Using a Zero Trust, Cloud-Based Tactical Network to Protect our Tactical Edge

zscaler™

Being connected to the internet 24/7/365 with high-speed communication networks is no longer a luxury—it's an expectation. We expect to find the information we need, when we need it, with no interruption. But for our tactical edge—the people deployed on the front lines—the environment is very different.

For those responsible for collecting and disseminating intelligence, the ability to securely connect to the internet from literally anywhere can be a matter of life and death; the difference between a successful mission and one that fails; or the difference between accurate intelligence delivered in time or too late.

In response to these needs, the Department of Defense (DoD) created the concept of the tactical cloud edge and tactical compute nodes. The tactical cloud edge is typically hosted in-theater, such as at a regional hub node or on a vessel close to the warfighter, to bring the cloud physically within reach. In addition, tactical compute nodes are easily transported inside smaller vehicles and provide localized computing and storage that syncs with the tactical cloud edge, when it is available.

But this begs a question: How do you secure communication to the open internet and the resources hosted within the tactical cloud without exposing the warfighter to the enemy or jeopardizing the mission?

And then there is the question of how to share resources with mission partners. How do you give someone from the army of the Republic of Korea access to the data they need without letting them have access to everything? How do you ensure NATO mission partners have access to data without compromising your security?

Finally, how do you make this capability simple to run and maintain globally, at the highest level of security, so you can move where the operations move without the need to deploy a cumbersome infrastructure that you have to transport?

You need a zero trust cloud solution, such as the Zscaler Government Cloud.

Choosing a zero trust cloud-based solution

Zero trust architectures maintain strict access controls, trusting no one by default—even those already inside the network perimeter. That is why a cloud-based zero trust solution, such as the Zscaler Government Cloud, is the answer to giving the tactical edge the security, mobility, access, and ease they need in the field.

The Zscaler Government Cloud provides the DoD and military components with secure access to the internet and internally managed applications. It is comprised of two services—Zscaler Private Access™ (ZPA™) and Zscaler Internet Access™ (ZIA™).

Zscaler Private Access (ZPA)

ZPA is a cloud service that provides zero trust, secure remote access to internal applications running on the tactical cloud, a tactical compute node, or a private data center. With ZPA, applications are never exposed externally, making them completely stealth to unauthorized users. The service enables warfighters to connect to mission applications via connections brokered in the Zscaler Government Cloud (or an on-premises extension) vs. extending the network to them.

Zero trust access is based on four key tenets:

- Application access no longer requires use of VPN or exposure of the backend network infrastructure.
- Inside-out connections ensure apps are stealth to unauthorized users.
- App segmentation, not network segmentation, connects users to a specific app and limits lateral movement.
- All traffic is secured via end-to-end encrypted TLS tunnels.

