Cilium Scale with netpol

Current Cilium Scale

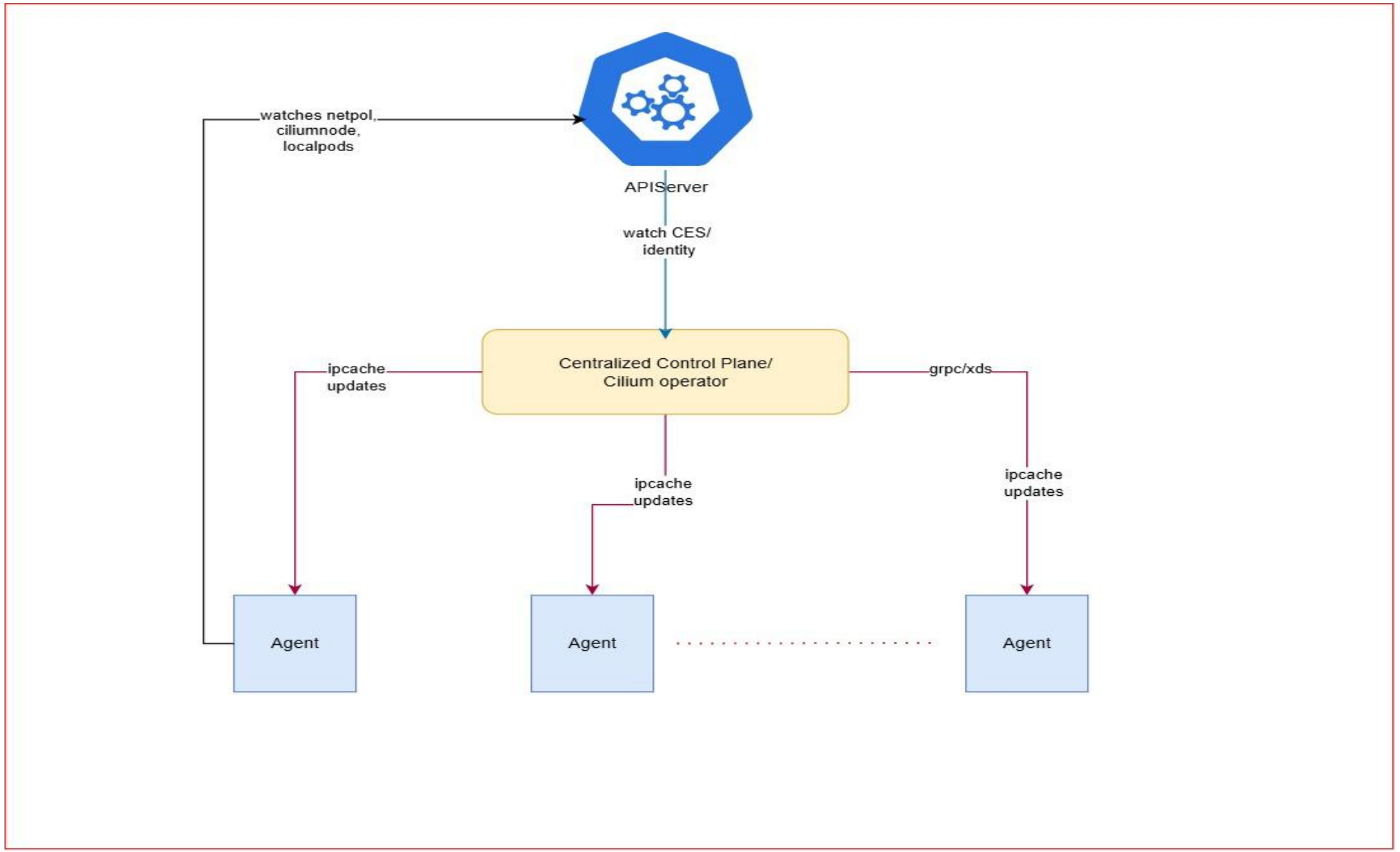
- Cilium with network policy disabled
  - No Cilium endpoints, cilium identity
  - No watchers on cilium specific resources
  - Supports pod->pod routing, service routing with ebpf
  - Basic observability without enriching data
  - Scales better (15k with 32 core apiserver)

- What about cilium scale with netpol?
  - Cannot scale as like cilium with netpol disabled
  - Main bottleneck - Cilium watch on all other CEPs
  - Puts load on apiserver which affects apiserver perf

Centralized Control Plane(CCP)

- CCP does apiserver watch on CES/Ciliumidentity
- Computes ipcahe and send updates to all cilium agents via xds/grpc
- All agents maintain long running connections with this CCP
- Reduce watch updates on apiserver
- CCP can be part of cilium operator or standalone entity

Centralized control plane



North Star

- Move policy computation to CCP
- Make cilium agent light weight. All resource heavy computation can happen on CCP. Saves resource usage on worker nodes
- Policy map can be constructed per identity instead of per endpoint