Zscaler Private Access for VPN Retirement

Zero trust access to internal applications without the hassles of VPN.

zscaler™

Securing your cloud transformation

Why enterprises use VPNs today

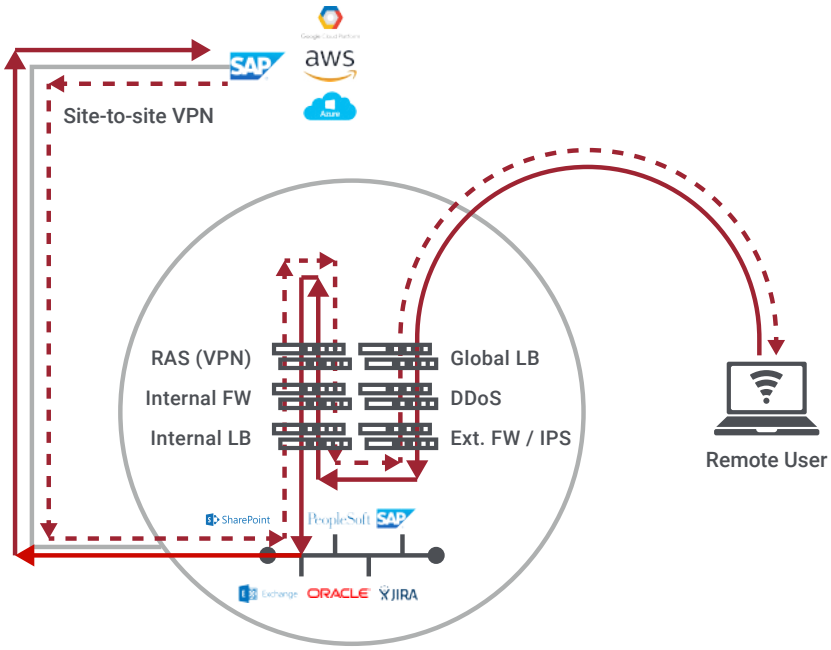
Think about network security 30 years ago. The network was static and so were employees, workstations and applications. This made network security straightforward, IT simply had to build a security appliance perimeter around the enterprise, resembling a castle and moat architecture. This strategy worked for a while, then something happened, users began moving off premise and off the network.

With personal computers and devices becoming mainstream in the 1990's, user mobility skyrocketed, becoming highly valued but underserved. Users needed to be able to access the network when working remotely, and so came the need for the Virtual Private Network (VPN).

The VPN was revolutionary for its time, allowing employees who worked remotely to access the network without having to physically move files between the office, home, and any other location. But like most early forms of technologies, it was not without its downfalls. The VPN gateway essentially opened up a hole in the organization's security perimeter, and as the number of remote users increased, so did the surface area of attack. To protect against this vulnerability, additional appliances were added to the inbound security stack including: firewalls, load balancers, DDoS prevention, and VPN concentrators. All contributing to the cost and complexity of the network as it needed to be replicated across every data center location.

These problems have only amplified since. With applications moving to cloud and users connecting from everywhere besides the office, why do we still leverage 30-year-old VPN technology that is still anchored in the datacenter and built before the public cloud even existed?

It's time to address the greater problem. It's time to rethink application access.



With a VPN, all remote user traffic is backhauled through the centralized data center security stack just to go back through the entire stack on the return trip.

Why change is needed

Now, with this new perimeter-less world, the data center is no longer the center of the IT universe, yet all user traffic, whether local or remote, continues to be backhauled to the data center that could be sitting thousands of miles away. The internet is the new corporate network, and how do you secure a network you don't control?

There is a need to move away from the network-centric security approach and instead focus on securing the user-to-application connection. We live in the era of cloud and mobility, and security needs to adapt to this new environment.

What's wrong with remote access VPNs?

Poor user experience

Companies have an obligation to keep users happy; if they don't, those users will find alternative ways to get their work done, such as bypassing security controls altogether. Users despise VPNs due to the constant login requirements every time application access is needed and grow frustrated of latency when connecting to an application when remote.

Risk of attack

A VPN extends the corporate network to the remote user, broadening the attack surface and risk of a breach. If a remote employee's device becomes infected with malware, that malware can infect the whole network the next time the user VPNs into the network. This means that application access is given prior to user authentication. In an attempt to lessen the impact of these security threats and achieve an app segmentation-like strategy, the networking team must repeatedly perform network segmentation and manually update access control lists (ACLs). All the while, users are still on the corporate network.

High costs and even higher complexity

The cost of a full VPN gateway appliance stack is exorbitant and requires significant resources to manage. They become even more expensive as latency and capacity limitations require the organization to replicate the gateway stacks at each of their data center locations. This amounts to a complex network environment that is difficult to scale, and still lacks strong remote access security to internal applications.

Zscaler Private Access: The software-defined solution for zero trust remote access

In today's security environment a remote access solution is needed that utilizes a zero trust strategy, where only authorized users are granted access to applications, never the network. In this fast-moving world, your users need to be enabled with swift and seamless access regardless of location. And as threats become more advanced, IT admins needs a higher level of visibility and control in order to keep the enterprise secure and functioning. This provokes the question; can your VPN do all of that?

Zscaler Private Access (ZPA) is the software-defined solution that is revolutionizing remote access to internal applications. Unlike VPN solutions, ZPA was specifically designed to be different and to overcome the remote access challenges of both today and into the future. It was built with the end-user, and IT admin in mind.

