Name: Umma Islam

Title:Remote access: VPN vs ZTNA and when to choose each

Majors: M.S. in Data Science

Email: ummaislamit@gmail.com

Content:

- How do ZTNA and VPNs differ in architecture, security mechanisms, and user experience?
- What advantages and limitations does each approach present in contemporary enterprise environments?
- Under what circumstances should organizations adopt ZTNA, continue with VPNs, or implement a hybrid strategy?

In scope: Technologies for remote access, security ramifications, deployment issues, and use cases are all included in the scope.

Out of scope: Detailed implementation instructions, endpoint security unrelated to access, and internal network architecture unrelated to remote access are all outside the purview of this article.

Proposed Outline:

1. Background: An outline of remote access, the use of VPNs in the past, and the creation of ZTNA.
2. Technical evaluation: performance, scalability, security frameworks, architecture, and authentication techniques.
3. Case Examples: Sectors or situations where ZTNA is more appropriate than VPN.
4. Trade-offs: Security user experience, cost, complexity, and compliance consequences are some of the trade-offs and factors to take into account.
5. Recommendations: Hybrid techniques, transition advice, and selection criteria for remote access solutions.

Remote Access, Legacy of VPN use, and The Rise of ZTNA

1. **Remote Access:** Remote access simply means connecting to work systems from a location outside the office. This could be home, school, or even while traveling. It helps organizations stay productive and flexible, especially with more people working from home.

2. **VPN:** Virtual Private Network is a service that creates a "secure tunnel" between a user and the company's network. In past, VPNs were easy to set up, affordable, and worked well when most systems were stored inside office buildings. They made remote work possible for thousands of companies.

3. **ZTNA:** Zero Trust Network Access is a security model that provides secure access to specific applications by verifying user identity and device health before granting access, based on the principle of "never trust, always verify"

ZTNA and VPN benefits and the use of business settings

VPN Benefits:

1. Easy to deploy and integrate with legacy systems
2. Cost-effective for small/medium organizations
3. Provides full network access
4. Useful for IT administrators and internal maintenance
5. Works well for on-premise servers and traditional networks

ZTNA Benefits:

1. “Never trust, always verify” – much stronger security
2. Application-level access reduces breach risk
3. Prevents lateral movement inside the network
4. Better user experience (no heavy VPN tunnel)
5. Cloud-ready, ideal for hybrid workforce
6. Suitable for BYOD (bring your own device) and third-party access

Use of business settings

VPN: Best for legacy applications, internal admin tasks, full-network access

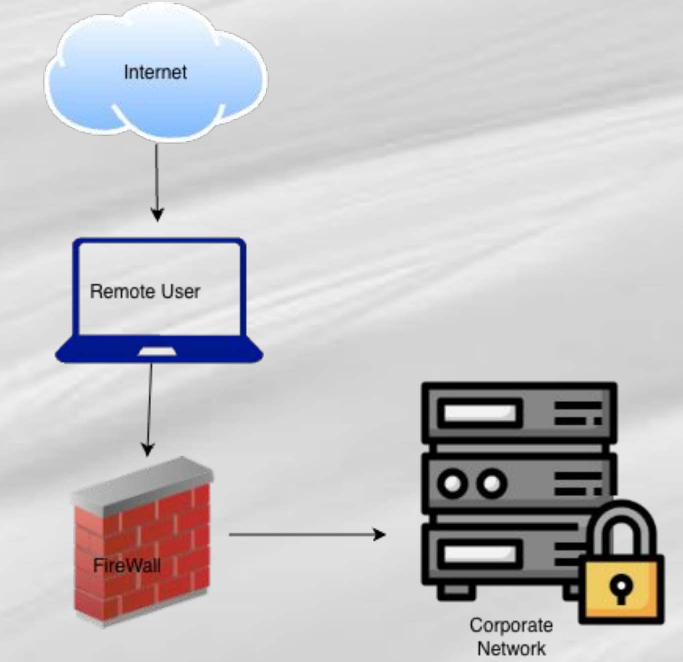
ZTNA: Best for modern cloud environments, remote teams, high security needs

