Sri Lanka Institute of Information Technology

Assignment 1- Year 2 semester 1

G. P. I. Perera
IT23360600
SLIIT KANDY UNI

Introduction to Cyber Security – IE2022

B.Sc. (Hons) in information Technology Specializing in Cyber Security

Terms of References

The detailed report document was submitted to fulfill the requirements of the IE2022 - Introduction to Cyber Security module assignment at Sri Lanka Institute of Information Technology.

Acknowledgement

I would like to extend my deepest gratitude to, Ms. Menaka Monamaldeniya for her unwavering guidance and insightful supervision throughout the course of this module. Her knowledge and support have been critical to the successful completion of my work.

Contents

The Evolution and Future of Zero Trust Architecture

Overview

The report contrasts the background foundation for ZTA which are limitations of perimeter-based security followed by the rise of ZTA as a solution. Then the report highlights key principles, tenets, logical components followed by Implementation methods, deployment methods and use cases in ZTA in modern digital landscape. Furthermore, the report explores future directions regarding AI enhanced ZTA and ZTA for cloud environments.

Introduction to the ZTA in modern digital landscape

Background

In traditional methods when a user or a device is once inside the network perimeter, they are often trusted with minimal addition verifications which imply "Trust but verify" model. In this traditional approach a clear perimeter boarders and boundaries were defined (ex – a company office protected by firewalls, VPN etc.) and users inside this network were trusted by default after a simple verification. Since the "trust" is granted once a user is "authenticated" they have broad access with minimal "verification". Therefore, although the system may provide comparative average security against external threats and perimeter security, because of the internal monitoring is less robust the system could get compromised by internal attacks [1].

Therefore, it is explicit that this system security is relied heavily on perimeter defenses like firewalls, VPN and Intrusion Detection/ Prevention Systems which are often based on network location.

Firewalls– filters network traffic and acts as a barrier between internal network and outside world.

Virtual Private network (VPN)– provides secure access and encrypts the traffic.

Intrusion Detection Systems (IDS) – monitors and alert suspicious traffic or activity. But doesn't take any actions to stop an attack

Intrusion Prevention Systems (IPS) – on the other hand blocks suspicious traffic and disconnect infected devices [2]

Limitations of perimeter-based security [3]–

1. Single point of failure - perimeter-based security relies on single barrier to protect the entire network. In terms of compromission the entire network become vulnerable.
2. Static nature – in modern systems users and devices change constantly across platforms, locations and roles. Parameter based security often resistant to these changes and fails to provide efficient security against these dynamic changes.
3. Lack of Continuous Verification – perimeter defenses often do not require constant verification regarding identity and trustworthiness of users, devices and their activities.
4. Difficult to Enforce Least Privilege Access – least privilege access means granting users and devices the access they only require, and this is often crucial and beneficial in access control and

to prevent data breaches. But perimeter defenses often make it challenging to imply least privilege access.

5. Limited Lateral Movement Prevention – lateral movement means when an adversary gains access to additional systems after an initial compromise. perimeter movement lack ability to prevent this cause which h allows attackers to freely move within networks after a compromise.

Rise of ZTA

In the modern era, due to many factors, trends like Work from Home (WFH), Bring Your Own Device (BYOD), COPE and cloud and virtual environments are becoming popular. Which blurs the boundaries of traditional network parameters, which is also a main definitive of these traditional security bases. [4]

Before the 2000s security relied heavily on above mentioned perimeter-based security architecture. But once an attacker breached this perimeter, they were able to move laterally within the network with a little resistance, exploiting the implicit trust given to internal devices and users.

Need of a better reliable security architecture arose during the period of 2000 – 2010 due to many factors such as growing sophistication of cyber-attacks day by day such as Advanced Persistent Threats (APTs) showed advanced attackers could easily penetrate a traditional system. Also, development of palm held devices and BYOD, WFH concepts decentralized the dynamic access needs. During this period organizers began to move to the cloud, therefore perimeter defenses struggled even more to secure distributed services.

ZTA was proposed by Jhon Kindervag, a researcher at **Forrester Research**, in 2010. Kindervag argued that implicit trust is a vulnerability, and the security should be based on verification at every access point. [3]

Although achievability of ZTA remained unresolved, Google launched BeyondCorp after the cyber-attack known as Operation Aurora in 2010, which provides secure access to applications without relying on VPN and in this model each access was continuously evaluated. Since BeyondCorp was a success, ZTA was proven as achievable at scale, and this inspired other organizations as well to explore ZTA strategies.

The Basics of Zero Trust Architecture: Principles, Key Tenants, and Components.

Zero trust architecture always emphasizes the practice "Don't trust, always verify." So, by default, all objects are untrusted. Implying assumptions such as all traffic cannot be trusted, and the physical location should not act as a basis for security and instead of traditional methods, access control, minimum access policies, traffic monitoring and analyzing should be implemented.

