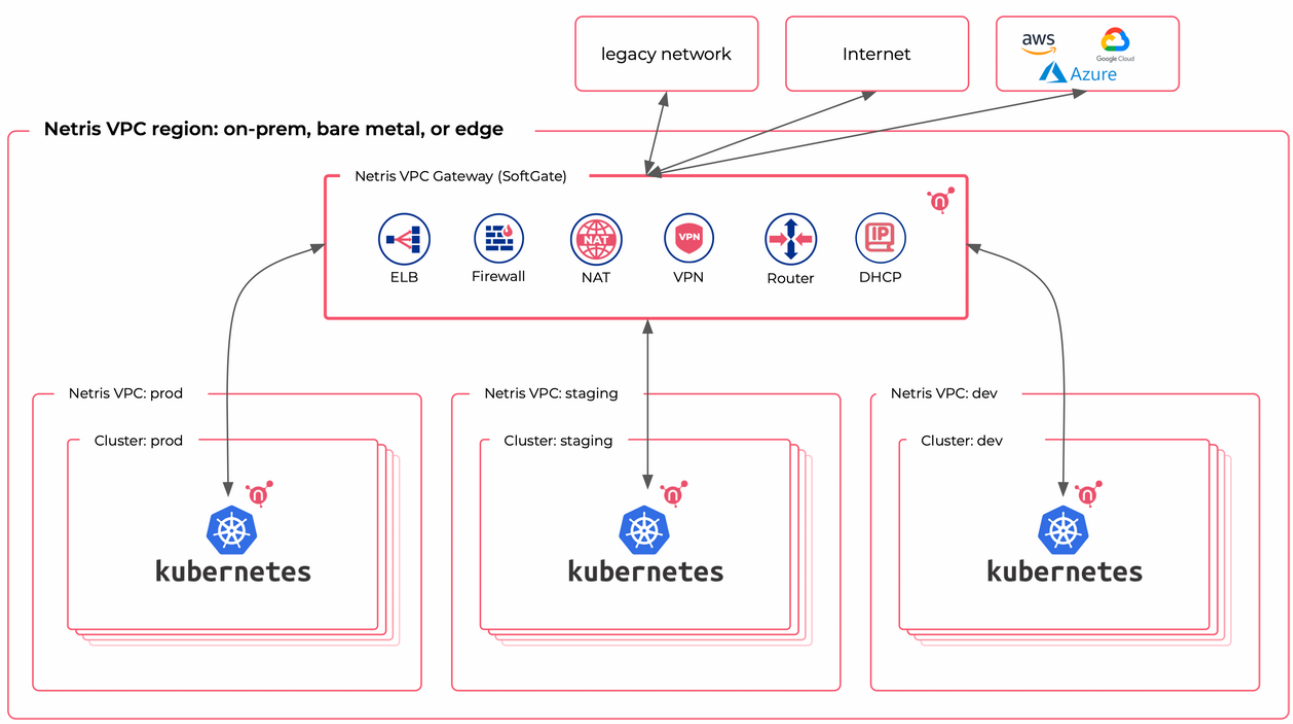
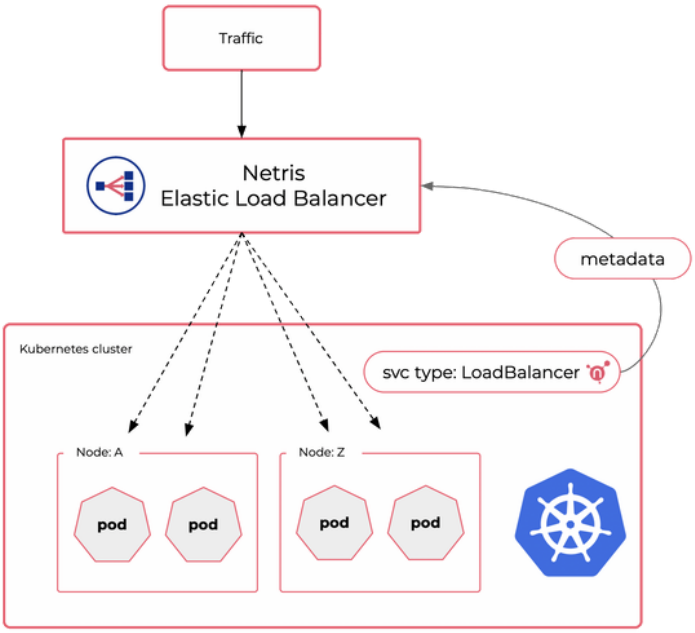
# VPC Networking for Kubernetes Clusters Beyond the Public Cloud




Netris software brings cloud-like VPC networking abstractions and APIs everywhere to help you apply your favorite cloud-native workflows and methodologies beyond the public cloud.