Difference of ZTNA and VPN

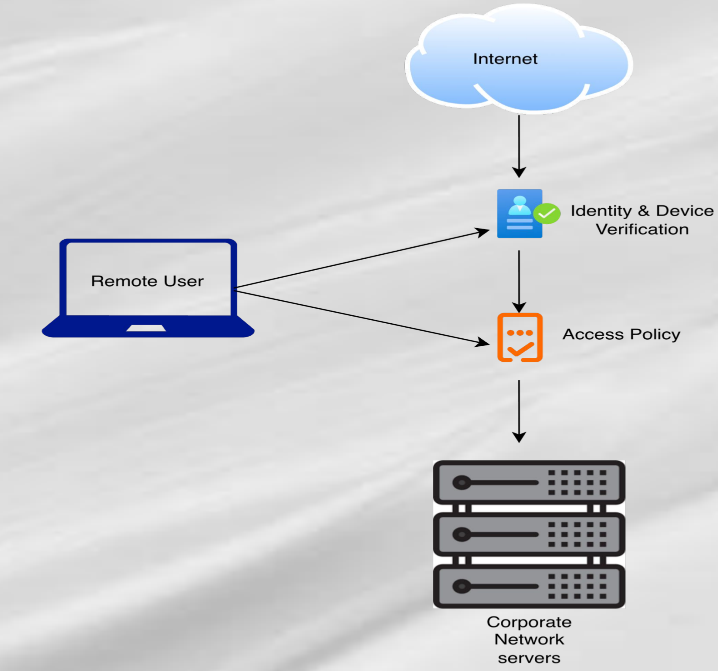
Feature	VPN	ZTNA
User experience	Slow, Requires client installation	Fast, only app level access
Approach	Implicit trust: If you are on the network will let you in.	Zero Trust always verify every user and device
Access	Grants access to the entire network once connected.	Grants access only to specific applications based on identity and context.
Firewall	Traffic passes through firewalls for network protection	ZTNA can provide direct application access without exposing the network, meaning there’s no need for a traditional firewall between the user and the app.
Risk if credentials stolen	High	Low

VPN & ZTNA Network Design

VPN



ZTNA



The times business should use ZTNA or VPN or Hybrid strategy

Use VPN When:

- Company has legacy on-premise systems
- Users need broad network access
- Budget is limited
- Infrastructure is small and stable
- IT teams require full administrative control

Use ZTNA When:

- Security is top priority
- Workforce is remote, global, or hybrid
- Company uses cloud and SaaS (Software as Service) applications
- Need to eliminate lateral movement
- Want continuous verification (Zero Trust model)

Use a Hybrid Strategy When:

- Organization is in transition from on-prem to cloud
- Some teams require VPN (IT admins), others need ZTNA
- Want gradual migration without disrupting users
- Need high security but must still support legacy apps

Key Sources:

1. Background on Remote Access and VPNs:

- *Garfinkel, S. (2023).* “Evolution of Remote Access Security in Enterprise Networks.” *Journal of Network Security and Management*, ProQuest.(https://search.proquest.com/openview/c6689ba21d788eb95159073c3b4c645f/1.pdf)

2. Rise and Principles of ZTNA:

- *Kindervag, J. (2010).* “No More Chewy Centers: The Zero Trust Model of Information Security.” *Forrester Research Report.* (https://media.paloaltonetworks.com/documents/Forrester-No-More-Chewy-Centers.pdf)

3. Technical Evaluation and Performance:

- *Kumar, A., & Banerjee, R.* (2023). “Performance Analysis of VPN vs. ZTNA in Multi-Cloud Environments.” *IEEE Access*, ProQuest. ((PDF) Implementing Zero Trust Architecture in Multi-Cloud ...ResearchGatehttps://www.researchgate.net › publication › 39211816…)

4. Trade-offs and Use-Case Comparison:

- *Okta Inc.* “Balancing Security and Usability: Why Organizations Move from VPN to ZTNA.” *Okta Whitepaper*, 2024. (https://www.okta.com/sites/default/files/2024-08/Okta-Secure-Identity-Commitment-Zero-Trust.pdf)

5. Standards and Framework References:

- *National Institute of Standards and Technology (NIST).* “Zero Trust Architecture.” *Special Publication 800-207*, 2023 Revision. (https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf)

Conclusion:

1. A well-defined scope that contrasts ZTNA and VPN for remote access.
2. Precise and current compilation of vendor and technical documentation.
3. High-quality references from reliable sources.
4. Logical, expertly organized framework with practical suggestions.
5. Fair evaluation of trade-offs to help businesses make decisions.