

Zero Trust Architecture Overview

Sérgio Pinto

Assistant Professor at ISTECS – sergioluz.pinto@my.istec.pt

Abstract: *The Zero Trust Architecture (ZTA) represents a significant paradigm shift in network security by moving away from the traditional perimeter-based model. Instead, it follows the principle of “never trust, always verify”, operating under the assumption that threats may originate both inside and outside the network. This shift requires rigorous verification of every user, device, and application requesting access to protected resources, regardless of their location. Consequently, the core elements of ZTA include strict identity verification and context control for every access request. Moreover, ZTA represents a transformative approach to addressing the limitations of traditional security frameworks. By emphasizing continuous authentication, least-privilege access, microsegmentation, and continuous monitoring, it establishes a robust foundation for protecting sensitive information in an increasingly complex threat landscape. As cyber risks evolve, adopting Zero Trust principles will be critical for organizations seeking to safeguard digital assets while ensuring that trust is never assumed but always verified.*

Keywords: *Cybersecurity, Zero Trust, “Verify, Control and Enforce”, Authentication, Least Privilege, Monitoring, Segmentation.*

I. Introduction

Traditional networks were secured using a set of security tools and firewalls in an architecture known as castle-and-moat security. The term derives from the analogy that security defenses created a protective network perimeter (the moat) around the network (the castle). This

model prevented access by anyone outside the network but granted broad privileges to anyone within. Such an approach served reasonably well when applications resided inside the protected perimeter and users worked on-site, accessing resources directly through the secured network [1] [3] [7] [8].

However, the rise of digital transformation—driven by remote work, cloud computing, and the Internet of Things (IoT)—has significantly expanded the organizational attack surface. Traditional perimeter defenses, such as firewalls, are no longer sufficient to protect sensitive information. As a result, ZTA provides a proactive approach to security by ensuring that every access request is validated, thereby minimizing the risks of data breaches and insider threats [2].

Zero Trust is therefore a security model that requires strict identity verification and context control for every user and device attempting to access resources within a network, regardless of their location. It operates on the principle of never implicitly trusting any entity, whether inside or outside the network [2].

This approach treats all network communications as potentially hostile. Therefore, communication between users and workloads, or between workloads themselves, is blocked until validated through identity-based policies. This ensures that inappropriate access and lateral movement are prevented. Validation applies consistently across any network environment, regardless of location, without relying solely on rigid network segmentation [1].

Finally, the purpose of this document is to provide a brief overview of ZTA, focusing on

its fundamental concepts, implementation, and operation.

II. Zero Trust/Legacy Security

Traditional security models typically focused on establishing a secure perimeter, allowing trusted users and devices nearly unrestricted access once inside. In contrast, Zero Trust dismantles the notion of a “trusted network” by enforcing strict access controls and continuous monitoring. This shift not only strengthens security but also supports regulatory compliance and data protection requirements in today’s complex digital environments.

The key differences between legacy network security architecture and the ZTA approach are summarized in Table 1 [1].

	Legacy Network and Security Architecture	Zero Trust Architecture
Attack Surface	Firewalls/VPNs published on the Internet Can be exploited, susceptible to DDoS	Apps not exposed to the internet You can't attack what you can't see
Connection	Apps access requires corporate network access, allows lateral movement of user and threats	Connects a specific, authorized user to a specific, authorized resource
Proxy/Pass-through	Firewall/Pass-through: Inspects a limited data buffer Unknown files pass through Alerts after infection	Proxy: Full content inspection, including SSL/TLS Hold ans inspect unknown files before reaching the endpoint
Tenancy	VMs of single-tenant appliances in a public cloud	Cloud-native, multitenant design like Salesforce/Workday

Table 1 – Legacy vs. Zero Trust Security Architectures

III. ZTA

Zero Trust Architecture (ZTA) is a cybersecurity framework based on the fundamental principle of “never trust, always verify”. Unlike traditional security models that assume entities within the network perimeter are trustworthy, ZTA treats all users and devices—whether inside or outside the network—as potential threats. This model requires strict identity verification and context control for every request to access protected resources, regardless of user location [1] [2] [4] [5].