ZTA follows the following 5 basic assumptions and principles. [5]

1. The network environment is never considered a trust zone – assets should always be protected, acted on and kept as if an attacker is present therefore all the enterprise actions should be done in the most secure way possible.
2. There could be devices that aren't owned by the corporation and that can't be configured.

3. Every device must be verified and not trusted by default. – every device must have a security posture that is evaluated by policy enforcement point.
4. All devices, users, and network traffic should be authenticated and authorized [3]
5. Security policies must be dynamic and calculated based on as many data sources as possible

Evolution of Zero Trust Architecture

Key tenets of ZTA

Although most of the definitions have the concept of discarding perimeter-based defenses, most of the ZTA variations relate or require perimeter-based components to fulfill their roles and accomplish obligations. Therefore, NIST defines the basic implantations to the architecture rather than excluding existing components. [5]

1. All data sources and computing services are considered resources.

This means that all computing services and data sources are considered resources. Regardless of whether they are enterprise owned or privately enabled, once they accessed the enterprise system, they are considered as a part of the security model.

This enforcement focuses on providing continuous security in distributed environment and provides control over BYOD and WFH.

2. All communication is secured regardless of network location

ZTA implies a location-agnostic security model. Therefore, devices on the internal network must meet the dame access and control standards as the external sources and every access request must undergo the identity verification, device health checks and policy enforcements.

According to this enforcement all communications are end-to-end encrypted to prevent eavesdropping. Therefore, even if the attacker gained access data remains protected.

3. Access to individual enterprise resources is granted on a per-session basis.

This approach plays a vital role in ZTA since the access to system is dynamically managed, based on the context of each attempt. Therefore, trust evaluation is also imposed dynamically based on trust factors and the granted access is the least privilege necessary to complete the given task. Trust is never inherited or implicit to a device and based on the authenticated session. This is crucial to prevent lateral movement.

4. Access to resources is determined by dynamic policy

In ZTA access decisions are based on multiple dynamic attributes.

Client identity – includes user accounts, service identifies such as roles and departments and authenticate individual users, community members and their automatized tasks.

Requesting asset state – include device characteristics such as software version, security patches, network location and device health and status.

Behavioral and environmental attributes. – usage patterns, unusual behaviors, network location, time of request, active attack and other factors that influence access decisions.

Enterprise policies – policies enforced by the enterprise these are mostly managed by the policy engine.

5. The enterprise monitors and measures the integrity and security posture of all owned and associated assets.

To resist rapidly evolving threats and provide immediate detection and response regarding potential threats and breaches ZTA continuously monitor all the assets that are owned and associated. Also, this tenet again refers no implicit trust is granted to any asset and that a ZTA always establish a continuous diagnosis and mitigation (CDM) or a similar concept to monitor and impose necessary patches or fixes accordingly. The monitoring and measuring also includes discovering subverted devices, devices that has known vulnerabilities such as not up to date devices or with harmful malwares and devices that are not abide by the company policies and treat them accordingly to ensure the devices are at their most secure state to interact with the enterprise system.

6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed.

NIST refers [9] this to a continuous cycle of obtaining access, scanning and assessing threats, adapting and continuously reevaluating trust in ongoing communications. When a ZTA is implemented in a platform, enterprise expected to have an ICAM, which is Identity, Credential and Access Management in place, meaning requiring the use of factors like Multi factor authentication (MFA).

7. The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.

In ZTA enterprises should actively gather and log comprehensive information about assets, network infrastructure and communication patterns such as security posture, network traffic and access requests.

How does ZTA work

ZTA is an end-to-end approach that focuses on resource protection, premising that trust is never granted implicitly. ZTA basically focus on authentication and authorization to shrink implicit trust zones. ZTA implements least necessary dynamic access rules known as policies that are enforced by policy decision point (PDP) and policy enforcement point (PEP). [5]

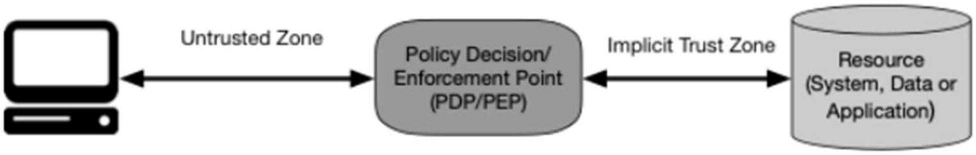
Untrusted Zone
Policy Decision/ Enforcement Point (PDP/PEP)
Implicit Trust Zone
Resource (System, Data or Application)

Figure 1: Zero Trust Access

PDP and PEP are considered as the gateways to provide least privileged access, at the end level of PDP and PEP a device can be trusted to the least level to provide access to the necessary task by authentication and authorization.

<u>Basic Logical Components of the model [5]</u>

According to NIST ZTA architectural design consists of 3 major logical components.

