

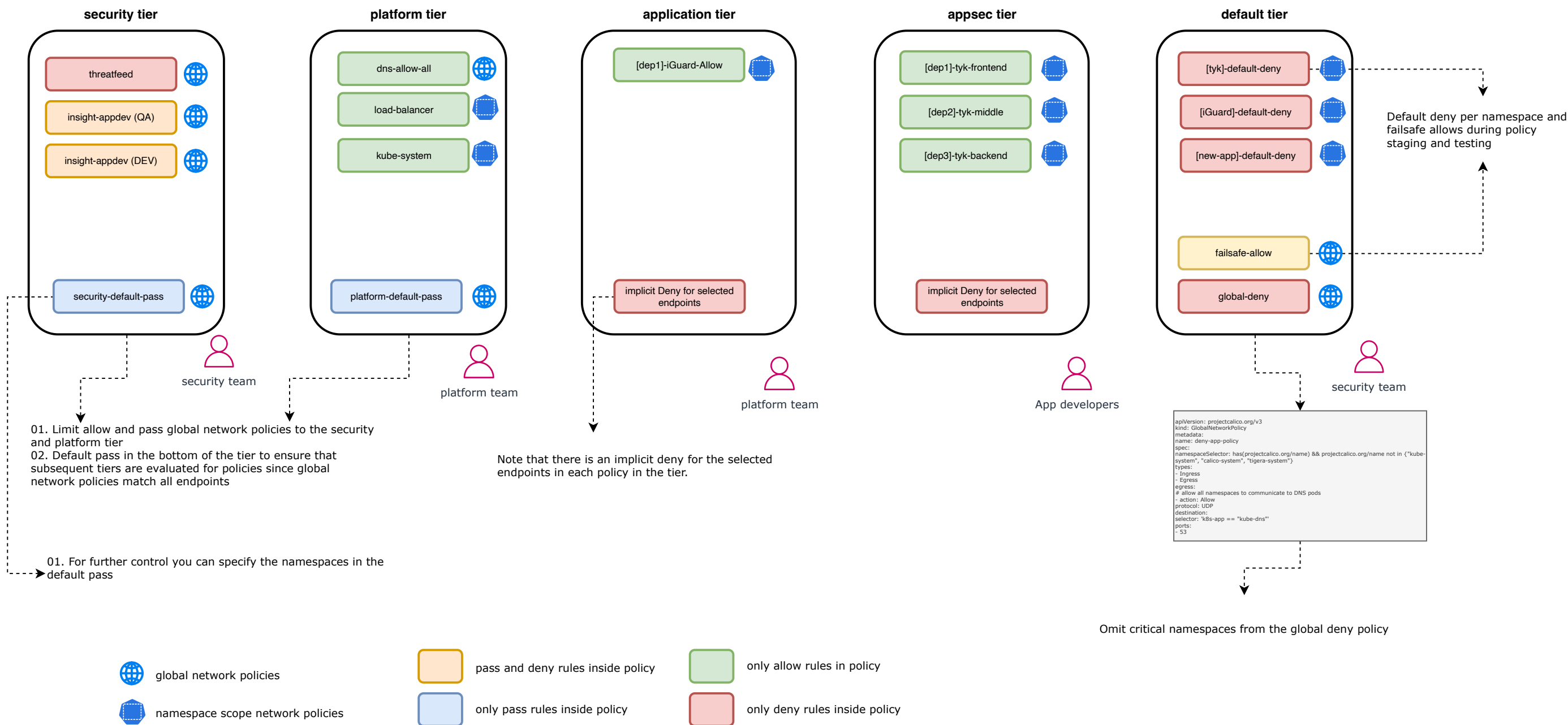
01. Blacklist policies using source and destination globalnetworksets
 02. Blacklist ports - 20:21, 23, 25, 69, 111
 04. External access whitelist/blacklist per tenant/application/environment
 03. Compliance controls - Pass policies per environment/application/tenant

01. DNS-ALLOW-ALL
 02. Access to private repo based on DNS policies and ports
 03. Access to external tools based on globalnetworksets (logging, datalake)
 04. Access for cluster tools (monitoring, logging, security etc.)
 05. Access to Git repo/GitOps tools using DNS policies
 06. Policies for ingress controller
 07. Access to API Service

01. Policies to permit traffic within applications/namespaces if required

01. Granular/Micro-segmentation policies per deployment

01. Global default deny
 02. Default deny per namespace
 03. Failsafe policies



HOOPP - Calico Cloud Security Policy Framework

Prepared by: Aadhil A. Majeed (Tigera) - Solutions Architect - Customer Success
 Date - 08/26/2022