Mission possible: protecting federal users anytime, anywhere

Enabling TIC-in-the-Cloud for secure, policy-based access to applications and SaaS services

zscaler™

Today, federal teams need secure access to data and applications from any device, anywhere. For years, the federal user's only access was in the office—a remote VPN was a luxury. However, as applications moved to the cloud, the office became problematic—accessing cloud-based applications over the internet or remotely requires a Trusted Internet Connection (TIC), which was not built for this high-volume, high-demand traffic.

When launched, the TIC initiative did significantly improve the federal government's security posture, but it has become increasingly inefficient over time. Times have changed, therefore, Zscaler has changed how we address cloud applications and remote access with TIC.

The TIC's current perimeter-based architecture limits the government's ability to take advantage of cloud and mobile technologies. With the TIC architecture, racks of security appliances are placed at limited gateways to funnel and monitor internet traffic. The forced hub-and-spoke network design that ensures all internet-bound traffic traverses the TIC is costly to manage and maintain. This design cannot quickly adapt to changing cybersecurity needs, and it makes traditional VPN traffic slow. The federal government needs need to find a way to optimize cost and increase cloud preference, yet maintain the security and reporting the TIC provides.

At the same time, the federal government's emphasis on telework increases the need for secure, remote access. For example, the General Services Administration (GSA)[1] has approved the majority of its workforce to work remotely. In order to keep up with these growing mobile demands, agencies must modernize their infrastructures. Recent government IT modernization initiatives—the Cybersecurity Executive Order, the Modernizing Government Technology (MGT) Act[2], and the Report to the President on IT Modernization[3]—were intended to help pave the way to a more efficient, modern government.

As agencies work to meet modernization goals of shared services, mobile workforce enablement, improved FITARA scores, and more—they need to shift away from a legacy hub-and-spoke network to a modern, direct-to-cloud, Zero-Trust architecture, no matter the device or location of the user.

[1] https://www.gsa.gov/node/78292

[2] https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/

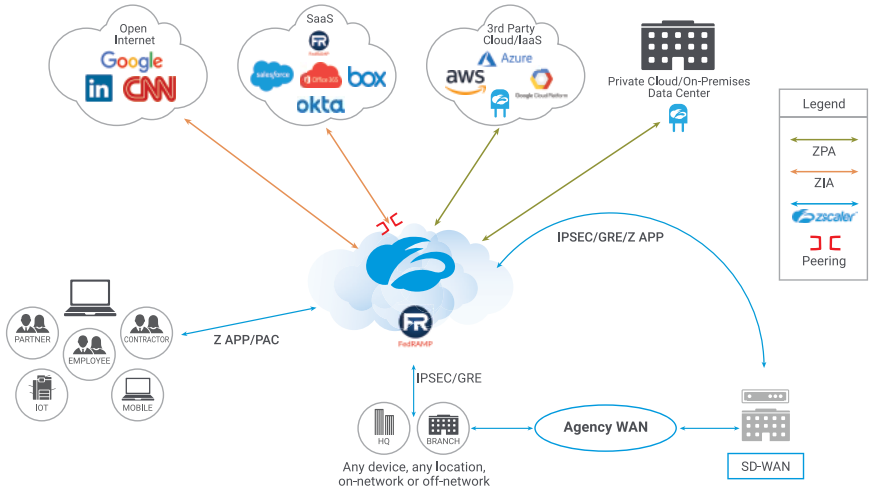
[3] https://itmodernization.cio.gov/assets/report/Report%20to%20the%20President%20on%20IT%20Modernization%20-%20Final.pdf

Improve security controls – keep IT focused on innovation

Federal IT leaders can improve how they see, protect, and control user traffic to the internet by moving TIC security controls and other advanced security services to a cloud platform. This approach offers agencies global POP access and peering with FedRAMP-authorized applications, while preserving Einstein features and keeping CDM reporting in place.

Industry must create a Zero-Trust environment that knows the secure and trusted user, and the only way to do that is to wrap the security policy around the user rather than the network. In this case, users are protected wherever they go, and through whatever internet connection they access. And, when repetitive, manual IT processes are automated, freeing an agency's in-demand IT resources to innovate and stay focused on mission priorities.

TIC-in-the-Cloud for secure, policy-based access to applications and SaaS services



"TIC-in-the-Cloud" is an innovative approach that enables agencies to route traffic directly to the cloud—and it doesn't require any hardware. Further, this approach is a mobile solution and enables users to securely and efficiently access data on their smartphones, laptops, tablets, and more.

Always-on security = productivity, flexibility

With a direct-to-cloud architecture, users take the shortest path to the application or internet destination, which in turn optimizes performance. In addition, purpose-built network security technology applies numerous techniques to minimize processing overhead, reducing latency as compared to an appliance-based solution.

To move the ball forward in an increasingly mobile world and keep up with the government's IT modernization initiatives, agencies must have secure, streamlined connections, regardless of device or location.

- **8 Consecutive years:** Named a Leader on Gartner's Magic Quadrant for Secure Web Gateways
- **100 Million Threats** Detected Per Day
- **120,000 Unique Security** Updates Per Day
- Internet Exchange Peering with **150+ vendors**, including **Office 365, AWS, Azure**

Zscaler™ Federal Cloud Services

The Zscaler multi-tenant cloud security platform applies policies set by the agency to securely connect the right user to the right application. Unlike traditional hub-and-spoke architectures, where traffic is backhauled over dedicated wide area networks (WANs) to centralized gateways, the Zscaler solution routes traffic locally and securely to the internet over broadband and cellular connections.

- Zscaler Internet Access (ZIA): Securely connects users to externally managed applications, including SaaS applications and internet destinations, regardless of device, location, or network
- Zscaler Private Access (ZPA™): Offers authorized users secure and fast access to internally managed applications hosted in enterprise data centers or the public cloud

The Zscaler FedRAMP Cloud enables modern, secure, cloud-based routing to deliver trust-to-trust connections using encrypted TLS over the internet, while still complying with the TIC mandate. At the same time, Zscaler technology identifies trusted user-to-untrusted user connections and routes them through the TIC to the open internet in compliance with the TIC mandate (M-08-05).

Future forecast – looking ahead

Zscaler provides the entire internet security stack as a service, continuously applying policies and threat intelligence to protect agencies from malware and other advanced threats. By moving security and access controls from the data center to a FedRAMP-compliant distributed cloud, the federal government can eliminate costly appliances, strengthen cybersecurity by delivering consistent protection to users everywhere they go, and improve user experience and productivity while reducing latency.

Identifying and understanding the user, while protecting the application with inside-out connectivity, precise access, and "trust no one" encryption, removes the network and the device used to access it from the security equation. Whether the user is in the office or working remotely in the field, the Zscaler FedRAMP Cloud provides the intelligence to optimize agencies' TIC spend and performance. Zscaler's patented technology allows policy to follow the user, while the Zscaler FedRAMP Cloud determines trusted and untrusted connections to make routing decisions appropriately, and create a Zero-Trust optimized TIC environment.

For more information, visit
zscaler.com/resources/ebooks/zscaler-cloud-security-platform

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