perimeter 81

ZTNA vs. VPN

How a ZTNA solution does what VPNs can't

How to Make Remote Access Safe Again

Once upon a time providing employees, partners or customers with remote access to the corporate network, servers, or applications was almost unheard of. Only a very few had the privilege to access their work network remotely because it was complex to deploy, often unreliable and posed a real security risk.

Those days are long gone. Remote access is the norm. And not just for work from home scenarios. For almost every key business process.

Until recently the gold standard solution for companies to provide remote access functionality was Virtual Private Networks (VPNs), introduced over 30 years ago. Legacy VPNs provided ostensibly secure, remote access to the corporate network through a point-to-point connection by creating an encrypted “tunnel” through which IP traffic flows.

But VPNs were made for a much simpler time. And much smaller networks.

The untold story is that the inherent design of VPN technologies can potentially make enterprises more vulnerable to attacks and data breaches. That’s because they give users within the organization access to the entire internal network in order to access company resources. Users are not restricted to specific network resources. This makes VPNs one of the weakest points of failure with respect to identity access and credential management. There is no segmentation, audit or control.

Besides the lack of network segmentation, VPNs lack traffic visibility, on-premises user security and an overall network security. VPNs are also not suited for dynamically expanding networks because they lack integrated management and cannot easily adjust to network or server changes. This makes it more complicated to scale and rapidly adjust for new users and network locations and increasingly difficult to effectively manage hybrid and cloud-based computing architectures.

Simply put, VPN technology has not kept pace with today’s security requirements and the ever-evolving threat landscape. It’s time to ask: Are VPNs past their prime?

The ZTNA Solution

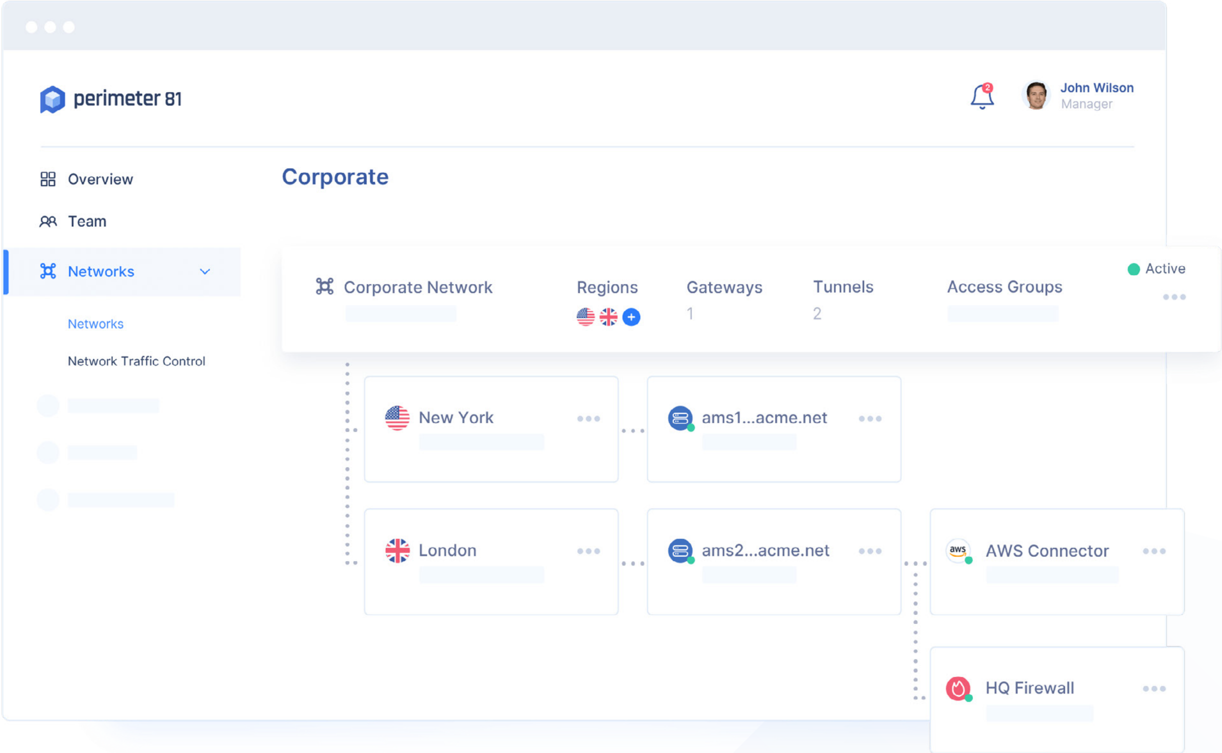
Today's answer to remote access security challenges is a zero trust security model.The zero trust model does exactly that: trusts no one!

