Securing Remote Access to Agency Applications

Zscaler Private Access™ for the Federal Government

FedRAMP

Authorized

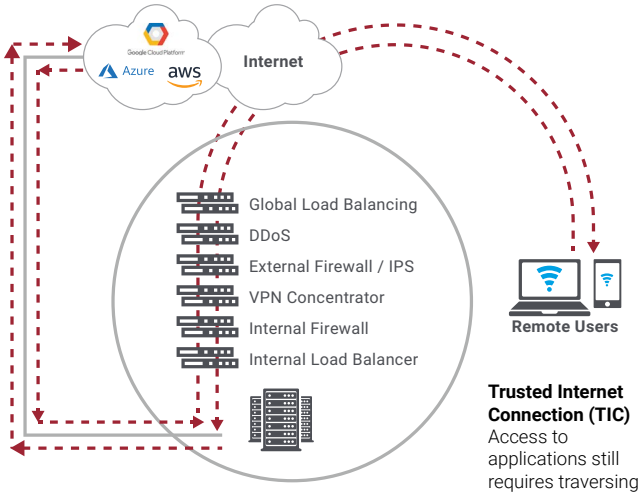
zscaler™

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, while users are continuing to move off of internal networks. 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. However, such services also extend the security perimeter to the internet, requiring agencies to consider how to best allow users to securely access applications from remote locations from any device—government issued or not.

Legacy remote access impedes the cloud mission

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.



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

Even when applications resided solely in the data center, VPN technology was never ideal. A VPN places remote users on the network, increasing the propensity for risk by enlarging the attack surface. Together, TIC and VPN technologies can slow cloud adoption by hindering its benefits in productivity and simplicity, among others.

In response to these challenges, Zscaler offers Zscaler Private Access (ZPA™) - Government, a cloud-based, zero trust remote access service that provides seamless and secure access to internal agency applications for authorized users.

Fast, zero trust access with ZPA-Government: Bypass the TIC

ZPA-Government is the first and only zero trust solution that is Joint Authorization Board (JAB) authorized at the High Impact level.

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

It also meets the Department of Homeland Security TIC Telework Guidelines, which allow for direct connections between authorized users and federal applications as a way to improve productivity and reduce cyber risks.

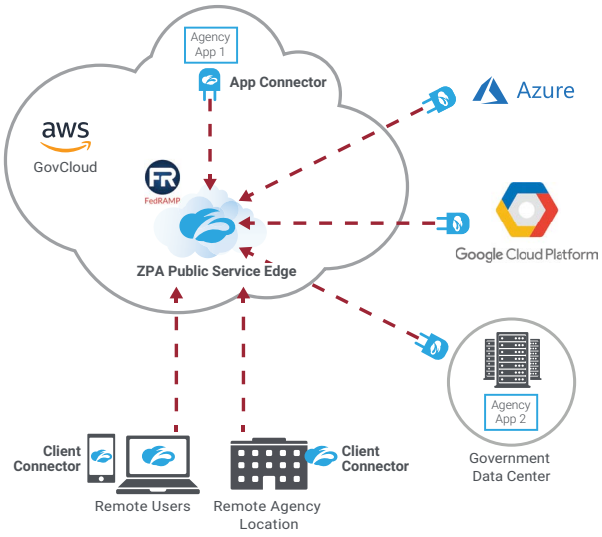
Built on a fully cloud-delivered architecture, not appliances, ZPA-Government provides comprehensive security and a fast, seamless user experience. Access is consistent to all agency applications, whether they're hosted in the government data center or in a cloud service provider such as AWS GovCloud or Microsoft Azure. ZPA is an alternative to VPN, providing least-privilege access that connects authorized users to specific approved applications via encrypted, mutually authenticated secure tunnels. Traffic does not traverse the open internet, and, because ZPA eliminates the need to go through TIC, it reduces overall traffic through the TIC and related expenses, while improving performance for users.

How ZPA works

ZPA works by brokering a connection between an authenticated user and application. A small piece of software called Zscaler Client Connector (formerly Zscaler App/Z App) is installed on the user device. Client Connector ensures the user's device posture, assigns a device fingerprint, and extends an encrypted microtunnel out to the ZPA Public Service Edge 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 App Connector, deployed as a VM. The App Connector establishes an outbound connection to the ZPA Public Service Edge running in the cloud via an additional encrypted microtunnel. If access policy is met, the ZPA Public Service Edge approves access and stitches together the user-to-application connection.

Secure connections in a FedRAMP Cloud

Agencies use Zscaler to remove the latency of legacy TIC/MTIPS and strengthen security rigor.



ZPA Public Service Edge: secure user-to-app connection

- Cloud Policy Engine: user-to-app access rights
- ZPA Public Service Edge runs within AWS GovCloud, East and West Clouds

Client Connector: installs on user's device, requests access to authorized apps

App Connector: front-ends agency application, establishes outbound connection to ZPA Public Service Edge

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 ZPA Public Service Edge 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 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 application 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
- App Connectors do not listen for inbound requests, which helps prevent DDoS attacks
- FedRAMP certified, TLS-based encrypted, microtunneling 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 with no hardware costs
- Reduce TIC spend by bypassing it
- Per-user pricing (easy to manage)

Get started with ZPA-Government

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 Client Connector — 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.

Learn more about ZPA-Government and ZIA-Government, the first secure internet and web gateway solutions to meet the guidance of the TIC 3.0 initiative
zscaler.com/solutions/government

About Zscaler

Zscaler enables organizations to securely transform their networks and applications for a mobile and cloud-first world. Zscaler services create fast, secure connections between users and applications, regardless of network and without the cost, complexity, and limitations of gateway appliances.

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