The definitive guide to secure remote access

The best VPN alternative is zero trust network access (ZTNA).

zscaler™

> "I remember I was sitting at home when WannaCry hit. Everything went down, computers were encrypted and the network was breached. At that time, I was connecting to internal applications with SDP when a thought hit me: if I was using my VPN and someone at the office had the malware, I too would be at risk of infection. However, with SDP I was still able to securely access my internal applications because I never was connected to the network. I was safer at home on my home network than I would have been at the office; that's when I realized we have been doing private application access all wrong."
>
> Tony Fergusson, IT Infrastructure Architect
> **MAN Energy Solutions**

Digital transformation changes everything

Enterprises are migrating their private applications to public clouds, and users are consuming more applications, connecting to them from everywhere and from any device. This has created a proliferation of perimeters around users, devices and applications. Although many organizations have already taken steps to embrace digitalization and enable a zero trust network, their connectivity is still operating on incumbent network-centric approaches. Teams struggle to retrofit network-centric VPN technology to meet the needs of the modern user and the transforming business, but retrofitted approaches can prevent digitalization. It's time to redefine secure remote access.

This guide is designed to walk you through:

- Challenges enterprises face when trying to retrofit VPN technology into today's digitally transformed world
- Remote access needs to reflect today's realities
- How business can embrace a modern approach to secure remote access through a zero trust network access (ZTNA) service

The way remote access used to be

For nearly 30 years, the remote access VPN has been providing secure remote access. Built on the castle-and-moat security model, the VPN worked well when applications lived in the data center. Fast-forward to today with applications migrating to cloud and hybrid environments—while remote access security remains tethered to the network.

This focus on network-centric security is the crux of the myriad problems surrounding remote access, making the VPN flawed by design. Enterprises relying on legacy VPN technology face increased risk in two fundamental areas:

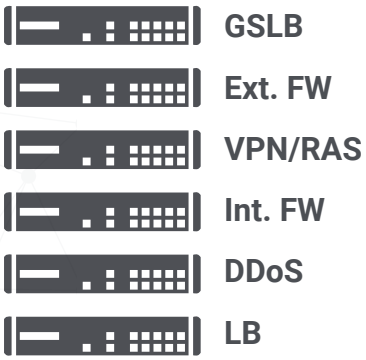
1 Trust is inherent to those inside the network

The castle-and-moat model keeps enterprises secure from external attacks by creating a hardened exterior perimeter, while the insides are soft and vulnerable. In this model, all employees working on-premises and on-network have already physically passed through your perimeter security. These users are on the network by default and are automatically classified as "trusted," gaining full and lateral access to enterprise applications. But what if a user had an infected device while on-net? Wouldn't that mean that east/west movement would enable horizontal attacks with limited resistance (like WannaCry)?

2 Risk of external access to the network

So what does this intrinsic trust mean as remote users VPN into the network to access internal applications?

- **The VPN tunnels users through the firewall—**Your firewall keeps harmful things off your network; however, your VPN tunnels users past the firewall without verifying the user or checking the posture of the device, creating holes in your security and increasing risk.
- **The network is detectable due to IP exposure to the internet—**Users connect to the network via inbound connections. This means network IPs are exposed to the internet, so anyone can ping the network architecture—authorized or not. These visible IPs create points of vulnerability for internet-based attacks, such as DDoS.
- **Once on the network, remote users are viewed as trusted—**The moment remote users tunnel into the network via VPN, they are viewed as "trusted." Whether they are trustworthy or not is unknown, but the remote user is still granted lateral network access. The surface area of attack increases, while network security is effectively put into the hands of your remote users and their devices.



The foundation on which the VPN was built creates points of exposure and leaves the network vulnerable to attack. As the need for additional security measures has increased, so too has the number of appliances found in the extensive inbound security stack we see today.

The fact is that the VPN grants too much trust to the user, and as enterprises look to implement zero trust networking, eliminating inherent trust is only the first step in securing private application access. The enterprise needs a modern remote access solution that operates on a conditional, adaptive trust basis.

adaptive trust /əˈdaptiv/ *adjective* /trust/ *noun*

The process of continually assessing the level of "trust" and access an entity is granted. Adaptive trust builds on the concept of zero trust but furthers the concept by enabling risk-minimized access to enterprise resources.

Redefine secure remote access with zero trust network access

Zero trust network access (ZTNA), also known as the software-defined perimeter (SDP), provides secure access to your private enterprise applications without the need for VPN. ZTNA is based on an adaptive trust model, where trust is never implicit, and access is granted on a "need-to-know," least-privileged basis defined by granular policies. Access is then monitored for continuous risk assessment as recommended by Gartner's CARTA approach. Because it's 100% software defined, ZTNA solutions require no physical appliances but can be deployed in any environment to support all REST-API applications.