The traditional approach, and the one on which VPNs are based, grants implicit trust to any device, user, and application within a given network that enters via the VPN tunnel. This means that compromised VPN credentials or exploitation of a VPN vulnerability 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 principle of zero trust, or least privilege. Users are granted access to what they need and where they need it to carry out their role. Nobody who has not been identified can access the corporate network.

ZTNA solutions address traditional VPN limitations while providing a flexible cloud-based platform, device and application configurability as well as accessibility, increased security, privacy and user-access control granularity and analytics. Moreover, they do it from a single management platform that gives IT a 360 degree view of access and security.

By reducing the attack surface of exposed hosts, ZTNA solutions help reduce data breaches and data loss, system and application vulnerabilities, advanced persistent threats (APTs), denial of service attacks, account hijacking and malicious insiders.



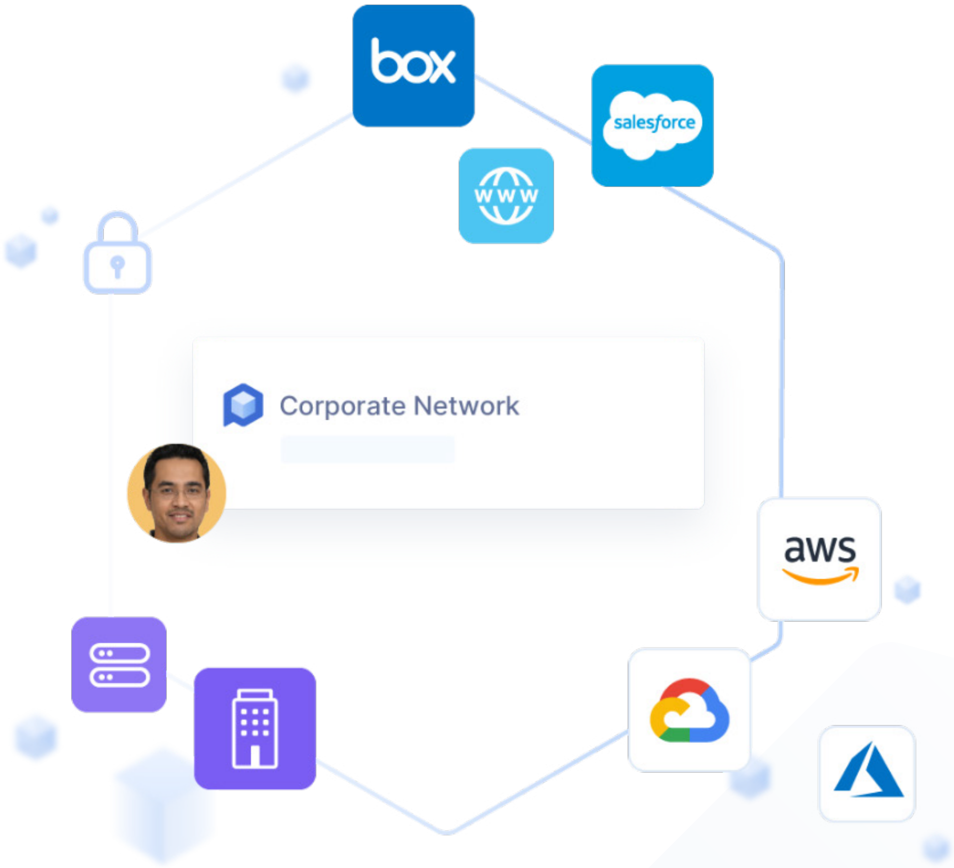
Corporate Network	Regions	Gateways	Tunnels	Access Groups	Active
		1	2		

What is ZTNA?

Zero Trust is a cybersecurity concept centered on the best practice that no network user should be automatically trusted to access any computing resource on the network or on the cloud. Zero Trust Network Access (ZTNA) implements this concept by first verifying the identity of the user, classifying them, and then allowing access based on who they are and what they need to do—not where they are located. Users are granted access only to applications they have a legitimate need for, with rights and permissions granted to reflect that need.