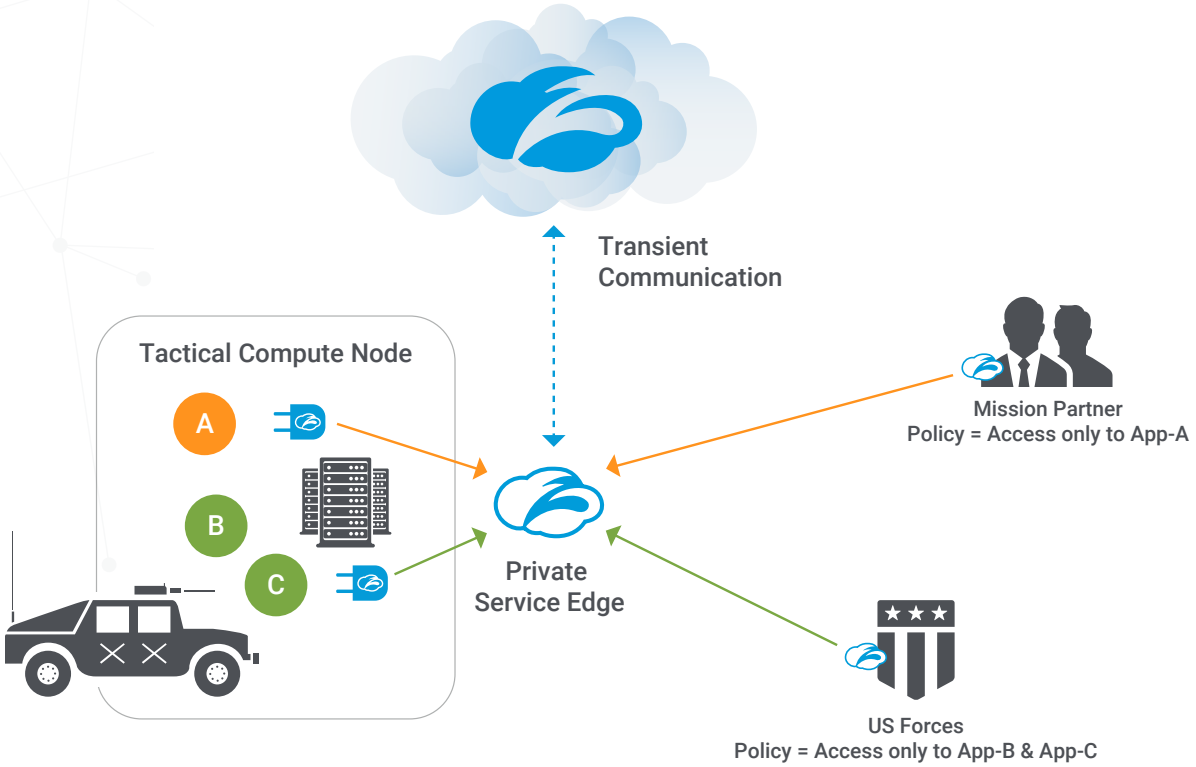
ZPA provides a simple, secure, and effective way to access internal applications. Access is hosted within the Zscaler Cloud and based on policies the DoD IT admin creates within the ZPA Admin Portal. A piece of software called Zscaler Client Connector (formerly known as Zscaler App) is installed on each user device, and helps validate the device's security posture.

Adjacent to an application running in a tactical compute node, tactical cloud edge, or tactical cloud, ZPA places a small piece of software called an App Connector, deployed as a virtual machine, which is used to extend a microtunnel out to the Zscaler cloud. The App Connector establishes an outbound connection to the cloud, and does not accept any inbound connection requests, thereby preventing DDoS attacks. Within the Zscaler cloud, a ZPA Public Service Edge (formerly known as Zscaler Broker) approves access and stitches together the user-to-application connection. The Zscaler Government Cloud can also be extended within the theater via the ZPA Private Service Edge software component for efficient traffic engineering.

ZPA has four key features that improve security while reducing cost and complexity and delivering a better user experience.

1. It is born in the cloud and is therefore highly scalable. For example, in response to the COVID-19 pandemic, the ZPA cloud expanded by more than 600 percent in a matter of weeks.
2. It has the ability to operate for extended periods of time disconnected from the wide area network, thus supporting expeditionary missions in disadvantaged networking environments.
3. It allows the DoD to define granular application access based on identity without having to expose the backend infrastructure to end users. Applications are essentially invisible to unauthorized warfighters and mission partners.
4. It is FedRAMP High approved. This means that Zscaler is meeting government requirements to provide a cloud-based security solution.

ZPA is 100-percent software-defined, so it requires no physical appliances and allows users to benefit from the cloud and mobility while maintaining the security of their applications. Below is a look at the architecture of the ZPA service.



The illustration shows various combatants in-theater accessing their authorized mission-critical applications using the zero trust architecture of the Zscaler Government Cloud via an extension of the cloud known as the ZPA Private Service Edge. The ZPA Private Service Edge is deployed alongside other components on the tactical compute node. Should the tactical compute node lose communication with the Zscaler Government Cloud, the service will still continue to operate and enforce whatever policy was defined prior to the disconnected state.

Zscaler Internet Access (ZIA)

ZIA is a secure internet and web gateway delivered as a service from the cloud. Think of it as a secure internet on-ramp—all you do is make Zscaler your next hop to the internet. This allows tactical users on expeditionary missions to utilize the enemy's networks to securely connect back to mission resources without being exposed to malicious threats.

