
AWS
re:Invent

NET303

Shared VPCs, lessons learned, and best practices

Evgeny Vaganov

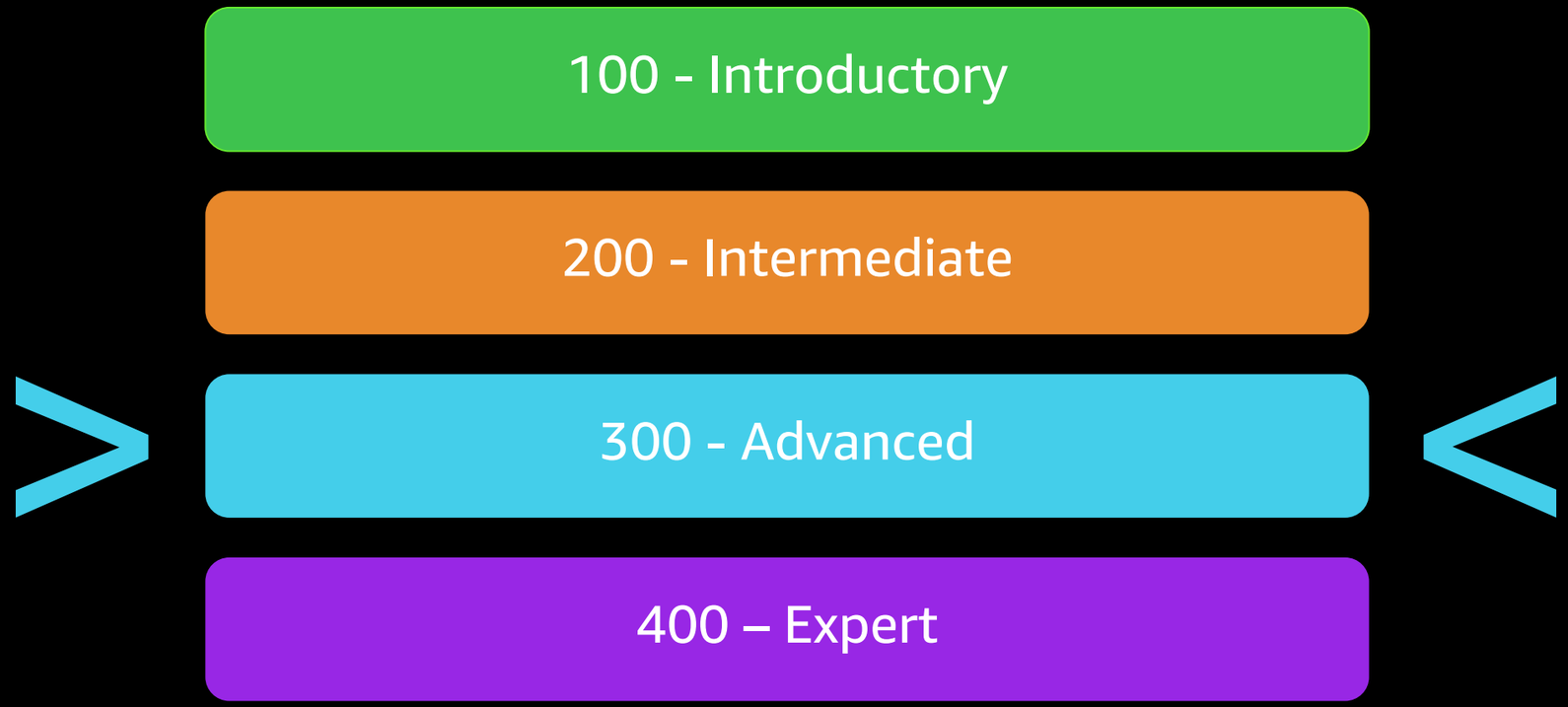
Specialist Solutions Architect, Networking

AWS

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Session level



What are we going to cover?

