cilium eBPF Packet Flow

ver1, 4-Jan-2025

Source Pod: pod-a (Namespace: tenant1, EndpointId: 676, Identity: 49503, VNI: 1001)
Destination Pod: pod-b (Namespace: tenant2, EnpointId: 2271, Security Identity: 59510, VNI: 1002).

namspace: tenant-1 namspace: tenant-2 Pod-A Pod-B EndpointId: 676 EndpointId: 2271 Security Identity: Security Identity: 49503 59510 Labels: Labels: -k8s: tenant-1 -k8s: tenant-2 -k8s: namespace=tenant1 -k8s: namespace=tenant2 eBPF XDP/TC Programs attached to Pod Interface Pod Network Interface eBPF Program Stages 1.Ingress/Egress eBPF Program Stages Identification 1. Intercepts packet entering - Intercepts packet leaving Pod-B Pod-A - Ingress/Egress 2.Meta-data Extraction Identification - Source/Destination IP - Ports/Protocols 2. Filters packets based on 3. Identity Association Cilium data plane - Maps packets to - If packet matches allowed source/destination ingress policy, if not, Endpoint ID dropped (src:49503 dst:59150) 4. Forwarding Decision - Send to Cilium agent or Drop Cilium Data Plane

1.Packet Processing - Sender Security Identity: 49503 (tenant-1) - Receive Security Identity 59510 (tenant-2) 2.Policy Lookup - Check CiliumNetworkPolicy based on: - Sender Label:

- Sender Label:
 k8s:tenant=tenant-1
 k8s:tenant=tenant-2
- 3. Policy Decision
- Allow/Deny packet based on

- 1.Recevice Decapsulated packet from VTEP
- 2.Extract Meta Data (5-tuple)
 - Src/Dst (IP,Port), Protocol
 - srcIP -> Endpoint Id (676)
 - dstIP -> Endpoint Id (2271)
- 3.Lookup Cilium Cache
 - src Endpoint Id (676) ->
 src security Identity: 49503
 Labels: (hash)
 - k8s:tenant=tenant-1=Pod-A
 - dst Endpoint Id (2271) ->
 dst security Identity: 59510
 Labels: (hash)

