Securing Mobility for Government Employees

Zscaler™ Government Cloud helps agencies enable a secure modern workforce

zscaler™

Government agencies are embracing mobility by providing users with access to agency resources through government-issued smartphones. However, these agencies also need a way to provide security to their users and this mobile traffic. In the past, they achieved this by backhauling mobile traffic to a legacy Trusted Internet Connection (TIC) 2.2 inspection stack. However, this process impedes mobile users' ability to effectively complete their work which, in turn, has a direct negative impact on the agency's mission.

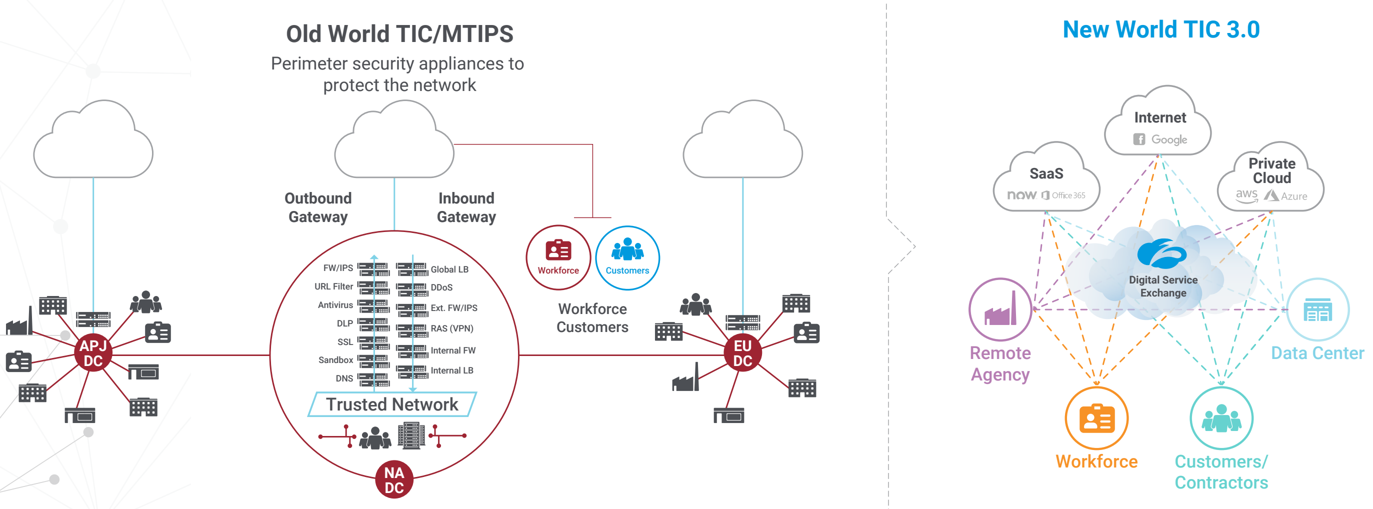
As a result, mobile users have been forced to find a way around TIC 2.2, which can be dangerous and introduce security threats to an agency's network. In some cases, agency users are simply unable to perform their jobs due to TIC 2.2 limitations. Thankfully, recent TIC 3.0 policy changes have enabled agencies to leverage cloud-based solutions to provide protection for mobile users.

Built in the cloud for the cloud, the Zscaler Government Cloud enables agencies to deploy protection and monitoring capabilities for mobile phones accessing systems and services on the internet, SaaS, and private applications, even when connected over mobile carrier networks. By deploying Zscaler, agencies can identify suspicious network traffic patterns, enable filtering and control of mobile traffic, and categorize traffic for easy filtering and restriction, all while having rich log data that provides insight into mobile traffic behavior for agency security operations center (SOC) teams.

Simple to deploy and use

To protect mobile users, a lightweight traffic-forwarding application, Zscaler Client Connector (formerly known as Zscaler App), is installed via mobile device management (MDM) on mobile devices. Client Connector makes a TLS 1.2-encrypted connection that forwards internet traffic to Zscaler Internet Access™ (ZIA™), a TIC alternative, for security inspection.