ZIA sits between tactical users and the internet, providing digital force protection and inspecting every byte of traffic inline—even traffic encrypted with SSL. It provides full protection from web and internet threats. With a cloud platform that supports cloud sandboxing, next-generation firewall, data loss prevention (DLP), and cloud application visibility and control, you can be assured that users won't be compromised by malicious content and sensitive information will not be exfiltrated.

This service is cloud-based and, as such, doesn't require any hardware to be deployed. Just point the internet connection to Zscaler and we will secure your communications while obfuscating your traffic's destination to the enemy.

This is important as tactical operations require the ability to be quickly stood up for a period of time and then be decommissioned and redeployed elsewhere.

Zscaler global cloud policies

Global cloud policies are critical for security because remote users are often outside the visibility and control of an enterprise.

One common byproduct of deploying, managing, and upgrading appliances for hundreds or thousands of users in the in the field is unpredictable security capabilities. Often, remote sites have fewer controls. For example, they might not be able to scan all encrypted traffic or divert potential risks into a sandbox. As a result, security policies are applied unevenly.

A global cloud, such as Zscaler, eliminates all those variables and provides uniform security for all internet-bound traffic at all locations for all users. The cloud-based controls—a security stack in the cloud—means it's always available to inspect all traffic, as well as all ports and protocols. There is no difference in policy control on base or in the field. Consistent policies that are administered in the cloud improve security, regardless from where the user connects.

The ZIA global security cloud has a purpose-built architecture to enforce policies equally on all cloud traffic at all locations and for all users—including our warfighters and mission partners.

In addition, the Zscaler solution can interoperate with the hardware the warfighter was issued. There is no need to worry about creating a new API to make other tools work. There is no need for ruggedized boxes or power cords. Whether it's wearable computing or something else, keeping the size, weight, and power down helps keep the tactical edge mobile.

And Zscaler transcends operation systems. Out of the box, the Zscaler Government Cloud supports Microsoft, Apple, Android, and iOS endpoints, allowing the warfighter to access everything they need.

That means seamless connectivity in disconnected operations. It also means giving the tactical edge the ability to have a standardized approach that makes sitting in the field accessing an application the same as if they were sitting back on base.

They can be in a hybrid cloud, a public cloud, or their own private data center with cloud offerings, and Zscaler is the bridge that assists them moving back and forth.

Stronger through partnerships

Zscaler provides a robust and mature security as-a-service platform, but also leverages tight integration with industry partners to ensure that the service can be easily deployed and integrated. 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 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 that Zscaler detects anywhere around the world can be detected on an endpoint subscribed to the CrowdStrike Falcon service.

Zscaler also integrates with a variety of security information and event management (SIEM) vendors, such as Splunk, Elastic, ArcSight, and others, to make it easy for those solutions to ingest our real-time streaming data. While Zscaler provides inline cloud access security broker (CASB) features, ZIA also has integration with third-party CASB solutions, such as Microsoft Cloud App Security (MCAS) and McAfee MVISION.

Conclusion

The Zscaler Government Cloud platform provides a standardized way for everyone to securely access the compute resources they need. Mission partners can access the information they need and are authorized to access without compromising the integrity of the underlying architecture's security itself. Regardless of whether the user is on ship, at base, or out in the middle of the desert, they have a common methodology for accessing their information. This is what keeps the tactical edge secure.

GOVERNMENT CLOUD KEY BENEFITS

- **Never place users on the network:** Authorized users have access to specific private apps without the need to access the network, reducing the risk of lateral movement and the spread of ransomware.
- **Segment by application, not network:** Microtunnels enable network admins to segment by application with no need to segment networks or manage access control lists or firewall policies.
- **Inside-out connectivity means apps are stealth:** The service-initiated zero trust architecture ensures apps connect outbound to authorized users. IP addresses are never exposed, and DDoS is impossible.
- **100-percent cloud-delivered zero trust access service:** Zero trust as a service allows for simple management, high availability, greater scale, and strong protection against DDoS attacks.
- **Discover and secure shadow IT applications:** Organizations gain visibility into previously undiscovered internal applications running in the data center or public cloud. Admins can set granular policies for discovered applications ensuring access is based on least-privilege.

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