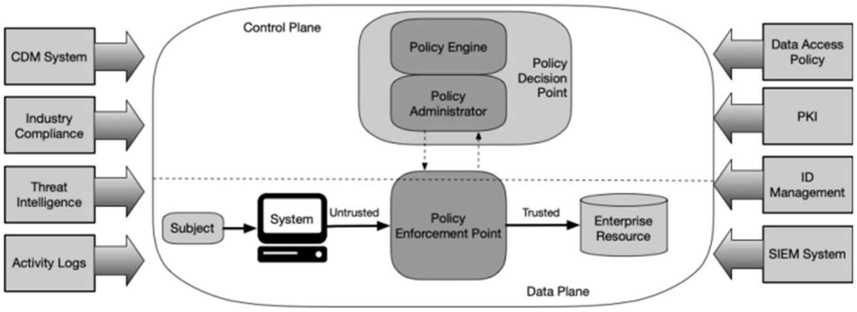

Figure 2: Core Zero Trust Logical Components

1. Policy Engine (PE)

   This is a crucial function to ZTA. Policy engine determines the final decision to grant resource access to a device or a network. Design of the PE is programmed according to the external and internal enterprise policies of the organization considering factors such as CDM systems, threat intelligence, and activity logs such as trust algorithms that grant, deny or revoke access to the resources.

   Key functions of PE can be contrasted as Decision making and logging decision records for audit purposes.

   PE closely works with policy administrator providing necessary information to implement access control.

2. Policy Administrator. (PA)

The policy administrator is responsible for executing and implementing the above external and internal working policies. PA is responsible for shutting down or granting access paths of communication based on the information provides the policy engine. PA generate session specific authentication, authentication token or credentials to access resources. PA establishes and manages communication pathways between users and resources. PA coordinate with PEP with the decisions provided by PE to establish or shut down communication access between resources and devices.

Key functions of PA are session management and coordination with PEP.

3. Policy Enforcement Point (PEP)

Responsible for enabling, monitoring and terminating connections between subjects and enterprise resources. Although this is one component basically can be divided into client and resource side. But in whole this can be considered as a single portal that acts as a gate keeper for communication paths. Beyond PEP is the trusted zone hosting the resources.

Policy engine paired with the policy administrator, defined as Policy Definition Point (PDP). Policy engine makes and logs policy-based decisions while policy administrator execute them. Therefore, based on the information from the policy engine, policy administrator authenticates and grant or deny access to users.

Policy administrator relies on PE decision to ultimately allow or deny a session. When a session is authorized and the request is authenticated, PA configures PEP to allow the session to start. If the session is denied, PA signals PEP to shut down. PA communicates with PEP to create the communication path.

Other important components of ZTA [5]

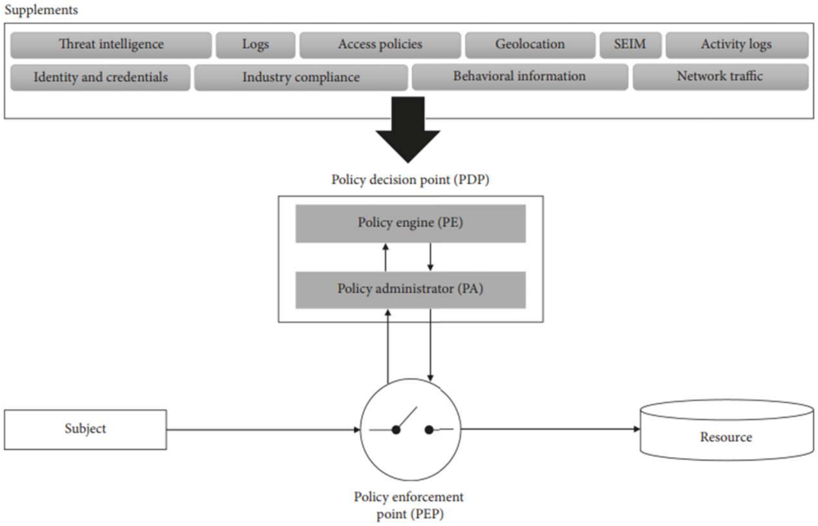

FIGURE 1: Logical components of the zero trust architecture (ZTA).

- Continuous Diagnosis and Mitigation (CDM) System. – CDM monitors the state of devices including their software and configurations across the system in real time. Functionalities of CDM include asset health monitoring to ensure device is up to date and properly configured, Vulnerability assessment to identify known vulnerabilities, policy enforcement to non-enterprise devices such as personal devices and providing input to policy engine. PE depends on CDM's data such as compliance status to make decisions.

- Industry Compliance system. – Industry compliance system ensures that enterprise background meets regulatory requirements and compliance standards. Regularity requirements include frameworks depending on various industries. (FISMA for federal organizations, HIPAA for healthcare, PCI DSS for financial transactions). The industry compliance system also supports decision making of PE through compliance standards. The system also performs audits to ensure system standards.