ZIA first determines if the mobile user is authorized to access the traffic being requested (via a SAML-based check with the agency's directory) and logs the connections that the device makes before sending traffic to the internet destination. The diagram below outlines how Zscaler allows any agency to reach its goal of moving to an approved TIC 3.0 architecture without worrying about how and where to install and maintain the physical appliances that are required in a TIC 2.2 environment.



Data center is the center of gravity → Cloud is the new data center.
Hub-and-spoke WAN (backhaul to DC) → Internet is the new network (direct access).
Castle-and-moat network security → Business policies connect apps, devices, and user.
User connects to the network for app access (trusted) → User connects to an app, not the network (ZTA).

Zscaler protects mobile users with multilayered security

Once mobile traffic has reached the ZIA Government Cloud using Client Connector, it undergoes inspection by a multitude of security engines that have been specifically developed by Zscaler, as described below.

SSL inspection

The Zscaler service can inspect HTTPS traffic from the organization in real time with no service degradation. It functions as a full SSL proxy or SSL man-in-the-middle (MITM) proxy that can scan data transactions and apply policies to them. The Zscaler SSL inspection service provides two options to protect the organization's HTTPS traffic—SSL inspection or, if SSL inspection is not feasible for the organization, an agency can configure a global block of specific HTTPS content.

URL filtering

Through URL filtering, an agency can limit its exposure to liability by managing access to web content based on a site's categorization. The URL filtering policy consists of agency-defined rules so that when an agency adds a rule, it can specify criteria, such as URL categories, users, groups, departments, locations, and time intervals.

File type controls

The file type control policy engine can restrict the upload and download of various types of files. For example, the agency can block audio (.mp3, .wav, etc.) and video (.avi, .mp4, .mpeg, etc.) files so they do not interfere with cellular bandwidth utilization or restrict the transmission of various files and apply them to individuals, groups, departments, and locations. An agency can also create rules for unknown file types by performing MIME-type checks for files it cannot identify initially. Any file that falls outside of well-defined MIME types for common apps is tagged as an unknown file type.

Antimalware engine

Malware protection prevents users from unwittingly downloading apps that are known to contain vulnerabilities or perform malicious activities while allowing the download of all other apps.

ZIA uses industry-leading antivirus vendors for signature-based detection and protection so it can provide comprehensive web security. In addition to virus and spyware protection, ZIA uses malware feeds from its trusted partners, such as Microsoft and Adobe, as well as its own technologies to detect and block malware.

Zscaler has mobile-specific malware engines to detect mobile phone apps that:

- Are malicious in nature.
- Have known vulnerabilities.
- Share unencrypted user credentials.
- Expose location information.
- Expose personally identifiable information (PII) and device identifiers.
- Communicate with ad servers.

Phishing detection

Using a combination of signature and on-demand AI/ML detection engines, Zscaler scans every web request to proactively identify likely phishing websites, based on characteristics of other phishing websites, to block users from access before the content is ever delivered to the endpoint.

Advanced threat protection

Today, web pages do not contain only plain text nestled inside HTML tags, but are filled with Java applets, Flash videos, ActiveX, and other objects designed to run programs. Hackers routinely embed malicious scripts and applications not only on their own websites but on legitimate websites they have hacked. To ensure mobile phone web security, the Zscaler advanced threat protection (ATP) platform can identify a variety of these objects and scripts and prevent them from downloading to the end-user's browser. The ATP policy engine protects agency traffic from fraud, unauthorized communication, and other malicious objects and scripts.

Risk index protection

Zscaler blocks users from accessing web pages with a PageRisk index score higher than the value set by the agency (determined by simply setting a slider to the desired PageRisk tolerance score in ZIA). The ZIA platform analyzes malicious content on a web page (such as injected scripts, vulnerable ActiveX, zero-pixel iFrames, and more) and creates a PageRisk index. Additionally, ZIA analyzes data from the domain (for example, hosting country, domain age, past results, links to high-risk top-level domains, and more) and creates a Domain Risk index. The PageRisk and Domain Risk indices are combined to produce a single PageRisk index score.