ZTA can be defined by the following key characteristics [2]:

- Continuous Authentication – ZTA requires constant validation of user identity, device security and context control throughout the entire session, rather than providing broad access after a single authentication event.
- Least-Privilege Access – Access rights are assigned according to the principle of least privilege, meaning users receive only the permissions necessary to fulfill their authorized roles, thereby minimizing the risk of misuse.
- Microsegmentation – The network is separated into smaller, isolated segments, limiting lateral movement by attackers and protecting sensitive applications and data.
- Continuous Monitoring – ZTA requires continuous monitoring and logging of user activity, enabling organizations to detect anomalies and respond to threats in real time.

In summary, ZTA adopts a proactive, risk-based approach to cybersecurity. It enhances organizational resilience against evolving threats by ensuring that trust is never assumed and always verified.

III.I ZTA 7 Elements

To have a complete understanding of ZTA, it is useful to break it down into individual building blocks (or elements) that are executed before any connection to a protected asset is established. These elements ensure that all

enterprise services—including users/devices, IoT/OT devices, and workloads—are subject to the same set of controls when requesting access to assets [1].

According to Zscaler, and as illustrated in Figure 1 [1], the ZTA can be divided in seven essential elements, grouped into three categories.



Figure 1 – 3 categories of the 7 essential ZTA elements

The complete stack of these seven elements and their corresponding control actions within a ZTA is presented in Figure 2 [1] and described in greater detail in the next sections.

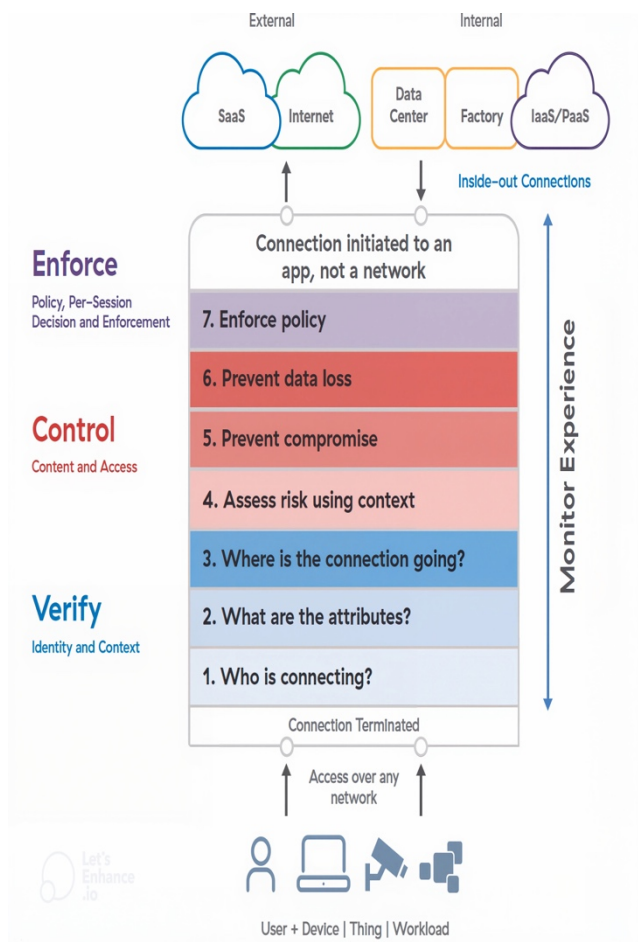


Figure 2 – The seven elements of ZTA

Group 1: Verify Identity and Attributes

When a user/device, IoT/OT device, or workload requests a connection to an asset—regardless of the access network—the ZTA first intercepts the connection and verifies identity and context by determining the “who, what, and where?”:

1. Who is connecting? – Verifies the identity of the user/device, IoT/OT device, or workload by interacting with Identity Providers (IdPs) as part of the enterprise Identity and Access Management (IAM) system.
2. What are the attributes? – Validates the characteristics of the entity requesting access, analyzing attributes such as role, responsibility, request time, location, and other relevant conditions. Profile data is aggregated from multiple sources, including IdPs.
3. Where is the connection going? – Ensures that the verified entity has the rights and meets the context requirements to access the requested application or resource, based on segmentation rules.

