CASE STUDY

NTSB Fast Tracks Cloud Transformation with Zero Trust TIC-in-the-Cloud

National Transportation Safety Board

www.ntsb.gov

Zscaler Products:
Zscaler Private Access, Zscaler Internet Access

Like most Federal agencies, the National Transportation Safety Board (NTSB) is modernizing and expanding the use of cloud-based applications in line with OMB's Cloud Smart strategy. The agency is laying the foundation to use a hybrid IT infrastructure to improve business and operational agility. NTSB has an important mission–to make transportation safer by conducting independent accident investigations, advocating safety improvements, and deciding pilots' and mariners' certification appeals. The workforce is highly mobile, with field teams conducting investigations throughout the U.S. in varied environments, from urban to highly remote.

NTSB's IT team, under the leadership of Angel Santa, CIO and Victor Pham, CTO, recognized their legacy network infrastructure, and the requirement to route all traffic through a legacy Trusted Internet Connection (TIC) was a significant challenge. The TIC was not designed to handle an increasingly mobile workforce. As a result, latency and connection issues created a poor user experience, negatively impacting NTSB's mission. They needed to find a way to deliver a seamless and secure path to the cloud.

Traditional VPN Frustrates Remote Users and Complicates Security

Under the traditional model, NTSB routed remote connections through a VPN client, to the agency data center, through a stack of on-premise security devices, and back out through the TIC, where it traversed another stack of security appliances to its destination – such as the open Internet, AWS, O365, etc. Next, the process is completed in reverse as the information requested via the remote connection returns to the user. This process also placed users on the network, which could lead to additional security risks and lateral spread across the network.

> "When our employees connected remotely to NTSB's servers and applications through the VPN and TIC, they had to leave one destination and head to another, and then repeat the laborious process, because they can't easily move between clouds. This added frustration during investigations."
>
> **– Angel Santa**
> CIO at **NTSB**

Secure TIC-in-the-Cloud with Zero Trust

To overcome these issues, NTSB uses a comprehensive SD-WAN architecture and designed an innovative, secure "TIC in the Cloud" solution that routes traffic locally and securely over broadband and cellular connections, using Zscaler, a multi-tenant cloud security platform.

NTSB makes Zero Trust possible by leveraging Zscaler Private Access (ZPA). The FedRAMP authorized remote access service creates dual inside out connections between an authorized user and specific applications using TLS encrypted micro-tunnels. These tunnels are on a per app, per session basis and provide seamless connectivity to any application regardless of where it's running, without ever placing users on the network. The dual tunnels are stitched together by a broker that runs in the Zscaler cloud or AWS GovCloud. If a user is unauthorized to access an app, then it remains completely dark to the user and to the Internet.

By creating a TLS encrypted segment of one between user and app, NTSB is able to fully embrace the zero trust model, without sacrificing user productivity.

> “The TIC-in-the-Cloud approach eliminates the need to manage traditional on-premises security appliances. So, agencies no longer need traditional VPNs that are difficult to maintain and compromise security, cost, and user experience.”
>
> **– Angel Santa**
> CIO at **NTSB**

Improved Collaboration and Faster Safety Recommendations

NTSB employees can now access mission-critical applications and share pertinent information faster. Logically, investigators report improved job satisfaction and reduced frustration.

"Before the implementation, it would take our investigators many hours to upload accident artifacts," adds Santa. "And, since we have regional offices as far as Alaska, we had to use a long-distance VPN over 1.5Mbps MPLS circuit, which caused issues with connectivity and slowed the workflow."

Access to agency applications and services has increased several hundred-fold, enabling NTSB's IT leadership team to understand, refine, and improve enterprise resources available to remote investigators. For example, on-line collaboration is now a viable tool.

"We can better observe and control access to enterprise applications and services, and more effectively pinpoint and address challenges," said Pham.

In addition to supporting improved efficiency within NTSB, the updated cloud capabilities support NTSB's collaboration with other Federal agencies and private industry partners that is critical to an accident investigation. The NTSB team can now share state-of-the-art research laboratory capabilities, such as the ability to retrieve vital information from all "black box" make and models, to all stakeholders/partners, remotely and in real time.

"Before implementation, a Transportation Safety Report typically took about a year to complete, but after implementation, our goal is to make such safety recommendation within 6 months," explained Santa.

Dynamic Routing for Maximum Flexibility, Agility

NTSB has started the process of moving on-premises servers hosting core applications to AWS GovCloud, with plans to move agency-specific applications, document management, and a cross-agency web application for accident management. The team plans to utilize database-as-a-service and a web application firewall as-a-service, and, importantly, will continue to connect to legacy applications and several key systems (including HR) hosted by other government agencies.

As NTSB moves into this increasingly hybrid IT environment, the agency is planning to use the ZPA solution to accelerate AWS adoption, enable dynamic best path routing for workloads across AWS regions, and to deliver a better customer experience during the transition.

"As we move into the AWS GovCloud, Zscaler gives us maximum flexibility and agility in terms of how we route traffic to the applications in the cloud, provides additional visibility into that traffic, and lets us control who is allowed access to what in that environment," says Santa. "We don't have to put every endpoint on our network, but we can give the users policy-based access across platforms through ZPA. This gives users the best possible experience and gives us the tightest security controls possible, using a Zero Trust model."

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 multi-tenant, 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.
110 Rose Orchard Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com