ZTNA
VPN REPLACEMENT

ENDIDA
NEXT GENERATION CYBER DEFENCE

WHAT IS ZTNA AND WHY IS IT BETTER THAN VPN?

Zero Trust Network Access (ZTNA) is a superior alternative to traditional VPN solutions, due to its no hardware approach and granular, policy-based access controls that align with the modern cybersecurity ethos of "never trust, always verify". Unlike VPNs, which grant broad access to a network once a user is authenticated, ZTNA ensures that access is strictly tailored to the user's specific needs, significantly reducing your organisation's attack surface.

SPEED OF DEPLOYMENT

ZTNA offers rapid deployment across diverse environments, enabling businesses to enhance their security posture with minimal delay.

COST SAVING

By eliminating the need for costly hardware and reducing operational overhead, ZTNA significantly lowers the total cost of ownership compared to traditional VPN solutions.

EASE OF CONFIGURATION

ZTNA simplifies security management with intuitive policy settings and automated processes with no firewall configuration required - far easier than complex VPN setups.

PRECISE ACCESS

ZTNA provides precise control over user access, ensuring individuals can only reach the specific resources necessary for their tasks. You can also set temporary times access.

SCALABILITY

The cloud-native nature of ZTNA allows for seamless scalability, accommodating business growth without the need for additional physical infrastructure or large reconfiguration.

ENHANCED SECURITY

Implementing ZTNA improves overall security by adopting a "never trust, always verify" approach, reducing the risk of data breaches and cyber attacks.

GET IN TOUCH TO FIND OUT HOW WE CAN HELP YOU TODAY

endida.com | 0238 2180 428 | info@endida.com

	VPN	Endida ZTNA
Serverless	✕ **VPN Server** Hub and spoke architecture	✓ **Serverless** Peers connect directly using UDP/TCP hole punching
On-demand connectivity	✕ **Always on** Tunnel is either on or off	✓ **On-demand** Tunnels are per-peer, and don't need to be always on
Unreachable network	✕ **Discoverable** VPN servers require open ports (e.g. udp/500, tcp/443, udp/1194)	✓ **Unreachable** Outbound only traffic. No open ports or ingress traffic, firewalls can be completely closed
Dynamic IP tolerant	✕ **Site-to-site VPNs require ACLs to isolate** Client-to-site requires advanced IP knowledge to isolate	✓ **Works with dynamic IPs** You don't care where the other side is ahead of time
Low-ops	✕ **Complex deployment** Segmenting is hard, configuration is complex	✓ **Low-ops deployment** Works on the network you've already got, no changes
Static IP address	✕ **DHCP** Reservations for static IP	✓ **Static IP** Private static IP addresses "out of the box"
DNS	✕ **Run your own DNS server** No native support for DNS	✓ **DNS** DNS built-in, no servers required
Precision access	✕ **Allows lateral movement** VPN places hosts directly onto the network	✓ **Zero Trust Network Access** Lateral movement prohibited, reduced attack surface

WHY ENDIDA'S ZTNA?

Endida's ZTNA solution delivers secure network access through dynamic, policy-based authentication, ensuring only verified users and devices can access specific resources. It assesses identity, device health, and access context in real-time, granting the least privilege necessary. This scalable, flexible approach supports remote work by integrating with corporate and cloud infrastructures, enhancing security while simplifying user access.

WIDEST DEVICE SUPPORT

GET IN TOUCH TO FIND OUT HOW WE CAN HELP YOU TODAY

endida.com | 0238 2180 428 | info@endida.com