Access Control Engine (ACE)

Access Control Engine service referenced by each Access Proxy (Identity Aware Proxy) that provides a binary authorization decision based on the Access Control Policy, output of the Trust Inferer, the Resource Inventory Service Entity requested, and real-time credentials.

Access Control Engine is within the Access Proxy provides service-level authorization to enterprise applications on a per-request basis. The authorization decision makes assertions about the user, the groups to which the user belongs, the device certificate, and artifacts of the device from the Device Inventory Service.

If necessary, the Access Control Engine can also enforce Geolocation Access Control. The inferred Trust Tier in the Digital Identity and the device is also included in the authorization decision.

For example, access to Google’s bug tracking system can be restricted to full-time engineers using an engineering device. Access to a financial application can be restricted to fulltime and part-time employees in the financial operations group using managed non-engineering devices.

Access Control Engine can also restrict parts of an application in different ways. For example, viewing an entry in our bug tracking system might require less strict access control than updating or searching the same bug tracking system.

Source: https://ldapwiki.com/wiki/Access%20Control%20Engine