Zero Trust Network Access (ZTNA)
The Next Level of Network Security
3/27/2026

Zero Trust Network Access (ZTNA) is a leading-edge cybersecurity framework that provides secure, identity-based access to specific applications and resources, rather than an entire network.

Unlike traditional security that trusts anyone inside a network perimeter (the "castle-and-moat" model), ZTNA operates on the core principle of "never trust, always verify." Each time a user tries to use a different app or resource, the system verifies that specific user has permission to access the app. This provides a much higher level of security than general network access approval alone.

Core Principles

- Verify Explicitly – Every access request is authenticated and authorized based on user identity, device health and real-time context (like location or time) before access is granted.
- Least Privilege – Users are granted the minimum level of access necessary for their specific role. They can only "see" and access the exact applications they are authorized to use, keeping the rest of the network hidden.
- Assume Breach – ZTNA assumes threats may already exist inside the network. It uses micro-segmentation to prevent "lateral movement," ensuring that if one account is compromised, the attacker cannot easily jump to other sensitive systems.

ZTNA vs. VPN (Virtual Private Network)

A Virtual Private Network (VPN) creates a secure, encrypted connection between a user's device and a private network over the public internet. It masks the original IP address and encrypts data traffic making it unreadable to unauthorized parties.

While both ZTNA and VPN provide remote access, they differ fundamentally:

- Access Level – A VPN typically grants broad access to an entire internal network once a user is logged in, while ZTNA grants access only to specific authorized applications.
- Trust Model – VPNs often use "one-time" authentication at the start of a session. ZTNA performs continuous verification, reassessing trust throughout the entire connection.
- Visibility – In a ZTNA model, applications are "dark," to an unauthorized user. They are not visible on the public internet, making them harder for hackers to discover or attack.

Key Benefits of ZTNA

- Supports Hybrid Work – It provides a seamless, secure experience for employees working in the office, from home or somewhere else without the speed bottlenecks of a VPN.
- Reduces Attack Surface - By hiding infrastructure and limiting user movement, it significantly lowers the risk of large-scale data breaches.
- Cloud-Native & Scalable – Most ZTNA solutions are delivered via the cloud, making them easy to scale as a company grows or moves more resources to platforms like Microsoft Entra or AWS.

The ZTNA – SD-WAN Advantage

ZTNA and SD-WAN (Software-Defined Wide Area Network) are complementary technologies that handle different aspects of advanced networking. SD-WAN focuses on how data travels between locations (the "pipes"), while ZTNA focuses on who is allowed to access specific data (the "gatekeeper"). SD-WAN optimizes network performance by intelligently routing traffic across various links like broadband or LTE.

Why Banks Need Both

Most banks can significantly benefit from having both:

- SD-WAN provides banks with fast, highly reliable connections between offices, excellent scalability, instant redundancy during outages and lower cost than private circuits like MPLS.
- ZTNA provides highly dependable security that safeguards access to all data on a request-by-request basis, limiting any potential breaches to a defined and isolated place on the network.

Together, they enhance a bank's security, access efficiency, customer service, compliance, profitability and more.

Grudi can help banks like yours gain the many benefits and peace of mind of ZTNA and SD-WAN. Learn how we can help your bank thrive at www.grudiassociates.com/banking or inquire at info@grudiassociates.com.