Inter-VPC Connectivity

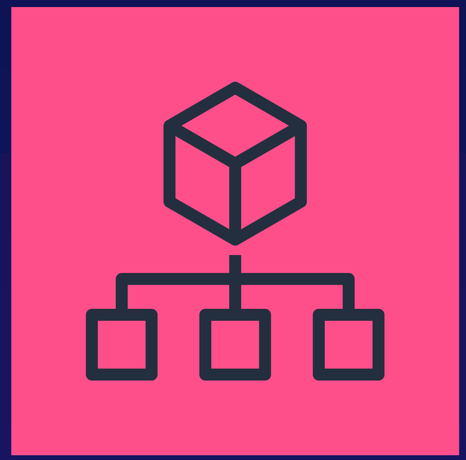
Steven Moran

TECHNICAL INSTRUCTOR

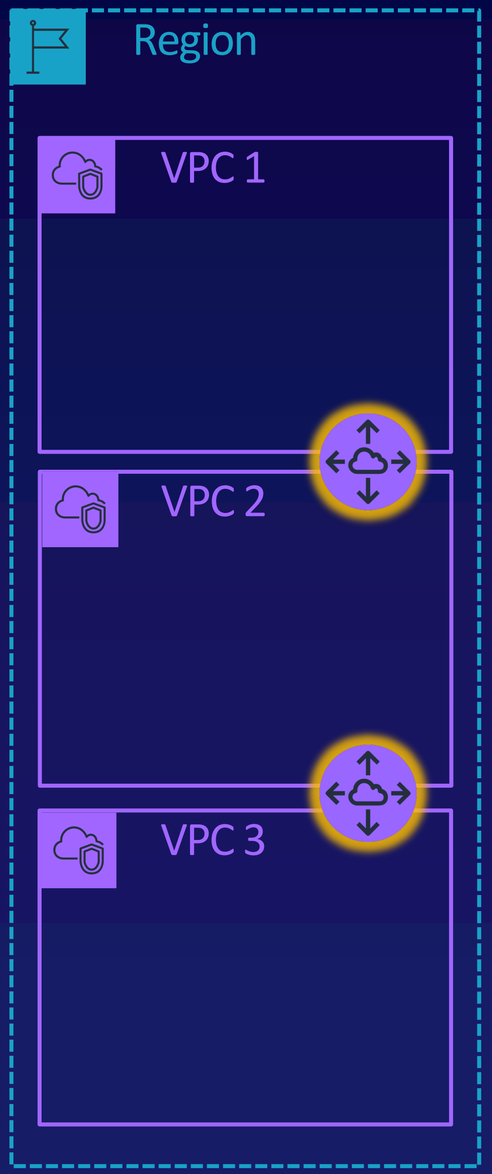
VPC Sharing

VPC sharing allows a subnet in one AWS account to be shared with other AWS accounts.

- Accounts must be part of the same AWS Organization.
- Subnets are shared via AWS Resource Access Manager.
- Once shared, other accounts may provision resources within that subnet as if it were native to their account.
- Only the owner account has management control over that subnet.