- Threat intelligence feeds. – TIF serves as a critical input for PE to rely on. ITF feeds PE with aggregate and real time data about malware, threats and vulnerabilities that help enterprises to adjust policies. These feeds could originate from both internal and external sources. This information includes vulnerability data, malware threats, IOCs, reported attacks, exploits, geopolitical or regional risks. ITFs
- Network and system activity log - This is essential for enterprise security monitoring. Asset logs, traffic logs, resource logs, event logs form security tools and authentication and authorization logs are basic components here.

- Data access policies – Data access policies define when, how and by whom enterprise resources should be accessed. These policies have several attributes they rely on to, for granular control. There are policy structures and access control methods to provide least privilege access for resources.

- Enterprise public key infrastructure (PKI) – this is a framework for creation, management, distribution and use of digital certificates. PKIs issue, authenticate and manage certificates. They encrypt and protect data as well as issue digital certificates.

- ID management system – IDMS securely manages user identities and ensures controlled access to enterprise resources by integrating with other security structures. IDMS stores ID data and integrates with authentication mechanisms such as MFA and SSO to ensure only authorized users gain access. IDMS also collaborates with external and non-enterprise systems grant temporary access to specific resources.

- Security information and event management (SIEM) system – this plays a critical role in monitoring, collecting and analyzing security related data to provide real time visibility from potential threats.

Approaches to ZTA: Basic Strategies for Adoption

ZTA offers a robust security framework and addresses modern threats. A full enterprise transformation in cyber security is not a one fit for all solutions. But in the digital era tailoring a modern suitable security model is crucial.

NIST states variations of ZTA for an enterprise to enact with a suitable framework. When moving to ZTA, the above tenants must be present in a ZTA implementation, and the organization can use one or more logical components as the main driver. An organization can adapt to a better security model using one or more variations of ZTA. NIST discusses 3 main strategic methods that an enterprise could adopt to implement ZTA. But it’s suitable that an organization find its own use case according to existing policies, current business flows and requirements for an implantation. [5]

Enhanced Identity Governance by ZTA [5]

Key component to policy creation in this approach is identity of actors (identity centric policies). Actors accessing enterprise resources is one reason to create access policies. In enhanced identity governance these access policies are based on the identity of users. Main principle is that access to resources is permitted only when the identity of the user matches the predefined enterprise policies. Therefore, the primary factor for accessing resources is the access privilege granted for the user. In the secondary level other factors such as the device used, asset status and environmental factors are considered to grant the necessary ultimate access and authentication to perform the necessary task (note that the access is always least privilege). In this model every access request is checked through PEP and PEP communicates with PE to verify if the user is allowed access.

This identity driven approach is often implemented as an open network model and mostly suitable for networks where external users or devices frequently access the system. Such as cloud systems, SaaS platforms and resource portals where enterprise security components are not fully implemented.

Micro Segmentation [5]

This is one of the crucial components when it comes to ZTA. This involves isolation of specific resources or small groups of assets to discrete segmentation and protecting these segmentations with advanced security devices such as NGFWs, software agents and intelligent switches and routers.

Functionality of micro segmentation involves segmentation gateways such as PEPs to monitoring and control, Dynamic policy enforcement and host-based segmentation. Also, micro segmentation relies heavily on robust identity governance since access policies that are defined by segmentation gateways are referred by the identity of users.

Micro segmentation grants granular control over a network meaning enforcing tight control over traffic and reducing network surface which helps to minimize the impact of a breach since attacker is contained within the segment preventing lateral movement.

Implementation of micro-segmentation is best for cloud and hybrid network environments where it is necessary to isolate resources and access paths.

ZTA in Network infrastructure and software defined perimeters. [5]

This approach is often applied through dynamic network control mechanisms. This is an integration of software defined networks and intent based networking. In this method PA acts like a network controller based on policies determined by PE.

In the application layer of OSI model, ZTA is used as a gateway model or an agent where agents on client devices communicate with resource gateways to establish a secure channel to enforces access control. These channels are end-to-end encrypted and intended to ensure access to only authorized resources and reduce lateral movement.

This method is also suitable for cloud environments and non-IP based environments that benefit from overlay works.

Using ZTA in network infrastructure and software defined perimeters grants scalability and agility by eliminating the need for methods such as VPN which often become a liability. Also, this provides a secure platform for enterprises against DOS and DDOS attacks.

Deployment Models of ZTA: Methods for Practical Implementation.

These practical implantation methods demonstrate how logical components of ZTA can be implanted in different forms. For instance, an enterprise might use hardware or software that fulfills the tasks of multiple logical components, likewise multiple hardware or software components might be required to complete the job of one logical component. However, enterprises are most likely to use a combination of logical components and deployment methods that are suitable for the workflow and security requirements. NIST discusses four deployment methods of ZTA.

