Zero Trust Access to Private Apps From Inside and Outside the Office with Zscaler™

We've seen thousands of organizations successfully embrace work-from-anywhere, overcoming many challenges around data protection, secure remote access, and scaling to enable business continuity. Undoubtedly, many were surprised by the urgency and speed needed to shift the majority of their in-office workforces to full-time remote, but in the midst of the chaos many turned to zero trust services for access to business resources as an alternative to traditional network-centric methods. Now, as IT teams begin to plan for the years ahead, many are left wondering what the future of work will look like and if work-from-home, or some hybrid of office and home, is here to stay.

zscaler™

From a security standpoint, users connecting from their laptops in and out of the office can increase security risks—especially if users are automatically deemed trusted and are granted network access. From a user perspective, ease-of-access should be the same, no matter where they are working.

Three Considerations for IT Teams Going Forward

While local governments are taking the right measures to reopen physical locations, there are three key elements that a security and/or network leader should consider before reopening.

1 Provide zero trust access to private apps from any location

Many companies make the mistake of thinking that zero trust is only key when providing remote access to private applications. They use zero trust services as an alternative to remote access technologies like VPN or VDI, which place users on the network. In-office employees are mostly allowed to connect to network resources due to the fact that the user is already inside the perimeter and is implicitly trusted. The team may have implemented network segmentation as an additional security measure, making the network extremely complex. That said, network segmentation is no longer required if the proper zero trust services are in use. The same zero trust service can be used when a user is remote, or when in the office, and can be used to provide an application level of segmentation, without the need to manage or deal with the complexity of network segmentation on-prem.

2 Deliver the best user experience possible by prioritizing consistency

Several surveys have shown employers and employees comfortable with working remotely. Many organizations indicate that productivity is continuing to increase despite their core workforces working remotely, while employees—more often than not—enjoy the flexibility of being able to work from anywhere. This is why several customers we speak with are leaning towards a hybrid model of work with employees dividing their time between the office and home. Therefore, network and security leaders must ensure that employees have seamless and consistent experiences when accessing applications from any location—including in the office.

3 Prevent dirty devices from accessing the corporate network

The increasing popularity of endpoint security services like CrowdStrike, Microsoft, and Carbon Black during remote work is also key. For a while now, laptop and smartphone users have been accessing apps while at home on their personal networks. As those same devices are carried into the office, building, it's important that IT leaders do not let them onto the corporate network. Instead, IT must ensure every device that comes back to the office is clean, to reduce the overall attack surface and minimize threats.Thus, understanding device posture and the health of the device is a key consideration, especially as the concept of hybrid work begins to take shape.

Using Zero Trust for Work Inside and Outside the Office

Zero trust is based on two key foundational elements: Identity and business policies.

Instead of using an IP address, identity provides the context for who the user is. The business policies, which are set by the network or security team, determine which private application an authorized user is allowed to access. The Zscaler Zero Trust Exchange™ platform, hosts these policies, enforces them, and, if allowed, then brokers the app-to-user connection on a 1:1, per-app, per-session basis.

Given that the location of the users will continue to change, the emphasis on the network is no longer required. As users prepare to return to office, it is even more essential to break away from implicit trust and implement zero trust policies. Zero trust network access ensures security, speed, consistency, and convenience to users, and provides flexibility and scalability for IT.

Zscaler Private Access for in-office or remote employee access to private apps

Zscaler Private Access™ (ZPA™) is a cloud service from Zscaler that provides seamless, zero trust access to private applications running on public cloud or within the data center. It can support legacy applications as well as web-based applications. The service consumes information from a SAML-based ID provider, and connects the authorized user to a specific application based on business policies defined by the customer. Unlike VPN or VDI, this is accomplished without placing the user onto the corporate network—removing the need for the inbound gateway stack. The service never exposes the application to the internet, making the app invisible to attackers—which is especially important for remote access.

ZPA uses encrypted inside-out tunnels—one from the app, and one from the user—then brokers the connections in real-time within one of its service edge locations based on the location of the user and the device. This is done in a way that ensures the fastest user-to-application path possible, and removes the need for backhauls to a central data center location. The service edge is either publicly hosted by Zscaler or privately hosted by the customer, in which case it's extended to the customer's on-premises branch or data center for local enforcement. In either case, service edges are managed by Zscaler.