- VPC sharing replay
- Shared VPC architectures and network segmentation
- DNS in shared VPCs
- Guardrails and service control policies (SCPs)
- Shared VPC size considerations



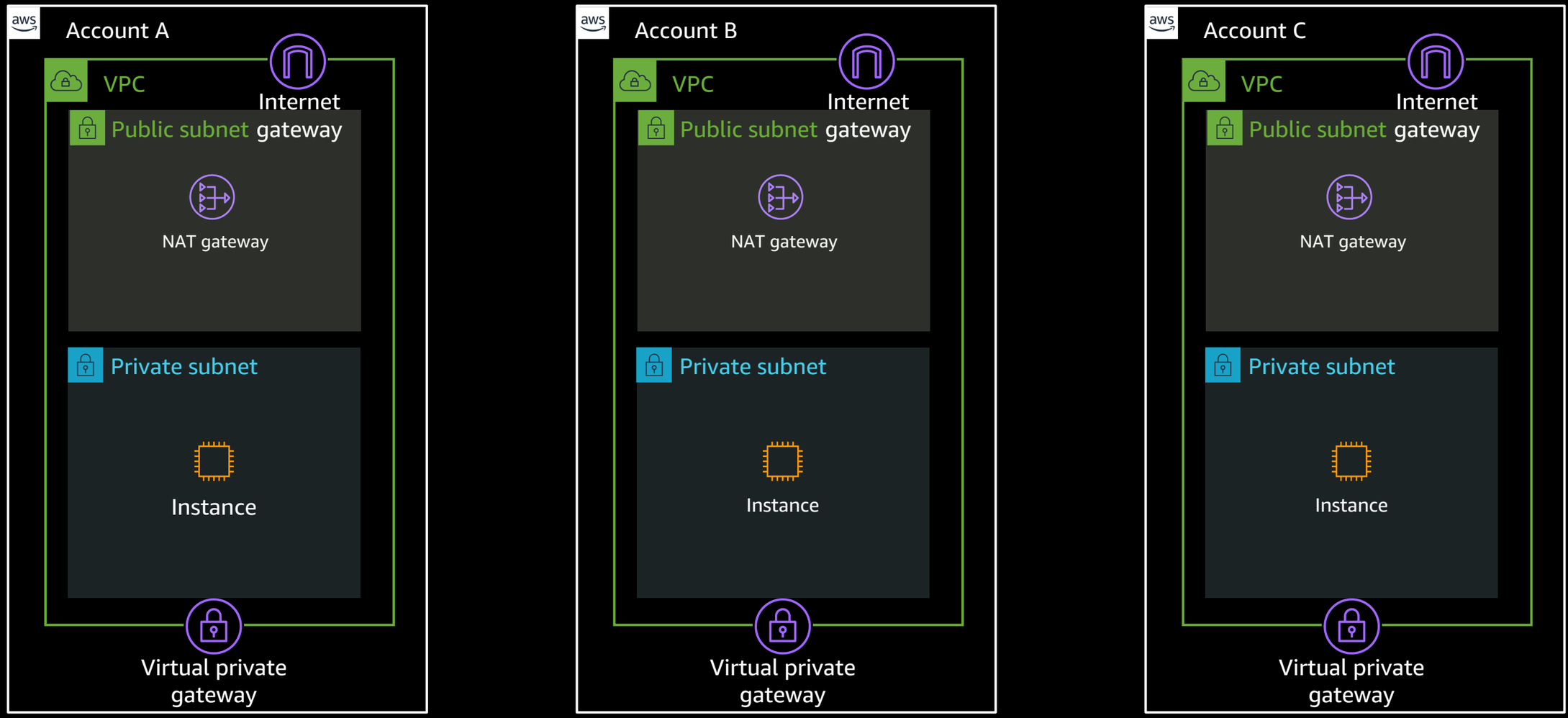
© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

How does VPC sharing work?