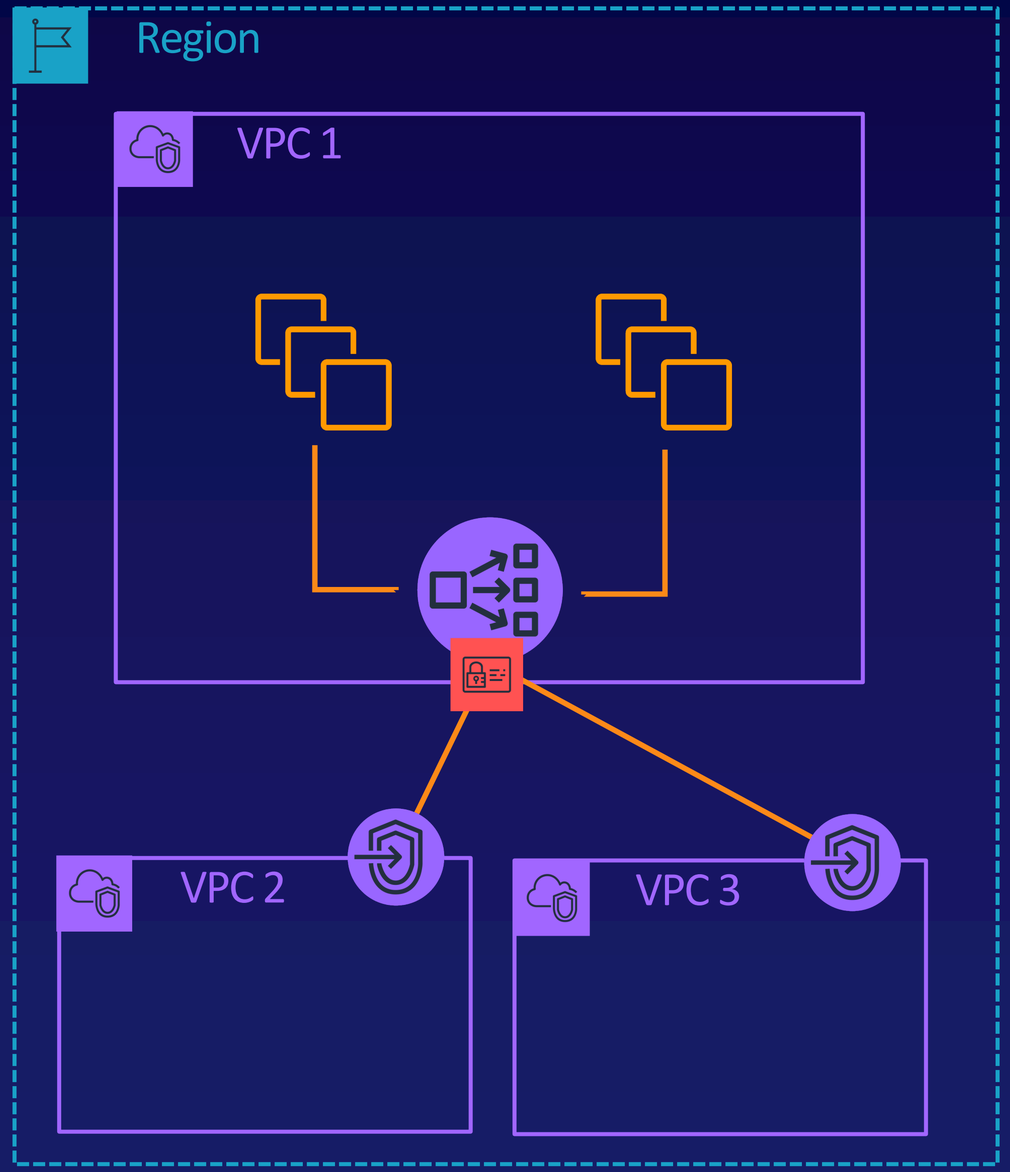


VPC Peering



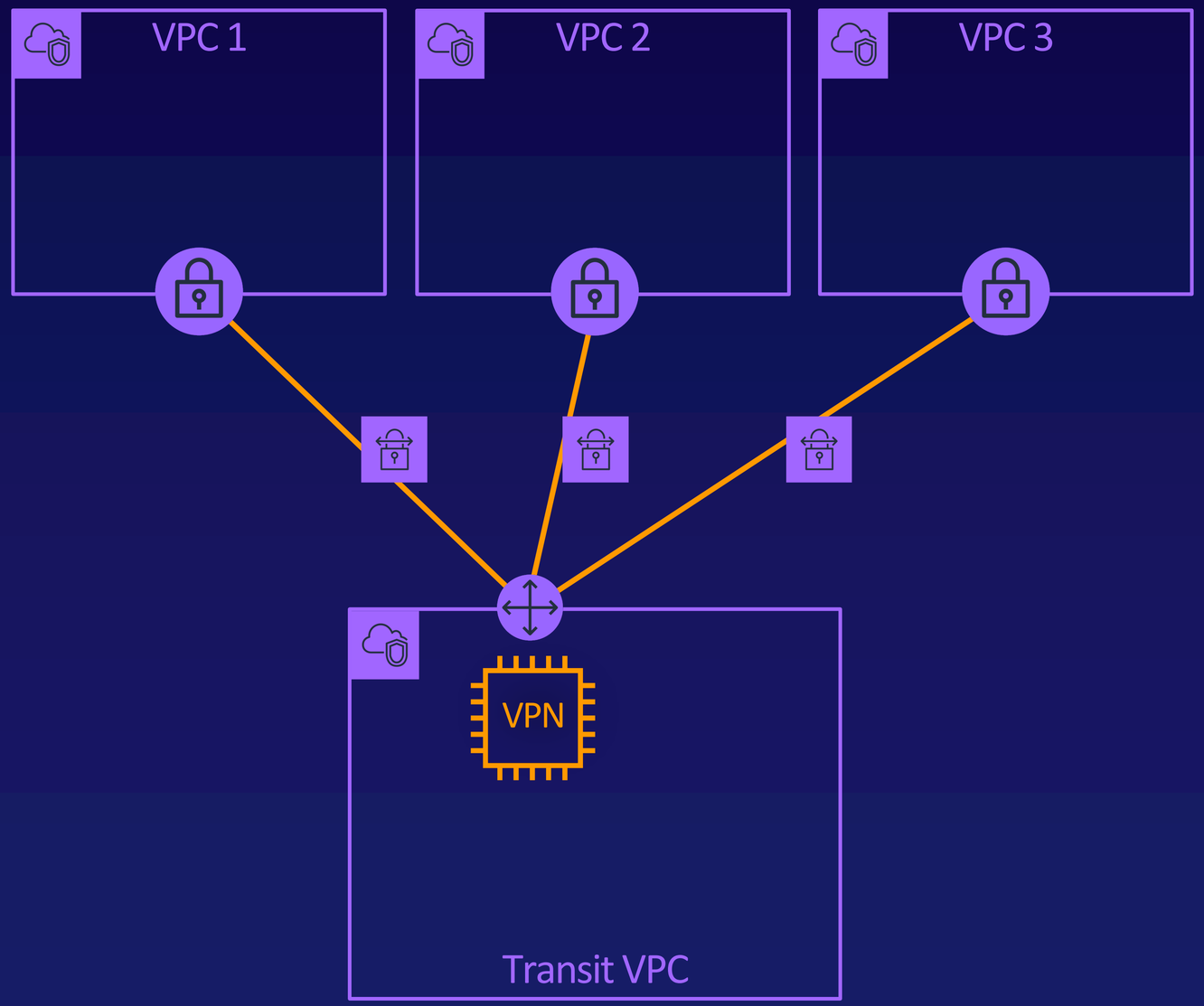
- VPC peering connections do not allow transitive connectivity.
- VPC Peering is not restricted by AWS account or region.
- Data transfer charges apply to inter-VPC traffic
- Minimum required configuration allows broad inter-VPC connectivity

