Zscaler Private Access for VPN retirement

Remote access to internal apps without the hassles of VPN

zscaler™

SECURE ACCESS TO THE MODERN CLOUD ERA

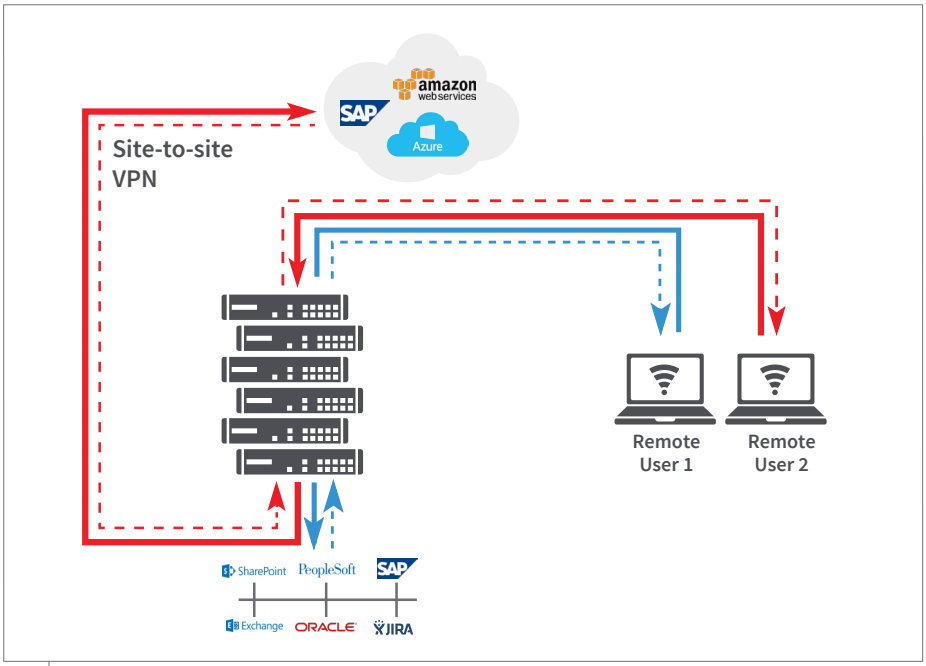
Why enterprises use VPNs today

With IT advancing so rapidly, no one should have to rely on technology that's not doing the job. This is particularly true if the technology also happens to be expensive, difficult to manage, and universally disliked. Yet this is the situation in which many enterprise network and security teams find themselves with virtual private network (VPN) technology.

When introduced in the 1990s, VPNs were revolutionary, enabling people to work remotely without having to physically move files between the office, home, and other locations—which was, of course, risky. But VPNs have risks of their own and, as more users became mobile and the risk of infiltration grew, enterprises began to place more VPN gateways within each of their data centers, leading to an ever-growing stack of expensive firewalls, load balancers, DDoS prevention, and VPN appliances—all needing regular management and updates.

A lot has changed since the nineties. The majority of users are working on mobile devices, and internal applications—once run solely in the data center—are now running in the cloud as well. But VPN technology has changed little.

So why do companies continue to rely on this outdated technology? For the simple reason that there has been no viable alternative.



Internet-bound traffic from remote users takes a slow, circuitous path as it's routed through the data center security stack before it can head out to the cloud or open internet, then goes back through the stack on its return trip.

The data center breaks cloud and mobility

For years, the data center has been the center of the IT universe, where all internal applications have been housed and through which all user traffic—local and remote—has been routed.

But this focus on centralized controls in the era of cloud and mobility is becoming counterproductive. It adds complexity when looking to migrate internal application workloads to cloud and it forces traffic from remote users and branch offices through VPN gateways that may be running in a data center thousands of miles away. User experience and productivity take a significant hit, while the risk of attack continues to increase.

Why focusing on the data center and VPN is a mistake

Poor user experience
Companies have an interest in keeping 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, since they require a new login every time application access is needed. VPNs are notoriously slow as they force remote user traffic through a centralized data center gateway.

High cost and complexity
The cost of a full VPN gateway appliance stack is exorbitant and requires significant resources to manage. They become even more expensive when your organization is spread across multiple geographies, as you will often times need to replicate the gateway stacks at each data center location. This adds up to a complex data center environment that still lacks adequate enterprise security for remote access to internal applications.

Risk of attack
A VPN extends the corporate network to the remote user, broadening its potential attack surface. And, if a remote employee's device becomes infected with malware, that malware can wreak havoc on the network the next time the employee VPNs into the network. To combat this potential threat, networking teams must segment internal networks or use access controls lists (ACLs). All the while, users are still on the corporate network.

