undetected for several months before being addressed. Equifax was subsequently fined $575 million.
2. **Yahoo**: In 2013, hackers compromised account details of 3 billion users, including unencrypted security questions and answers. The following year, a separate breach exposed data from 500 million accounts, which included names, birthdates, email addresses, hashed passwords, and security questions with their answers.[4]
3. **Marriott**: Approximately 383 million customer records were exposed in a breach at Marriott. The compromised data included passport numbers (both encrypted and unencrypted) and payment card details.[4]

# Introduction to Zero Trust Networking

Zero Trust Network Access (ZTNA) is a security framework that assumes no user or device, whether inside or outside an organisation's network, should be trusted by default. Instead, ZTNA requires continuous validation of identity, user roles, and device posture before granting access to applications or data. This model contrasts with traditional perimeter-based security approaches and has gained traction due to the rise of cloud computing, remote work, and highly interconnected systems like 5G and 6G networks. ZTNA emphasises strict access controls, micro-segmentation, and real-time monitoring to protect against modern cyber threats.

## Core Components of Zero Trust Architecture

In a Zero Trust Networking (ZTN) model, every access request is treated as untrusted until verified and approved, ensuring strict control over access to network resources. This model relies on several key components to evaluate and enforce security policies in real time, maintaining the integrity of the network.



Zero Trust Architecture Components [10]

**Policy Engine (PE):**

The Policy Engine is tasked with making the definitive decision on whether access to a resource should be granted, denied, or revoked. This process involves calculating trust scores and evaluating access requests by applying organisational policies alongside inputs from supporting systems. The PE ensures that every access request is rigorously examined using established trust algorithms. Depending on the size and structure of the organisation, the PE may function as a standalone system or as part of a distributed network of systems that govern distinct sectors within the ZTA framework. Each system operates under the overarching enterprise policies to maintain uniform security standards throughout the organization.[10]

**Policy Administrator (PA):**

The PA enforces the PE’s decisions, managing communication between users and resources. It also generates session-specific credentials or authentication tokens to secure access for authorised users.[10]

**Policy Enforcement Point (PEP):**

The Policy Enforcement Point serves as the security gateway, implementing access controls by monitoring and managing interactions between users and resources based on the Policy Administrator’s instructions. It manages access by enabling, monitoring, and terminating interactions between subjects (users or devices) and resources, as instructed by the Policy Administrator. This component ensures that access policies are enforced in real time, maintaining compliance with the directives provided by the PA. [10]

In Zero Trust Networking (ZTN), various components and strategies work together to provide secure and real-time access controls. Below is a table showing the key terms and their roles within the ZTN framework:

| **Term** | **Description** |
| --- | --- |
| **Policy Decision Point (PDP)** | Combines the Policy Engine (PE) and Policy Administrator (PA) to make access decisions. Relies on input from Policy Information Points (PIPs). |
| **Policy Information Points (PIPs)** | Supply relevant telemetry and contextual data necessary for the PDP to make informed access decisions. |
| **Policy Enforcement Point (PEP)** | Implements the access decisions made by the PDP at the point of interaction, ensuring real-time enforcement of policies. |
| **Enterprise Identity Governance (EIG)** | A strategy for managing identity and access controls across the organisation to ensure consistent application of policies. |
| **Micro-segmentation** | Restricts user access to specific network segments, enabling fine-grained control over resource access. |
| **Software-Defined Perimeter (SDP)** | The PA acts as a network controller, establishing secure communication channels between users and resources through the PEP. |

## Zero Trust for Cloud and Hybrid Environments

In hybrid environments, beyond the foundational principles of Zero Trust Architecture (ZTA), additional security measures can be implemented through rigorous inspection of traffic entering and exiting cloud infrastructure. This inspection is essential to ensure that only authorised and secure communications occur within the cloud environment. One effective method involves the deployment of in-cloud network layer solutions, such as Network Access Control Lists (NACLs), which function similarly to traditional Access Control Lists (ACLs). NACLs provide a robust mechanism for controlling inbound and outbound traffic at the network layer, thereby enhancing perimeter defences within the cloud.

Further refinement of traffic control can be achieved through the use of Network Security Groups (NSGs), which offer Layer 4 filtering. This enables organisations to manage traffic based on IP addresses and ports, ensuring that only legitimate traffic is permitted to pass through. For deeper inspection and control at the application layer (Layer 7), Application Security Groups (ASGs) can be employed to filter traffic based on application-level protocols and behaviours, thus providing granular control over data flow within the cloud.

Moreover, traffic entering the cloud via direct connections, such as VPN-based links or dedicated connections (e.g., AWS Direct Connect or Azure ExpressRoute), should be subject to thorough filtering and monitoring. Next-Generation Firewalls (NGFWs) play a critical role in this context by enforcing advanced security policies and implementing rule-based allowances for traffic. NGFWs not only monitor and filter traffic but also offer capabilities such as intrusion prevention, deep packet inspection, and application-aware filtering. These layers of defence ensure that hybrid cloud environments maintain strong, adaptable security postures in alignment with Zero Trust principles.