VPC Endpoint Services



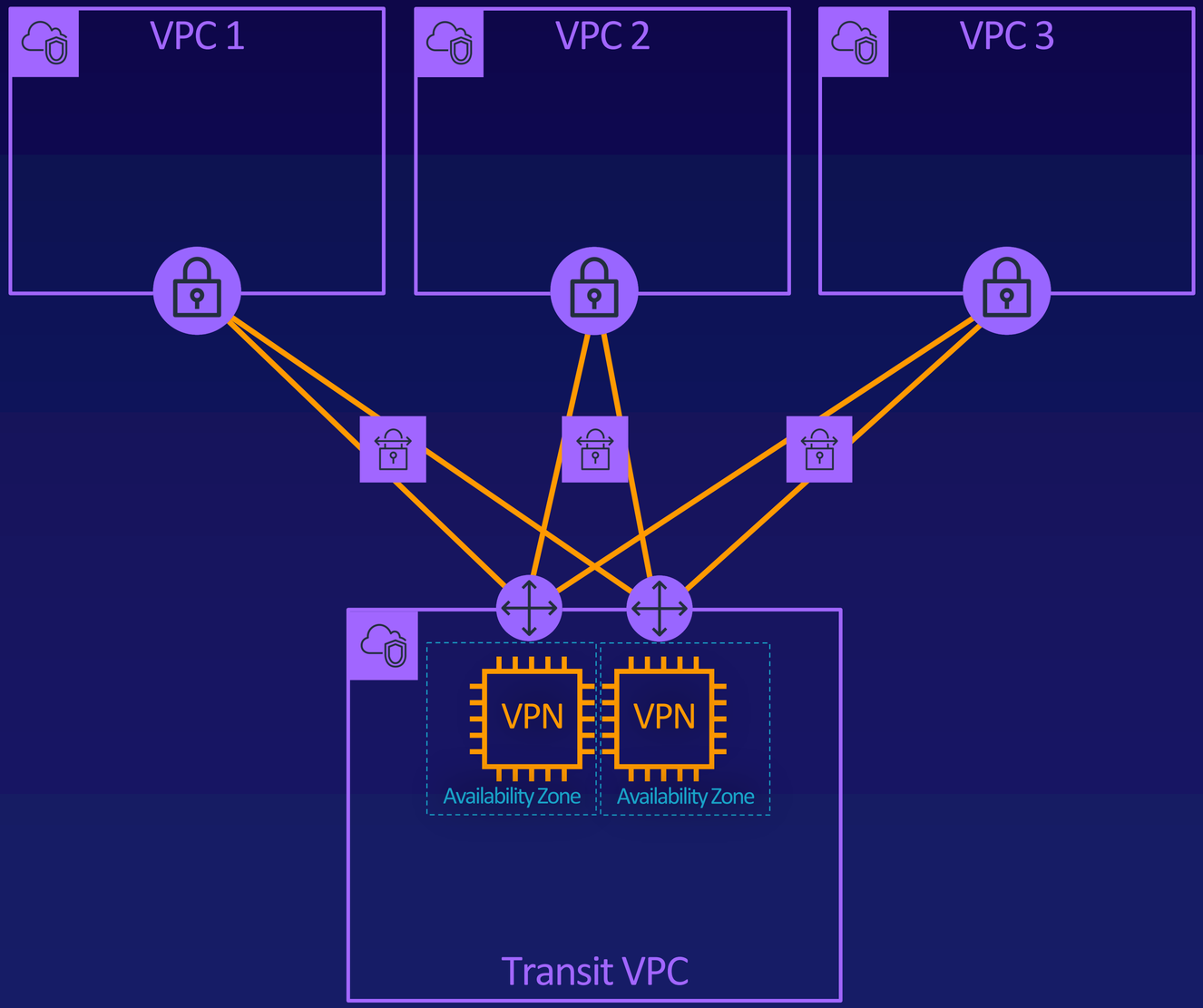
- Exposes an NLB-fronted application to selected consumers in the same region.
- Consumers connect to application by creating a VPC Interface Endpoint.
- Access can be restricted by AWS account, IAM user, or IAM role.

Transit VPCs



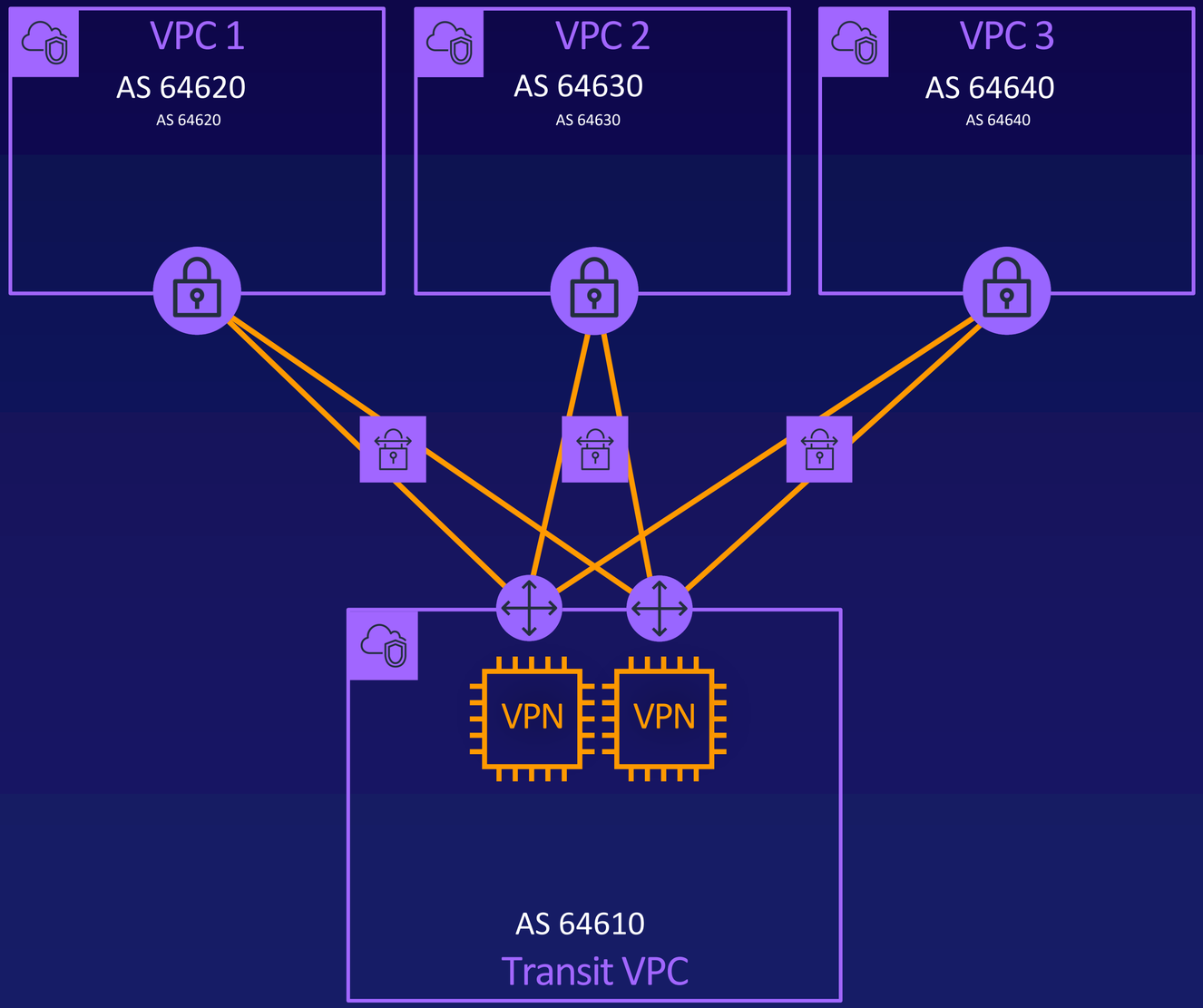
- Transit VPCs contain an EC2-hosted VPN solution.
- EC2 VPN solution is the customer gateway for AWS VPN connections to spoke VPCs.
- VPN connections over the internet allow VPCs to be in any AWS account in any region