Device Agent/Gateway Based Deployment [5]

This model divides PEP into two parts. –

1. Device agent (Installable on enterprise-issued devices.)
2. Resource gateway (placed in front of the enterprise resource)

This approach has connections between enterprises ensure that all communications follow ZTA principles.

In this approach there is a device agent that is installed in enterprise owned assets that intercepts traffic that is forward through PEP that would authenticate users, monitor the devices. And the only traffic that is routed through the gateway is traffic that is approved by the PA.

There is a resource gateway that's located in front of a protected source acting as a proxy that would ensure that resources are never exposed to unauthorized devices in the network. This gateway communicates with PA to configure the authorized sessions.

In this deployment PE and PA either can reside on premises or in the cloud.

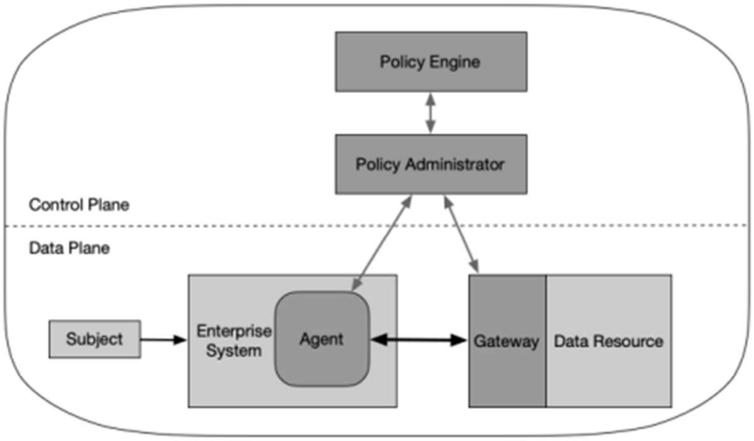

Figure 3: Device Agent/Gateway Model

Enclave-Based Deployment [5]

This is a variation of device/ agent gateway model that focuses on multiple resources that is grouped in a secure isolated area, rather than placing gateways directly in front of individual assets. This model is ideal for the organizations that has traditional interfaces since the model focus on the security at the perimeter of a resource group.

Key components of this model could be highlighted as resource enclave that may represent local enterprise data centers, a private cloud or a microservice and enclave gateway that is positioned at the boundary of the enclave. This gateway is the communicator between PA and resources and handle traffic.

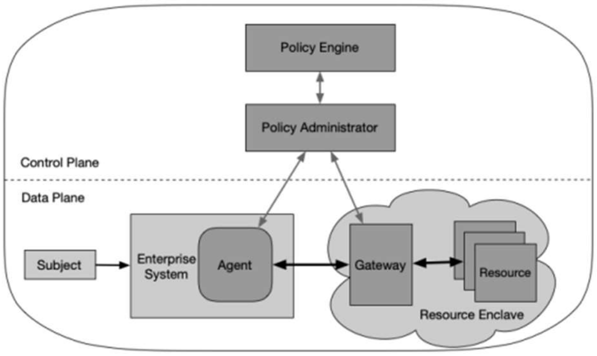

Figure 4: Enclave Gateway Model

Resource Portal-Based Deployment [5]

This model simplifies user access management by consolidating the access through a centralized portal. This is ideal for BYOD environments to reduce visibility and security risks.

In this modal PEP acts as the central access points for users and devices that serves as a gateway to a single resource or an enclave. PE and PA evaluate each request and there are no local installed agents therefore, the portal is responsible for analyzing the user device. The portal may imply browser isolation as a security measure.

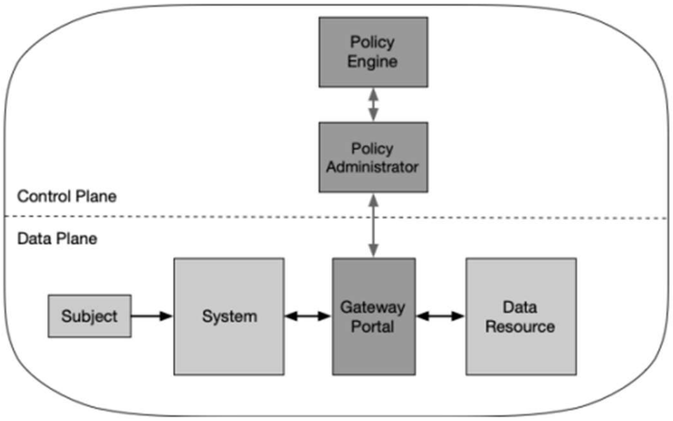

Figure 5: Resource Portal Model

Device Application Sandboxing [5]

This security model isolates specific vetted applications or processes that are in a demented area which is called a sandbox. This ensure even if the host device got compromised critical information remain protected. This is useful for enterprises that have endpoint security measures where direct control over user devices may be limited.

