perimeter 81

ZTNA vs On-Premises VPNs for the Hybrid Workforce

Securing Today's Remote Workspaces

Legacy hardware VPNs don't answer today's needs for secure remote access. This leaves organizations vulnerable to security breaches and increases the risk of cyberattacks.

By default, they provide users within the organization access to the entire internal network, even though very few actually need this. In addition, the complex configuration of legacy firewalls makes it difficult to restrict users and devices to accessing only the specific applications they need. Without granular access controls, there's a significant increase in security risk and a larger attack surface.

From segmented user access to seamless scalability, Zero Trust Network Access (ZTNA) supports companies with an all-encompassing solution to secure resources whether they're on-prem or in the cloud.

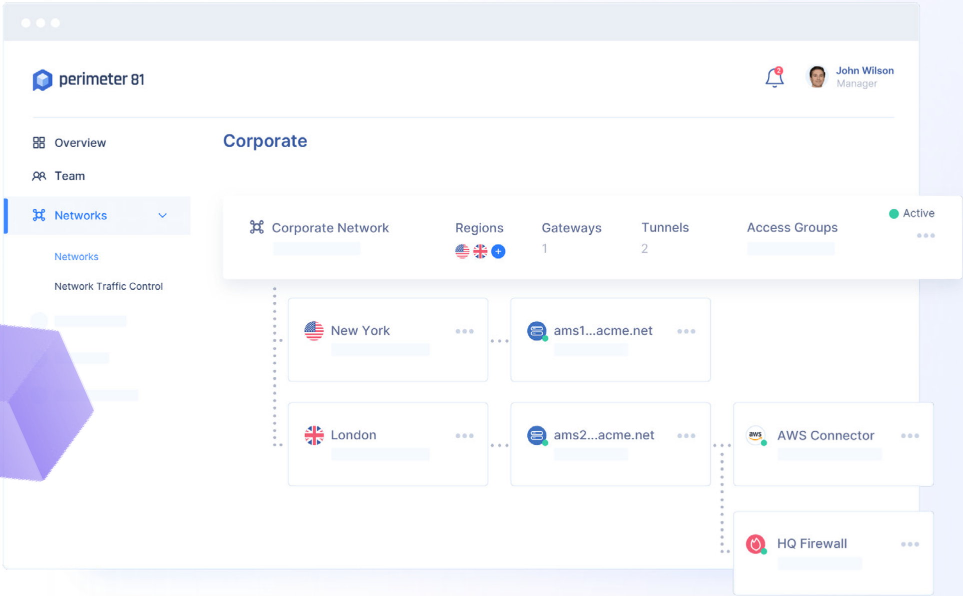
Enterprise-Grade Network Security for All Businesses

The traditional perimeter-focused approach grants implicit trust to any user that enters the network via an approved VPN tunnel. This means that compromised VPN credentials can lead to malicious “authenticated” access by attackers who can move laterally through the network.

Zero Trust Network Access (ZTNA) grants access to corporate resources based on the principles of zero trust, which is an evolution of the principle of least privilege (PoLP): only specific employees may access specific company applications. In addition, continuous verification using context-based rules ensures that only approved users who meet certain security conditions can access resources.

These strict access control enforcements enable ZTNA solutions to narrow the organization’s attack surface and help reduce data breaches and data loss, system and application vulnerabilities, advanced persistent threats (APTs), denial of service attacks, account hijacking, and reduce the impact of malicious insiders.

Ideal ZTNA solutions are delivered from a flexible cloud-based platform that converges the secure connection of a VPN with easily implemented granular access rules for better overall security. Moreover, this all happens inside a single management platform that provides a 360-degree view of network activity.



The ZTNA Adoption Pipeline

ZTNA isn't a switch you flip. Instead, it's a strategy that employs a set of technologies to identify, authenticate and verify each company user in order to access company applications and resources.