- On-premises & colocation
- Bare Metal Cloud
- Edge

# Load Balancer



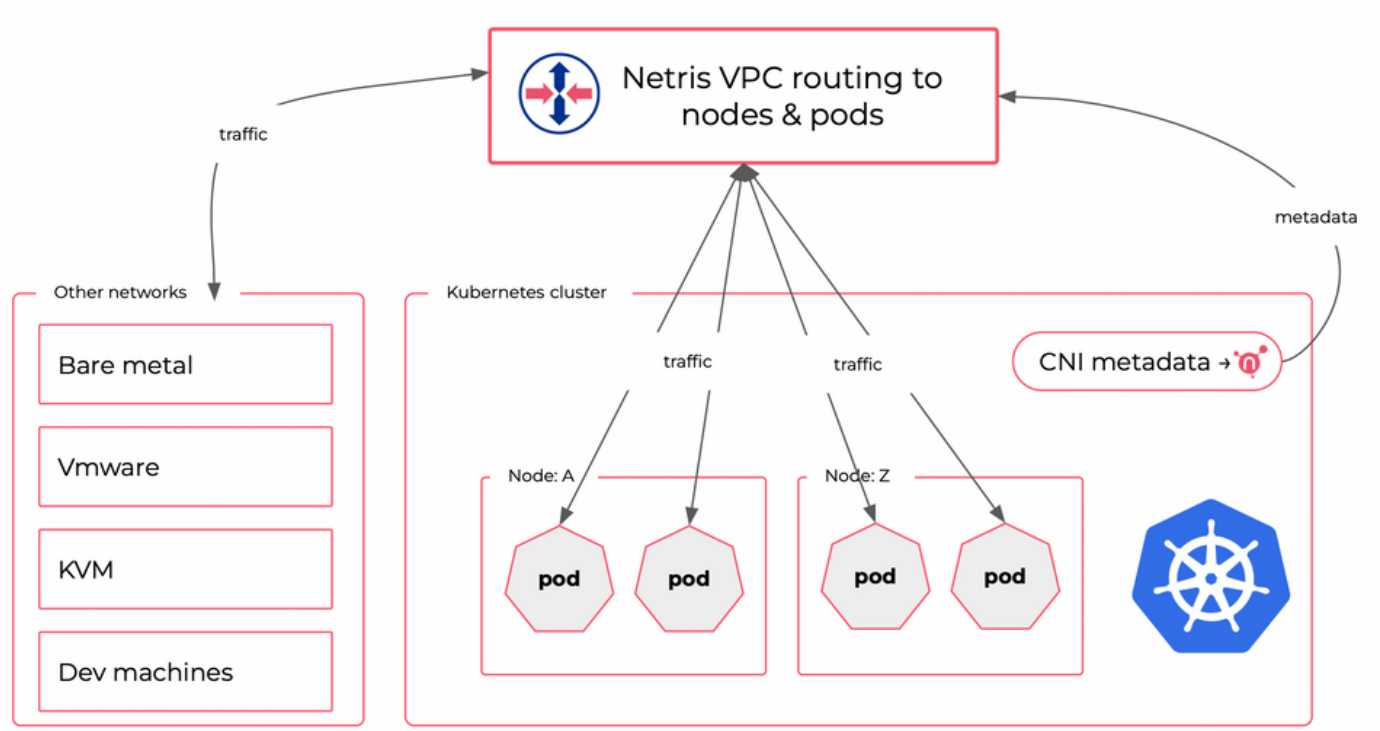

Kubernetes implementation of network load balancers (Services of type LoadBalancer) relies on cloud environment provided elastic load balancer service. Kubernetes requires an external load balancer to route service traffic into the cluster. In the public cloud (GCP, AWS, Azure, ...), such load balancer functionality is available by default. But when running a Kubernetes cluster beyond the public cloud, your LoadBalancers will remain in the "pending" state indefinitely when created.

Kubernetes users on-prem, colo, or bare metal are left with a handful of options that do the work but usually are not a fit for a mission-critical production.