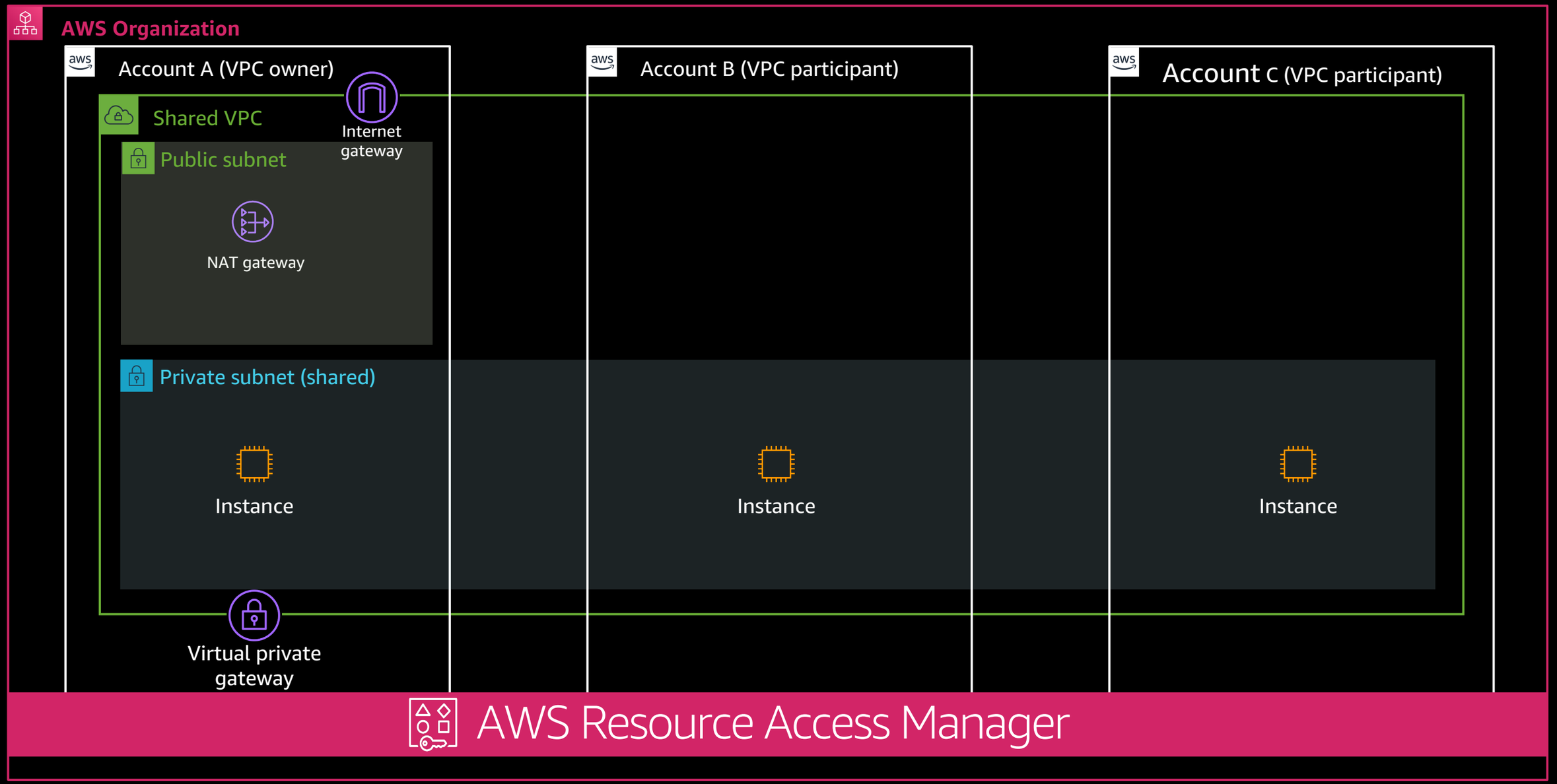


© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Without VPC sharing



With VPC sharing



Previous shared VPC content

Cost optimization and other benefits of VPC sharing - amzn.to/31U1rXO

