Zscaler Private Access for the Federal Government

Secure remote access to agency applications

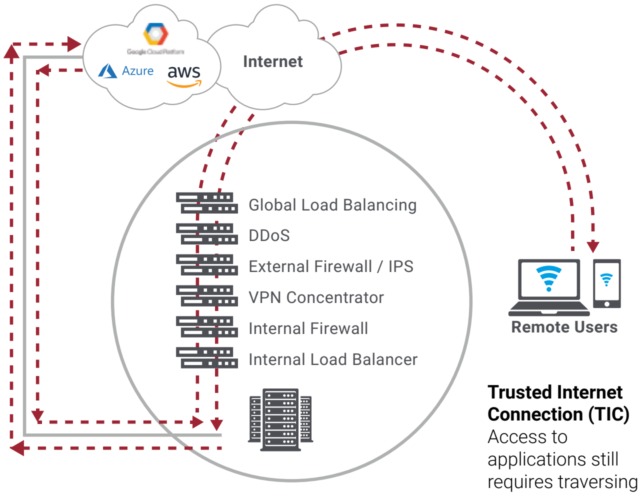
FedRAMP

Authorized

The changing IT terrain within federal agencies

Government agencies are in the midst of a transformation. Applications are moving out of the data center and into the cloud and users have moved off the internal network. The adoption of Amazon Web Services (AWS), as well as Microsoft Azure and other cloud service providers, brings massive benefits, such as scale, simplicity, productivity, and reduced costs. But such services also extend the security perimeter to the internet. And they require agencies to consider how best to allow users to access applications from remote locations from any device—government issued or not—without introducing risk.

Legacy remote access impedes the cloud mission



Trusted Internet Connection (TIC)
Access to applications still requires traversing 30-year old inbound gateway technology

With an increasing percentage of traffic moving off the network and heading to the internet, the Federal Government has invested heavily in Trusted Internet Connection (TIC) as a way to consolidate external connections and thus improve security and visibility. But for those working remotely and connecting via virtual private networks (VPNs), TIC adds a layer of complexity—another barrier between users and their applications—worsening what is already a poor experience.

Even when applications resided solely in the data center, VPN technology was never ideal. The VPN extends the network, increasing the attack surface. And it places remote users on the network, which introduces risks on its own. Together, TIC and VPN technologies can slow cloud adoption by hindering its benefits in productivity and simplicity, among others.

Zscaler has introduced a cloud-based solution that provides secure access to applications, reduces cost and complexity, and improves security and the user experience.

Zscaler Private Access: “Bypass the TIC”

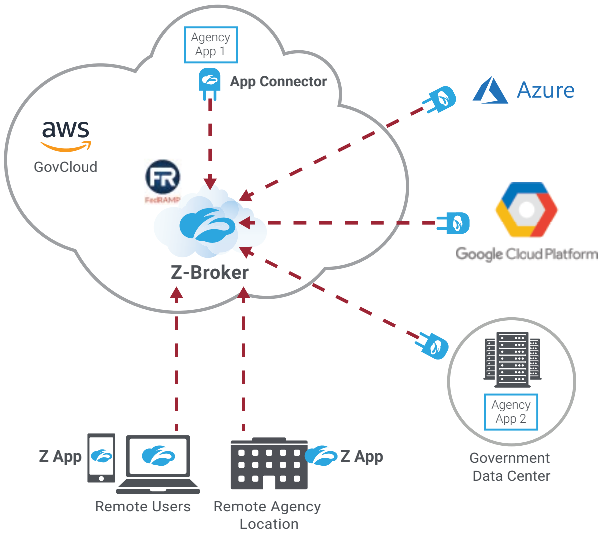
Zscaler Private Access (ZPA™) is a cloud-based, FedRAMP-certified service that provides seamless and secure zero-trust access to internal applications for authorized users. The service uses a software-defined perimeter, not appliances, to provide comprehensive security and a fast, seamless user experience. Access is the same whether agency applications are hosted in the government data center or in the AWS Government Cloud or another service. ZPA replaces VPN and provides encrypted (NSA) connections to applications. Traffic does not traverse the open internet, bypassing the need to go through TIC. This reduces overall traffic through the TIC, and increases performance.

How ZPA works

ZPA works by brokering a connection between an authenticated user and application. A small piece of software called Z-App is installed on the user device. Z-App ensures the user's device posture, assigns a device fingerprint, and extends an encrypted micro-tunnel out to the Zscaler broker (Z-Broker) running in the cloud using TCP. Adjacent to an agency application running in the cloud or the data center, ZPA places a piece of software called Z-Connector, deployed as a VM. The Z-Connector establishes an outbound connection to the Z-Broker running in the cloud via an additional encrypted micro-tunnel. If access policy is met, the Z-Broker approves access and stitches together the user-to-application connection.

