EKS Architecture For Runtime Fabric Manager

AWS

VPC

AZ-1

NAT Gateway

Public Subnet

Public Subnet Route Table

Destination	Target
VPC CIDR	Local
0.0.0.0/0	igw

Firewall Endpoints

Firewall Subnet

Firewall Subnet Route Table

Destination	Target
VPC CIDR	Local
0.0.0.0/0	NAT Gateway

EKS Node

Private Subnet

Private Subnet Route Table

Destination	Target
VPC CIDR	local
0.0.0.0/0	firewall-az-1

AZ-2

NAT Gateway

Public Subnet

Public Subnet Route Table

Destination	Target
VPC CIDR	local
0.0.0.0/0	Igw

Firewall Endpoints

Firewall Subnet

Firewall Subnet Route Table

Destination	Target
VPC CIDR	local
0.0.0.0/0	NAT Gateway

EKS Node

Private Subnet

Private Subnet Route Table

Destination	Target
VPC CIDR	local
0.0.0.0/0	firewall-az-2

AZ-3

NAT Gateway

Public Subnet

Public Subnet Route Table

Destination	Target
VPC CIDR	Local
0.0.0.0/0	igw

Firewall Endpoints

Firewall Subnet

Firewall Subnet Route Table

Destination	Target
VPC CIDR	local
0.0.0.0/0	NAT Gateway

EKS Node

Private Subnet

Private Subnet Route Table

Destination	Target
VPC CIDR	local
0.0.0.0/0	firewall-az-3

EKS Managed ENI

Internet Gateway

VPC

AWS Managed VPC

AWS EKS Control Plane

Kubectl

Ingress Managed Load Balancer

Client

- Private, Public and Firewall Subnet spin up across multiple AZ for High Availability.
- Separate Route Tables for Private, Public and Firewall Subnet.
- Outbound Traffic from Private Subnet will be route through Firewall Subnet and ensure outbound traffic to destination is allowed.
- Client can connect to application via Ingress Load Balancer.

Request from Private Subnet

Firewall Subnet Validate whether traffic is allowed or not

Traffic routed to NAT Gateway in Public Subnet

Traffic routed outside via Internet Gateway

Response from outside comes to IG and routed to NAT in Public Subnet

Response will send to Firewall Subnet for filtering and validation

Response will send to Private Subnet