Solution Brief

Zero Trust Citizen Access™ (ZTCA)

Overview

As government applications move to the cloud and more and more services are provided digitally, the number of citizens accessing services online has increased dramatically. With many organizations adopting work from home policies, and COVID–19 encouraging people to spend less time in public places, government agencies are under pressure to provide online services.

The 2021 Adobe Digital Government Services Survey showed that 77% of citizens surveyed would use more government services if they were accessible from the Internet. At the same time, few government agencies say they have the capabilities to deliver their services from the Internet in a secure and effective manner.

One of the challenges many agencies face with online services is aging applications that are becoming increasingly more vulnerable to attack due to reliance on legacy software that is no longer being updated and patched. Public sector agencies are under increasing pressure to find ways to provide secure access to government services on the Internet, while also maintaining ease of access for citizens.

Zscaler's Zero Trust Citizen Access (ZTCA) approach is built on the Zscaler Private Access (ZPA) zero trust security architecture, which provides secure, fast, and seamless access to public services.

The Traditional Approach

Traditionally, citizens access government services by typing a URL into a web browser. Data flow in this scenario is shown in figure 1.

There are inherent security risks with this approach, as citizens (users) are connected directly to the web application over the internet. The firewalls protecting the application provide attack surfaces for bad actors, and vulnerabilities in firewall or applications can be exploited.

Furthermore, because these firewalls and the applications they protect are "listening" for connection requests from the internet, they are subject to DDoS and brute force attacks. If an attacker were able to successfully breach the firewall, they could move throughout the network laterally to discover, and possibly exploit, other resources in an agency's network.

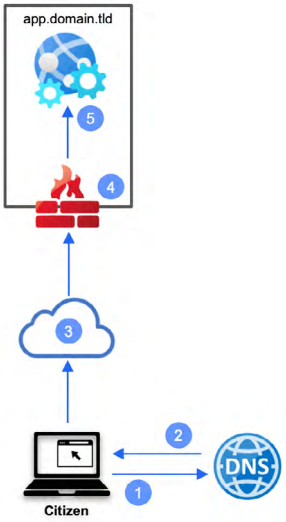

Figure 1

1. Citizen (client) opens a web browser and sends a request for "app.domain.tld".
2. DNS resolves the URL to the public IP address of the firewall protecting the web application .
3. User is routed over the Internet to the firewall protecting the application.
4. Firewall allows connection to the server hosting the application on port 80 or 443.
5. Citizen is connected directly to the server or application via TCP/TLS.

The First Step

Some agencies have taken a first step to addressing these challenges by adopting some concepts of a "Zero Trust Architecture". Zero Trust states, among other things, that no user should have access to any resource, without first being authenticated. When citizens are authenticated prior to gaining access to services, agencies gain significant visibility and control over application access. As a result, many agencies have adopted identity programs that allow citizens to authenticate via social media platforms (Instagram, Google, LinkedIn, etc) as well as using Multi Factor Authentication (MFA). This eliminates the need for agencies to manage login credentials for all citizens, while still providing the ability to manage access. Login pages leveraging social media credentials can look something like figure 2.

This step is essential in the journey to Zero Trust, but still leaves some gaps. Even after athentication, an agency's firewalls, applications, and services are still visible to the internet, and bad actors can still discover and attempt to compromise those components. Firewalls and applications are still vulnerable to attacks such as DDoS, web server exploits and brute force attacks. If a bad actor is able to compromise a firewall or an application, they can still move laterally within an agency's network and cause additional harm.

