ZERO Networks

SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS

USE CASES

Securely Connect Remote Employees and Vendors

TL;DR

VPN and ZTNA have so far been the main solutions to securely connect remote employees and vendors to the network. With the rise of work from home, security architects are facing a Faustian bargain: Prioritize speed and cost (VPN) or zero trust security with a compromise on user experience (ZTNA)?

VPNs are fast, but less secure given their open port on the internet. ZTNA are secure, but expensive and slower given their routing all traffic through someone else's cloud.

Zero Networks combines the speed of VPN and the security of ZTNA in a unified platform that connects any user and segments any asset. It offers direct connectivity with no obfuscation, has no open ports to the internet, segments vendor access and packs unrivaled network speeds via WireGuard®.

So... VPN or ZTNA?

With the rise of work from home and hybrid work environments, IT teams have been grappling with how to keep their networks and data safe from potential security breaches stemming from remote access.

VPN (Virtual Private Network) and ZTNA (Zero Trust Network Architecture) have emerged as the two main solutions, but each comes with its own baggage.

VPN works by creating a secure tunnel between a user's device and the VPN server, essentially extending the private organizational network into the public network. While VPNs provide direct network connection with optimal performance, they must keep open ports on the internet, making them visible to hackers and therefore susceptible to vulnerability exploitation and other attacks. In fact, searching for port 3389, Microsoft's RDP, is a common ransomware attack method.

Glossary

What is Zero Trust Network Access (ZTNA)?

View →

ZTNA solves this security weakness by hiding itself through a proxy on the vendor's cloud service. However, ZTNA also introduces latency and higher costs as all traffic is routed through the vendor's cloud. Plus, due to their NAT architecture, ZTNA solutions obfuscate the identity of all users connecting through it, making it appear as if all users are connected from a single IP address. This can break various technologies and blind detection solutions.

Zero Networks Connect: The Best of Both Worlds

Zero Networks Connect is a secure remote access solution that combines the speed of VPN and the security of ZTNA, eliminating their flaws. It is the only remote access solution on the market that provides zero trust architecture and an optimal network performance, and is part of the unified network security platform that can connect any user and segment any asset.

Zero Networks Connect enables maximum network performance with direct peer-to-peer connectivity via WireGuard®, widely accepted as the fastest open-source VPN with best-in-class cryptography.

Like ZTNA, Zero Networks Connect has no open ports to the internet. Only an approved asset (after MFA validation) can "see" and connect to the port.

Moreover, Zero Networks Connect allows vendor access segmentation based on user access configuration, ensuring that vendors can only access the resources they need within the network. A VPN does not support this unless additional security products are deployed.

Unlike ZTNA, Zero Networks Connect offers direct connectivity with no obfuscation, meaning that once logged in, each user keeps their IP address with no NAT-ing involved.

How does it work?

1. The user connects using Zero Connect Client.
2. MFA authentication is enforced by Zero Networks.
3. The Cloud service allows access from the user's IP to Zero Connect VPN by dynamically opening the VPN port only for the user's IP.
4. A tunnel is established, and the user can access the company's corporate data based on their required permissions.