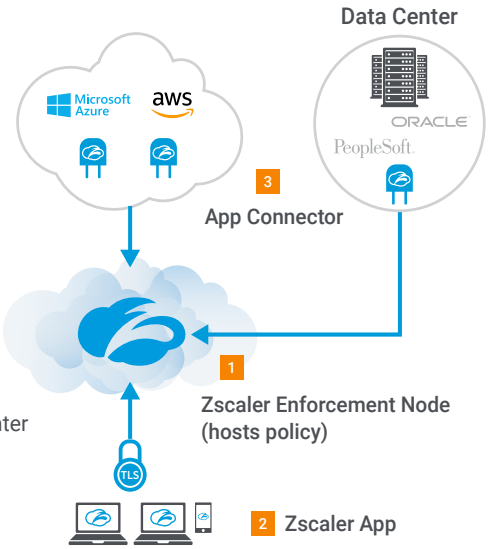
ZPA allows enterprises to break free from the pains that their VPN has caused for years and move to a cloud-first approach; fundamentally decoupling security from the data center and moving enterprise security to the scalability and reliability of cloud. The ZPA solution applies the latest innovations in cloud computing and leverages Zscaler's real-world experience to create a new secure remote access service that requires no hardware infrastructure and delivers zero trust security.

Zero trust security architecture

1. **Zscaler Enforcement Node (ZEN)**
   - Secures the user-to-app connection
   - Enforces all customized admin policies

2. **Zscaler app**
   - Securely routes user traffic to the ZEN
   - Requests access to an application

3. **App Connector**
   - Sits in front of apps in cloud and data center
   - Listens for access requests to apps
   - No inbound connections. Responds with inside-out connections only.



The Zscaler Enforcement Node (ZEN) sits between the Zscaler App and the App connector, brokering zero trust access from end-user to application from within the cloud.

How ZPA works

Users need the ability to access apps seamlessly while IT needs to be able to keep the enterprise secure. In the past these two concepts have had an inverse relationship, but now with ZPA you don't have to choose. Here is how ZPA works:

A mobile user tries to access the enterprises' internal applications. Instead of logging into their VPN client (and continuing to do that every time they start a session), the user simply opens up the Zscaler app on their laptop, mobile phone, or tablet.

The Zscaler App instantly routes traffic directly to the nearest Zscaler Enforcement Node (ZEN). The ZEN is the "broker" that is hosted within the global Zscaler cloud platform, supported from all locations and available at all times. The ZEN first verifies the user; operating on a zero trust basis and integrates with the enterprises' identity provider to authenticate the remote user. This is based on contextual access rather than relying on ACLs or IP addresses which are tethered to individual devices. Before access is granted the ZEN applies all customized policies established by the IT admins, making only authorized applications visible. The ZEN then sends a signal calling out to all App Connectors.

The App Connector often deploys as a small VM that sits in front of all applications, whether that be in the data center, public cloud, or private cloud. The App Connector closest to the requested application receives the call and responds with an inside-out connection down to the ZEN. This inside-out connection is key to how ZPA delivers zero trust. This creates a secure segment

of one between a user and application using encrypted micro-tunnels, avoiding the need to perform network segmentation at all and keeping applications invisible as IP locations are never exposed. DDoS attacks become impossible.

The ZEN then securely stitches together both the application and the user within the Zscaler cloud, granting application access, not network access. The user receives the fast application access they want, and the IT admins can implement zero trust security while gaining the visibility and control they need.

What sets ZPA apart from other remote access solutions?

The ZPA cloud-based security approach enables enterprises to determine who has access to which internal applications, even as they are migrated from the data center to cloud. ZPA is built upon four key security and design tenets that set the service apart from all other remote access security services:

1 | **Users are not on the network** – ZPA's unique inside-out connectivity ensures that users are never placed on the network. Not only is network access decoupled from application access, but also only authorized users can access the named application, meaning absolutely no lateral movement between apps or the network. Instead, application access is segmented, with no need for network segmentation or having to define policy by IP address or ACL.

2 | **Applications are never exposed to the internet** – Internal IP addresses are never exposed to the internet. Your sensitive internal applications are completely invisible—effectively on a "darknet"—unless users are authorized to access them through zero trust policies.

3 | **The internet becomes the new corporate network** – ZPA leverages the internet for dynamic, app-specific, TLS-based end-to-end encryption. All data remains private and customers can use their own PKI.

4 | **Application segmentation not network segmentation** – Only authorized users gain access to authorized applications. This model allows for application micro-segmentation via zero trust policies rather than needing to perform complex network segmentation on a repeated basis. Each application session has its own micro-tunnel which are spun up on demand per session (and destroyed once session ends), providing secure and granular user-to-app access.

Why Retire your VPN for Zscaler Private Access?

A better experience for remote users

- Faster access to apps in the datacenter and/or cloud
- Provides enjoyable experience all the way from Executives to DevOps
- No more VPN client for each login session
- Seamless experience to apps regardless of hosted environment

Zero trust access to internal apps

- Application access is granted solely on a zero trust basis
- Users access apps while never being on the network
- No lateral access to additional internal applications
- Granular policy-based access to applications
- Real time visibility into all user and application activity at any given moment

Eliminates complexity for administrators

- Single platform solution, works in all environment, whether that be the datacenter or cloud
- Easy to deploy and implement within one hour; no need to set up VPN gateways
- Enables application segmentation without performing network segmentation
- Integrates with single sign-on (SSO) providers
- Can be deployed in tandem with existing VPN solution

Better for the business

- No need to purchase physical or virtual appliances resulting in cost savings
- Increase in remote user productivity
- The most comprehensive security for remote access to internal applications

Getting started with Zscaler Private Access

ZPA has redefined the way remote users access internal applications. The enterprise is no longer stuck with the pitfalls of the VPN but can move to the zero trust model with ZPA and provide an enjoyable remote user experience while receiving the highest quality security. So are you ready to retire your VPN?

For more information about ZPA, VPN replacement, or to see a live demo of the service, please send a meeting request to Zscaler by emailing **sales@zscaler.com.**

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