zscaler™

DATA SHEET

ZPA™ Private Service Edge

Zero Trust Access to private applications delivered on-premise for all users: Remote and In-office

Gartner recommends enterprises adopt zero trust network access (ZTNA) services for private applications, to ensure that access is based on identity thus removing the need for network access and minimizing application exposure to the internet. Whether a user is connecting remotely or from the office, zero trust services should be used to access applications while implementing application segmentation instead of complex on-premise network segmentation. The same zero trust solutions used for remote work will be relevant and effective when employees connect from the office.

The sudden switch to remote work has seen many organizations embrace zero trust solutions for remote users. ZPA has been widely adopted due to its zero trust policies allowing employees to connect to private apps in a secure manner. As organizations are considering evolving from remote work to hybrid work it is imperative that IT teams consider this evolution to provide seamless and consistent experience for users splitting their time between home and office. While user experience is key, hybrid workforce demands IT teams have full visibility while providing secure application access. In order to achieve fast access in many situations it would make sense to deploy application connectivity services within organizations own environments to ensure the shortest travel time for the traffic. With this the customer has full control hosting the service. Zscaler Private Access adheres to this philosophy and brings to you ZPA Private Service Edge, hosted at the customers site but managed by Zscaler.

Now available as an added feature of the ZPA service, ZPA Private Service Edge is a fully functional single-tenant (per customer) instance broker that is hosted by the customer organization but managed by Zscaler. ZPA Private Service Edge resides within the customer's site or in a public cloud service. Like the ZPA cloud service, the on-premises service enforces policies and stitches together the connection between an authorized user and a specific private application. This is now a zero trust solution that is designed for all users, from any location and any device.

> “We've been using ZPA since 2018 as a VPN alternative. When we heard about ZPA Private Service Edge, we realized that we could extend the zero trust access capabilities of the public ZPA cloud with software that can run in our own network. We're now able to better protect our business-critical private apps, and deliver the best user experience possible, by using our ZPA Private Service Edge that runs on-premises, but is managed by Zscaler.”
>
> **Nicholas Pandola,** Global Director Information Security

TRINSEO

The functionality of the ZPA cloud service, but in closer proximity

With the cloud-delivered ZPA service, when a user requests access to a private application, the user's traffic is forwarded to a Zscaler™ cloud data center over the internet. The connection between an authorized user and a private app is stitched together in the cloud. This makes ZPA ideal for remote users, such as mobile employees and third-party contractors, looking to access private applications running on-prem or in public or private clouds, as ZPA eliminates backhauls. In cases where on-premises users are looking to access an application that is also running on-premises, the connection between the user and the application is made with ZPA Private Service Edge which is now the shortest path to connectivity.

As with the cloud service, ZPA Private Service Edge manages the connections between a Zscaler Client Connector (formerly Zscaler App) and App Connector. When deployed, it registers with the Zscaler cloud. This allows ZPA Private Service Edge to download the relevant policies and configurations so they can be enforced. It also caches path selection decisions. ZPA Private Service Edge deploys as a lightweight virtual machine/RPM that is installed by customers within their own network environments. Once set up, ZPA Private Service Edge functions in the exact same way as the ZPA cloud service. For on-premises users, or even remote users in countries where there is no ZPA cloud service, access to private applications is brokered through ZPA Private Service Edge and is always seamless, fast, and secure.