Cloud Sandbox

Zscaler Cloud Sandbox provides an additional layer of security against zero-day threats and advanced persistent threats (APTs) through sandbox analysis (an integrated file behavioral analysis) for EXE and DLL files. Zscaler Cloud Sandbox also handles JAR, PDF, SWF, DOC(X), XLS(X), PPT(X), APK, ZIP, RAR, and RTF file types, and provides file quarantine, policy controls, full IOC reporting, APIs, and zero-day alerting.

Data Loss Prevention

Zscaler Cloud DLP features an inline data loss prevention engine that scans the full packet and payload of every element of traffic that passes through the Zscaler cloud. This engine is designed to protect agencies from data exfiltration through web mail, cloud storage, social media, and a variety of other applications.

Enable zero trust access to internal apps and services without VPN

Traditional mobile phone remote access tools rely on full-tunnel virtual private network (VPN) solutions that extend the agency network to the mobile phone, which can expose the agency to risk from east-west traffic flows on infected mobile devices. What's more, as agencies adopt cloud services, such as AWS and Azure, the traditional VPN access method hairpins traffic through the legacy TIC on its way to the cloud and back, severely degrading the user experience for remote workers.

Zscaler's FedRAMP High-certified solution, Zscaler Private Access™ (ZPA™), provides secure access to private applications from mobile phones, dramatically improving the end-user experience while enhancing security, and reducing cost and network complexity. ZPA provides seamless and secure access to internal applications for authorized users by leveraging a software-defined perimeter, not appliances. ZPA access is the same whether agency applications are hosted in the government data center or in the AWS Government Cloud, Azure, or any other cloud service provider. Most importantly, ZPA can completely replace traditional VPNs to provide encrypted connections to applications from any mobile phone by:

- Making agency applications invisible to the public internet by hiding their internal IP addresses and network infrastructure.
- Preventing mobile users from accessing the agency network.
- Providing true zero trust access to specific agency applications based on access policies and application-level segmentation.
- Using the internet for app-specific TLS-based tunnels to private applications.

Deliver a cloud-like experience for remote users

- Consistent user experience for agency applications in AWS Government Cloud and data centers.
- One-click integration with Okta and other single sign-on providers for simplified access.
- Users are routed directly to their apps via the nearest Zscaler cloud instance (one of 150+ globally) for shortest-path access.
- Zero trust access from any mobile device (phone, laptop, and tablet) to mission-critical agency applications.

Provide zero trust access to mission-critical 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, eliminating the need to segment by network or use ACLs.

Reduce the attack surface

- Users are never placed on the network, which limits insider threats and risks.
- Applications are made "dark" to unauthorized users, which prevents lateral access to other apps.
- Authenticated users connect to their authorized apps in the Zscaler cloud; there are no inbound requests, which helps prevent DDoS attacks.
- FedRAMP-certified, TLS-based encrypted microtunneling for compliance.

Detect application and user activity

- 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 providers.
- 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.

Welcome to the new workforce

Government employees, just like their private sector counterparts, don’t want to be confined to the desk in their cubicle. And there are a host of government employees who, by the nature of their job, must be on the road and in the field. Supplying these employees with government-issued smartphones allows them to be more efficient and productive. And, thanks to the recent TIC 3.0 policy changes, government organizations no longer have to backhaul all of this mobile traffic to legacy security stacks. With the Zscaler Government Cloud, federal organizations can provide their mobile users with a seamless user experience while still ensuring sensitive data is secure.

Are you ready to provide your employees with a smooth and secure mobile work experience?
Let Zscaler show you how.

About Zscaler

Zscaler enables the world’s leading organizations to securely transform their networks and applications for a mobile and cloud-first world. Its flagship services, Zscaler Internet Access™ and Zscaler Private Access™, create fast, secure connections between users and applications, regardless of device, location, or network. Zscaler services are 100% cloud delivered and offer the simplicity, enhanced security, and improved user experience that traditional appliances or hybrid solutions are unable to match. Used in more than 185 countries, Zscaler operates a multitenant, distributed cloud security platform that protects thousands of customers from cyberattacks and data loss. 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