

VPN vs. ZTNA Checklist

For decades, VPNs have been a steadfast technology for remote access for the business, a digital drawbridge to the corporate castle. Yet, with applications migrating to the cloud and users now mobile, VPN technology finds itself outpaced as both security and experience leave the business wanting for more.

Replace your VPN with a modern technology, Zero Trust Network Access (ZTNA). See why many organizations are turning to ZTNA as a VPN alternative.

VPN

ZTNA



Security

- VPNs reinforce the traditional perimeter-based security model, which grants implicit trust to any device, user, and application within the network boundary.
- VPNs expose ports to the internet to allow network access, making it a target for malware and ransomware attacks.
- VPNs provide users full access to a network's resources and run the risk of exposing the network.
- VPNs work on the network level and only have control and visibility of low-level network traffic.
- VPNs allow BYOD devices to access the corporate network from unmanaged, non-corporate endpoints, which may introduce malware or other cyber threats.
- VPNs are vulnerable to distributed denial-of-service (DDoS) attacks that can overwhelm the VPN server and disrupt the service.

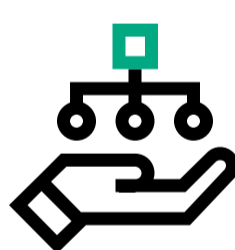
- ZTNA implements the zero-trust security model, which works on a "never trust, always verify" basis and does not rely on a fixed perimeter.
- ZTNA solutions never expose IPs to the internet, making the corporate network invisible to unauthorized users or bad actors.
- ZTNA limits lateral movement and user connections to specific applications and continually verifies the user and device trust, reducing risk and building security resilience.
- ZTNA works on the application level and can set up granular access policies based on a user-to-app basis. The result is higher levels of control and in-line visibility of activity.
- ZTNA can enforce strict device posture checks and policies before granting access to any resource, ensuring that only the compliant devices can connect.
- ZTNA solutions can mitigate DDoS attacks by using distributed cloud infrastructure that can scale up or down as needed, as well as applying rate limiting and filtering mechanisms.



Flexibility

- VPNs are designed to provide secure remote access to the corporate network, but often have limited support for cloud-based resources.
- VPNs often suffer from performance issues due to bandwidth limitations, network congestion, and latency.

- ZTNA can provide secure remote access to both on-premises and cloud-based resources, as well as hybrid environments.
- ZTNA solutions can optimize performance by using cloud-based architecture that ensures the closest access path to the user and the application, as well as scaled capacity as a result of the cloud.



Management

- VPNs require users to install and configure client software on their devices which can be cumbersome and prone to errors.
- VPNs are difficult to monitor and audit as they do not provide granular visibility into the user activity and application usage.

- ZTNA solutions can provide clientless access to applications via a web browser, which simplifies the user experience and reduces IT support costs.
- ZTNA solutions can provide detailed logs and reports on user identity, device posture, application access, and network traffic, enabling better compliance and security analysis.

Is it time for you to say goodbye to VPN?

Learn how you can make the switch from VPN to ZTNA.

[Read the eBook](#)

Our solution partner



BlueAlly is an authorized partner of HPE

(800) 886-5369
contact@blueally.com
www.blueally.com

For more information about HPE Aruba Networking, visit our partner website: www.securewirelessworks.com

Learn more at

arubanetworks.com/resource/making-the-switch-from-vpn-to-ztna

Visit ArubaNetworks.com

Make the right purchase decision. Contact our presales specialists.



Contact us