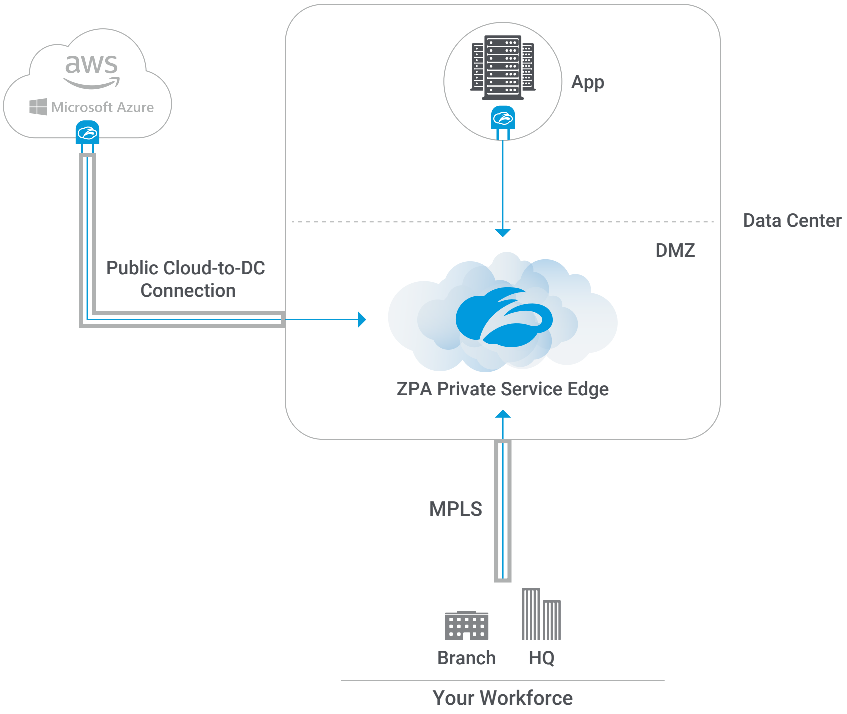
It's important to note that admins can always configure ZPA in a way where both ZPA Private Service Edge and the ZPA cloud service can be used to ensure the best experience for users looking to connect to private applications.

Common use cases for ZPA Private Service Edge

Extending the ZPA service to your on-premises environment helps you succeed in a variety of scenarios:

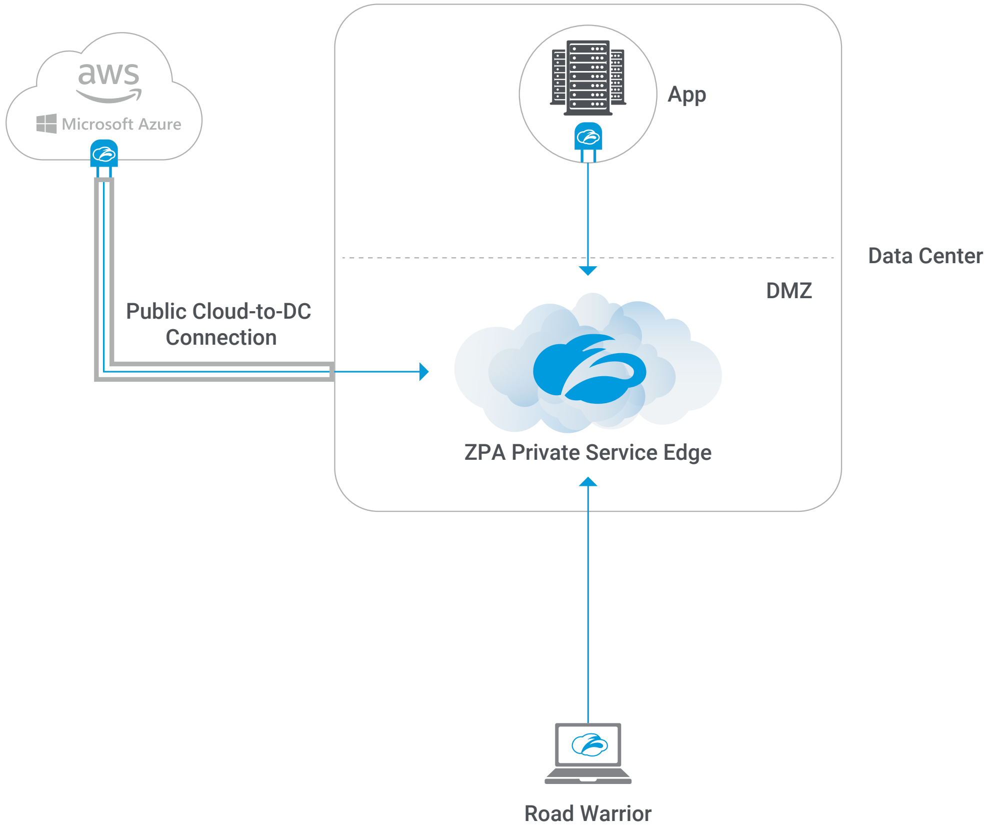
Zero trust network access for on-premises workforce

