The role of a service mesh in Zero Trust success

The infrastructure layer is a key tool for enforcing security standards and limiting the damage an attacker can do

Zack Butcher
Tetrate

FOR LARGE COMPANIES AND GOVERNMENT agencies, it's safe to assume that a committed attacker is already inside their networks. Executive Order 14028 mandates that every federal agency develop a Zero Trust architecture because it is the most effective approach to mitigating what attackers can do once they've made their way inside.

To help agencies create action plans for mitigation, I have been working with the National Institute of Standards and Technology (NIST) to write the Special Publication 800-204 series about microservices security and 800-207A about Zero Trust. The primary goal of the latter publication is to provide a clear picture of what Zero Trust looks like at runtime. One of the key topics is identity-based segmentation, which involves conducting five policy checks for every request in the system: encrypted connection between service endpoints, service authentication, service-to-service authorization, end user authentication, and end user-to-resource authorization.

ACHIEVING A STRONG SECURITY POSTURE

Doing all five activities at runtime limits who can do what inside a network. However, it can be challenging to implement that approach for every application, and that's where a service mesh comes into play. NIST's 800-207A and the 800-204 series both talk about why a service mesh is effective for achieving a strong security posture.

Tetrate helped create and leverages the Istio service mesh, which is an infrastructure layer that intercepts all the network traffic in and out of an agency's applications and gives us the opportunity to enforce identity-based segmentation as well as other policies. We've built our flagship product Tetrate Service Bridge to operationalize the service mesh for use by some of the largest organizations in the world, including the Defense Department. For example, the U.S. Air Force has been leveraging Tetrate for several years to secure its cloud platform with FIPS-compliant encryption in transit, single sign-on for mission applications, and runtime service authentication and authorization — all without changing mission application code.

DIFFERENT VIEWS FOR DIFFERENT USERS

A service mesh has the added benefit of bringing together various stakeholders. Teams that are building mission-critical applications can use the service mesh to update their applications more rapidly and safely. The security team can incorporate security measures while the networking and platform teams can update load-balancing settings or facilitate networking between different data centers or clouds.

Tetrate Service Bridge gives different views and user interfaces for different stakeholders so they can leverage the capabilities of the service mesh for the sub-part of the problem they need to solve. As a result, they don't have to learn everything about the service mesh to ensure that they are creating and deploying secure applications. ■

Zack Butcher is a founding engineer at Tetrate and co-author of the NIST SP 800-200 series and SP 800-207A.