In this model there is a sandbox area for applications and access requests for these sandboxed applications are validated by PEP. Policy management is centralized via PE and PA.

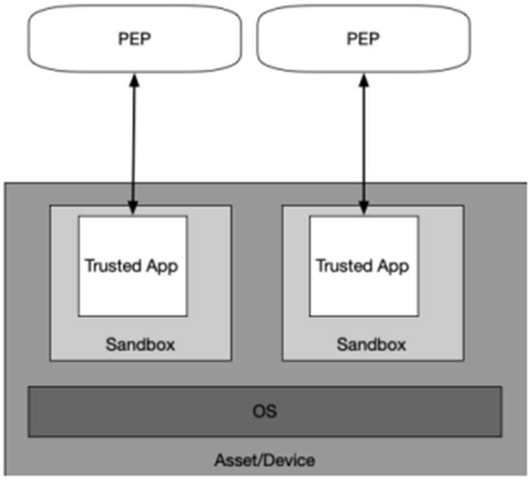

Figure 6: Application Sandboxes

Use case Scenarios of ZTA

Enterprise with Satellite Facilities [5]

When an organization has multiple distributed satellite locations or remote working employees, securing communications between locations and headquarters could be challenging. Traditional approaches use methods such as multiprotocol label switching (MPLS) but when it comes to cloud traffic those methods could introduce bottlenecks such as limited bandwidth on MPLS, less secureness of sensitive data, offload traffic and tunnel traffic.

As a solution, Cloud based PE and PA are introduced where PE and PA are hosted as cloud services. This method offers high availability, redundancy, direct access of resources that are in the cloud and centralized policy management.

In some cases, End point agents are installed on user devices before granting access to resources that would monitor device status, establish secure connections (VPN, ZTNA) and provide identity-based access that ensure accesses are authenticated and encrypted.

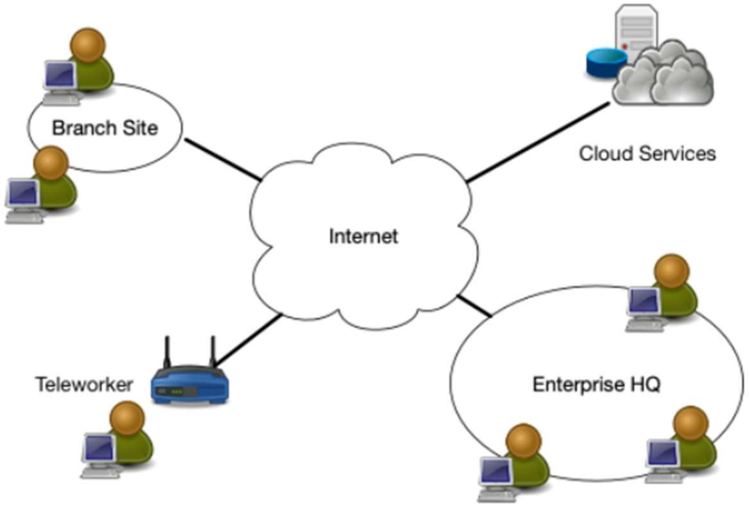

Figure 8: Enterprise with Remote Employees

Multi-cloud/Cloud-to-Cloud Enterprise [5]

This includes enterprises that utilize multiple cloud providers to host applications, services or data which is an environment that requires direct communication between cloud and enterprise network. in these environments key principle of ZTA is the network ownership does not affect access control and that all traffic should be treated as untrusted by default therefore require continuous verification.

Key components of this infrastructure are policy enforcement at access points, PE and PA, direct cloud to cloud communications and clients accessing through portals or agents.

Security benefits of multi cloud ZTA includes reduces latency, improved performance, centralized security with distributed controls, scalability, resilience and cloud native security posture.

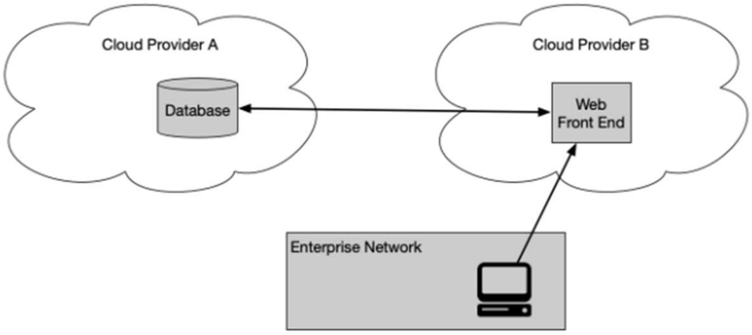

Figure 9: Multi-cloud Use Case

Enterprise with Contracted Services and/or Nonemployee Access [5]

This use case addresses the challenges of accommodating non-employee access, such as on-site visitors and contractors while protecting enterprise networks. Therefore, granular and temporary access methods with better defined access policies are necessary to keep internal applications, databases and other sensitive data protected. Unauthorized users shall not discover services, hosts via network scans or perform lateral movements in the network.

