Technical overview - Zero Networks Connect™

ZERO. Networks

SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS

All of the benefits and none of the downsides

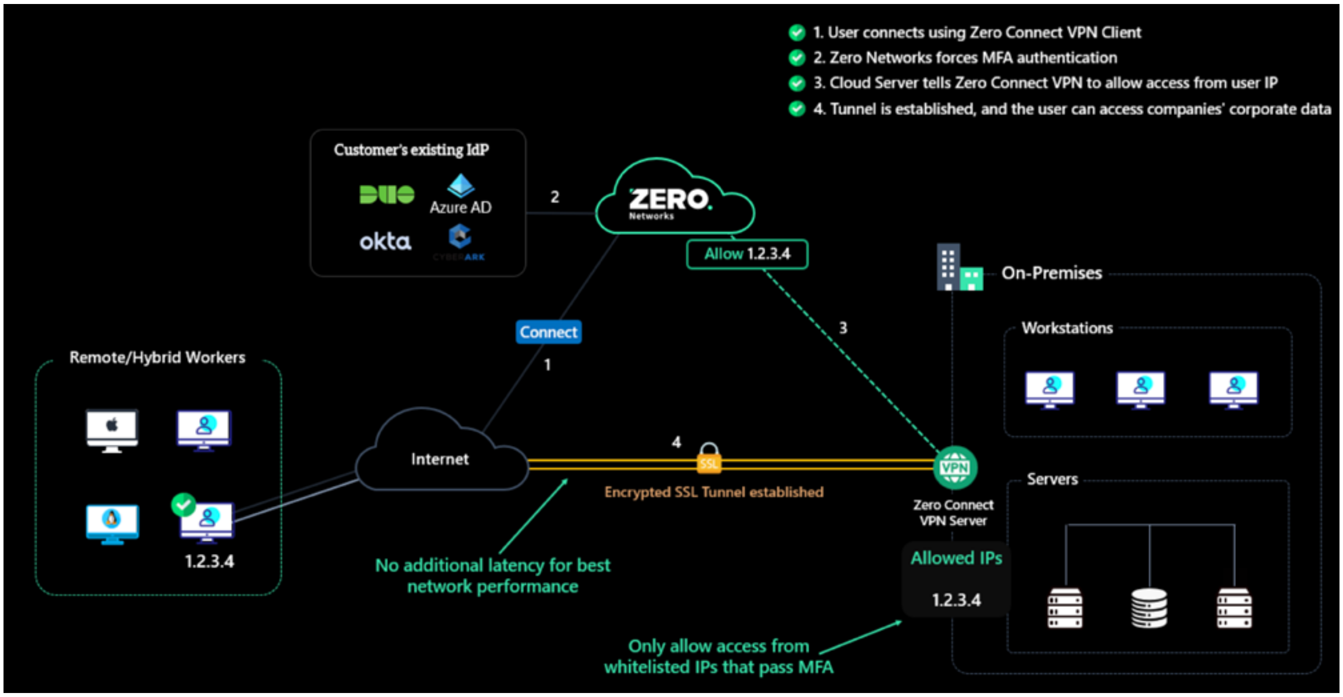
Remote work has changed the security landscape. In response, vendors have turned to two solutions to keep networks safe in the era of remote access: VPN and ZTNA. But each solution comes with its own pros and cons, leaving IT teams wishing there was a ‘best of both worlds’ secure remote access solution.

While VPNs offer direct and reliable networking performance, the downside is having to leave ports open and vulnerable to anyone on the internet to hack (which happens periodically).

ZTNA gets around that problem by concealing itself through a proxy that can sit on the vendor’s cloud service. However, as a result it suffers degraded performance, bad user experience, as well as potential privacy concerns, as all traffic is routed through some Vendor’s cloud. Plus, obfuscating the identity of all the users connecting through it creates a security blind spot.

Zero Networks Connect™ combines the best aspects of VPN and ZTNA and eliminates their flaws.

How does it work?



✓ 1. User connects using Zero Connect VPN Client
✓ 2. Zero Networks forces MFA authentication
✓ 3. Cloud Server tells Zero Connect VPN to allow access from user IP
✓ 4. Tunnel is established, and the user can access companies' corporate data

Zero Connect client:

An auto-updatable light-weight client, based on WireGuard®, deployed on each asset that requires remote connectivity and does not require any maintenance.

