SECURE ACCESS REDEFINED: VPN VS. ZTNA

Transitioning from Legacy VPNs to Zero Trust Network Access (ZTNA)

INTRODUCTION

As remote work becomes the norm, secure access to private apps has become more critical. Traditional VPN solutions, provide network wide access, making it vulnerable to lateral threats. Modern Zero Trust Network Access (ZTNA) offers a next-generation approach, built to tackle these challenges and deliver a more secure, efficient, and scalable solution for remote access.

WHY THE SHIFT FROM VPN TO ZTNA?

VPNs, were designed for rigid perimeter-based networks, that rely on a "implicit trust" model, which trusts everything inside the network. ZTNA, however, operates on Zero Trust principles — granting access after identity is verified and context aware access is enabled, location is no longer relevant — ensuring secure and flexible access. ZTNA is increasingly becoming the de facto access control for campus users and hybrid workforce.

KEY CHALLENGES OF LEGACY VPN

Performance Degradation: VPNs increase latency due to extra travel time, encryption and servers that can handle only limited capacity

Security Risks: susceptible to Man-in-the-Middle (MitM) attack, data leaks, weak VPN protocols, limited logging

Complex Management: Managing VPN access and permissions is time-consuming and error-prone, especially in dynamic environments

> **56% of organisations experienced cyberattacks exploiting VPN vulnerabilities in the last year***

INTRODUCTION TO ZTNA

According to Gartner, Zero trust network access (ZTNA) creates an identity and context-based, logical access boundary around an application or set of applications. The applications are hidden from discovery, and access is restricted via a trust broker to a set of named entities. The broker verifies the identity, context and policy adherence of the specified participants before allowing access and prohibits lateral movement in the network.

ZTNA is built on the principle of "never trust, always verify." By enforcing least-privilege access, ZTNA significantly reduces the attack surface, protecting critical resources even in complex, hybrid environments. ZTNA grants application-specific access based on user identity and context, ensuring that users can only reach resources relevant to their role.

KEY DRIVERS OF ZTNA DEMAND

Secure remote access

Protecting sensitive data

Enabling BYOD (Bring Your Own Device) policies

ZTNA VS VPN: FEATURE COMPARISON

Feature	ZTNA	VPN
Security Model	Zero Trust, identity-based	Perimeter-based
Access Control	Application-specific access	Broad network access
User Experience	Optimised and adaptable to user location	Prone to latency, especially over long distances
Scalability	Scales easily with cloud-based access	Limited, challenging for large and distributed remote workforces
Risk Management	Reduced risk with least-privilege access	Higher risk due to lateral movement

TATA COMMUNICATIONS SASE GETS YOU THE ZTNA ADVANTAGE

Tata Communications delivers a carrier-grade and fully managed SASE solution that combines performance with insight-driven security, making secure access both seamless and powerful. Through our offering, customers can leverage unified SD-WAN and SSE solutions to kick-start their SASE journey.
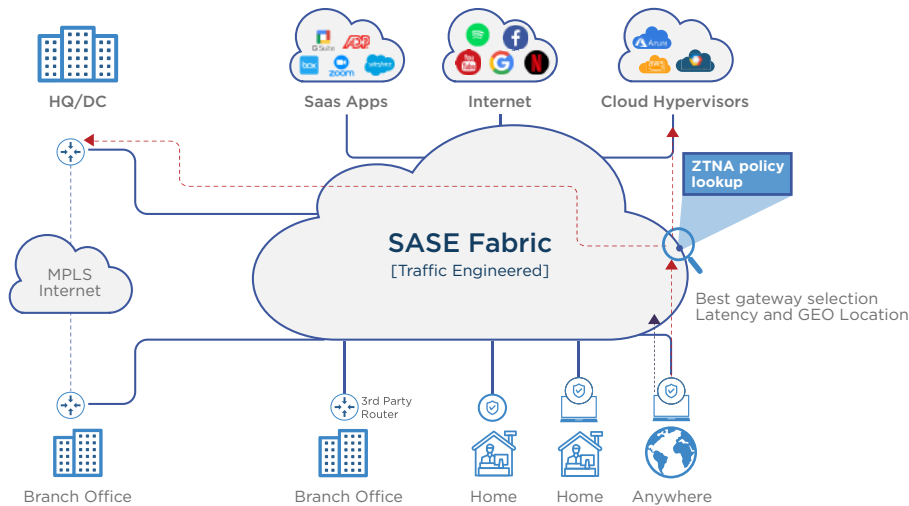
ZTNA SOLUTION OVERVIEW

Global SASE Points of Presence (POPs): Our extensive worldwide POP network ensures low-latency enabling seamless and efficient remote access.

Enhanced Visibility and Control: Comprehensive visibility, of underlay, overlay and security across distributed sites, hybrid users and applications.

Managed SASE Services: Handles the complexity of deployment, monitoring, and ongoing support and maintenance, allowing your teams to focus on strategic priorities.

Scalability: Easily supports a dynamic workforce with high scalability, ideal for hybrid and remote access needs.

CONCLUSION: WHY ZTNA IS THE FUTURE OF REMOTE ACCESS?

Remote working is here to stay and is expected to increase up to 77% in the upcoming decade as per a report by Global Workplace Analytics. By leveraging ZTNA organisations can meet the security and performance needs of remote workforce while protecting critical assets. Tata Communications' globally distributed SASE POPs and managed services make ZTNA implementation efficient and effective, helping businesses stay secure and productive.

EXPERIENCE ZTNA. START YOUR FREE TRIAL OR REQUEST A DEMO

*Zscaler ThreatLabz 2024 annual report