Security-as-a-Service Transformation for State and Local Government

The evolution of information security within Public Sector

Background

Traditionally, each State agency built out its own network and designed its own security architecture. Each one of these IT and security silos in a State agency, lead to continued duplication of effort and ever-increasing costs for the overall design. As a result of these inefficiencies, State and Local government agencies established consolidated Enterprise Architecture Frameworks with the goal of a unified way in which agencies would modernize their information technology networks. An enterprise framework helped ensure that agencies and mission partners could share information securely while reducing wasted manpower and continued infrastructure expenditures.

Cloud computing

One of the challenges that was identified early on with regards to cloud computing was the management of cyber security. In response to this challenge, agencies develop policies and standards usually in alignment with Federal policies, standards, and guidelines such as following the NIST 800-53, StateRAMP or FedRAMP controls.

Evolving to a cloud-first approach

Most if not all agencies have approved policies and laws in efforts to get out of the infrastructure business and consume information technology as-a-service from cloud service providers. Unfortunately, many of the legacy systems are rooted in architectures that were developed more than 10 years ago. The on-prem infrastructure traditionally took many years to roll out into production and the associated infrastructure costs created a large total cost of ownership.

Moving from a network-centric to resource-centric framework

Most legacy enterprise designs are network-centric, meaning that the focus is on securing the network itself with the assumption that once the network is secured, resources and users will be protected as well. This belief has been experientially proven wrong and there are many examples of exploitations that have occurred because too much trust was placed on the secured network. What State and Local Governments need now is a modern approach that adopts the zero trust architecture as it is being defined by NIST.

> “Zero trust (ZT) provides a collection of concepts and ideas designed to reduce the uncertainty in enforcing accurate, per-request access decisions in information systems and services in the face of a network viewed as compromised. Zero trust architecture (ZTA) is an enterprise’s cybersecurity plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies. Therefore, a zero trust enterprise is the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of a zero trust architecture plan.” (Scott Rose, 2020)

The basic tenets of the zero trust architecture defined by NIST are:

- All data sources and computing services are considered resources.
- All communication is secured regardless of network location.
- Access to individual enterprise resources is granted on a per-session basis.
- Access to resources is determined by dynamic policy—including the observable state of client identity, application, and the requesting asset—and may include other behavioral attributes.
- The enterprise ensures that all owned and associated devices are in the most secure state possible and monitors assets to ensure that they remain in the most secure state possible.
- All resource authentication and authorization are dynamic and strictly enforced before access is allowed.
- The enterprise collects as much information as possible about the current state of network infrastructure and communications and uses it to improve its security posture.

Many agencies have already begun exploring zero trust solutions and ZTA is becoming the focus for protecting resources from inside the network. Once ZTA is embraced and implemented, the network itself becomes just a means of information delivery.

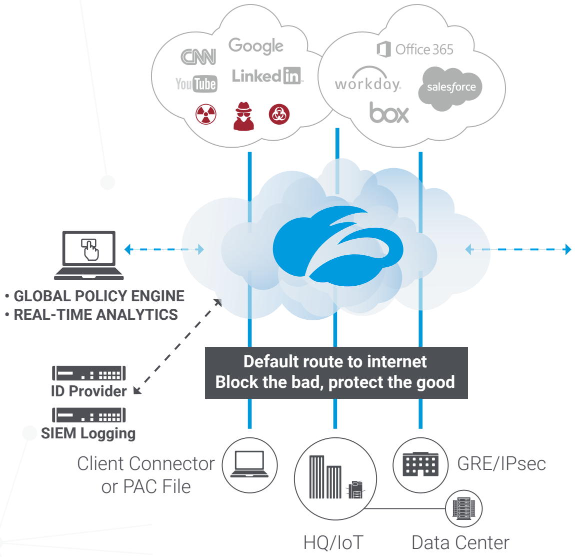
Zscaler – Security delivered as a service

For more than a decade, Zscaler has delivered security as a service to some of the largest commercial enterprises around the world. In late 2018, Zscaler became the first cloud-based security solution to achieve FedRAMP accreditation. Zscaler offers two services – Zscaler Internet Access™ (ZIA™), which is FedRAMP Moderate, and Zscaler Private Access™ (ZPA)™, which is FedRAMP High.

Zscaler Internet Access

Zscaler Internet Access (ZIA) is a secure internet and cloud service provider (CSP) gateway delivered as a service. Think of it as a secure on-ramp to the internet and CSP — all you do is make Zscaler your gateway to the CSP. For on-premise installations, simply set up a router tunnel (GRE or IPsec) to the closest ZIA Public Service Edge. For mobile employees, you can forward traffic via our lightweight Zscaler Client Connector or PAC file.

The main function of the IAP and CAP within the SSA is to provide a comprehensive and robust security stack to protect the DISN from the internet and CSP, respectively. ZIA has a proven track record of providing this a comprehensive and robust security stack to protect its customers worldwide, from the internet and the CSP. ZIA sits between your users and the internet or CSP, inspecting every byte of traffic inline across multiple security techniques, even within SSL. You get full protection from web, internet and cloud threats.