Transit VPCs



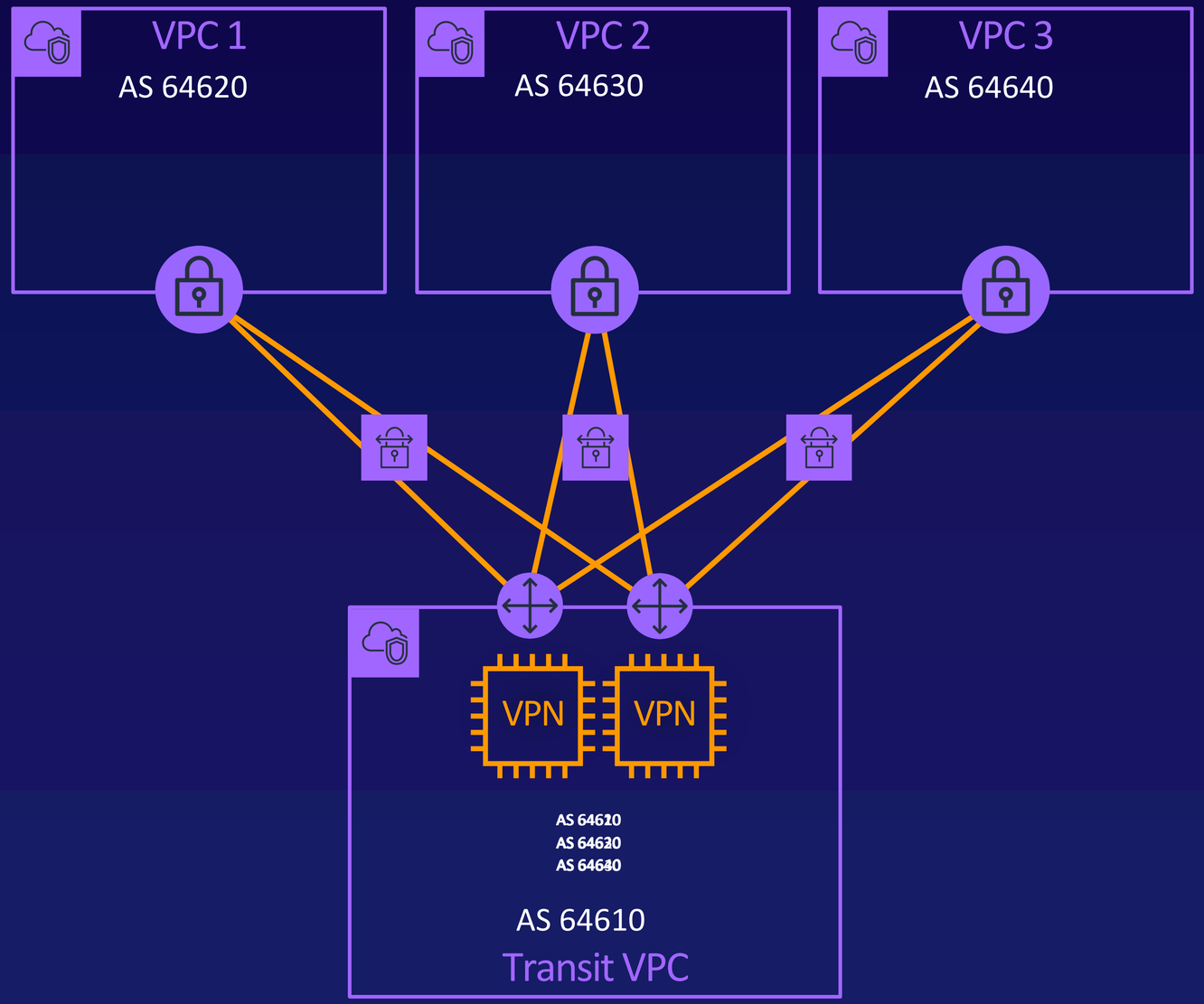
- Additional EC2 VPN systems should be implemented for high availability.