It starts by identifying users (via Identity Provider integration and Multi-Factor Authentication) and the context behind their requests for access through the unified ZTNA solution. Access is either blocked or permitted by the ZTNA solution based on identity, context, and ZTNA rules that determine what identity and context are required to access each resource. When combined with virtual network segmentation using Firewall as a Service (FWaaS) implemented in the ZTNA platform, a hacker with stolen credentials will have their access limited to only specific areas and will not be able to fully traverse the network. This approach will reduce the level of exposure by an order of magnitude.

Using a Zero Trust model approach to secure network access services, a ZTNA solution lets organizations deploy a managed high-security, enterprise-wide network service virtually, on a subscription basis.



Why ZTNA Beats VPN Hands Down

More and more companies are choosing to deploy a ZTNA solution for central management of security and access. ZTNA provides clear benefits to growing businesses who need more security measures than the average VPN can provide.

Central Management and Control

ZTNA solutions provide a single dashboard for managing network access and security. All access rules can be managed in a single location, avoiding human error and configuration gaps.

Easy Expansion and Scalability

Beyond the extra security measures it enables, ZTNA allows network access to expand with the organization, while the capacity or bandwidth limitations of traditional VPNs prevents them from expansion and scalability. It is also difficult and costly to support widely deployed VPN agents and outdated hardware as the organization grows.

Securing the Real Perimeter

ZTNA solutions secure the real perimeter of the organization, not just the physical one. As more employees work from home and company resources move to the cloud, ZTNA secures the cloud perimeter that includes both remote workers and cloud resources. This software perimeter also allows the micro-segmentation needed to protect assets in the cloud, without requiring users to first access the on-premises network. VPNs can only “stand guard” at the physical perimeter, which is no longer viable or effective.

Granular Access

By individually authorizing each access request, ZTNA solutions ensure users only get access to what they need, rather than allowing “authorized” entry to the entire network, including all its devices and assets. By only making the resources that users need visible, ZTNA makes it more difficult for malicious attackers to laterally move across the network and makes the network less vulnerable to DDoS attacks.

ZTNA solutions that have powerful application-level access management allow even more control by managing policies at the application, query, and command levels. VPNs offer none of this flexibility.

User Identity & Easy Onboarding

The identification of users in a ZTNA flows from a seamless integration with Identity Providers and integrated Multi-Factor Authentication. This ensures that new users are easily onboarded while protecting the network from some of the most common hacks.

ZTNA solutions that offer a clientless configuration also enable easy onboarding of external partners or vendors. There is no need to install VPN hardware or software on partners' devices in order to safely connect to specific assets within the corporate network. Moreover, clientless configurations for third parties can limit these third parties to a single resource without giving them any visibility into the network as a whole.

Device Posture Security

Another important aspect of a ZTNA solution is its ability to ensure that all devices that connect to a VPN are authenticated and have the correct device posture. Using ZTNA, IT can define what file or certificate a device needs to have to connect to the network, and can ensure that all connecting devices are protected with antiviruses and other measures. The authentication enforced by built-in device posture security prevents breaches due to phishing attempts and similar hacks.

Compliance

ZTNA solutions comply with international standards like SOC 2 Type 2 and ISO standards, unlike most VPNs. This compliance can be crucial for businesses that need their own solutions to meet these requirements as well.

ZTNA vs. VPN

ZTNA	VPN
Centrally managed network security policies	No central network policies
Zero Trust, least privilege access for remote users	Lack of remote user security measures; remote users can access entire network
Precise segmentation and context-based access rules	No granular access rules
Multiple security measures at the network and device levels	Lacks business security functionality such as device posture security
Streamlined identification and multifactor authentication	Doesn't integrate with Identity Providers
Seamless audit and reporting	Little network traffic visibility; no network activity reports
Complies with international standards	Does not comply with international standards

Do More with Zero Trust

Remote Access to the Cloud

Protect your network, your employees, and your critical corporate applications with a single solution that allows secure remote access to all on-premises and cloud resources for managed agent devices and unmanaged agentless devices.

Secure Third-Party Access

Easy to enable secure collaboration with 3rd party contractors through agent or agentless access with no exposure to the Internet. Complete segmentation and granular security policies for differentiated access, so third parties do not have general access to the network.

Distributed VPN Replacement

Multi-regional deployment ensures that employees are secured from anywhere in the world. User- and device-based segmentation, FWaaS and 2FA and user-access rules for a scalable, user-friendly and pay-as-you-grow solution.