Secure connections in a FedRAMP Cloud **Phase 1**

Bypass the TIC thru secure policy-based access to applications and SaaS services via Zscaler Federal Cloud



Z-Brokers: secure user to app connection

- Cloud Policy Engine: user to app access rights
- Brokers runs within AWS Government, East and West Clouds

Z-App: installs on users device, requests access to unauthorized users

Z-Connector: front-ends agency application, established outbound connection to Z-Broker

ZPA is based on four key design tenets:

1. **Users not on the network** – Connect users to applications without placing users on the network
2. **Applications are invisible** – Internal IP addresses never exposed to internet. Apps are "dark" to unauthorized users
3. **Application-level segmentation** – Zero-trust access to specific agency applications based on policies
4. **Internet becomes the new network** – ZPA uses the internet for app-specific TLS-based encryption; agencies have ability to use their own PKIs as well

Why ZPA for federal agencies?

Cloud-like experience for remote users

- Consistent user experience for agency applications in AWS Government Cloud and data centers
- The service integrates with Okta and other single sign-on providers for simplified access
- Users are routed directly to the app via the nearest Z-Broker for faster access
- Secure access from any mobile device (phone, laptop, and tablet)

Zero-trust access to mission-critical agency applications

- Global policies hosted in the AWS or Azure Government Cloud determine which users can access which applications
- Admins create and manage policies for users, user groups, applications, and application groups
- IT can segment access by applications with no need to segment by network or use ACLs

Reduce the attack surface

- Users are never placed on the network, which helps to limit risk
- Applications are made “dark” to unauthorized users, preventing lateral access to other apps
- Z-Connectors do not listen for inbound requests, which helps prevent DDoS attacks
- FedRAMP certified, TLS-based encrypted, micro-tunneling for compliance

Application and user activity reconnaissance

- Discover unknown applications and apply granular access controls
- Identify users who are interacting most frequently with these applications
- View user activity and stream logs to SIEM provider
- View the health of applications, servers, and connectors in your environment

Simplify remote access to apps

- Provides direct user-to-application access via software, not rigid VPN appliances
- Removes the need for TIC appliance stacks for access to applications
- Reduces the complexity of network and security architectures
- Accelerates migration of agency apps to cloud

Optimize costs and resource usage

- Opex vs CapEx w/no hardware costs
- Reduce TIC spend by bypassing it
- Per user pricing (easy to manage)

Get started with Zscaler Private Access

FEATURE	FEDERAL
Global visibility for users and application — Single pane of glass shows which users are accessing private, internal apps	✓
Secure Private Application access — Access to unlimited private internal applications (whether public/private/hybrid cloud or legacy datacenters) without exposing the network to users or applications to the Internet	✓
App and server discovery — Wildcard policy shows application and server locations as they are requested by users	✓
Enterprise DarkNet with DDoS protection for applications — Applications are only visible to users that are authorized to connect to them	✓
Single console for policy definition and management — All policy for global deployment via a single pane of glass	✓
Passive health monitoring — Application health is monitored when access is requested	✓
Zscaler App — Lightweight application used to provide access to Zscaler Internet Access and Zscaler Private Access	✓
Microsegmentation by application (up to 5 application segments) — Granular access control by user or group for up to five specific application definitions, each of which may contain multiple hosts and/or ports.	✓
Microsegmentation by application (up to 10,000 application segments) — Granular access control by user or group for up to 10,000 specific application definitions, each of which may contain multiple hosts and/or ports.	✓
Continuous health monitoring — Application health is continuously monitored to ensure that ports are available and users can connect to the app	✓
Device posture enforcement — Checks device fingerprint and certificate, as well as other postures	✓
Customer-provided PKI — Customer-provided certificates ensure complete privacy	✓
Double encryption — Provides encryption to microtunnel using customer's PKI	✓
Real-time user transaction view — Instantaneous logs for end-user support	✓
Log Streaming Service — Automatically streams logs to SIEM provider	✓

Note: An application segment is any number of FDQNs/IP addresses on a standard set of ports.

To learn more about Zscaler Private Access visit
zscaler.com/products/zscaler-private-access

About Zscaler

Zscaler was founded in 2008 on a simple but powerful concept: as applications move to the cloud, security needs to move there as well. Today, we are helping thousands of global organizations transform into cloud-enabled operations.

zscaler™

Zscaler, Inc.
110 Rose Orchard Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com