Transit VPC Routing



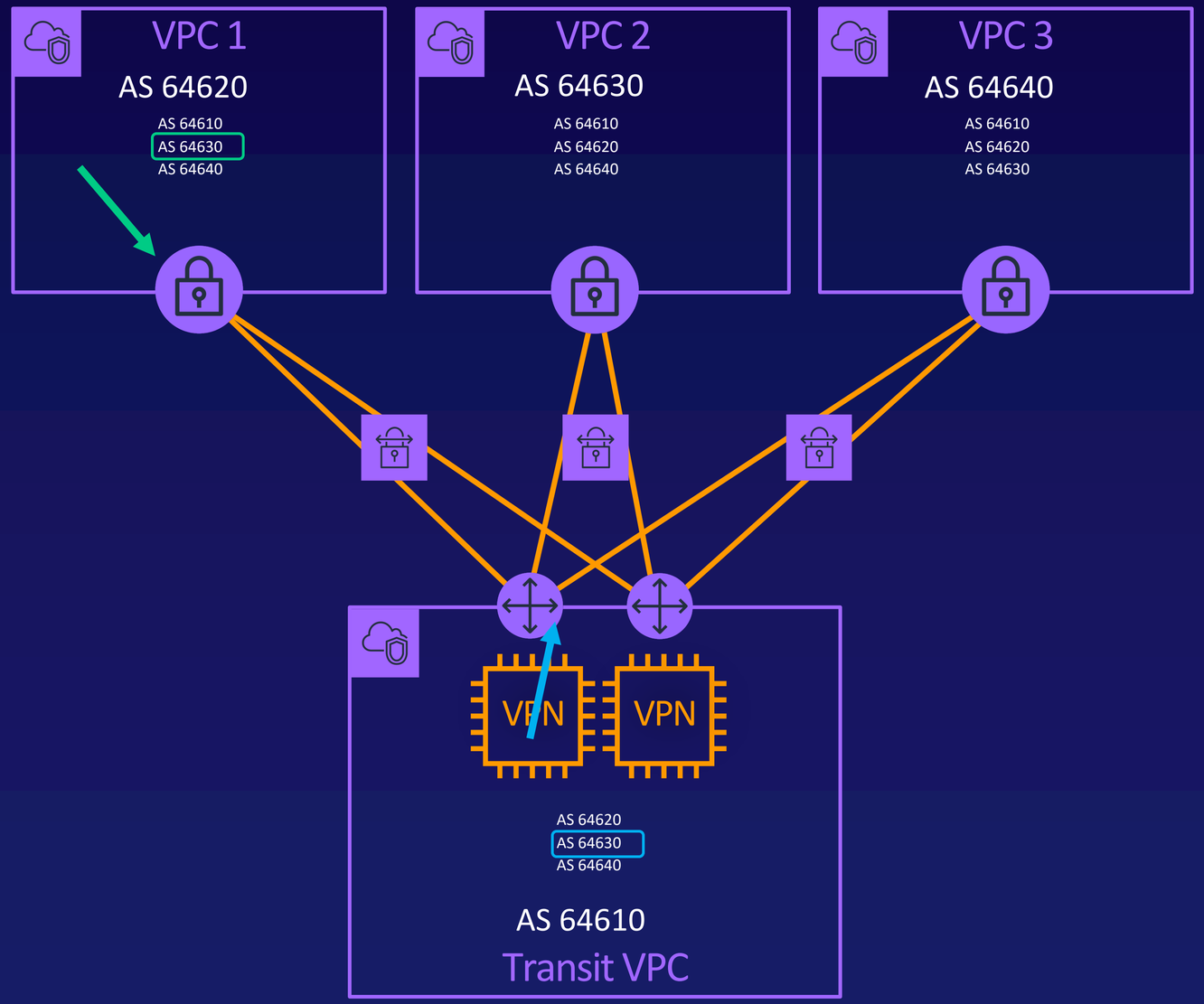
- Dynamic routing is strongly recommended but is not a requirement.
- Spoke VPC VGWs advertise their local CIDR prefix to transit VPC VPN systems.

Transit VPC Routing



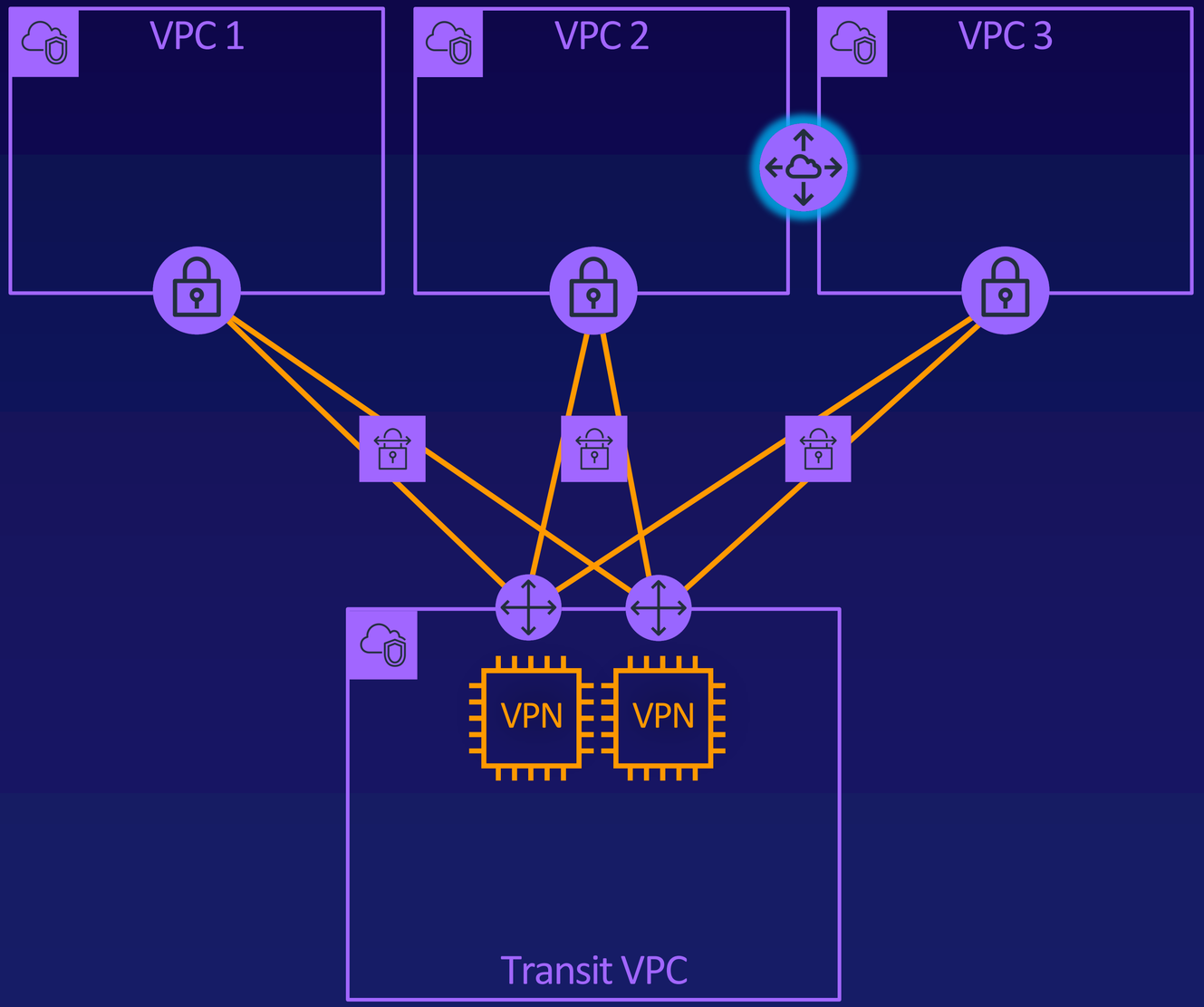
- Dynamic routing is strongly recommended but is not a requirement.
- Spoke VPC VGWs advertise their local CIDR prefix to transit VPC VPN systems.
- VPN systems advertise all prefixes back to spoke VPCs.