The four tenets of ZTNA

1 | ZTNA completely isolates the act of providing application access from network access. This isolation reduces risks to your network, such as infection by compromised devices, and only grants application access for authorized users.

2 | Inside-out connections from app to user ensure that both network and application infrastructure are made invisible to unauthorized users. IPs are never exposed to the internet, creating a "darknet" and making the network impossible to find.

3 | Apps segmentation ensures that once users are authorized, application access is granted on a one-to-one basis, so that authorized users have access only to specific applications rather than full access to the network.

4 | ZTNA takes a user-to-application approach rather than a network-centric approach to security. The network becomes deemphasized and the internet becomes the new corporate network, leveraging end-to-end encrypted TLS micro-tunnels instead of MPLS.

Understand the types of ZTNA services

Although ZTNA solutions are all based on the idea of adaptive trust, ZTNA is available in two flavors: ZTNA as a gateway and ZTNA as a service:

ZTNA as a standalone offering

Stand-alone offerings require customers to deploy and manage all elements of the product. In addition, several IaaS cloud providers offer ZTNA capabilities for their customers. The ZTNA sites at the edge of your environment, whether that's in the data center or cloud, and brokers a secure connection between user and application.

Benefits include:

- The customer has direct control and management of their ZTNA infrastructure which can be required for compliance needs
- IoT services that are hosted on-premises can benefit from optimized speeds
- Performance speeds can increase if local users do not have to connect out to internet to access apps that are hosted on-premises

ZTNA as a cloud service

The other option is ZTNA as a service. This is a cloud-hosted service, where customers leverage a vendor's cloud infrastructure for policy enforcement. The enterprise simply purchases user licenses and deploys lightweight connectors that front-end applications in all environments; the vendor delivers the connectivity, capacity, and infrastructure needs. Access is established through brokered inside-out connections between user and application, effectively decoupling application access from network access while never exposing IPs to the internet.

Benefits include:

- Easier deployment since there is no need to deploy ZTNA gateways
- Simplified management since services are not hosted on-premises
- Optimal pathway always selected for global coverage for all remote and local users

Why ZTNA is a strong VPN alternative

User experience

- A better user experience for remote users. No concept of logging in and out; instead, access is continuous regardless of changes to network connectivity.
- Reduced latency for users, resulting in faster access and increased productivity.
- Consistently fast access, whether users are remote or at HQ.

Connectivity

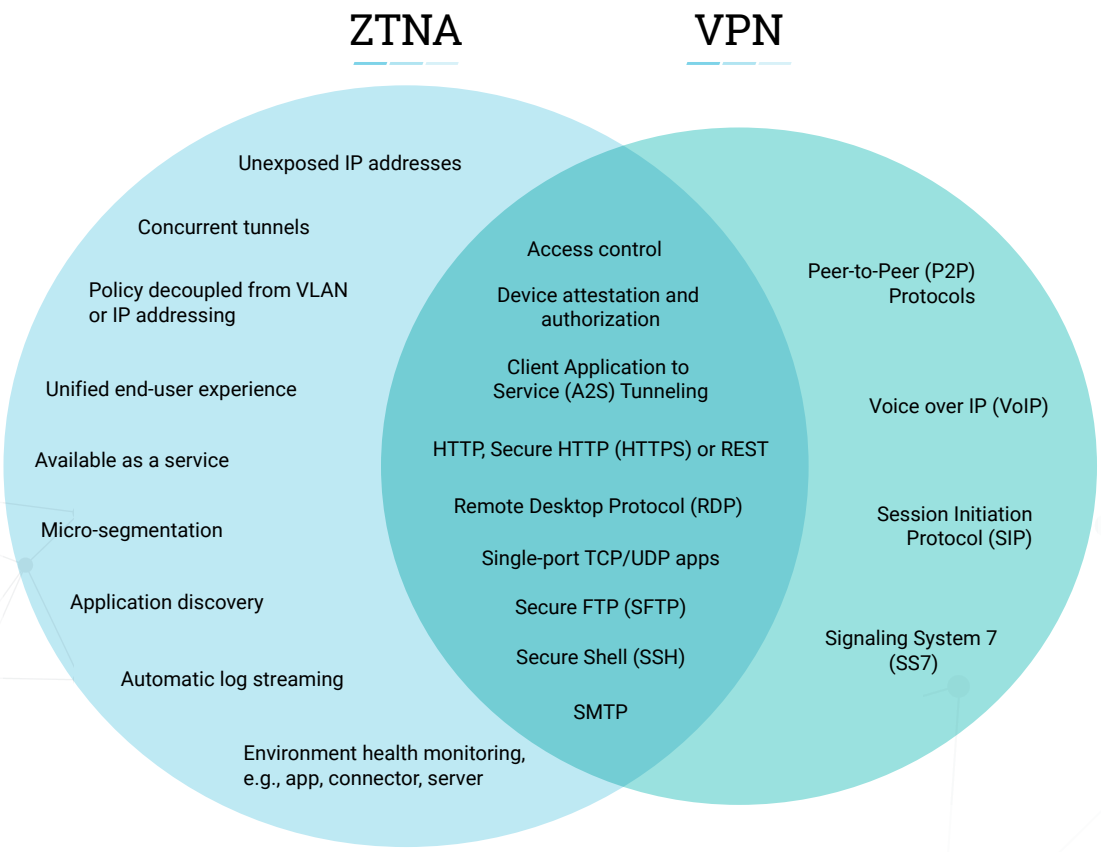
- Inside-out connectivity keeps the location of the network secret while enabling application access to individual applications within the network. This approach optimizes connectivity and minimizes latency. In contrast, with a VPN, connections are inbound going from VPN client > to VPN concentrator > and directly onto the network.
- ZTNA optimizes the traffic path from each user to each application using micro-tunnels. These tunnels are created on a per-session, on-demand basis. So, if a user is looking to access another private application at the same time, or even from another device, ZTNA spins up different micro-tunnels. VPNs use a single tunnel per user through which all apps run.