Easily Scalable Networking

Single platform for easily adding and managing users, networks, tunnels and access points, and adding more layered security as needs grow. Global data centers support all networking needs.

Perimeter 81's ZTNA Solution

Perimeter 81 offers a powerful cloud-based ZTNA solution built into its Cybersecurity Experience (CSX) Platform. The CSX Platform is the first platform to streamline ZTNA. Perimeter 81 has been selected by Forrester as a New Wave ZTNA Leader.

The Perimeter 81 ZTNA solution ensures that users access cloud resources via encrypted tunnels directly from the Perimeter 81 network, to lock down network resource and application access using Zero Trust policies, rules, and permissions. The Perimeter 81 network is global with over 40 PoPs located across the globe. Perimeter 81 ZTNA ensures that users only have access to the resources they need, even after they are connected. DNS filtering adds another layer of protection to ensure users cannot access risky websites. The Perimeter 81 solution secures access to any network resource: on-prem data centers, public cloud (AWS, Azure, GCP), or private cloud via an IPsec or Wireguard tunnel. And Perimeter 81 supports all ports, all protocols, including non-web applications like VoIP. Each Perimeter 81 gateway offers 1 Gb/s of bandwidth.

The Perimeter 81 CSX platform is the right solution in a world where accelerating complexity is the single greatest threat 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. Quickly scalable microservice architecture and transparent pricing allow you to easily grow, backed by our 24/7 Customer Success engineers.

Unified Management

Effortlessly manage and onboard network users, instantly deploy secure cloud gateways, create multi-regional networks, and install cross-platform applications across all endpoints within a single dashboard.

Full Visibility

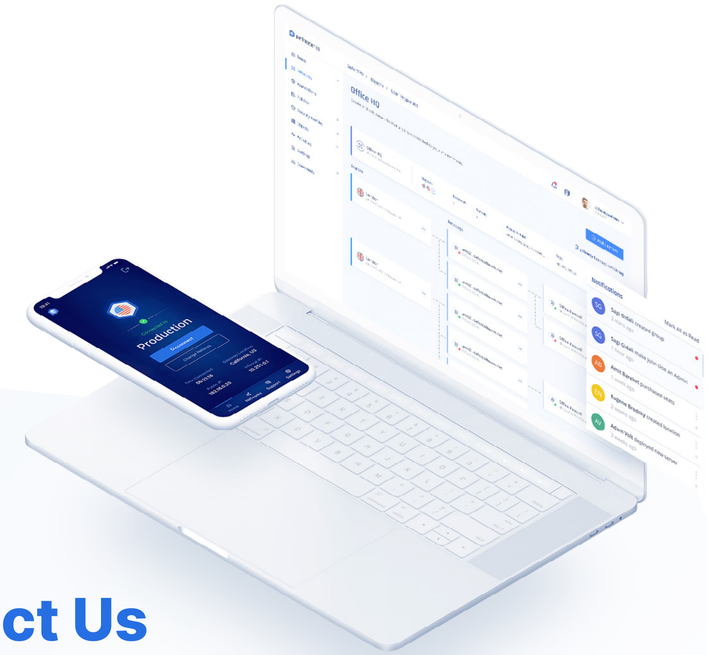
Effectively monitor network health, view employee resource access, integrate with leading SIEM providers, and identify any suspicious activity with a unified view of your network security

Integrated Security

Avoid the complexity of using dozens of cybersecurity solutions with a single well-designed platform that makes it easy to configure your network, implement security policies, detect active attacks, and defend against data breaches perimeter 81

About Perimeter 81

Perimeter 81 radically simplifies cybersecurity with the world's first Cybersecurity Experience (CSX) Platform. As a holistic, cloud-based solution,Perimeter 81 allows organizations of all industries and sizes to easily support the decentralized, hybrid workplace while avoiding the cyber complexity that hurts IT's ability to defend corporate cloud and on-prem networks. Backed by Tier 1 Investors such as Insight Partners, Toba Capital, and others, Perimeter 81 is headquartered in Tel Aviv, the heart of the startup nation, and has US offices in New York and Los Angeles. Our 2,100 customers range from SMBs to Fortune 500s across a wide range of industries, and our partners are among the world's leading integrators, managed service providers, and channel resellers.



Contact Us

Perimeter 81, LTD.
+1-646-518-1997
www.perimeter81.com

Request a Free Demo