Transit VPC Routing



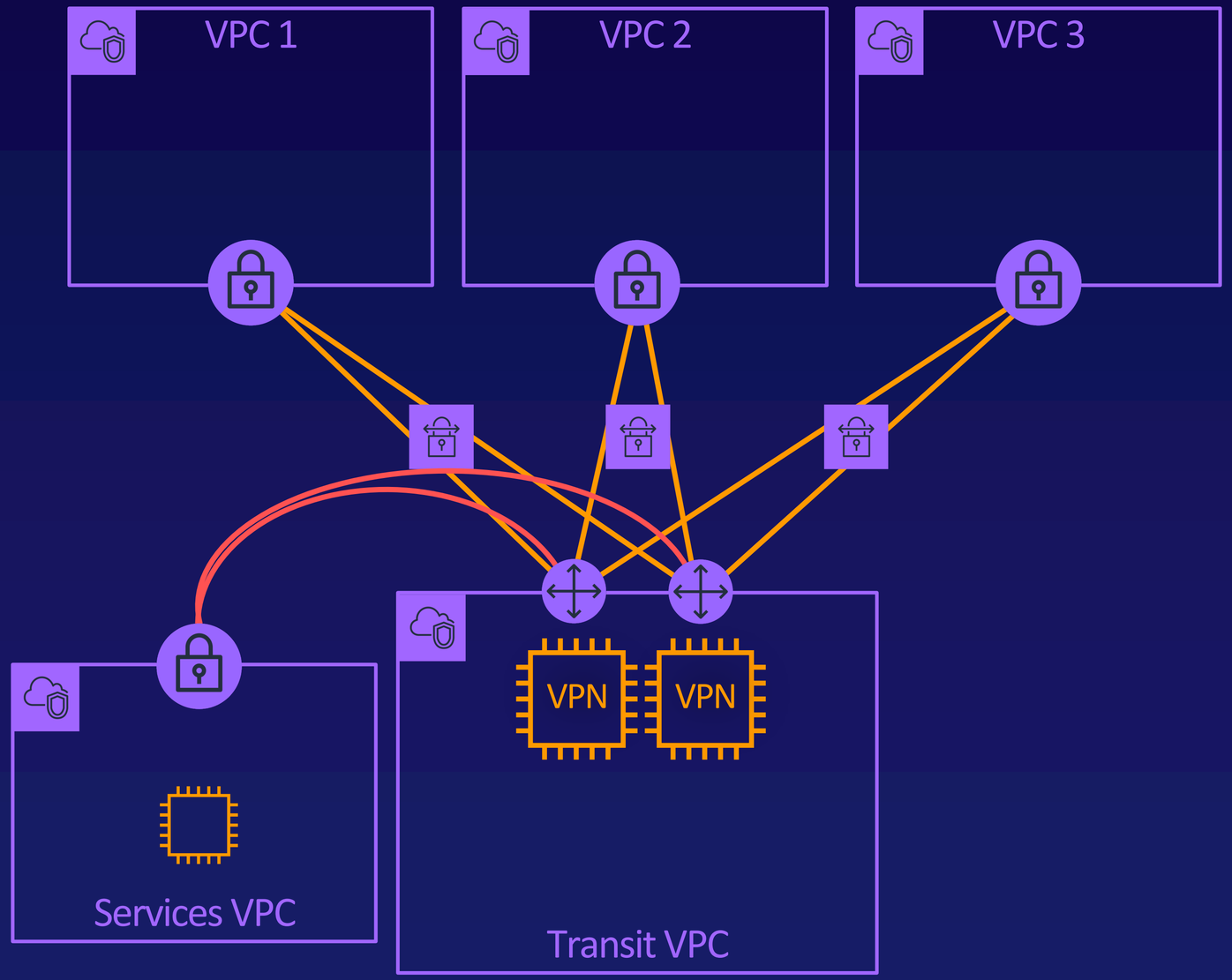
- Dynamic routing is strongly recommended but is not a requirement.
- Spoke VPC VGWs advertise their local CIDR prefix to transit VPC VPN systems.
- VPN systems advertise all prefixes back to spoke VPCs.
- Spoke VPC VGWs route traffic to other spoke VPCs via the transit VPC's VPN systems.