Group 2: Control Content and Context

After verifying identity and attributes, and applying segmentation rules, ZTA evaluates the risk associated with the connection request and inspects traffic for threats and sensitive data:

4. Assess risk using context – Artificial intelligence dynamically computes a risk score for the user/device, IoT/OT device, or workload based on factors such as device security configuration, threat intelligence, destination, behavior, and policies.
5. Prevent compromise – Inline decryption and deep content inspection of entity-to-resource traffic are applied to identify and block potentially malicious content.
6. Prevent data loss – Decryption and inspection of entity-to-resource traffic are also used to detect sensitive data and prevent exfiltration, either through inline controls or by isolating access within a controlled environment.

Group 3: Enforce Policy and Per-Session Decision

Once identity, context, and content are validated, policies are enforced before a connection to internal or external applications is established:

7. Enforce policy – This element uses the outputs of previous steps to determine the appropriate action for the connection request, which may result in either an allow or block decision.

It should be noted that each element feeds into the next, creating a dynamic decision tree that evaluates identity, profile, user risk, site risk, content, and context for every connection request. As illustrated in Figure 3 [1], these criteria determine whether access is conditionally allowed (pass) or blocked (fail).

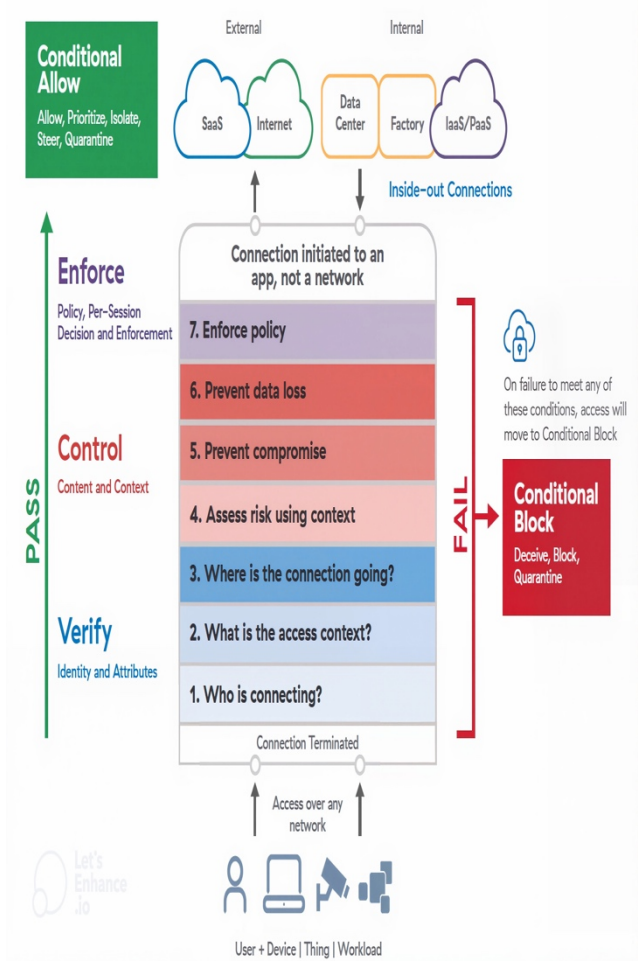


Figure 3 – Allow or block connections based on Zero Trust principles

Importantly, none of these elements should degrade the user experience. Therefore, ZTA must be capable of monitoring performance and diagnosing user-experience issues to ensure that the seven elements do not impose unnecessary burdens.

III.II ZTA Implementation

ZTA can be implemented through a Zero Trust Exchange platform. This integrated set of services protects users and workloads by leveraging identity and context to securely broker communications between users/devices, IoT/OT devices, and workloads over any network and from any location [1].

As illustrated in Figure 4 [1], the Zero Trust Exchange uses identity-based controls to enforce policies that securely enable: user-to-workload connections, third-party access, workload-to-workload interactions, and location-to-location segmentation. These connections are brokered without ever granting broad network access, thereby minimizing exposure and reducing security risks.