Zscaler Private Access: secure, remote access for the modern era

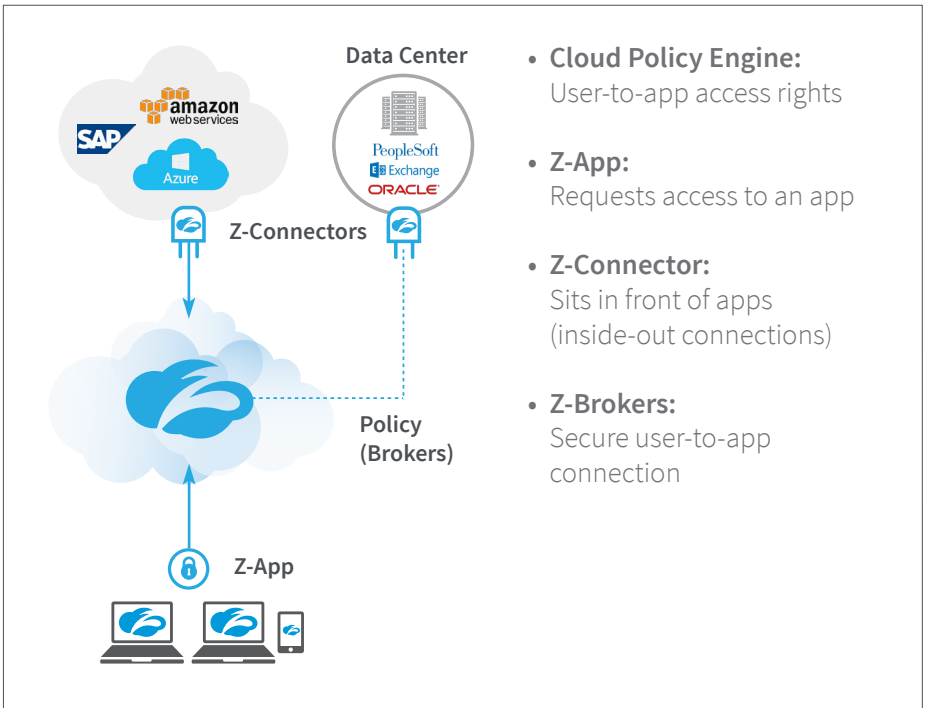
It's time for a revolution in secure remote access

The cloud has shown that the data center is no longer the ideal place for all applications. The cloud enables a productive user experience, greater elasticity, and the ability to scale without adding costly gateway appliances.

The important piece that is still lagging has been how to provide secure remote access. Routing traffic through the VPN gateway stack is suboptimal for the many users working from home, in branch offices, and on the road. But what if you could use the cloud to route remote users' traffic directly to the internal applications they need? And what if you could do it in a way that works seamlessly, regardless of where the applications are running. Now you can with Zscaler Private Access.

Zscaler Private Access (ZPA) is a revolutionary service from Zscaler that uses the Zscaler cloud to provide secure remote access to internal applications. ZPA enables enterprises to break free from the VPN-driven mindset that is centered around the data center to one of a more modern, cloud-based approach.

Key to its value is ZPA's ability to give remote users the seamless experience they want when accessing internal applications, while giving enterprises the security they need, and the simplicity to make network transformation a success.



The Zscaler cloud brokers a secure connection. Because access is provisioned through the Zscaler cloud, rather than via a network connection, ZPA makes it impossible to route back to applications.

Fast and direct access to internal applications for remote users

Users appreciate the ability to seamlessly access internal applications wherever they are running. ZPA gives them a similar experience when accessing private, internal applications, no matter where they're hosted or where in the world remote users are connecting from. Here's how it works:

ZPA comprises a Zscaler Enforcement Node (ZEN), the Z-App mobile client, and the Z-Connector. It all runs within the Zscaler global cloud platform, which is distributed across multiple locations around the world. The ZEN applies policies and stitches together a connection between a mobile user attempting to access and application and the application itself. ZPA ensures that user traffic consistently traverses the optimal path based on the user's location. This fast access leads to greater business productivity.

With ZPA remote users get a seamless experience when access internal applications. With VPNs, they have to log in each time to establish a connection with the network. With Z-App, the mobile software installed on all user devices, authenticated users only log in once, and they have the same experience whether the application is running within the data center or cloud. This is achieved without accessing the corporate network.

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 –** Users are never given access to the corporate network. Instead, access is application specific, with no need to define policy by IP address or ACL.

2 | **Applications are invisible –** 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.

3 | **The internet becomes the new secure 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 | **Policies provide application-level segmentation –** Users go direct to the specific applications based on policies. This allowing for application segmentation, and removes the need to segment networks. Each application session has its own micro-tunnel, providing granular, user-to-app access.

Why retire your VPN for Zscaler Private Access?

A better experience for remote users

- Faster access to apps in data center and/or cloud
- No more VPN client for each login session
- Seamless experience for apps regardless of environment in which they're hosted

Less complexity for administrators

- Easy to implement within one hour; no need to set up VPN gateways
- Application segmentation, not network segmentation
- Integrates with single sign-on (SSO) providers, such as Okta
- Can be deployed in tandem with existing VPN solution

Secure remote access to internal apps

- Users are never on the network
- Policy-based access to specific applications
- No lateral access to additional internal applications
- Visibility into all apps running
- Visibility into user activity taking place

Increased business value

- No need to purchase hardware results 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 redefines the way remote users access internal applications. It enables an experience that remote users appreciate, as well as the secure remote access fit for any enterprise embarking on a transformation journey.

For more information about ZPA, why it's time to retire your VPN or to see a live demo of the service, please send a meeting request to Zscaler by emailing **sales@zscaler.com.**

Ready to retire your VPN?

If so, ask our reps about the VPN competitive transition program and how you can receive six months of free ZPA service by retiring your VPN solution.

zscaler

SECURE ACCESS TO THE MODERN CLOUD ERA