Security

- Application access is decoupled from network access. ZTNA moves away from network-centric security and instead focuses on securing the connection between user and application.
- Access is granted on a one-to-one basis, allowing only authorized users to access specific applications. Lateral movement is impossible, and the attack surface is reduced.
- Network and applications are cloaked to unauthorized users, and IPs are never exposed, reducing the threat of internet-based attacks.

Management

- ZTNA is 100% software-based and easy to deploy. There's no need to install, configure, and manage appliances, but ZTNA can also be deployed in tandem with the VPN.
- ZTNA is not IP address centric, so there's no need to manage ACLs, firewall policies, or translations.
- Granular policies can be applied at the application and user level, enabling hyper-focused security to applications, and least-privileged access to users.
- ZTNA provides enhanced visibility into:
  - User activity with real-time log streaming
  - Previously undiscovered applications
  - Health monitoring of environment



ZTNA and VPN have similar functions, but contrasting approaches. This diagram illustrates the differences between ZTNA and VPN technology from a feature perspective.

Factors to consider for ZTNA

There are two things you want to think about when considering ZTNA as your VPN alternative:

Your existing environment

Take a moment to consider your organization's existing environment. Think about your ecosystem and its effectiveness in meeting the needs of your business. Some questions to consider include:

- What protocols must be supported for access to your private apps (peer-to-peer, SIP, etc.), as not all are supported by ZTNA
- Where are your enterprise applications located?
- Where are your users located?
- Who is trying to access applications? Employees, third-party users, etc.?
- How satisfied are you with your solution?
- How satisfied are your users with your solution?

Based on your answers to these questions, you can determine the current needs of your business, particularly those areas where your current solution not performing. With this information, you can determine what's needed for those areas to improve?

Your future environment

Now consider what your company looks like in the near or distant future, and what its needs will be. Some questions to consider include:

- Is the enterprise growing? Are there mergers and acquisitions (M&As) in your future?
- Will there be additional apps and users? Will user consumption change?
- Will branch office locations access cloud apps?
- What will the capacity and availability needs be?
- Will cloud adoption increase? Will you need to adopt a hybrid or multi-cloud strategy?

With these considerations in mind, do you believe your current remote access services meet the digitalization needs of your organization? If not, you may need to consider an ZTNA service.

ZTNA top use cases

Get started

IT has changed, and the way we provide connectivity to applications must change with it. Private application access should no longer rely on network-centric security, but instead should be based upon a user- and app-centric approach. One made possible with zero trust network access.

Learn more about the zero trust network access (ZTNA) and how it can be a viable alternative to your VPN. Read about Gartner's Market Guide for **Zero Trust Network Access** (ZTNA).

About Zscaler™

Zscaler enables the world's leading organizations to securely transform their networks and applications for a mobile and cloud-first world. Its flagship services, Zscaler Internet Access™ and Zscaler Private Access™, create fast, secure connections between users and applications, regardless of device, location, or network. Zscaler services are 100% cloud delivered and offer the simplicity, enhanced security, and improved user experience that traditional appliances or hybrid solutions are unable to match. Used in more than 185 countries, Zscaler operates a multi-tenant, distributed cloud security platform that protects thousands of customers from cyberattacks and data loss. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

Zscaler, Inc.
110 Rose Orchard Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com