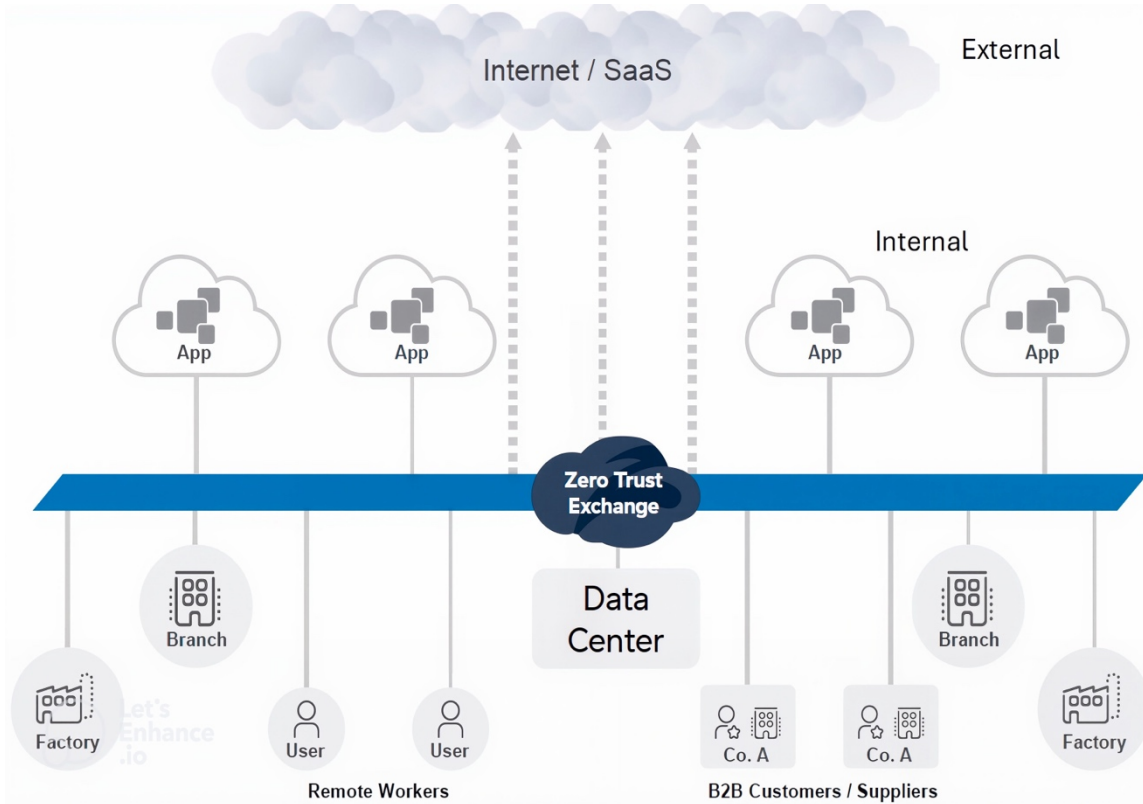


Figure 4 – ZTA Implementation

III.III ZTA Operation

ZTA should operate through the Zero Trust Exchange platform, which inspects all traffic generated and received by network users and workloads. This inspection includes full content analysis—covering encrypted SSL/TLS traffic and unknown files—before reaching the endpoint [1].

As illustrated in Figure 5 [1], the Zero Trust Exchange functions as a proxy, intercepting connections initiated by clients to examine activity (verify, control, and enforce). Afterwards, connections are re-established to the destination only if they fully comply with predefined security requirements.