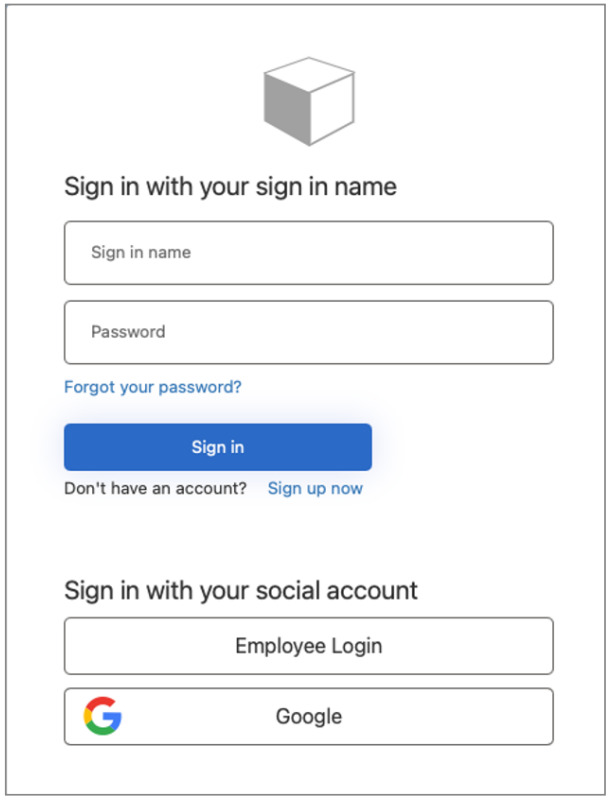

Figure 2

Zero Trust Citizen Access

ZTCA provides a complete Zero Trust architecture for government agencies by not only requiring user authentication for every citizen, but also removing firewall and application attack surfaces by "hiding" web applications – including legacy apps – from the internet, making them undiscoverable to potential attackers. ZTCA is built on Zscaler's Zero Trust Exchange, which provides secure, fast, and seamless access to public services for citizens everywhere.

Here's how it works. In contrast to the traditional approach discussed prior, citizens do not establish direct connections to firewalls, web servers, or applications. Citizen users are connected only to the Zscaler cloud once they are authenticated. The Zscaler cloud validates access policy for that user and leverages a technology called "Application Connectors" to connect that user to their requested application.

Application Connectors sit in front of applications and allow them to communicate with the Zscaler cloud, but not the public Internet. This means that applications are not visible or discoverable from the internet, and because they can't be seen, they can't be attacked. Application Connectors effectively remove the attack surface from the process.

When a citizen successfully authenticates, Zscaler proxies the connection between the citizen and the Application Connector — it "stitches" the connections together temporarily, for only the duration of the web session. This means the application is only accessible to authorized users (citizens) who have authenticated to the Zscaler cloud. This approach also allows for a number of other measures to be taken that provide mitigation against a wide range of network-based attacks. The process is illustrated in figure 3.