For users working at HQ or branch offices looking to access applications that are running on-premises or in public clouds, it does not make sense for traffic to first go out to a ZPA public broker, then back in to the application running locally. ZPA Private Service Edge provides local brokering between on-prem users and on-prem applications, which creates a faster experience for users, less complexity for network admins, and less risk for business data by enabling least-privilege access.



Local service edge for remote workforce

In countries (such as Algeria) with no ZPA Public Service Edge, remote users will need to connect out to a ZPA Public Service Edge running in a foreign country (such as Germany) to get access to an app running on-prem at their HQ. With ZPA Private Service Edge, these remote users can access applications running on-prem, and ZPA automatically determines the fastest path for each user and selects the broker that is best for the job.



Private infrastructure required for compliance

Some countries, especially those prone to natural disasters, and regulated industries (such as banking) require security services to be running on-prem—not hosted within the cloud—to ensure high availability. ZPA Private Service Edge allows customers to comply with in-country industry regulations by running locally, and handling all brokering within the customer's own environment.

> “ZTNA provides controlled access to resources, reducing the surface area for attack. The isolation afforded by ZTNA improves connectivity, removing the need to directly expose applications to the internet. The internet becomes an untrusted transport, and access to applications occurs through an intermediary. The intermediary can be a cloud service controlled by a third-party provider or a self-hosted service.”

Gartner, Market Guide for Zero Trust Network Access | Steve Riley, Neil MacDonald, Lawrence Orans, April 2019

KEY BENEFITS OF ZPA PRIVATE SERVICE EDGE

The ability to host ZPA brokering services on-premises (based on identity), without network segmentation, leads to a host of benefits for existing Zscaler Private Access™ customers as well as new ones.

- **Simplified segmentation** – Move away from "Source IP to Destination IP" to "User to hostname" policies. Reduce the complexity of network segmentation that includes maintaining a list of IP addresses for firewalls and setting different policies for local or remote users. With ZPA Private Service Edge, the policy framework becomes flatter and easier to manage.
- **Accelerated adoption of hybrid and multicloud** – ZPA Private Service Edge can run within the data center or a public cloud. This means there is no change to the access policy, even after a private app migrates to public cloud services like Azure, AWS, and Google.
- **Least-privilege access for local users** – The ability to enable zero trust network access on-premises creates a 1:1 surgical and brokered connection between an authorized local user and a specific app, preventing lateral access across the network and minimizing risk.
- **High availability** – Areas of the world with poor internet connectivity can benefit from ZPA Zscaler Private Service Edge, which caches access policies for weeks, allowing for secure connectivity even in the event of internet connectivity being lost.
- **Fast and seamless user experience** – Access is identical when working remotely or locally. Dual access capabilities of on-premises and public cloud brokering automatically optimizes the experience for local users when accessing private apps running on-premises, and for remote users within countries where there is no ZPA cloud broker in-country.
- **Cost avoidance** – The use of internal firewalls can be reduced and the need for new investments can be avoided altogether. There is no need to purchase additional firewalls or create new network segments just for local users to get access to apps.
- **Compliance** – For highly regulated industries, this private infrastructure can help customers comply with any standards that prevent the use of cloud-hosted technology.

Contact us with questions about the ZPA service or visit **zscaler.com/zpa**. For more in-depth information about ZPA Private Service Edge, read the **Zscaler Help documentation**.

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