Cost-effective multi-account microservice architecture - amzn.to/31TvFdz

Atlassian discusses migration to VPC sharing - youtu.be/S9NMA3ACZDM

Amazon Managed Blockchain in shared VPC - amzn.to/2SErMnE

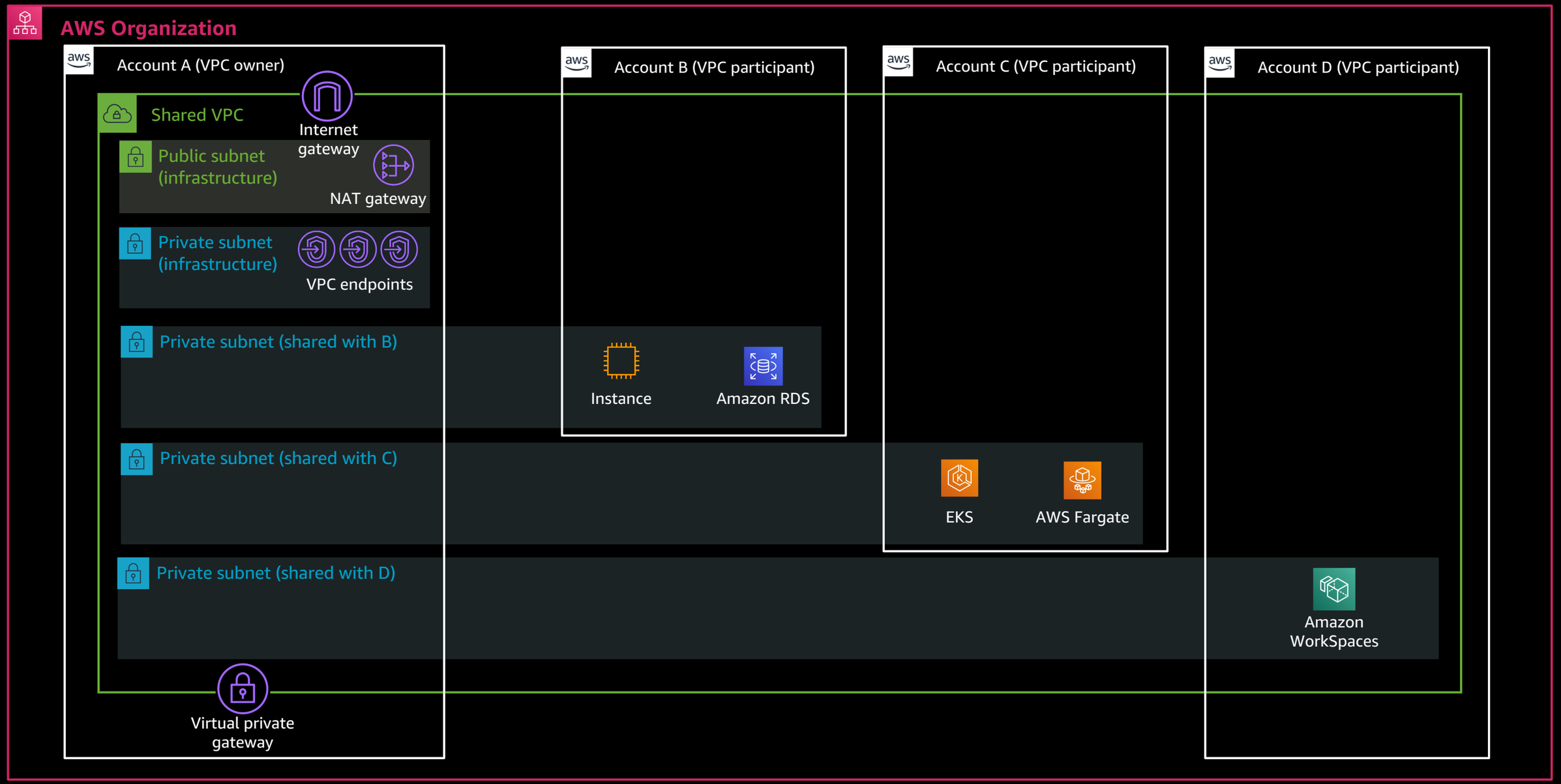
Shared VPC architectures



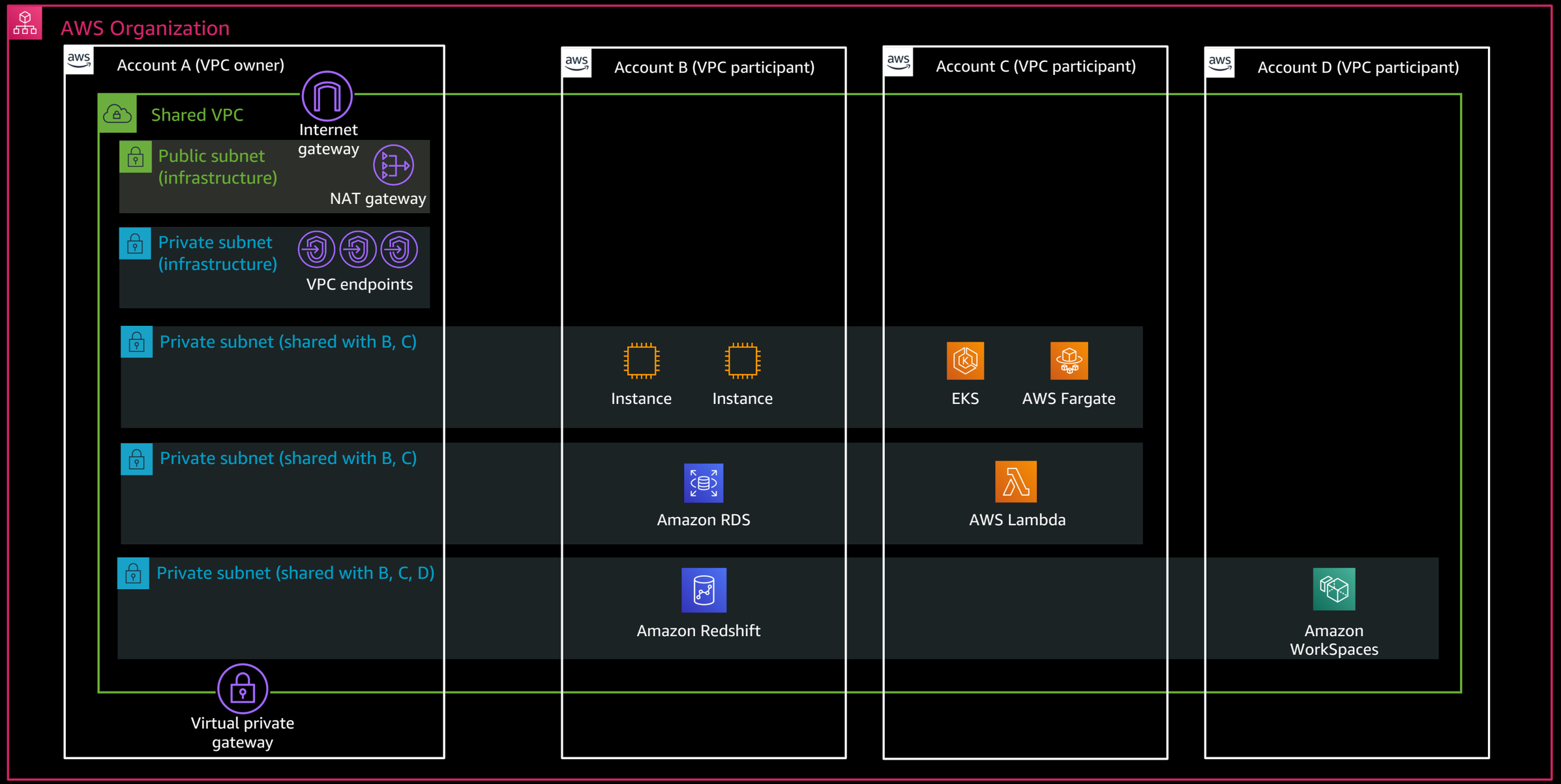
AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Shared subnet per VPC participant