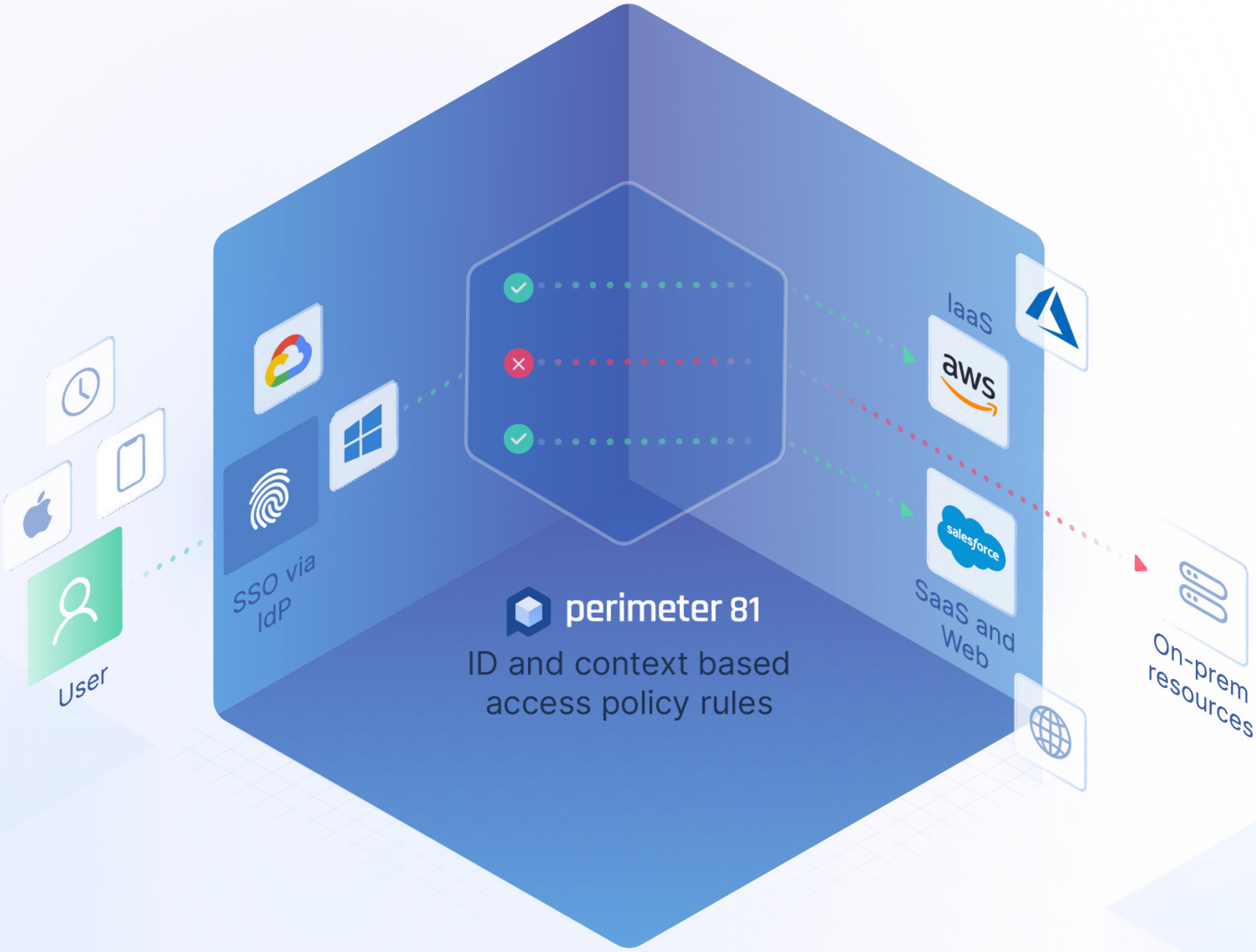
- ZTNA starts by identifying users through integration with a company's **Identity Provider** that ideally supports **Single Sign-on (SSO)** and **Multi-Factor Authentication.**
- Access is either blocked or permitted based on the user identity, context, device security posture, and access rules required for each resource.
- Thus a malicious actor with stolen credentials will have their access limited to specific areas and will not be able to fully traverse the network. This significantly reduces the level of exposure and potential damage to the company network.

In order to limit the attack surface and decrease the chances of online threats, ZTNA adoption in place of on-prem solutions is quickly becoming the norm.