The key capabilities of the client include:

Routing architecture

Direct connectivity with no obfuscation. Each user has their own IP address with no NAT-ing involved. Other solutions that use NAT-ing which break various technologies and cause most detection solutions blind.

Light-weight client

The client is auto-updatable and fully managed by Zero Networks (deploy it once and forget about managing it).

Zero Connect cloud service: The gatekeeper

When the user connects using the Zero Connect client, our cloud receives the request from the agent to connect and forces an MFA authentication to the user. Based on configuration, this can happen on every connection or once every X days alongside other potential asset health checks.

Zero Networks Connect™ leverages your identity provider to enable MFA. Today, we support any SAML based identity provider for MFA including Azure AD, Duo, Okta, RSA, NetIQ, CyberArk and many more.

Once the MFA is approved, the cloud service sends a command to the Zero Connect server to open an inbound allow rule in the host-based firewall of the Connect server. This allows connectivity from the specific IP address of the user.

The firewall rule is maintained as needed to track IP address changes on the client side, and the rule is automatically deleted when expired.

The key capabilities of the cloud service include:

- **Management** - The admin portal.
- **High availability and flexibility** - Worldwide data centers US, EU and APAC, both for redundancy, scale and compliance.
- **Highest standards of security and compliance** - We comply with SOC2 Type 2 and GDPR.
- **SIEM/SOAR** - If you want to integrate Zero Networks Connect™ with your SIEM or SOAR solution, using an open API can easily synchronize data to any desired SIEM that has API support including Splunk, Azure Sentinel, IBM Qradar.
- **Vendor access segmentation** - Based on user access configuration, vendors can be segmented to get access only to resources they need inside the network.
- **"Always on" VPN** – when the machine starts, the connectivity to the organization starts, with a policy on how many times per day/week/month MFA is needed to keep the connection on and secure.

Zero Connect server:

The Zero Connect server is based on Linux OS and WireGuard® VPN infrastructure for maximum network performance and security. Read more here:

Once the port is open for the specific IP of the user, anencrypted SSL tunnel between the client and the Connect server is established, allowing the user to access assets inside the corporate network.

The key capabilities of the VPN server include:

- **Maximum network performance** - Direct peer-to-peer connectivity via WireGuard®, the fastest VPN ever built.
- **State-of-the-art cryptography** - It has top-notch cryptography such as the Noise protocol framework, Curve25519, ChaCha20, Poly1305, BLAKE2, SipHash24, HKDF, and secure trusted constructions to make sure the connection is authentic and private...
- **No open ports on the internet** - only an approved asset that passes MFA validation can see the port and then connect over it.
- **The WireGuard® infrastructure** uses mutual certificate authentication - each client also has its own certificate which must be pre-registered with the server and is automatically managed by Zero Networks (no overhead for this complex and secure infrastructure)
- **Connect to the closest Connect server** - No need for complicated load balancing between VPN servers (each of our Connect servers has its own unique port and the cloud load.

What does a POC / deployment look like?

- **Installation (one hour)** - Login to the Zero Networks Admin Portal, download the Connect server setup, click a few next buttons and you are done.

- **Start piloting** by deploying the Connect client on a few machines.

- Experience the most performant **VPN solution** out there with a Zero Trust architecture while having full visibility and control on who is connecting from where and where they can connect to

- **High availability deployment (one hour, optional)** – An extra Connect server virtual appliance can be deployed to avoid any single point of failure and to experience the automated load-balancing.

- **Long term maintenance** – As a SaaS solution, no maintenance or manual operation is required from the IT and security teams.

About Us

At SRC Cyber Solutions LLP, we provide Next Generation , Highly Automated , User - Friendly and scalable solution . Our robust solutions include Comprehensive Email Security , Automated Patching and Endpoint Management , Asset Risk Visibility and Management with Policy Enforcement (ARM), Third- Party Data Flow Security solutions ,Agentless Micro Segmentation, Endpoint Management and Compliance Platform and an Online Gamified Simulation Platform for Cyber Security Trainingattacks.

To see a demo and learn more about Agentless Micro segmentation , Visit Us: srccybersolutions.com

ZERO. Networks

SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS

For more information please visit us today

www.srccybersolutions.com | +91 120 232 0960 /1 | sales@srccybersolutions.com