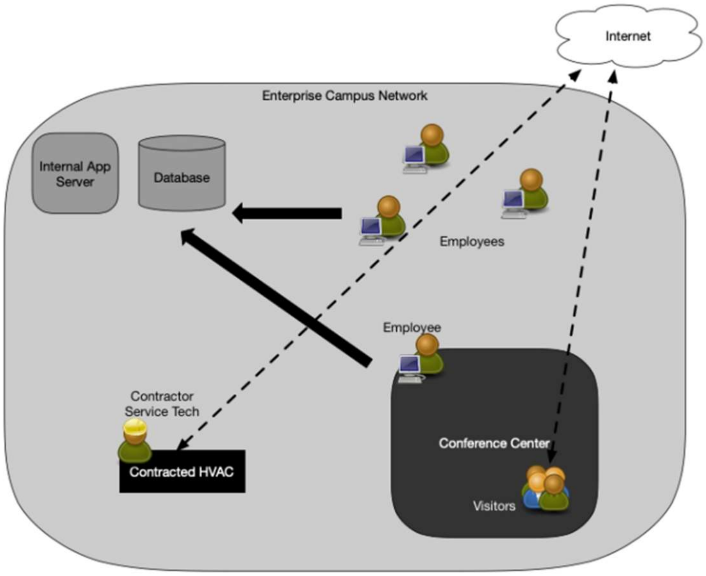

Figure 10: Enterprise with Nonemployee Access

In this case PEP is deployed for role-based access control to enforce trust policies at key access points such as Wi-Fi routers and portals to ensure non-employees are strictly limited to specific resources. PE and PA are deployed based on the context of users or devices to determine who can access what and when. Resource agents or resource portals could be used to access resources to ensure secure access without exposing unnecessary infrastructures.

Key challenges of this scenario are managing multiple access levels between various types of personnel such as long-term contactors and short-term visitors and device compliance against security posture. Therefore, implementation of a combination of access control mechanisms such as RBAC and ABAC, micro segmentation and requiring device health checks before accessing enterprise resources should take place.

This use case implantation highlights key benefits of ZTA such as granular access control, Reduced risk from insider threats and improves user experience.

Collaboration Across Enterprise Boundaries [5]

This use case scenario involves sharing resources or data between two or more separate organizations. These could be government G2G, B2B or G2B but the common objective is to enable secure communication and secure access. ZTA offers dynamic and flexible cross- enterprise collaboration.

Key components of ZTA for cross identity collaboration includes federated identity management that allows organizations to trust each other's identity systems, federated identity framework that enables SSO and cloud hosted PA and PE that allows access to shared resources without relying on VPNs or manual firewall rules and agent-based access or web gateway to resources.

Challenges in managing user accounts across enterprises and maintaining security posture across organizations might make the implementation hard but this use case grans ideal security benefits such as reduced attack service and real time context aware access control.

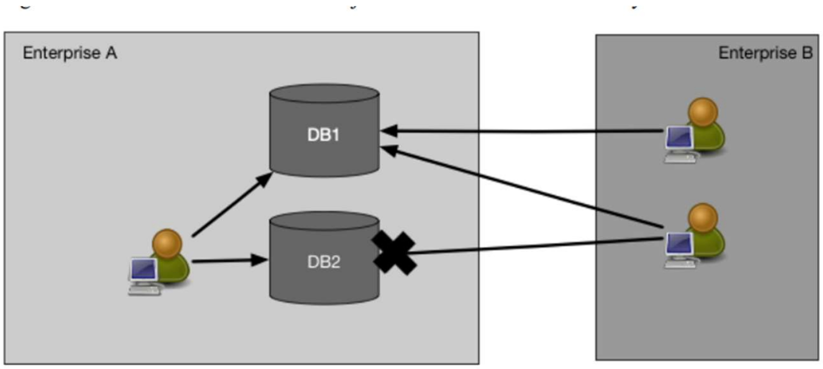

Figure 11: Cross-Enterprise Collaboration

Enterprise with Public- or Customer-Facing Services [5]

Public facing services that are designed to host customers and employee dependents hold a complicated security posture due to asset accessing of these services are not fully enterprise owned. In this case ZTA is adapted to balance usability, security and regulatory compliance although traditional ZTA principles may not be fully applicable when public or anonymous users are involved. This can be divided into anonymous public resources where no login is required therefore authentication or identity management is not involved. Also, the services could be vulnerable to DOS and bot traffics. When it comes to registered user services where login credentials or identity required at portals, enterprises can enforce policies such as passwords or MFA.