Shared subnet across multiple VPC participants

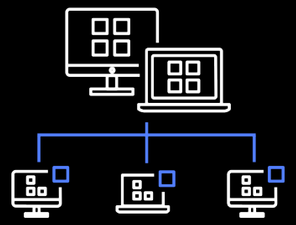


Subnets best practices



Monitor

Alarm when subnets get critically low on free IPs



Density

Larger subnets reduce IP wastage



Blast radius

Dedicated subnets reduce radius to a single VPC participant



Isolation

Network ACLs could be used to isolate VPC participants

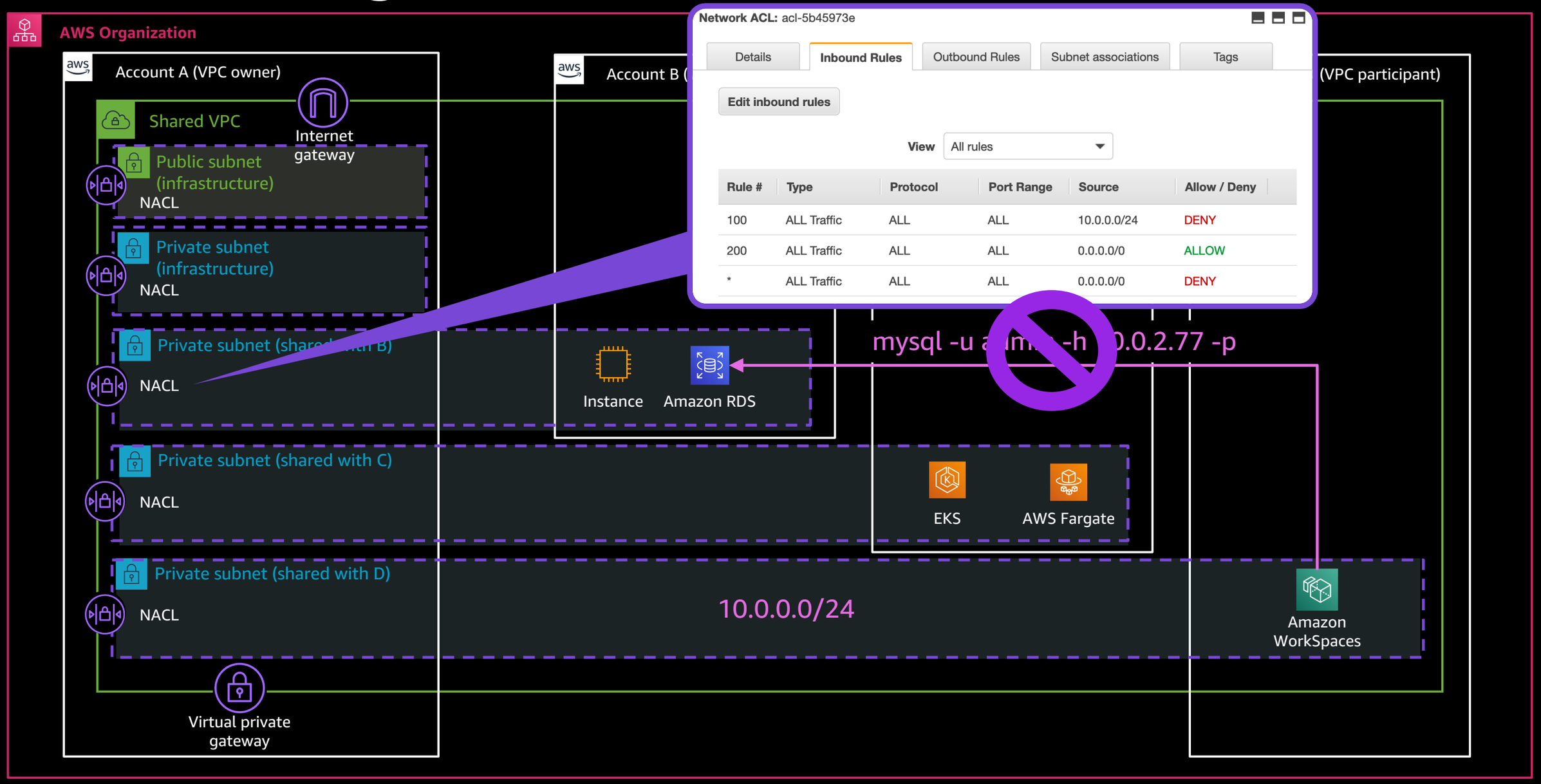
Network segmentation in shared VPC



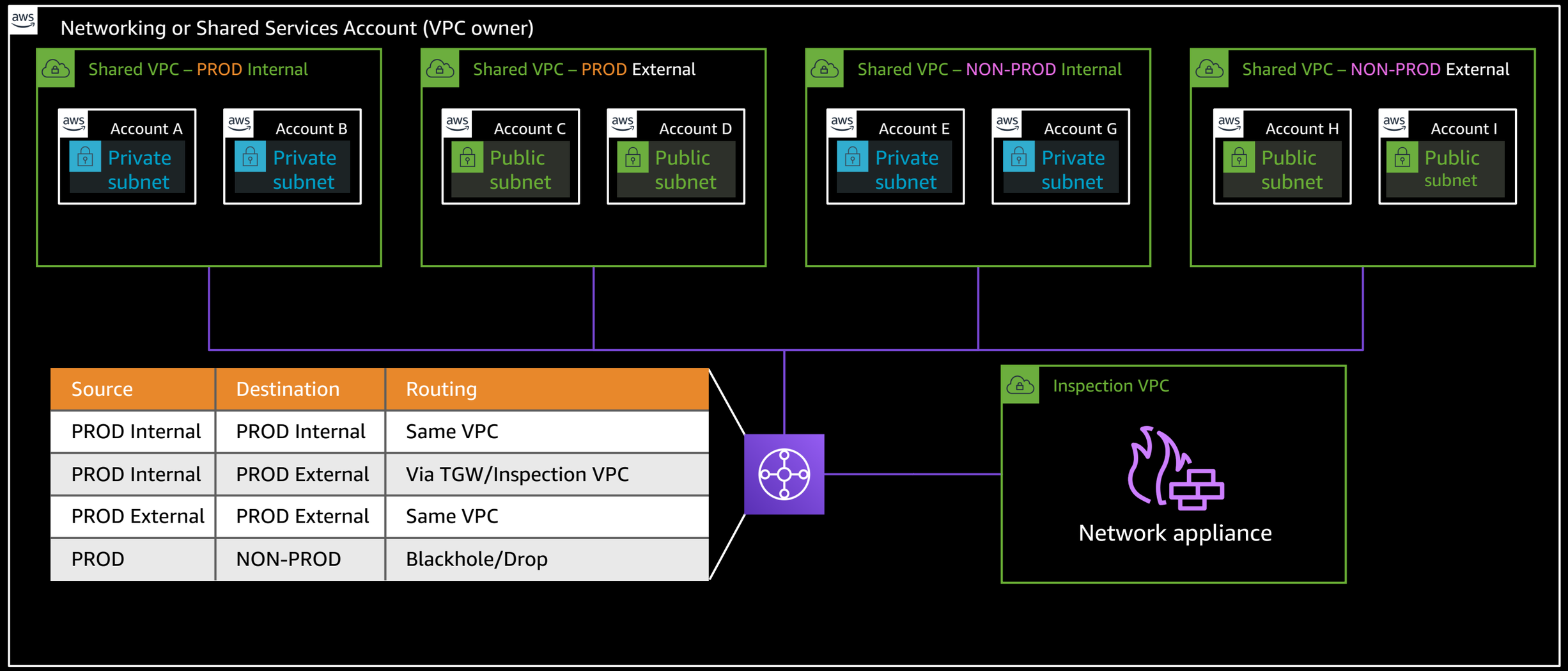
AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Network segmentation with NACLs



Network segmentation with network appliances



Source	Destination	Routing
PROD Internal	PROD Internal	Same VPC
PROD Internal	PROD External	Via TGW/Inspection VPC
PROD External	PROD External	Same VPC
PROD	NON-PROD	Blackhole/Drop

Guardrails



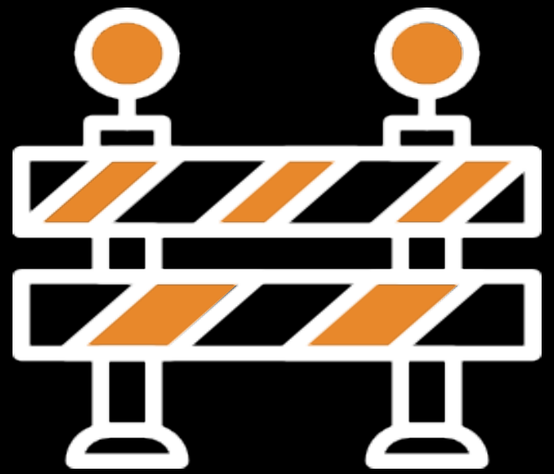
AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Guardrails in shared VPCs