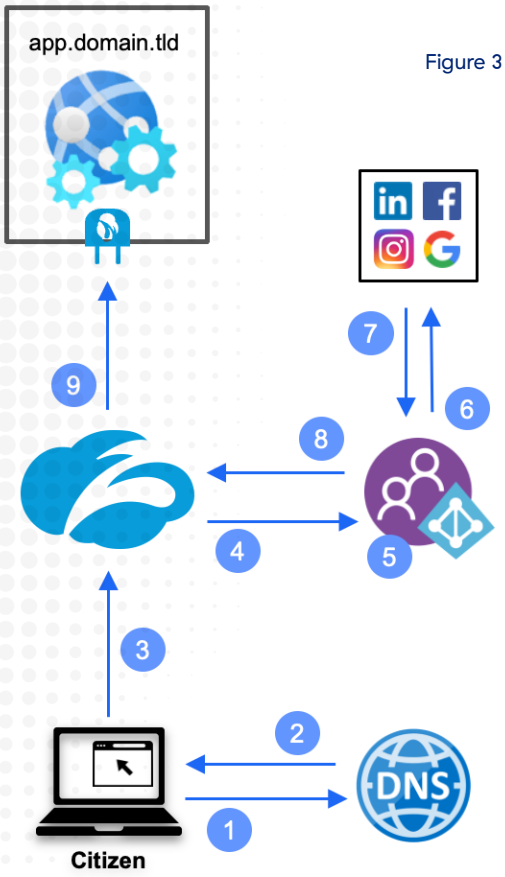

Figure 3

1. Citizen (client) opens a web browser and sends a request for "app.domain.tld".
2. DNS directs the request to the Zscaler cloud.
3. Citizen is routed over the Internet to the Zscaler cloud.
4. Zscaler forwards a SAML request to the configured Identity Provider (IdP).
5. The IdP determines if the citizen passes the authentication requirements. If the citizen passes, it presents the citizen with a login page, consisting of a choice of social media services that have been configured for authentication.
6. The citizen provides credentials and the IdP validates those with the social media service.
7. If the credentials are valid, the social media service returns an authorization to the IdP.
8. The IdP returns a SAML assertion to Zscaler, validating that authentication is successful.
9. Zscaler evaluates access policies for the user and initiates the connection between the user and the requested application via the App Connector.

Zscaler supports integration with multiple IdP vendors to authenticate citizens via social media logins, login.gov or ID.me. The provisioning process is flexible and is dependent on the level of identity proofing and level of assurance required for access to applications. A framework agencies can adopt is FISMA, NIST, RMF, and NIST SP 900-63 for end user identity requirements, in the case of a higher assurance level requirement, Zscaler is able to offload user access to a remote browser isolation container that allows users to access content without the ability to download or inject data to applications.

Summary

The concept of Zero Trust Citizen Access (ZTCA) is to establish an adaptive identity-based access control system between the citizens and the web-hosted government services. The key capabilities of Zscaler's Zero Trust Citizen Access Architecture revolve around: identity-based schema, secure application access, continuous trust evaluation, and an elevated citizen experience that scales dynamically.

ZTCA is a new capability in Zscaler Private Access (ZPA) that has been designed specifically to provide citizens with simple, secure and highly scalable access to any public web or legacy applications. Citizens simply open their favorite web browser and securely access public services from any device. ZPA continues to enforce zero trust policies for existing applications by default.

ZTCA leverages application segmentation, a key facet of ZPA that creates a segment of one between a named citizen and a named application. **It means that citizens are never brought on the network and the application is never exposed to the Public Internet.**

Public agencies can rely on ZTCA to deliver real-time visibility into citizen activity, identify citizens who access applications via browsers, eliminate the public attack surface, reduce the risk of lateral movement all while greatly increasing the scalability of their services.

Zero Trust is the most discussed security model across Public Sector customers

78%

of IT security teams are looking to embrace a Zero Trust model in the near future*

53%

of enterprises have a false sense of confidence in current security technology**

Sources:
* Gartner — Zero Trust Architecture and Solutions
** Cyber Security Insiders — Zero Trust Adoption Report

Additional Considerations

While leveraging third party or social media account credentials can make it easier for your citizens to access Zscaler protected applications, many organizations choose to leverage additional measures during the authentication process that can reduce the risk of stolen or compromised credentials. Contextual access policies and multi-factor authentication are two methods that any organization should consider when choosing authentication policies. Some recommendations are:

- **Geo or Network Location —** Allow, deny, or limit access based on geographic location or by known IP ranges. For example, as a condition of access the agency could deploy a policy that only allows access from within a particular country, state, or even from within the agency's network itself.
- **Endpoint Device Posture —** Allow, deny, or limit access based on certain criteria of the endpoint. For example, if the citizen's device is a member of your agency's domain or if there is an antivirus program running.
- **Social Network —** Agencies can limit authentication to only specific social networks, for example, only allowing LinkedIn.
- **Multi Factor Authentication (MFA) —** Validate a citizen's identity with a second form of authentication like a soft token, one-time code, push notification to a cell phone, or biometric device.

For a demo of Zero Trust Citizen Access, contact your Zscaler Regional Sales Manager or complete a contact us form.

Note: Zscaler does not develop, provide, or support solutions on behalf of third-party Identity providers such as Microsoft and Okta, therefore there may be additional development activities that customers may need to perform to fully configure these solutions for production use.

Zscaler always recommends you periodically review your public facing services and applications using the Internet Threat Exposure Analysis found here: zscaler.com/tools/security-assessment. This tool provides a comprehensive risk assessment and security posture and of your public facing assets.

zscaler™ | Experience your world, secured.™

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**.