Mapping ZTA components to SDP

The following table depicts a mapping of National Institute of Standards and Technology (NIST) ZT architecture components to the corresponding Cloud Security Alliance (CSA) Software-Defined Perimeter (SDP) architecture components. Based on these mappings, components in NIST's Zero Trust Architecture (ZTA) model are directly mapped to SDP components, further illustrating how SDP can be used to meet Zero Trust (ZT) objectives and achieve interoperability between the ZTA frameworks.

ZTA: NIST SP 800-207	SDP: CSA	Definitions
Subject/Entity	Initiating Host (IH) or Client	Subject/entity/IH/client: represents an individual or entity accessing resources. These accessing entities can be user devices or non-person entities such as hardware, network devices, software applications, and services. An SDP user may use an SDP client or browser to initiate. [1]
Policy Decision Points (PDPs) Policy Administrator (PA), & Policy Engine (PE)	SDP Controller	PDPs determine the "rules" applicable to each authenticated identity and communicates them to the PEP. The PDP is made up of a PA and a PE. The PE makes and logs the decision (as approved, or denied), and the PA executes the decision.[2] The SDP Controller is a policy definition, verification, and decision mechanism (a ZT PDP). It maintains information about which users/groups via which IHs (i.e., user devices) have permission to access which organization's resources via AHs (on-premises or in the cloud).[3]

[1]Cloud Security Alliance (2022). Software-Defined Perimeter (SDP) Specification v2
[2]NIST. (2020). Zero Trust Architecture (SP 800-207)
[3]Cloud Security Alliance (2022). SDP and DNS Enhanced Zero Trust Policy Enforcement

Policy Information Points (PIPs)	IAM, Endpoint & Data Security, Resource Protection, and Analytics	PIPs are an access control mechanism component that provides telemetry and other information generated by policy or collected by supporting components (IAM, analytics, etc.) that the PDP needs for making policy decisions.[4]
Policy Enforcement Points (PEPs)	Accepting Host (AH) or SDP Gateways	The PEP acts as a logical gateway to ensure that the correct access has been granted to the right entity, with the proper access levels to an approved resource. A PEP may be implemented in SDP-specific software or hardware. It allows or disallows network traffic to a target service (which may be an application, a lightweight service, or a resource) based on instructions from the SDP controller.[5] AHs entities are logical components that front applications, services, and resources being accessed and protected by the SDP. In some SDP deployment models, the AH function is performed by an SDP Gateway). In SDP, the AHs are the ZT PEPs that ensure the "rules" used to determine "who" can access to "what," "when," for "how long," and "for what purpose" are enforced.[6]
Resource	Resource	The applications, services, and resources being accessed.

[4]NIST. (2022). *Implementing a Zero Trust Architecture* (SP 1800-35B)
[5] Cloud Security Alliance (2022). Software-Defined Perimeter (SDP) Specification v2
[6] Cloud Security Alliance (2022). SDP and DNS Enhanced Zero Trust Policy Enforcement