Zero Trust

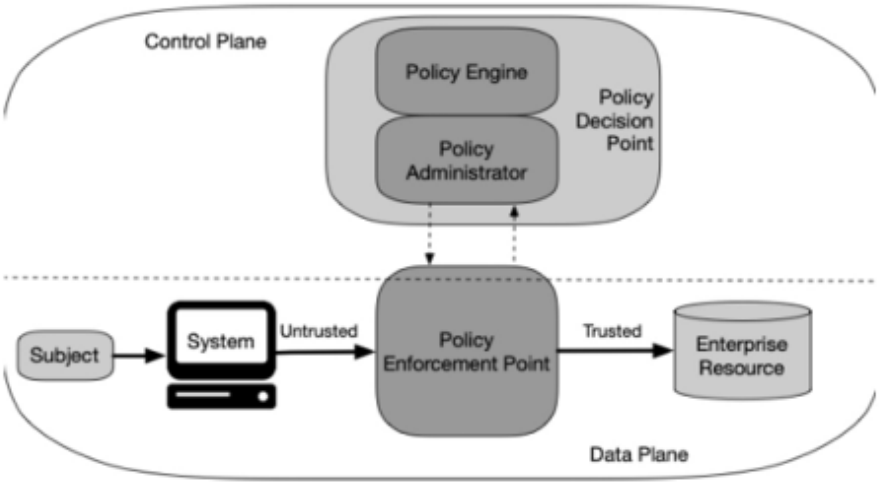
Centers on the belief that organizations should not automatically trust anything inside or outside their perimeters and instead must verify everything trying to connect to its systems before grant access

Control Plane -> Manage all actions of data plane deciding how data packets should be forwarded

- Adaptive Identity -> Based on context adjust dynamically user/system identity verification (adjusts authentication requirements based on user behavior, context, and risk factors)
- Police-driven Access Control -> Access granted based on policies
- Policy Administrator -> Responsible to establish and shut down the communication path based on Police Engine decision
- Police Engine -> Responsible for the decision to grant access to resource for a given subject
- Threat Scope Reduction -> Minimize the attack Surface

Data Plane -> What process the connection with security

- Subject -> Entity requesting access
- Implicit Trust Zone -> Place with Zero Trust
- Policy Enforcement Point (PEP) -> Enable/Disable (based on policies from Control Plane) and monitor connections between subject and resource



No Zero Trust
Connect computer to switch -> Get access to intranet

Zero Trust
Connect computer to switch -> Get log in while the minimum access -> Get access to intranet -> Logs of actions done Admin

Strict Identity Verification (identify users)
Least Privilege Access (minimum access needed, if you just need to read the info, you will not get edit permission)
Multi-Factor Authentication (MFA)
Monitor and Log All Traffic