Netris VPC provides a production-grade cloud-like load balancer for your on-prem, bare metal, and edge Kubernetes clusters.

| | Netris LB | Metallb | kube-vip | NodePort |
|---|---|---|---|---|
| Routing Service Traffic into cluster | Yes | Yes | Yes | Yes |
| Virtual IP for HA | Yes | Yes | Yes | No |
| Load-Balancing (L3) | Yes | Yes (requires BGP routers & extra configs) | Yes (requires BGP routers & extra configs) | No |
| Load-Balancing (L4) | Yes | No | No | No |
| TCP probes | Yes | No | No | No |
| HTTP probes | Yes | No | No | No |
| DPDK accerleration | Yes | No | No | No |
| Free Version | Yes | Yes | Yes | Yes |
| Enterprise support | Yes | No | No | No |

# Routing to Nodes and Pods

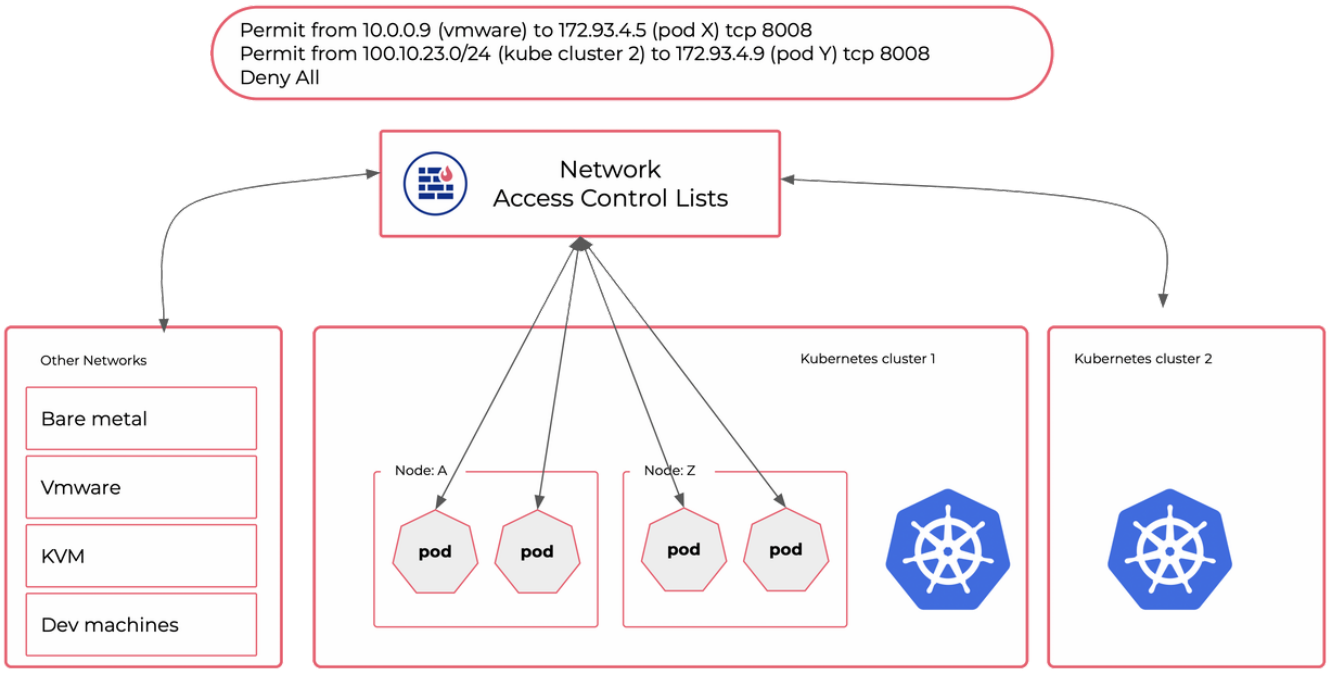



Kubernetes nodes usually sit in a single flat network; however, that's only a tiny part of Kubernetes networking. Kubernetes runs a separate network inside the cluster that connects pods to pods and services. Kubernetes internal networking is managed through CNI (Container Network Interface) plugins. Kubernetes internal CNI network is typically significant to the single cluster and is not accessible from other networks. You access your services using constructs like LoadBalancer or NodePort.

Sometimes for development, troubleshooting, or security reasons, you need to have means for accessing some pods (containers) directly. It is not a trivial task to organize network routing between your other networks (from Vmware, bare metal, KVM, and dev machines) due to Kubernetes CNI network architecture that is isolated by Kubernetes design.

Netris VPC has the functionality to leverage standard CNI plugin metadata to seamlessly enable routing with pods and get you access to containers from your other networks, as you need.