Patterns – Trusted VPCs



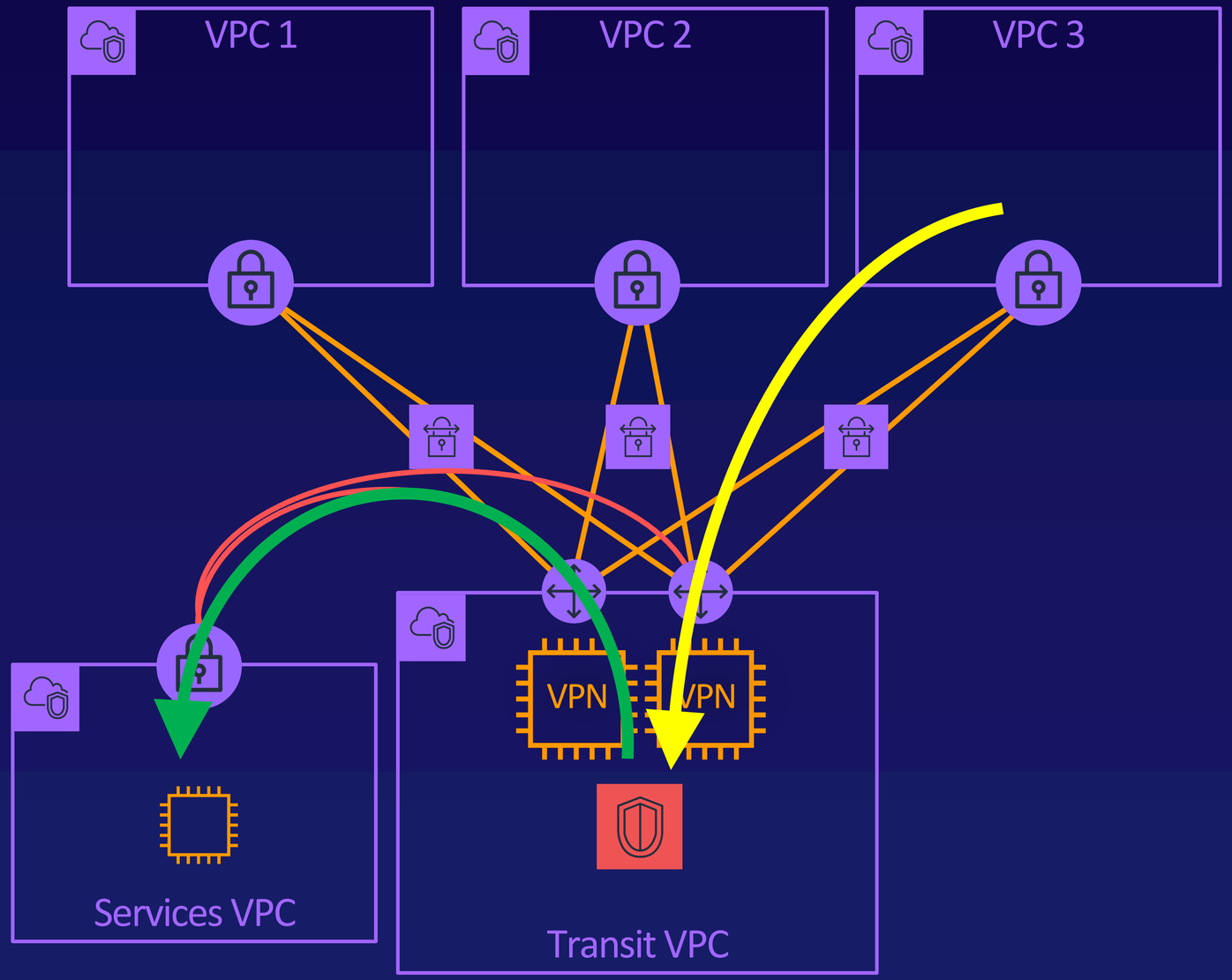
- VPCs that trust one another can still be connected by VPC peering.
- Static routes using the PCX will still need to be manually added to the VPC route tables.

Patterns – Shared Service VPCs



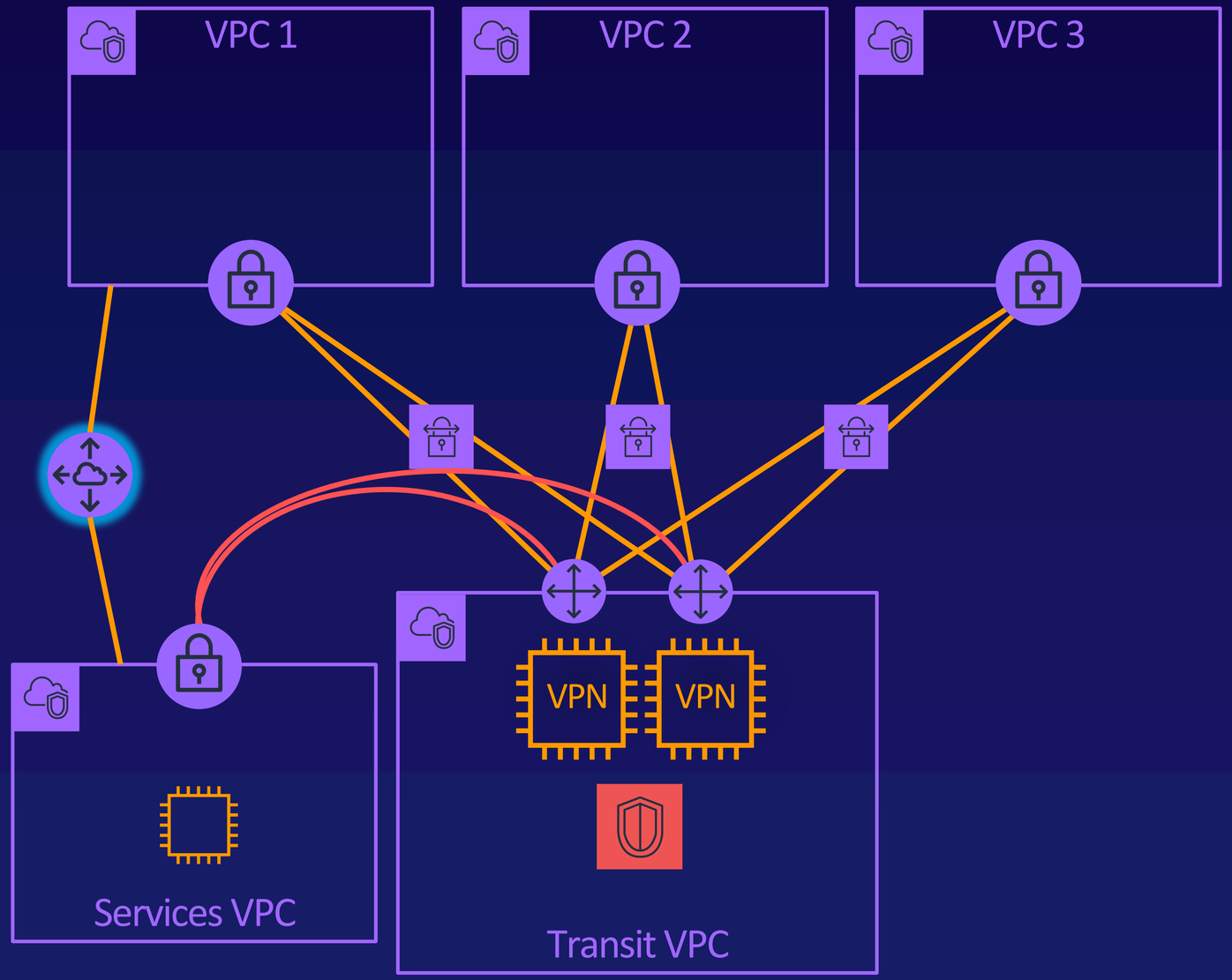
- Resources or services used by other VPCs may be placed in a central VPC.
- Service VPCs are connected to transit VPCs in the same way as other spoke VPCs.

