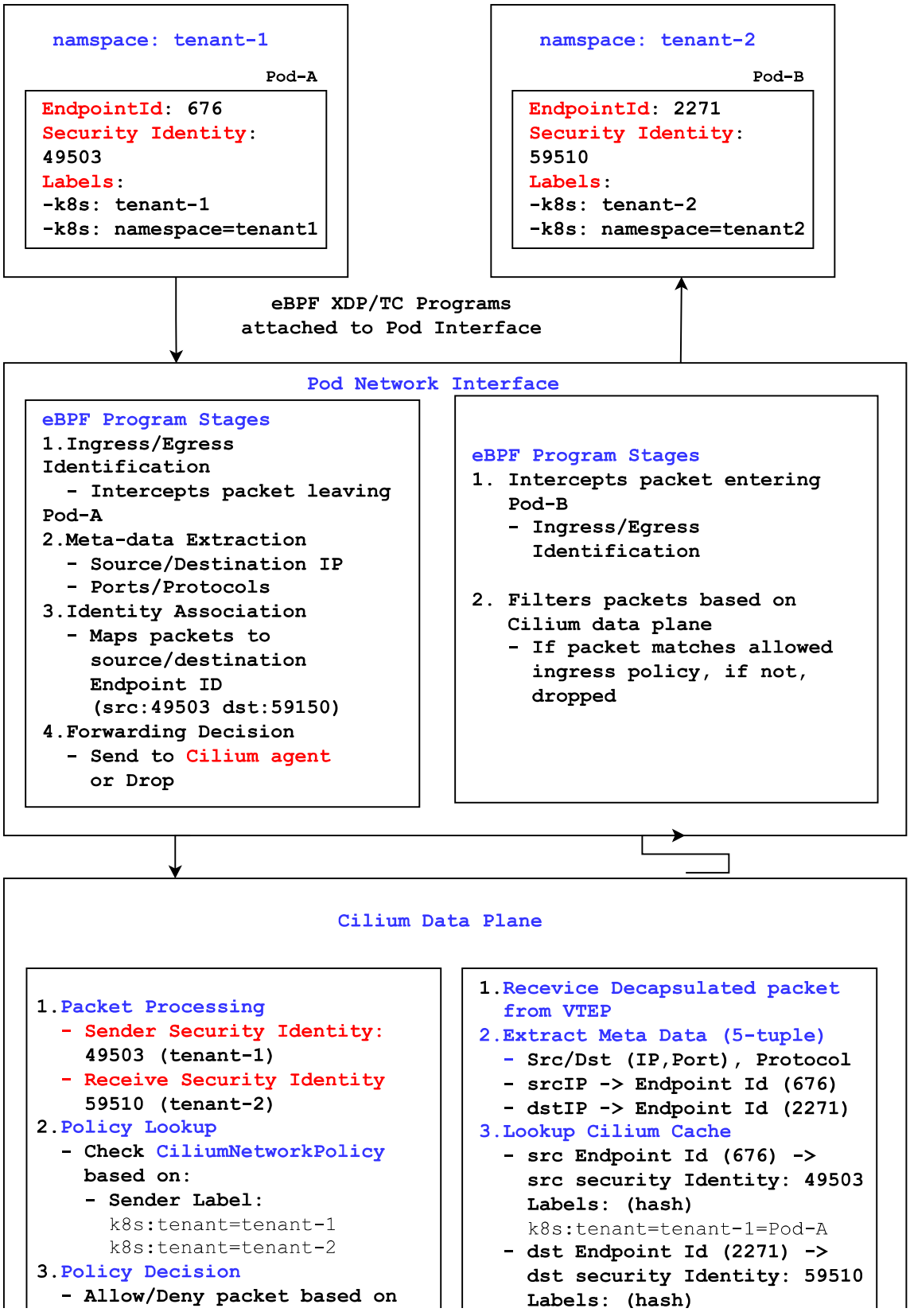
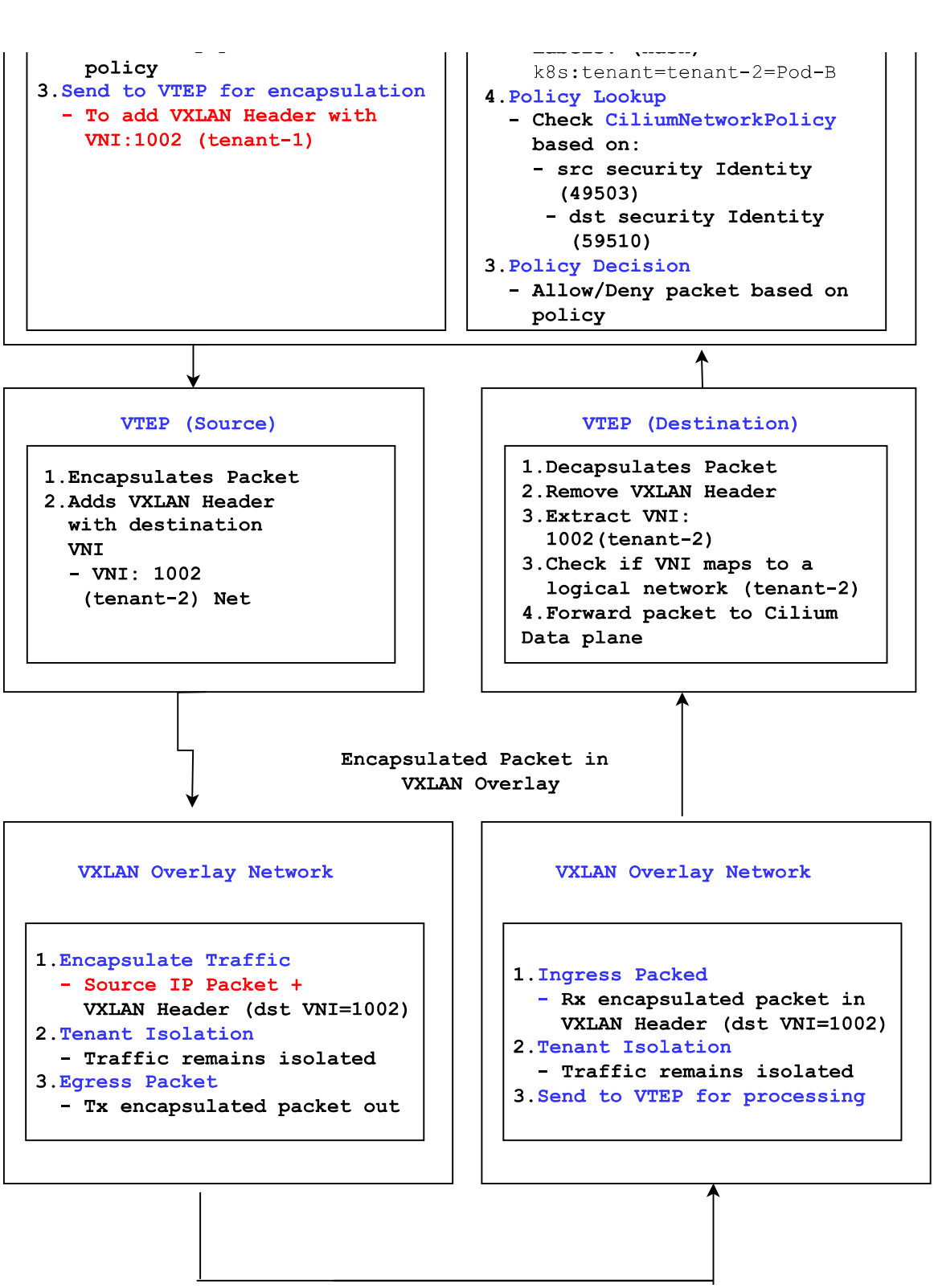
cilium eBPF Packet Flow

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).




policy
3.Send to VTEP for encapsulation
- To add VXLAN Header with VNI:1002 (tenant-1)
k8s:tenant=tenant-2=Pod-B
4.Policy Lookup
- Check CiliumNetworkPolicy based on:
- src security Identity (49503)
- dst security Identity (59510)
3.Policy Decision
- Allow/Deny packet based on policy
VTEP (Source)
1.Encapsulates Packet
2.Adds VXLAN Header with destination VNI
- VNI: 1002 (tenant-2) Net
VTEP (Destination)
1.Decapsulates Packet
2.Remove VXLAN Header
3.Extract VNI: 1002(tenant-2)
3.Check if VNI maps to a logical network (tenant-2)
4.Forward packet to Cilium Data plane
Encapsulated Packet in VXLAN Overlay
VXLAN Overlay Network
1.Encapsulate Traffic
- Source IP Packet + VXLAN Header (dst VNI=1002)
2.Tenant Isolation
- Traffic remains isolated
3.Egress Packet
- Tx encapsulated packet out
VXLAN Overlay Network
1.Ingress Packed
- Rx encapsulated packet in VXLAN Header (dst VNI=1002)
2.Tenant Isolation
- Traffic remains isolated
3.Send to VTEP for processing