Secure internet and web gateway as a service

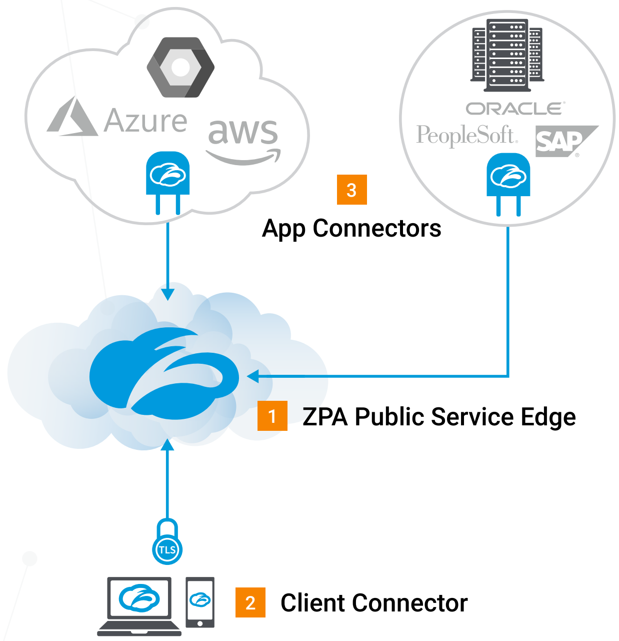
Zscaler Internet Access delivers a completely integrated gateway that inspects all ports and protocols, even across SSL.

ACCESS CONTROL	THREAT PREVENTION	DATA PROTECTION
Cloud Firewall	IPS/Adv. Protection	Data Loss Prevention
URL Filtering	Cloud Sandbox	Cloud Apps (CASB)
Bandwidth Control	Antivirus	File Type Control
DNS Filtering	DNS Security	

Just point your traffic to the Zscaler cloud. For offices, you can set up a tunnel from your edge router. For mobile, you can use our Client Connector or a PAC file.

Zero trust access is based on four key tenets:

- Application/service access no longer requires access to the network or use of VPN.
- Inside-out connections ensure apps and services are invisible to unauthorized users.
- App segmentation, not network segmentation, connects users to a specific app or service and limits lateral movement.
- Secure network communication is achieved via end-to-end encrypted TLS tunnels.



Zero Trust Architecture

1 ZPA Public Service Edge

- Brokers a secure connection between Client Connector and an App Connector
- Hosted in cloud
- Used for authentication
- Customizable by admins

2 Client Connector

- Mobile client installed on devices
- Requests access to an app

3 App Connector

- Sits in front of apps in Azure, AWS, and other public cloud services
- Listens for access requests to apps
- No inbound connections

ZPA provides a simple, secure, and effective way to access internal services. Access is based on policies created by the IT admin within the ZPA Admin Portal and hosted within the Zscaler cloud. On each user device, a piece of software called Client Connector is installed. Client Connector ensures the user's device posture and extends a secure microtunnel out to the Zscaler cloud when a user attempts to access an internal service.

Both services integrate with an agency's existing identity providers via an industry standards-based SAML 2.0 connection and also have the ability to stream transaction logging information to the agencie's SIEM architecture. This means that Zscaler will integrate with the agencie's existing cybersecurity platform and big data initiatives. Both ZIA and ZPA can be extended on-premises allowing for highly efficient traffic engineering. ZIA provides cloud-based protection at the perimeter, and ZPA provides a zero trust architecture to protect connections within the office.

Stronger through partnerships

Zscaler provides a robust and mature security-as-a-service platform but leverages tight integration with industry partners to ensure that the service can be easily deployed and integrated for a best-of-breed overall solution. Zscaler performs some basic device posture checking as part of the ZPA service and takes that capability further through integration with endpoint detection and response (EDR) companies, such as CrowdStrike, Carbon Black, and SentinelOne. By integrating with leading industry partners, Zscaler ensures that the EDR capability is active on the endpoint before connecting a user to any resources. ZIA and CrowdStrike also share threat intelligence between their clouds, meaning a threat signature detected by Zscaler anywhere around the world can be detected on an endpoint subscribed to the CrowdStrike Falcon service. Zscaler also integrates with a variety of SIEM vendors, such as Splunk, Elastic, ArcSight, and others to make it easy for those solutions to ingest our real-time streaming data.

Conclusion

Having taken the first step of consolidating security under a unified security architecture, agencies are ready to begin the next transformational step, moving from managing and maintaining that architecture itself, to having it provided as a service. With a cloud-based security stack being delivered as a service, Zscaler is positioned to provide the perimeter security that today is being delivered by legacy on-premise infrastructure. The zero trust framework of Zscaler, combined with cloud-based EDR solutions, can replace the overly complex and expensive regional security stacks that have proven to be a major bottleneck to performance. The benefits for agencies in transforming on-premise appliance stacks to an as-a-service model will be realized in cost savings, greater scalability, better performance for the end user and warfighter, and ultimately in a greater cybersecurity capability.

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