Patterns – Shared Service VPCs



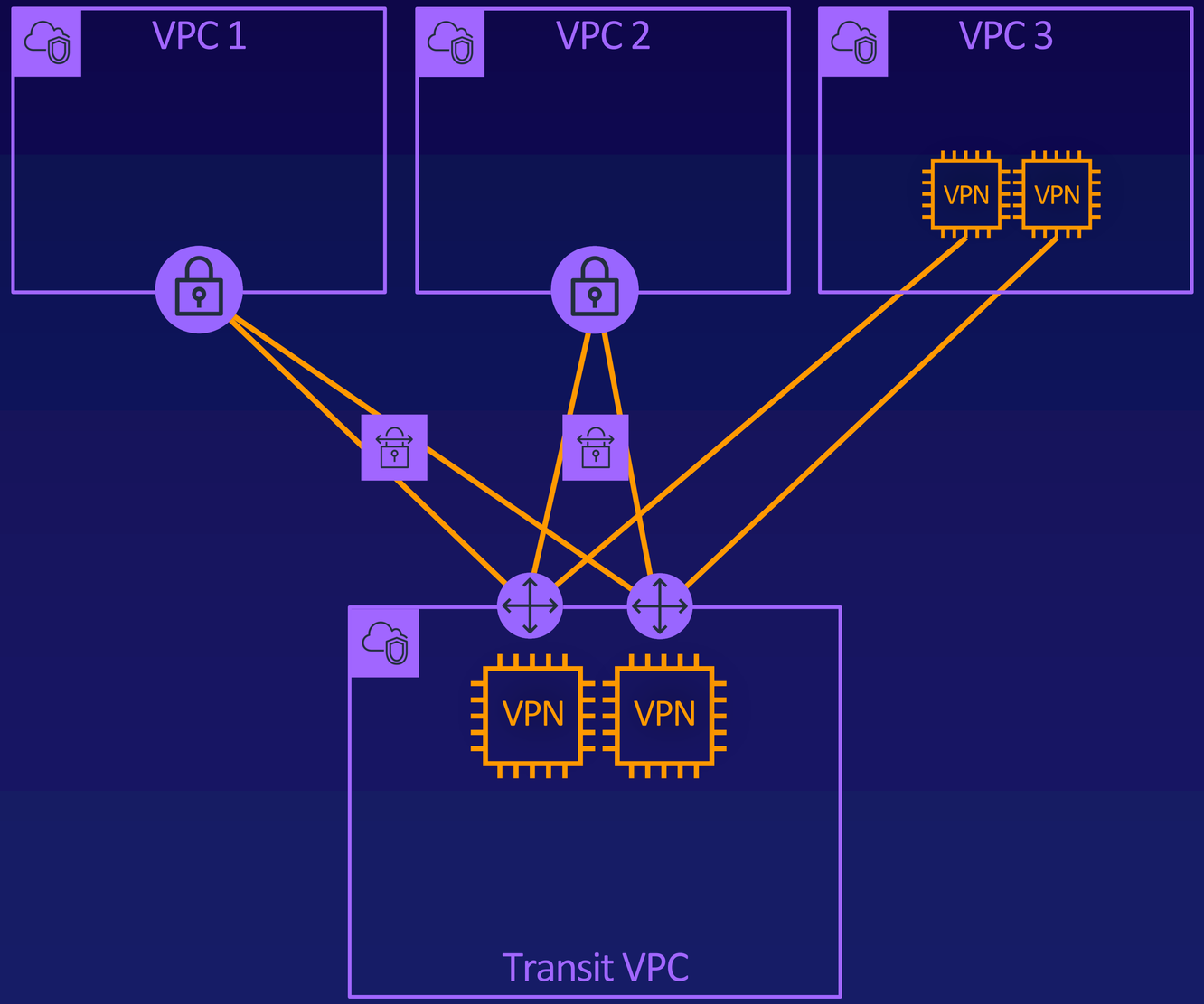
- Access to service VPCs may require connecting through authentication or security services in the transit VPC.

Patterns – Shared Service VPCs



- Access to service VPCs may require connecting through authentication or security services in the transit VPC.
- Trusted VPCs may be directly peered

Patterns – EC2-Hosted VPN in Spoke VPC



- Spoke VPC uses EC2-hosted VPN instead of VGW and AWS VPN connection.
- Can be used to overcome AWS VPN connection limitations.
- Customer is responsible for maintaining unmanaged services

Fast Takeaways

Most methods of inter-VPC connectivity are not transitive.

Transit VPCs use EC2-hosted systems to forward from one spoke VPC to another.

Transitive connections are controlled by restricting the advertisement of route prefixes from the transit VPC.

Different inter-VPC connectivity systems can be mixed and matched, as necessary.