Lack of control over client devices, mitigating automated attacks and bots and securing user privacy and data governance regulations are key challenges to this model

Future Directions of ZTA

Integrating ZTA with AI and Machine Learning. [6]

Both ZT and AI are emerging trends in digital era. ZT components integrated with artificial intelligence could boost the performance and strengthen the security of a system since AI can examine a vast amount of data and identify patterns also threats and vulnerabilities.

AI in identity access management.

Integrating with AI, IAM could implement the following enhancements in basic characteristics.

- Authentication –
  - Adaptive and continuous user authentication via behavioral biometrics such as typing styles screen gestures and UEBA.
  - Biometric recognition such as voice and speech recognition, facial recognition.
  - AI driven anomaly detection.
- Authorization in RBAC –
  - Intelligent role assignment – AI analyzes historical data and proposes optimal roles to reduce human error.
  - Automated RBAC – AI handles dynamic access for new identity roles and prevents unnecessary privileges accumulating on them.
  - Role mining and optimization and continuous role reviews – AI monitoring user activity and trigger reviews when anomalies and suggesting improvements to existing roles and their existing structures.
- Administration
  - Automated user provisioning and de provisioning – AI automates account creation and deletion
  - Access request management and intelligent user profile management.
- Auditing, governance and compliance
  - AI suggest and updates policies based on trends, evolving regulations to maintain alignment with LPA and facilitate audit, reports and project generation.

Adaptive Multi factor authentication

MFA strengthens security by requiring multiple authentication factors. Real time scoring and adjustments where AI powered algorithms establish a bassline user profile and detect anomalies, dynamically adjusting the authentication factors and biometric authentication and assessing contextual information are ai enhancements in this area.

AI in ZT Network Access

AI in ZTNA enhances intelligent application grouping to enable precise least privilege access, and recommend policies for micro segmentation, automating security configurations and monitors network activity and traffic behavior to detect anomalies are AI enhancement in this component.

ZTA enhancements in the cloud area. [7]

Cloud computing id a rapidly evolving sector in technology. cloud computing revolutionizes how organizations handle data and applications. Although this offers flexible and scalable communication methods, they also introduce complex security issues. ZTA provides a robust framework that provides enhanced security measures in cloud environments.

Identity and access management in cloud environments decentralized identity management are deployed as well as AI powered adaptive authentication. When it comes to cloud security posture management automated remediation, multi cloud and hybrid visibility and SOAR techniques are widely used. Also, when building a secure cloud network architecture, micro segmentation, zero trust edge, and encrypted everything concepts are used.

Conclusion

ZTA is a trend that reshapes cyber security by redefining how an organization approaches trust and access to their resources. In precent cyber threats grows and evolve and grow in complexity and traditional cyber security methods has become obsolete. ZTA provides proactive, adaptive and more dynamic security solutions integrating with AI and new trends. While ZTA offers significant benefits, it also presents many challenges such as infrastructure complexity and compliance. But by embracing ZTA enterprises can build a resilient and scalable security framework. Organizations must carefully plan their ZTA adoption strategy, balancing security with usability and performance.

References

[1] A. M. Z. A. Zillah Adahman, "An analysis of zero-trust architecture and its cost-effectiveness for organizational security," *Computers & Security,* vol. 122, no. 102911, pp. -, 2022.

[2] K. A. O. S. S. S. Nurun Nahar, "A Survey on Zero Trust Architecture: Applications and Challenges of 6G Networks," IEEE, 2023.

[3] D. H. L. C. Y. N. a. X. M. Yuanhang He, "A Survey on Zero Trust Architecture: Challenges and," *Hindawi - Wireless Communications and Mobile Computing,* vol. 2022, no. 15 June 2022, p. 13, 2022.

[4] T. U. A. I. Songpon Teerakanok, "Migrating to Zero Trust Architecture: Reviews and Challenges," *Hindawi - Security and Communication Networks,* vol. 2021, no. 25 May 2021, p. 10, 2021.

[5] O. B. S. C. S. Rose, NIST Special Publication 800-207 : Zero Trust Architecture, NIST, 2020.

[6] S. H. Kayode Sheriffdeen, "Zero Trust Architecture: Strengthening Cyber Defenses with AI-Driven Policies," -, -, 2024.

[7] M. Blessing, "Zero Trust Architecture in Cloud Environments," -, -, 2024.

Please note that although many resources were referred, only few selected articles were chosen to refer in the report and even from those The NIST special publication on ZTA was chosen to define key components and tenets etc., since the many key details such as key principles and components details are inconsistent and discrepant from one material to the other.

Other Sources -

- **https://perception-point.io/guides/zero-trust/what-is-a-zero-trust-architecture-zta/**
- https://www.nccoe.nist.gov/sites/default/files/2022-12/zta-nist-sp-1800-35c-preliminary-draft2.pdf
- All the figures and diagrams are referred from – NIST Special Publication 800-207 : Zero Trust Architecture.