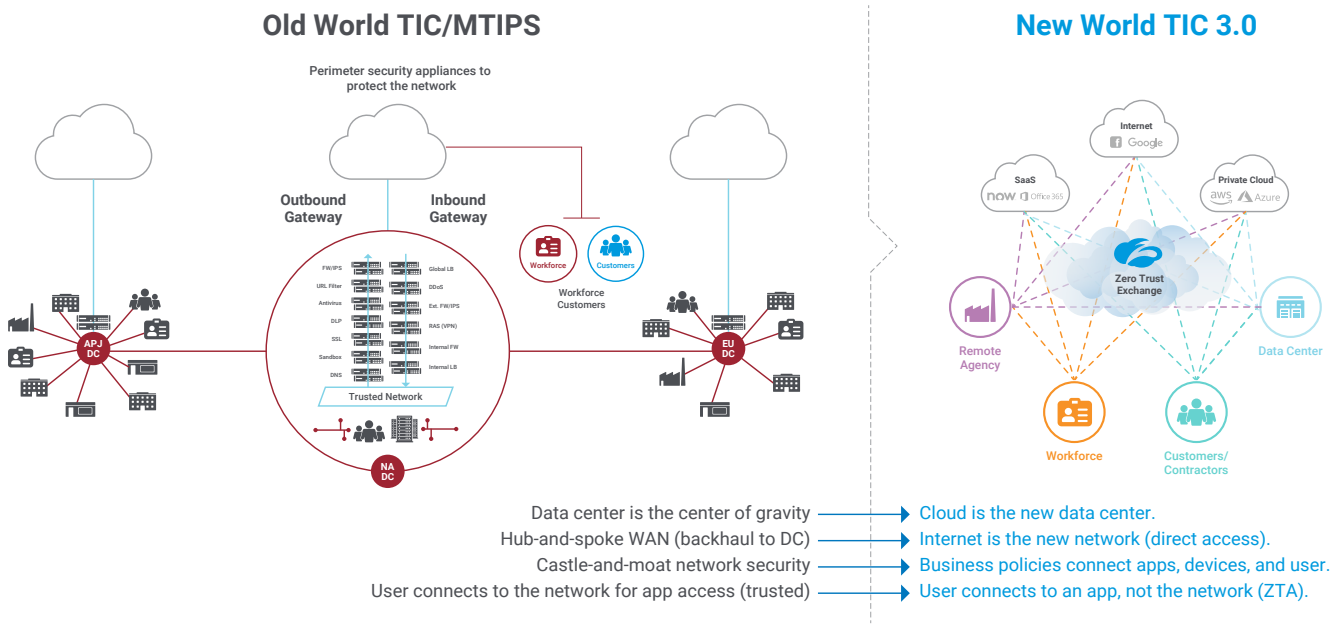
TIC 3.0 Guidance Means You Can Use Cloud to Accomplish Your Telework Mission

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

zscaler™

Federal employees have demonstrated that increased telecommuting has led to greater productivity and contentment. That is why the Office of Management and Budget (OMB) moved swiftly to approve the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) TIC 3.0 guidelines for telework/remote access.

This guidance gives agencies new flexibility to keep employees connected to the applications they need wherever they are. Now agencies can use Direct-to-Cloud™ connections with specific reference to zero trust and the importance of connecting authorized users directly to cloud service providers for telework. This modern architecture eliminates the need for legacy TIC/MTIPS for remote access, giving federal leaders an opportunity to quickly enable employees to work from anywhere with a faster experience and stronger security than possible with VPNs.



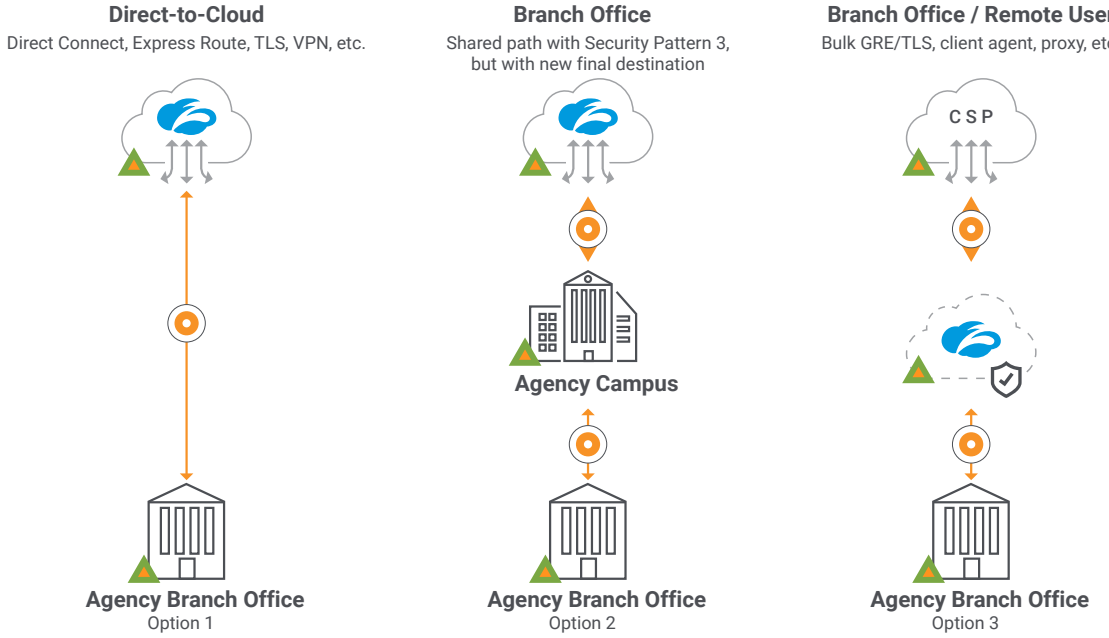
Teleworking requires access to a mix of resources on the agency campus, agency-sanctioned cloud services, as well as the public web. In the past, providing access to an agency application required first connecting through the trusted internet connection (TIC). But, this introduced latency, which impacts 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 CISA TIC 3.0 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 CISA TIC 3.0 guidance



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

The Zscaler FedRAMP Authorized Zero Trust Exchange™ 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 Exchange 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 (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest inline cloud security platform. 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