

POINT OF VIEW

Beyond the VPN

Universal ZTNA Is the Future of Secure Remote Access



Executive Summary

In today's increasingly connected world, remote access is no longer a luxury but a necessity for many organizations. This has led to the widespread adoption of virtual private networks (VPNs) to facilitate secure remote access. While VPNs are secure, they are architecturally limited to address modern security needs. Zero-trust network access (ZTNA) has emerged as a superior solution, offering a more secure, scalable, and user-friendly approach to remote access.

Risks of Laterally Moving Malware and Ransomware

Cyberattacks are by no means a new threat, but one of the rising concerns for network security professionals is attempts at lateral movement after an infection. Lateral movement refers to a group of methods cybercriminals use to explore an infected network to find vulnerabilities, escalate access privileges, and reach their ultimate target. It is called lateral movement because of the way the hacker moves sideways from device to application and so forth.

While VPNs provide secure connectivity, they are architecturally limited to prevent lateral movement. The risks associated with lateral movement of malware become even more critical in the context of a hybrid workforce, where work-from-anywhere (WFA) employees seamlessly switch between working remotely and on-site.

The Evolution of ZTNA

Universal ZTNA, an advanced evolution of ZTNA, addresses these challenges head-on. It uses a "never trust, always verify" philosophy, continuously authenticating users and devices and granting access only to the specific application or resource needed. This least-privilege approach significantly reduces the attack surface and minimizes the potential impact of breaches. Moreover, ZTNA utilizes dynamic access control mechanisms, continuously verifying user identity and device posture before granting access. This ensures that only authorized and trusted users can access sensitive data, and access can be removed in real time if they are compromised.

In addition to improved security, Universal ZTNA offers several other advantages over VPNs. Universal ZTNA solutions are inherently scalable, able to accommodate fluctuating numbers of remote users without impacting performance. This makes it ideal for organizations with a rapidly growing workforce or those experiencing seasonal peaks in remote access needs.

A More Seamless, Efficient Experience

From a user perspective, Universal ZTNA offers a more seamless and efficient experience. It eliminates the need for manual VPN configuration, allowing users to access applications quickly and easily from any device. Additionally, Universal ZTNA does not require backhauling all traffic through a central VPN server, which can significantly improve performance, especially for geographically dispersed users.

While Universal ZTNA offers substantial benefits over VPNs, it is important to acknowledge that it is not a perfect solution. Some potential challenges include the need for integration with existing security infrastructure and the possibility of performance bottlenecks and traffic latency if not implemented correctly. However, with careful planning and execution, these challenges can be easily overcome.

Conclusion

Universal ZTNA represents a significant leap forward in secure remote access. By eliminating the inherent-trust model of VPNs and adopting a least-privilege approach, Universal ZTNA addresses critical security concerns while offering improved scalability, user experience, and operational efficiency. Furthermore, these security principles for remote access can be brought to secure internal network access using a Universal ZTNA solution, lowering the risk for the new hybrid working model.

As the world continues to evolve toward a more remote work environment, Universal ZTNA is undoubtedly the future of secure remote access. Organizations that prioritize security, flexibility, and user experience should seriously consider transitioning from VPNs to Universal ZTNA to ensure a robust and future-proof solution for their WFA employees.

Harness the Power of GDT & Fortinet

Universal ZTNA provides distinct advantages over traditional, VPN-based approaches. However, adopting Universal ZTNA means overcoming challenges such as legacy equipment, network design decisions, identity controls, and more. It's a lot to contend with — especially without the right expertise.

That's where GDT can help. As a Fortinet Engage Preferred Services Partner, GDT has invested in building advanced knowledge and expertise, with 28 certifications across the Fortinet product line.

GDT offers a complimentary Zero Trust and SASE Readiness Workshop designed to help you accelerate your ZTNA journey. This half-day, interactive session with GDT security experts delves into your organization's unique needs and challenges, infrastructure, applications, data, users, and identity functions. GDT experts combine workshop findings with insights and industry best practices to deliver a high-level roadmap to ZTNA success.

Claim Your Zero Trust
and SASE Readiness
Workshop



www.fortinet.com