Comparing ZTNA vs On-Prem Firewall VPN

	Zero Trust Network Access	On-Premises VPN
Device Security Posture Enforcement	Devices are checked for security posture before gaining access.	Devices do not undergo a posture check.
Cost Reduction	Cloud-based ZTNA reduces configuration complexity and onboarding time. Plus, it eliminates the need for hardware maintenance and upgrades.	Hardware requires manual installation, configuration, physical storage space, cooling, ongoing maintenance, and trained personnel to install and maintain. VPN upgrades via concentrators can be very costly and complex to manage.
Unified Management	Networks and users are easily managed from a single dashboard.	Each on-prem appliance is individually managed often with complex interfaces and spread across multiple offices.
Improved Network Performance	Direct to cloud access enables faster connections, and better network performance.	Traffic backhauling to the corporate physical location means the user experiences high latency, and a less efficient workflow.
Simpler and More Secure User Authentication	Centralized management of user access with identification and multi-factor authentication. Wide support of IdPs, for easy single sign-on (SSO).	User identities managed across multiple firewalls. Only some IDPs are supported.

Support for Unmanaged and Third-Party devices	Clientless access to apps for unmanaged devices, without exposing those users to the whole network.	Not supported.
Easy and Fast User Onboarding	Adding users and expanding networks can be done in minutes.	Scaling is often a complicated and manual process.
Full Network Visibility	Single interface for entire network visibility.	Network visibility is fragmented across different locations.
Traffic Encryption	All traffic is end-to-end encrypted.	Only for the client to the VPN appliance.
Secure Granular Access Control	Segmented user access across network resources.	Segmenting user access can be complicated and performance may be hindered.
Converged Advanced Security Capabilities	Features such as SWG Web Filtering and Malware Protection should be integrated alongside ZTNA to maximize network security.	Firewall capabilities extend to anti-malware and intrusion prevention systems.


User
SSO via IdP
perimeter 81
ID and context based access policy rules
IaaS
aws
salesforce
SaaS and Web
On-prem resources

Perimeter 81’s ZTNA Solution

Perimeter 81 offers a powerful cloud-based ZTNA solution as part of its cloud-based, converged networking and network security platform.

1 Perimeter 81’s ZTNA solution ensures that users access cloud resources via encrypted tunnels directly from the Perimeter 81 network, with granular access rules that lock down network resources and application access.

2 The Perimeter 81 network is global with over 50 PoPs located across the world, ensuring minimal latency and a faster user experience to any user anywhere in the world.

3 Web filtering and Malware Protection add another layer of protection to ensure users are secure while interacting with the open Internet.

4 The Perimeter 81 solution secures access to any network resource: on-prem data centers, public cloud (AWS, Azure, GCP), or private cloud, via IPsec or more advanced Wireguard tunnels.

5 Perimeter 81 supports an array of ports and protocols, including non-web applications like VoIP.

6 Perimeter 81’s global backbone uses dual Tier-1 carrier networks and peering agreements with all the major cloud providers with reserved bandwidth for optimized delivery

7 Agentless access supporting a wide range of protocols: SSH, RDP, VNC, Telnet

The Perimeter 81 platform is the right solution for a network environment of accelerating complexity, which is the single greatest obstacle to effective network security.

Instant Deployment

In just a few clicks, Perimeter 81 allows you to purchase, provision, and enable secure zero-trust access on-prem, in the cloud, and anywhere in between. Easy scalability and transparent pricing allow you to easily grow, backed by our 24/7 Customer Success engineers.

Unified Management

Effortlessly manage and onboard employees, instantly deploy a multi-regional network, and install our cross-platform agent across all endpoints within a single dashboard.

Full Visibility

Effectively monitor network health, view employee resource access, integrate with leading SIEM providers, and identify any suspicious activity for a unified view of your network security.

Converged Security

Avoid the complexity of using dozens of cybersecurity solutions in favor of a single, well-designed platform that makes it easy to configure your network, implement security policies, detect attacks, and defend against data breaches.

About Perimeter 81

Perimeter 81 is a robust, yet easy-to-use, converged networking and network security platform that connects all users, in the office or remote, to all resources, located on-prem or in the cloud. It is a cloud-native service that includes advanced capabilities such as Zero Trust remote access, Internet access control, malware protection and firewall as a service. It enables any business to build a secure corporate network over a private global backbone, without hardware and within minutes. The entire service is managed from a unified console and is backed by an award-winning global support team that has you covered 24/7.

CONTACT US

Perimeter 81, LTD.

sales@perimeter81.com

perimeter81.com

Request a Demo