Private Communications Corporation

What is ZTNA?

Introduction

Zero Trust Network Access (ZTNA) is reshaping how companies secure their networks, data, and users in an increasingly remote and cloud-based world. Managed Service Providers (MSPs) play a pivotal role in helping businesses adopt this next-generation security framework, offering the expertise necessary to navigate its implementation. However, explaining ZTNA to clients, particularly in relation to its advantages over traditional security solutions like Virtual Private Networks (VPNs), can be a challenging task.

This white paper is designed to assist MSPs in effectively presenting ZTNA to their clients. It outlines key selling points, explains the benefits of ZTNA over VPNs, and clarifies why this technology is essential for modern businesses.

Understanding ZTNA

At its core, ZTNA is a security framework that embodies the principle of "never trust, always verify." Unlike traditional network security models that allow wide access to the internal network once a user is authenticated, ZTNA operates on a more granular level. It continuously verifies and authenticates users, devices, and access permissions, providing only the necessary access to specific applications or data based on real-time assessments.

In short, ZTNA eliminates the inherent trust that VPNs and firewalls extend to authenticated users.

Key Benefits of ZTNA for Businesses

When presenting ZTNA to potential clients, the conversation should focus on how ZTNA strengthens security, reduces complexity, and enhances the overall user experience.

Below are some of the most compelling advantages MSPs can use to highlight the value of ZTNA:

- **Improved security posture -** ZTNA addresses a critical shortcoming of traditional VPNs: the “all-or-nothing” approach to access. With VPNs, authentication occurs once at the connection point, and from there, users are typically granted broad access to the entire network. This model creates significant vulnerabilities, especially when credentials are compromised. In contrast, ZTNA ensures that authentication is ongoing, limiting access strictly to what’s needed for the task at hand. This model reduces the attack surface, making it far more difficult for bad actors to exploit stolen credentials.

- **Elimination of single points of failure -** Traditional VPN and firewall-based solutions rely on entry points that can become targets for exploitation. These systems inherently trust authenticated users, which means that once inside, a malicious actor can move laterally across the network. ZTNA, on the other hand, removes the need for a single network entry point. Instead, it employs multiple gateways, referred to as Gateways, which create secure outbound connections. By eliminating inbound connections, ZTNA makes it harder for attackers to gain unauthorized access, even if they manage to breach one gateway.

- **Reduced complexity -** Many companies today operate hybrid environments, where legacy systems coexist with cloud-based applications. This setup often requires complex security protocols and constant rerouting of traffic, which can slow down networks and increase costs. ZTNA offers a unified security approach that covers both on-premises and cloud environments. It treats cloud networks not as extensions of a legacy system but as part of a broader network that needs real-time, dynamic security measures. For MSPs, this is a strong selling point for businesses planning or in the process of cloud migration, as ZTNA can simplify security management across these environments.

- **Reduced costs -** Many businesses are concerned about the cost of transitioning from VPNs to ZTNA. However, ZTNA often results in long-term savings. By eliminating the need for a WAN (wide-area network), ZTNA can reduce bandwidth costs significantly. Additionally, since ZTNA provides more precise control over network access, it streamlines compliance processes and reduces audit costs. MSPs can present ZTNA as a cost-effective solution that not only enhances security but also reduces operational expenditures over time.

- **Improved User experience -** One of the most frequent complaints about VPNs is the poor user experience. VPNs often introduce latency and connection instability, especially when rerouting traffic through centralized servers. This can slow down workflows and frustrate end users. ZTNA improves the user experience by providing secure, direct access to applications and data without the bottleneck of centralized VPN servers. Whether a user is working from an office, remotely, or while traveling, ZTNA delivers seamless, secure access that is virtually invisible to the end user. For MSPs, this improved user experience is a strong selling point, as it directly addresses the frustrations many employees have with their existing VPN solutions.

- **Ease of transition -** For companies currently relying on VPNs, the transition to ZTNA can seem daunting. However, MSPs can position ZTNA adoption as a low-risk project by emphasizing that the VPN can remain as a backup during the initial stages of ZTNA implementation. Furthermore, ZTNA doesn't require businesses to rip out their existing infrastructure. It can be implemented alongside existing VPNs, offering companies a gradual transition with minimal disruption. MSPs should highlight the flexibility of this approach, reassuring clients that they don't have to abandon their current security solutions overnight.

VPN Replacement: A Gateway to Zero Trust

For MSPs, positioning VPN replacement as an entry point into Zero Trust is a strategic move. VPNs, while familiar, are ill-equipped to handle the evolving security threats that businesses face today. They struggle to adapt to changing risk levels and enterprise environments, and the requirement to manually create and update fine-grained access rules makes them cumbersome to maintain. ZTNA's dynamic, automated access control is not only more secure but also more agile and cost-effective.

Moreover, with many organizations facing the expiration of their VPN contracts, this is an ideal time to present ZTNA as a future-proof alternative. MSPs can reassure their clients that transitioning to ZTNA is not only secure but also strategically sound, allowing businesses to address current security needs while preparing for future growth.

ZTNA: The Future of Network Security

Zero Trust Network Access represents a fundamental shift in how businesses approach network security. For MSPs, it offers a powerful solution to address the security shortcomings of VPNs while delivering better performance, enhanced compliance, and reduced operational complexity.

By positioning ZTNA as a strategic, cost-effective security upgrade, MSPs can help their clients navigate the future of secure, flexible, and resilient network access.