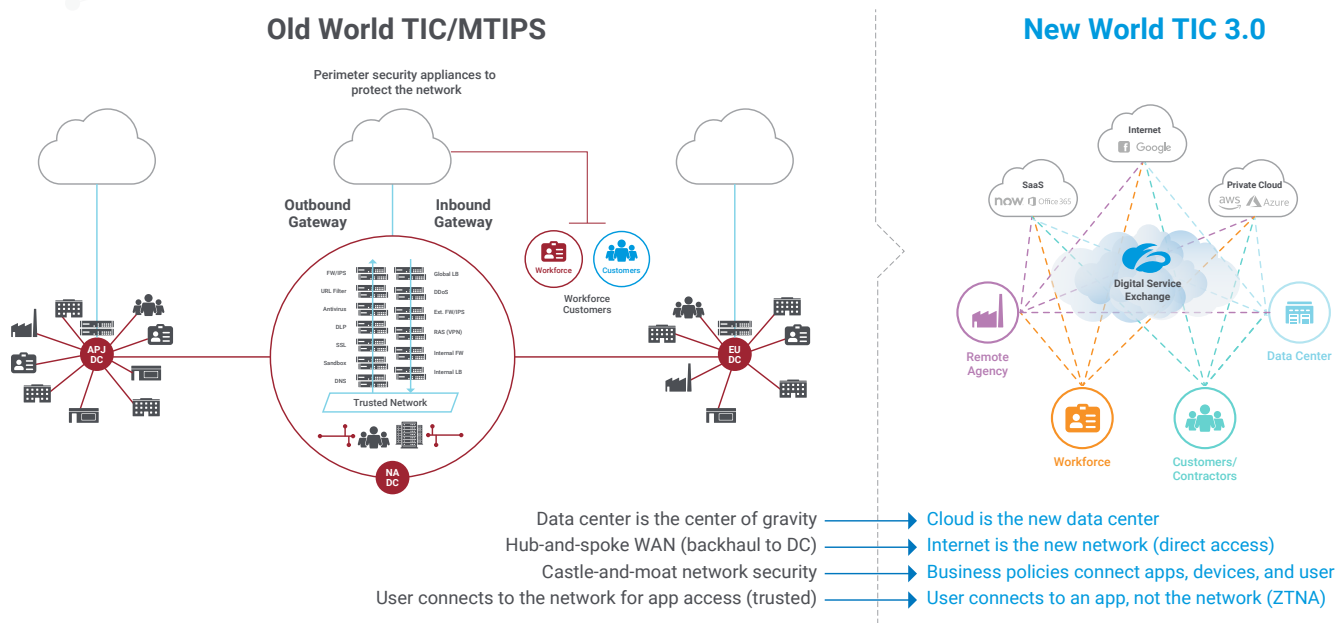


Interim TIC 3.0 Guidance
Means You Can Use
Cloud to Accomplish Your
Telework Mission

Agencies use Zscaler™ to
remove the latency of TIC
and strengthen security rigor



Due to the sudden surge of agency employees working remotely as a result of COVID-19, the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) has issued new interim TIC 3.0 guidance to give agencies new flexibility to keep employees connected to applications. Effective immediately, they are allowing new options for including the potential for Direct-to-Cloud™ connections with specific reference to zero trust and the importance of connecting authorized users directly to cloud service providers for telework that will negate the need for legacy TIC/MTIPS when it comes to remote access. This modern architecture will give federal leaders an opportunity to quickly enable employees to work from home with a faster experience and stronger security than possible with VPNs.



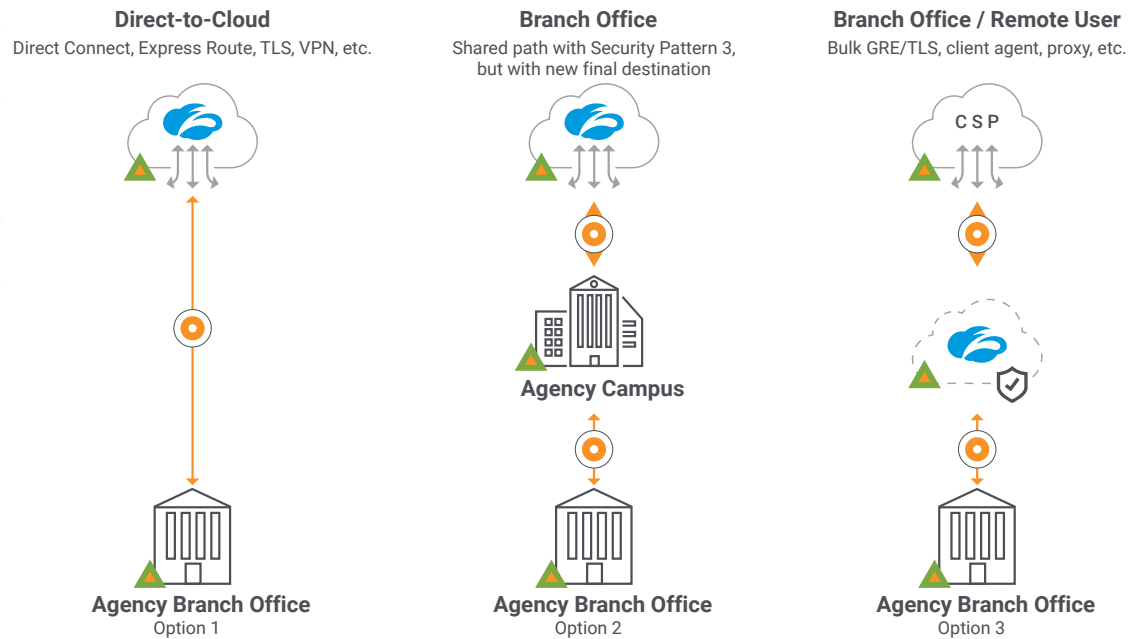
Teleworking requires access to a mix of resources on the agency campus, agency-sanctioned cloud services, as well as the public web. In the past, providing access to an agency application required first connecting through the trusted internet connection (TIC). But, this introduced latency, which impacts the user experience for applications like Office 365 or private apps within AWS, impacting productivity. Virtual private networks would backhaul traffic to the agency campus first, and then out to the cloud service provider, while increasing the attack surface by placing users on the network and exposing servers to bad actors.

The need to reduce both latency and risk has led to the use of cloud-delivered security services that sit in line between remote users and agency applications, and provide a faster, simpler, and more secure experience than with a virtual private network.

The new CISA guidance provides a catalogue of approved network architectures, allowing agencies to select the best architecture to minimize latency while complying with security mandates.

Also highlighted within the guidance are important compliance controls, such as the continued requirement to collect and stream telemetry data to DHS as specified under the TIC 3.0 policy, and the continued requirement to meet critical NIST 800-53 guidelines, which govern FedRAMP. Zscaler’s FedRAMP authorized platform meets both requirements.

Architectures approved by the new CISA guidance



Make the Rapid Transition to Telework. Support Mission Continuity with Zscaler.

The Zscaler FedRAMP Authorized multitenant 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 via VPNs to centralized gateways, Zscaler routes traffic locally and securely to the internet over broadband and cellular connections. The zero trust architecture shifts security functions to focus on protecting the user/device in any location, rather than securing a network perimeter. This ensures that users get secure, fast, and local connections no matter where they connect.

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](https://www.zscaler.com) or follow us on Twitter [@zscaler](https://twitter.com/zscaler).