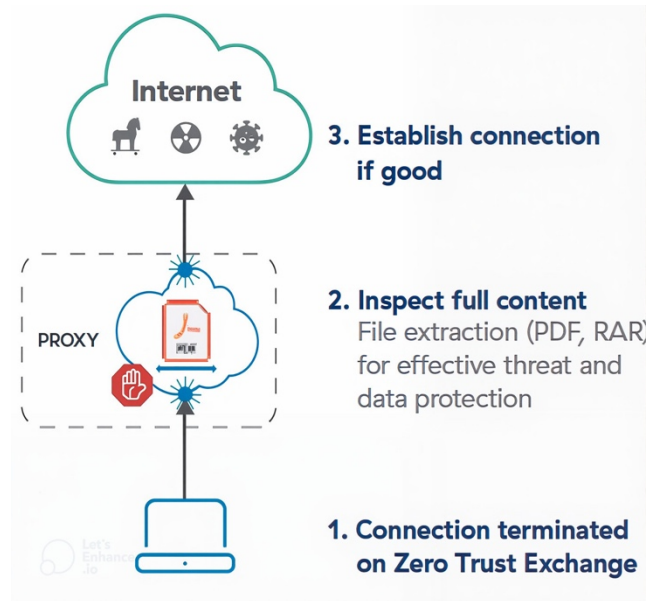


Figure 5 – Zero Trust Exchange Proxy

Encrypted Traffic Example

A core task of the Zero Trust Exchange platform is the ability to inspect encrypted traffic. This requires a forward proxy architecture capable of performing intensive inspection with minimal latency. For internet-bound traffic, decryption must support security protocols such as SSL/TLS and detect evasion techniques like DNS tunneling. The inspection process further enhanced through the integration of advanced technologies, such as [1]:

- Sandboxing – where potentially risky files are executed (“detonated”) in a controlled environment before being delivered to the user.
- Browser isolation – where only pixels are streamed to the user instead of the actual web page, thereby mitigating the risk of malicious content delivery.

Because threat actors continue to evolve their tools, techniques, and procedures—including misuse of legitimate storage providers—ZTA must be configured to function as an SSL/TLS person-in-the-middle proxy, as illustrated in Figure 6 [1]. This configuration enables comprehensive inbound and outbound content analysis and immediate blocking of threats detected anywhere within the enforcement plane.

Beyond blocking malicious activity, SSL/TLS inspection is also valuable for detecting when employees intentionally or unintentionally leak organizational data. Consequently, SSL/TLS inspection is critical not only for protecting against external attackers but also for ensuring regulatory compliance and safeguarding sensitive information.

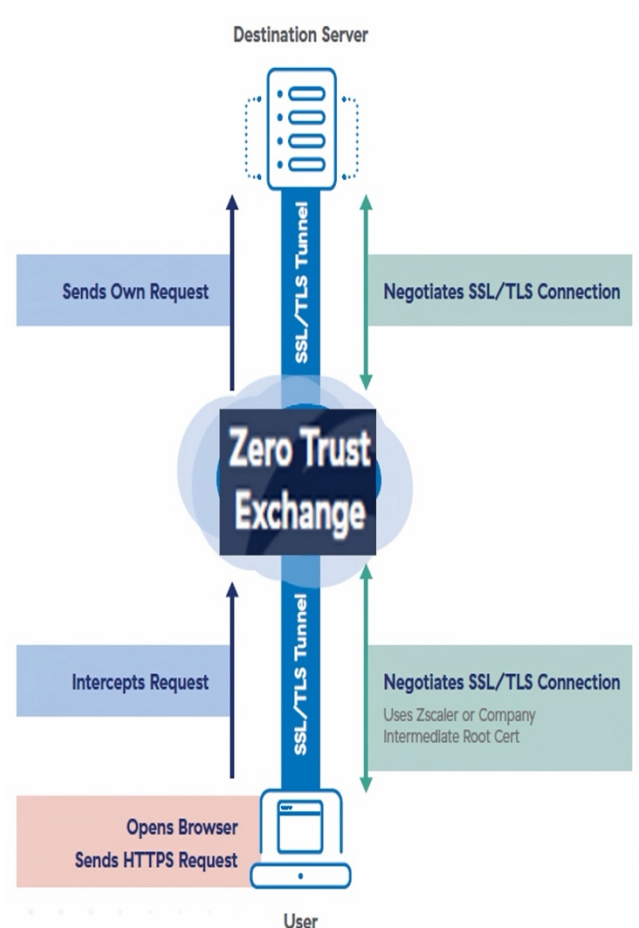


Figure 6 – Process by which a client negotiates a secure session with a destination server

IV Conclusion

Zero Trust Architecture (ZTA) represents a transformative shift in network security, fundamentally redefining how organizations safeguard their digital assets. By adhering to the principle of “never trust, always verify”, ZTA challenges traditional perimeter-based models that relied heavily on implicit trust. This paradigm emphasizes the continuous verification of users, devices, and applications, thereby significantly reducing the attack surface and strengthening the overall security posture [3] [4] [6].