# Network Access Control & Tenancy

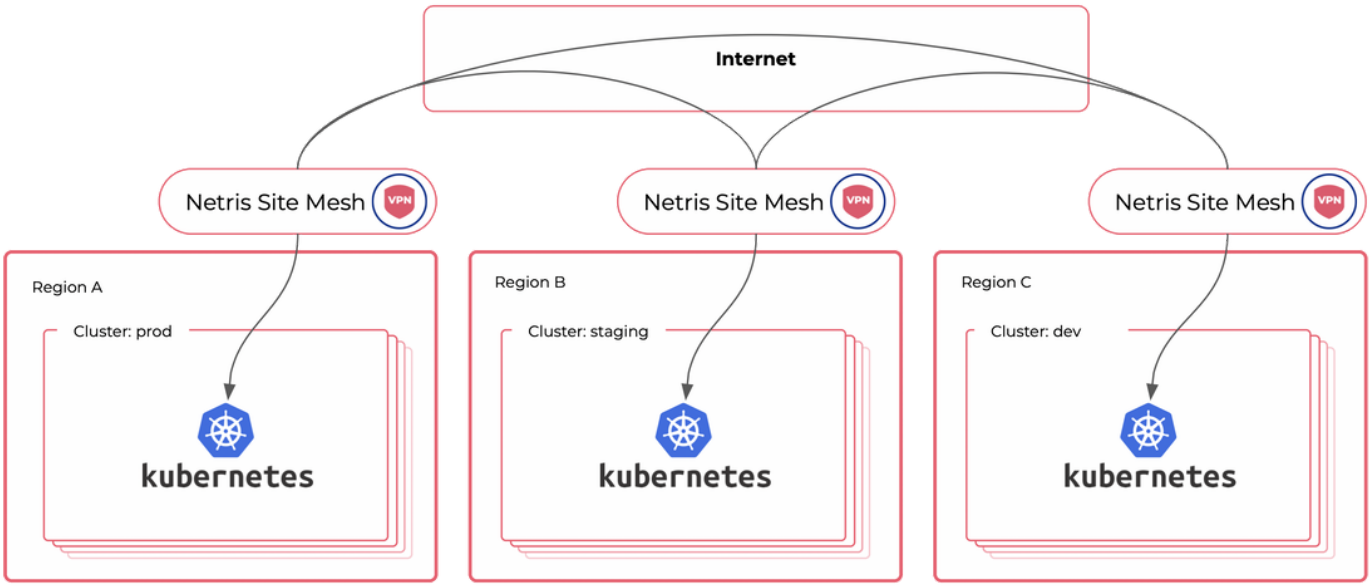



Kubernetes provides NetworkPolicies, a construct designed to control traffic flows between pods, namespaces, and IP blocks. There are various products for adding more granular traffic control in addition to Kubernetes NetworkPolicies. These methods are great for controlling traffic flows inside the cluster.
However, there are cases when you need an additional layer of Network Access Control. Especially when you need to:

- Enforce traffic policies before packets hit your Kubernetes cluster.
- Control traffic flows between multiple Kubernetes clusters.
- Control traffic flows between the Kubernetes cluster and your other networks such as VMs, bare metal, dev machines, Internet, or remote regions.
- Set your Elastic Load Balancer to bind specific IP pools to a particular Kubernetes cluster for further network access control.
- Comply with various security standards that require a Network Access Control as an additional security layer.

Netris VPC provides Tenant and ACL (Access Control Lists) constructs to help you match your security requirements. The basic use of network ACLs is to permit/deny various network traffic flows between various VPCs (V-Nets). Additionally, various VPCs inside Netris can be associated with different Tenants (can be a team, a project, or a Kubernetes cluster). Then you can use Tenant-aware ACLs with our built-in intra-Tenant ACL request & approval workflows. Or you can configure Elastic Load balancer to bind to distributing public IP addresses from designated pools to proper Kubernetes clusters.

# Site Mesh




How to network applications hosted in multiple regions? Many multi-region applications can communicate over the Internet. In this case, traffic enters the remote Kubernetes cluster through a service of a type LoadBalancer or an Ingress. But some types of data, due to architectural or security requirements, are not suitable for shuttling through the Internet without traffic encryption. There are many ways to encrypt traffic. Wireguard is a fantastic product that provides secure and highly performant traffic encryption.

Netris VPC provides this functionality that we call Site Mesh. When you enable Site Mesh, Netris automatically creates a full mesh of Wireguard tunnels between your regions and automatically makes the network routing work. Like zero code site-to-site VPN. With Netris Site Mesh, your VPCs spread across multiple regions are getting accessibility between each other using The Internet as a transport for encrypted traffic. With Site Mesh, you can control multi-region traffic flows as if they were located in the same region.