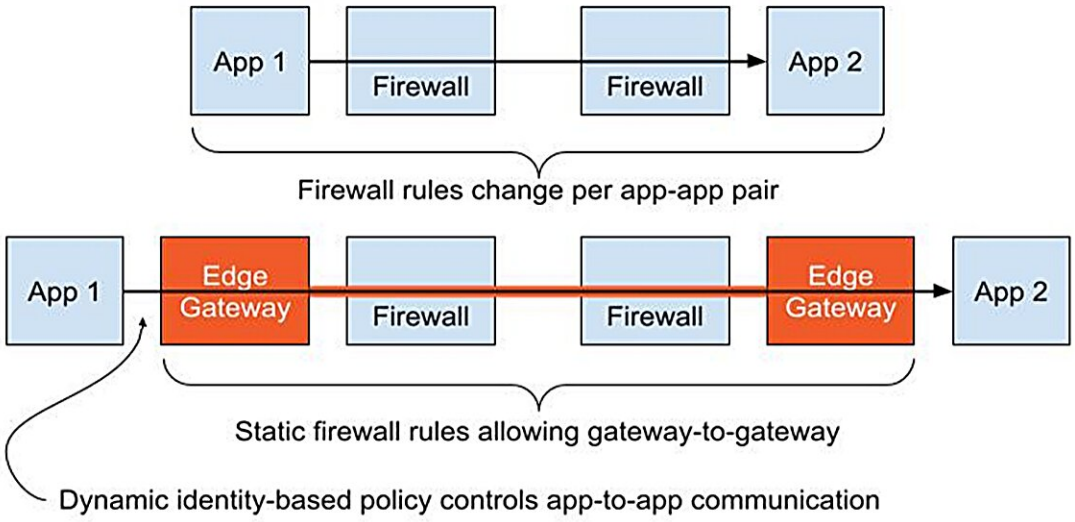
A zero-trust architecture model for access control in cloud-native applications in multi-location environments

September 14 2023



Flexibility provided by multi-tier policies. Credit: *NIST* (2023). DOI: 10.6028/NIST.SP.800-207A

NIST announces the release of Special Publication (SP) 800-207A, A Zero-trust Architecture Model for Access Control in Cloud-Native Applications in Multi-Location Environments.

Enterprise application environments consist of geographically distributed

and loosely coupled microservices that span multiple cloud and on-premises environments. They are accessed by a userbase from different locations through different devices. This scenario calls for establishing trust in all enterprise access entities, data sources, and computing services through secure communication and the validation of access policies.

Zero-trust architecture (ZTA) and the principles on which it is built have been accepted as the state of practice for obtaining necessary security assurances, often enabled by an integrated application service infrastructure, such as a service mesh. ZTA can only be realized through a comprehensive policy framework that dynamically governs the authentication and authorization of all entities through status assessments (e.g., user, service, and requested resource). This guidance recommends:

- The formulation of both network-tier and identity-tier policies
- The configuration of technology components that will enable the deployment and enforcement of different policies (e.g., gateways, infrastructure for service identities, authentication and authorization modules that enforce policies)
- A comprehensive monitoring framework that provides coverage for various tasks, such as observing the status of resources and tracking events (e.g., user access requests, changes to enterprise directories)
- The use of telemetry data to enhance security by fine-tuning access rights and enforcing step-up authentication

More information: Ramaswamy Chandramouli, A Zero Trust Architecture Model for Access Control in Cloud-Native Applications in Multi-Location Environments, *NIST* (2023). DOI: 10.6028/NIST.SP.800-207A