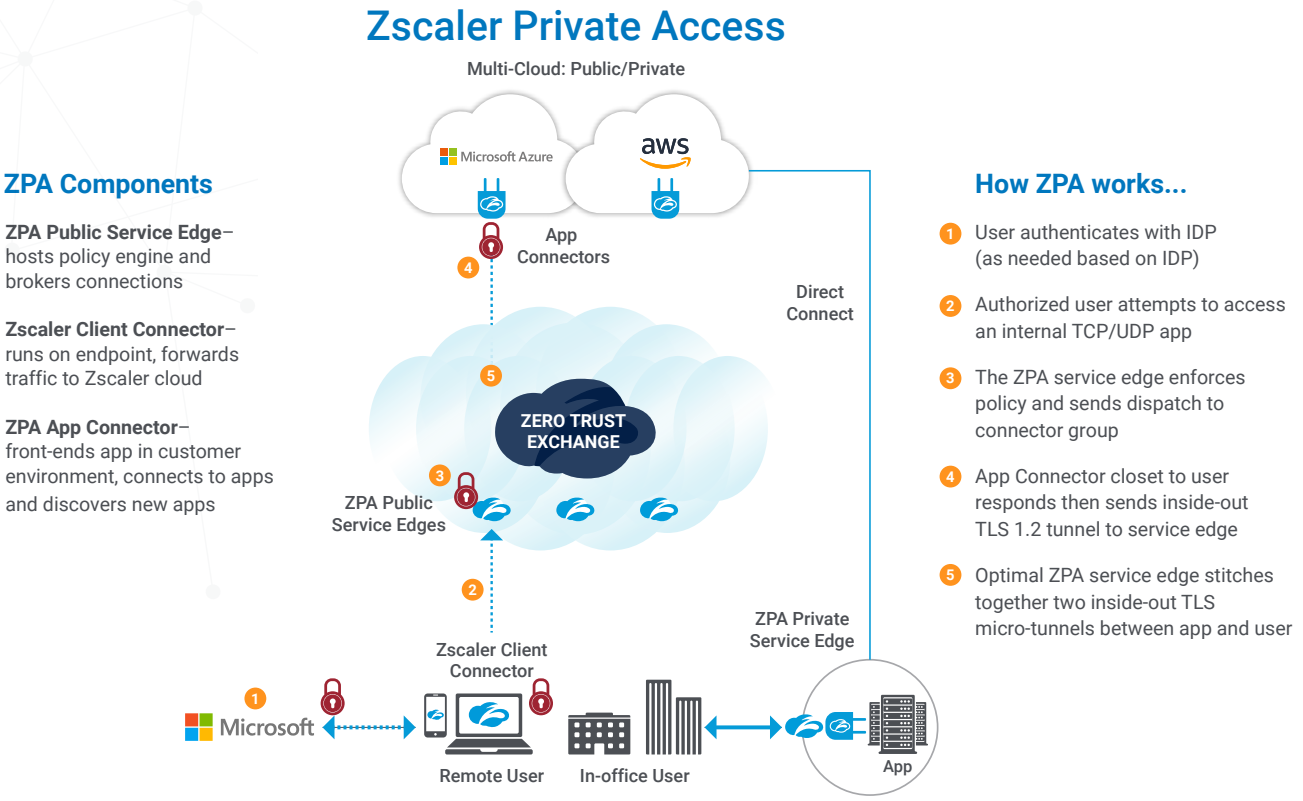
Since the service is connecting on a per-user and per-app basis, it provides application segmentation without the need for network segmentation. This simplifies segmentation, allowing IT to define policies by username and host name instead of source IP and destination IP.

ZPA uses encrypted inside-out tunnels—one from the app, and one from the user—then brokers the connections in real-time within one of its service edge locations based on the location of the user and the device.

The same advantage of zero trust architecture, but hosted on-premises

For companies preferring to host a ZPA service edge themselves, we,ve introduced ZPA Private Service Edge. ZPA Private Service Edge is a private, single-tenant instance that provides the complete functionality of a public ZPA Service Edge in an organization's own environment. The customer hosts ZPA Private Service Edge onsite or on a cloud service, and it's managed by Zscaler. ZPA Private Service Edge downloads the relevant policies and configurations from the cloud, so it can enforce all ZPA policies locally.

The ZPA Private Service Edge and classic ZPA services hosted by Zscaler can be used in tandem. ZPA will automatically choose the fastest path between the user and destination to eliminate latency.



Key benefits of ZPA Private Service Edge

Reduced complexity and costs

With ZPA Private Service Edge, internal firewalls and additional appliances are no longer needed. This not only reduces costs, but also the need to build complex network segments used to provide application access to local users.

High availability

ZPA Private Service Edge caches access policies for weeks, allowing users to connect securely, even if internet connectivity is lost. This ensures the continued availability of application access irrespective of connectivity.

Fast user experiences

ZPA automatically decides which path is the shortest and fastest for the user to connect to applications—prioritizing the local ZPA service edge. The dual access capabilities of on-premises and public cloud brokering automatically optimizes performance for the user, regardless of where the user and applications are located.

Compliance

Industries such as banking and financial services demand strict guidelines around the use of cloud-based services. ZPA Private Service Edge helps companies comply with these regulations by allowing them to host the service on-premises.

Centralized policy with local enforcement

ZPA Private Service Edge remains up to date with business policies by connecting with the ZPA cloud service. This ensures all relevant policies and configurations are enforced. In the event of internet failure, ZPA Private Service Edge caches all policies for 14 days to ensure local user access to private applications is still enforced.

ZPA Private Service Edge provides a simpler way to enable secure access to private apps and enables an identical experience for local or remote users accessing apps in the data center or cloud.

Need to learn more about ZPA? Reach out to our team at any time: **sales@zscaler.com**.

Learn more about **ZPA Private Service Edge**

Request a demo

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com