The adoption of ZTA is becoming increasingly essential in modern cybersecurity, as threats grow more sophisticated. Furthermore, as IT environments expand in complexity—integrating cloud services, remote workforces, and interconnected devices—the perimeter-based model proves insufficient. On the other hand,

Zero Trust provides a more resilient approach by ensuring that security measures are applied consistently across the entire protected network, regardless of location or access source. This model not only addresses vulnerabilities within the network perimeter but also mitigates risks posed by both internal and external threats.

Looking ahead, Zero Trust principles should play a central role in the future of network security. The continuous advancement of technologies such as artificial intelligence, machine learning, and behavioral analytics will further enhance ZTA implementations. These technologies enable more accurate threat detection, dynamic access control, and stronger monitoring capabilities. As organizations accelerate digital transformation and face increasingly sophisticated attacks, Zero Trust will serve as a foundational framework for building adaptive and secure network environments [9] [10] [11].

In conclusion, ZTA offers a comprehensive, forward-looking approach to network security. Its emphasis on continuous verification, least-privilege access, and granular policy enforcement represents a significant advancement over traditional security models. As the cybersecurity landscape continues to evolve, Zero Trust will remain a critical component of effective defense strategies, driving both resilience and innovation in the protection of digital assets.

V References

- [1] N. Howe, S. Ganguli, and G. Festa, Seven Elements of Highly Successful Zero Trust Architecture: An Architect's Guide to the Zscaler Zero Trust Exchange. Zscaler, 2024. [Online]. Available: <https://info.zscaler.com/resources-ebooks-seven-elements-of-highly-successful-zta>
- [2] E. Ok, J. Williams, and J. Nicee, "Understanding Zero Trust Architecture," 2025. [Online]. Available: https://www.researchgate.net/publication/389713227_Understanding_Zero_Trust_Architecture
- [3] O. E. Ejiofor, O. Olusoga, and A. Akinsola, "Zero Trust Architecture: A Paradigm Shift in Network Security," Computer Science & IT Research Journal, Apr. 2025. [Online]. Available: https://www.researchgate.net/publication/390558157_Zero_trust_architecture_A_paradigm_shift_in_network_security

- [4] O. Christopher, T. Tenebe, E. Etu, A. Ayuwu, J. Emakhu, and S. Adebisi, "Zero Trust Architecture: Trend and Impact on Information Security," International Journal of Emerging Technology and Advanced Engineering, 2022. [Online]. Available: https://www.researchgate.net/publication/361758378_Zero_Trust_Architecture_Trend_and_Impact_on_Information_Security
- [5] National Institute of Standards and Technology (NIST), Zero Trust Architecture, NIST Special Publication 800-207, 2020. [Online]. Available: <https://csrc.nist.gov/pubs/sp/800/207/final>
- [6] J. Keshav, "Zero-Trust Security Models Overview," 2023. [Online]. Available: https://www.researchgate.net/publication/377247838_Zero-Trust_Security_Models_Overview
- [7] D. Holmes, "The Definition of Modern Zero Trust," Forrester, 2022. [Online]. Available: <https://www.forrester.com/blogs/the-definition-of-modern-zero-trust/>
- [8] J. Hietala, "Zero-Trust Architecture: Why Trusting No One Is a Smart Way to Protect Your IT Infrastructure," Red Hat, 2022. [Online]. Available: <https://www.redhat.com/architect/zero-trust-architecture>
- [9] Zscaler site, available: <https://www.zscaler.com/resources/security-terms-glossary/what-is-zero-trust-architecture>
- [10] Cloudflare site, available: <https://www.cloudflare.com/learning/security/glossary/what-is-zero-trust/>
- [11] CrowdStrike site, available: <https://www.crowdstrike.com/en-us/cybersecurity-101/zero-trust-security/zero-trust-architecture/>

VI Abbreviations

AI:	Artificial Intelligence
DDoS:	Distributed Denial of Service
IdP:	Identity Provider
IAM:	Identity and Access Management
IoT:	Internet of Things
OT:	Operational Technology
NIST	National Institute of Standards and Technology
SSL/TLS:	Secure Socket Layer / Transport Layer Security
VM:	Virtual Machine
ZT:	Zero Trust
ZTA:	Zero Trust Architecture