

Zscaler Private Access for VoIP and Server-to-Client Apps at a Glance

Accelerate zero trust transformation and consolidate remote access with Zscaler

Challenge

When embarking on a zero trust transformation journey, large enterprises start by migrating their modern web-based and cloud applications from VPN to a zero trust network access (ZTNA) solution. However, many organizations still rely on network-based systems such as VoIP and server-to-client applications, which require constant IP-to-IP communication.

For these organizations, the transformation journey remains incomplete because these applications are incompatible with true ZTNA solutions. Security gaps persist as VPNs remain part of the remote access infrastructure. Organizations need a solution that empowers them with a phased approach to zero trust while completely transitioning away from traditional VPN solutions.

Solution

Zscaler Private Access™ (ZPA) will support VoIP and server-client applications using a network tunnel. The solution leverages the Zscaler Zero Trust Exchange™, operating on a zero trust model that verifies identity, device posture, and access permissions for every user and device before granting access to these network applications. It uses a separate, dedicated tunnel that is available for applications that are not compatible with ZPA's ZTNA service.

Solution Benefits



Improved security: Immediately strengthen security with the Zscaler platform while laying the foundation for comprehensive zero trust adoption.



Reduced IT complexity: Streamline and phase your app migration to ZTNA, with ZPA's solution acting as a bridge to zero trust by supporting secure access to network connected apps.

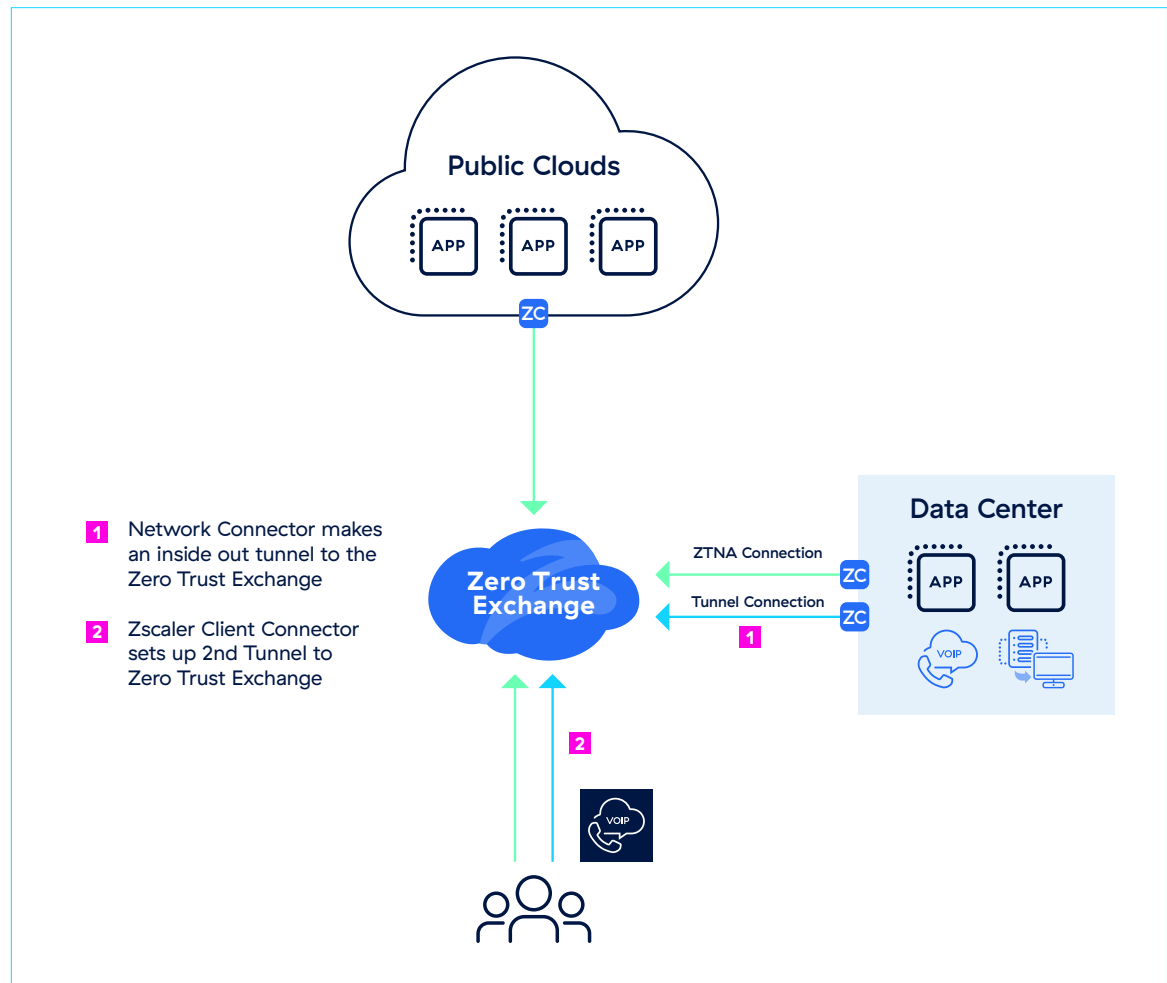


Lower total cost of ownership: Consolidate remote access to a single-vendor solution that includes network connectivity hosted and managed by Zscaler.

The solution includes a Network Connector that securely links network applications to the Zscaler Service Edge. The connections are always inside-out, which lays the foundation for a more secure remote access. Administrators can now manage remote access for all private applications from a single console. This also facilitates an easier migration path for network applications towards true ZTNA service when the applications are compatible. For end users, the connectivity experience is seamless using the same Zscaler Client Connector, whether accessing applications over ZTNA service or a network tunnel.

With this solution, IT and security practitioners gain control in planning their IT modernization projects, such as moving traditional VoIP apps to modern UCaaS alternatives, helping them complete zero trust transformation in a phased manner. They also gain the cost benefits of consolidating remote access with a single vendor solution, and the security benefits of the Zero Trust Exchange platform: minimizing the attack surface.

[Learn more about Zscaler Private Access >](#)



 | Experience your world, secured.™

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](https://twitter.com/zscaler).

© 2024 Zscaler, Inc. All rights reserved. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™ and other trademarks listed at zscaler.com/legal/trademarks are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.