## Implementation and Case Studies

### Case Studies of ZTNA

* Collaboration Systems with zero Trust  
  ZTNA and blockchain-based decentralised identifiers (DiDs) and real time identity validation can provide secure exchange between organisations. [6].
* **Kubernetes and Zero Trust Implementation**Kubernetes was used to implement a Zero Trust Architecture, where containers were deployed in a cloud environment with Role-based access control and micro-segmentation to prevent breaches and ensure scalability and resilience in cloud-native applications [7].
* **6G Network Security**6G networks could use the ZTNA, using software-defined perimeter controls to protect against DDoS attacks and zero-day exploits combined with dynamic user access control [8].
* **Zero Trust in 5G Network Slices**5G networks with ZTNA and AI-driven trust evaluations providing real-time monitoring. This prevented unauthorised accesses across different components of the 5G architecture [9].

## Challenges and Future Trends

### Future Trends of Zero Trust

* **Integration with AI and Machine Learning**

The future of ZTNA is closely linked to the use of artificial intelligence (AI) and machine learning (ML) for dynamic trust evaluation and decision-making in distributed environments. This will enhance real-time responses to threats and enable autonomous policy enforcement, like 5G and 6G networks [4], [3].

* **Blockchain for Trust and Identity**

Decentralised identity (DiD) systems based on blockchain with transparency and integrity of transactions will be a significant factor in securing cross-domain interactions in Zero Trust models [1], [4].

* **Zero Trust for IoT and 6G**

The IoT architecture will need to manage heterogeneous environments with dynamic, fine-grained access controls, safeguarding data and devices from attacks across an expanding attack surface [3].

### Challenges in Implementing ZTNA

* **Scalability Issues**

A major challenge in scaling Zero Trust architectures, particularly in large-scale environments like 6G is to implement fine-grained, continuous access control across multiple domains with significant computational resources, which may be limited in edge devices or remote areas [8].

* **Integration with Legacy Systems**

Integrating Zero Trust models with legacy systems that rely on perimeter-based security models. Transitioning from traditional methods like VPNs and firewalls to a fully adaptive Zero Trust model requires a complete overhaul of the infrastructure, which is both time-consuming and expensive [6], [7].

* **Real-time Threat Detection**

While ZTNA enhances security, real-time threat detection, behavioural analytics and response present a major challenge in fast-paced environments like 5G and Kubernetes-based cloud systems. [7], [8].

* **Privacy and Trust Management**

ZTNA systems that require constant verification of user identities and access may collect excessive data, raising privacy concerns [5]. Additionally, managing trust across different organisations and cloud providers is complex, especially when using blockchain-based trust mechanisms [5], [9].

# Appendix

1. Cloudflare, "Castle-and-moat network security," *Cloudflare*. [Online]. Available:<https://www.cloudflare.com/en-au/learning/access-management/castle-and-moat-network-security/>. [Accessed: Oct. 14, 2024].
2. Palo Alto Networks, "What is network segmentation?, "*Palo Alto Networks Cyberpedia*. [Online]. Available:<https://www.paloaltonetworks.com/cyberpedia/what-is-network-segmentation>. [Accessed: Oct. 14, 2024].
3. Cisco, "Configure remote access VPN," *Cisco*. [Online]. Available:<https://www.cisco.com/c/en/us/td/docs/security/firepower/623/fdm/fptd-fdm-config-guide-623/fptd-fdm-ravpn.html>. [Accessed: Oct. 14, 2024].
4. Abnormal Security, "Data breach," *Abnormal Security*. [Online]. Available:<https://abnormalsecurity.com/glossary/data-breach>. [Accessed: Oct. 14, 2024]
5. Uniserve IT Solutions, "How to protect your business from insider threats," *Uniserve IT Blog*. [Online]. Available:<https://uniserveit.com/blog/how-to-protect-your-business-from-insider-threats>. [Accessed: Oct. 14, 2024].
6. K. R. N’Goran et al., “Zero Trust Security Strategy for Collaboration Systems,” in *2023 International Symposium on Networks, Computers and Communications (ISNCC)*, 2023, pp. 20-30, doi: 10.1109/ISNCC58260.2023.10323911.
7. D. D'Silva, D. D. Ambawade, “Building A Zero Trust Architecture Using Kubernetes,” in *2021 6th International Conference for Convergence in Technology (I2CT)*, 2021, pp. 1-4, doi: 10.1109/I2CT51068.2021.9418203.
8. X. Chen, W. Feng, N. Ge, Y. Zhang, “Zero Trust Architecture for 6G Security,” *IEEE Network*, vol. 38, no. 4, pp. 224-230, Aug. 2024, doi: 10.1109/MNET.2023.3326356.
9. H. A. Kholidy et al., “Toward Zero Trust Security in 5G Open Architecture Network Slices,” *2022 IEEE Military Communications Conference (MILCOM)*, 2022, pp. 577-580, doi: 10.1109/MILCOM55135.2022.10017474.
10. Rose, S., Borchert, O. , Mitchell, S. and Connelly, S. (2020), Zero Trust Architecture, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.SP.800-207, https://tsapps.nist.gov/publication/get\_pdf.cfm?pub\_id=930420 (Accessed October 20, 2024)