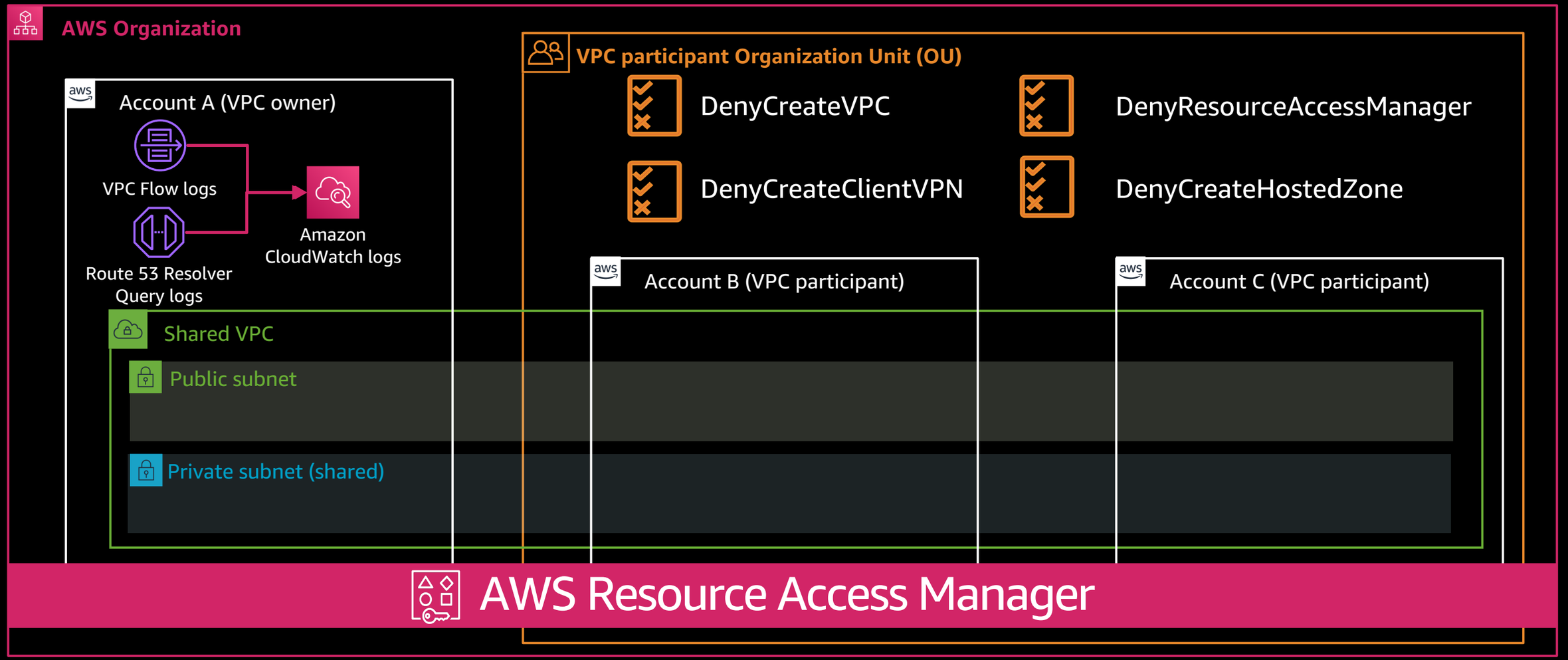
Guardrails are detective and preventative controls for ongoing governance of your AWS environment

- Preventative – disable ability to deploy services such as AWS Client VPN and VPC endpoint services (AWS PrivateLink) for VPC participants.
- Detective – enable VPC flow logs in the VPC owner account



Service control policies

SCPs define the maximum available permissions for IAM identities in your AWS account(s); limit unintended access to network related functions by VPC participants



DNS in shared VPCs



AWS re:Invent

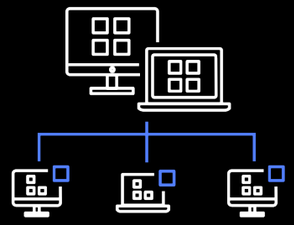
© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

DNS in shared VPCs



Simple

Consistent DNS view for every VPC participant



Centralized

VPC owner configures DHCP and Route 53 Resolver



Scalable

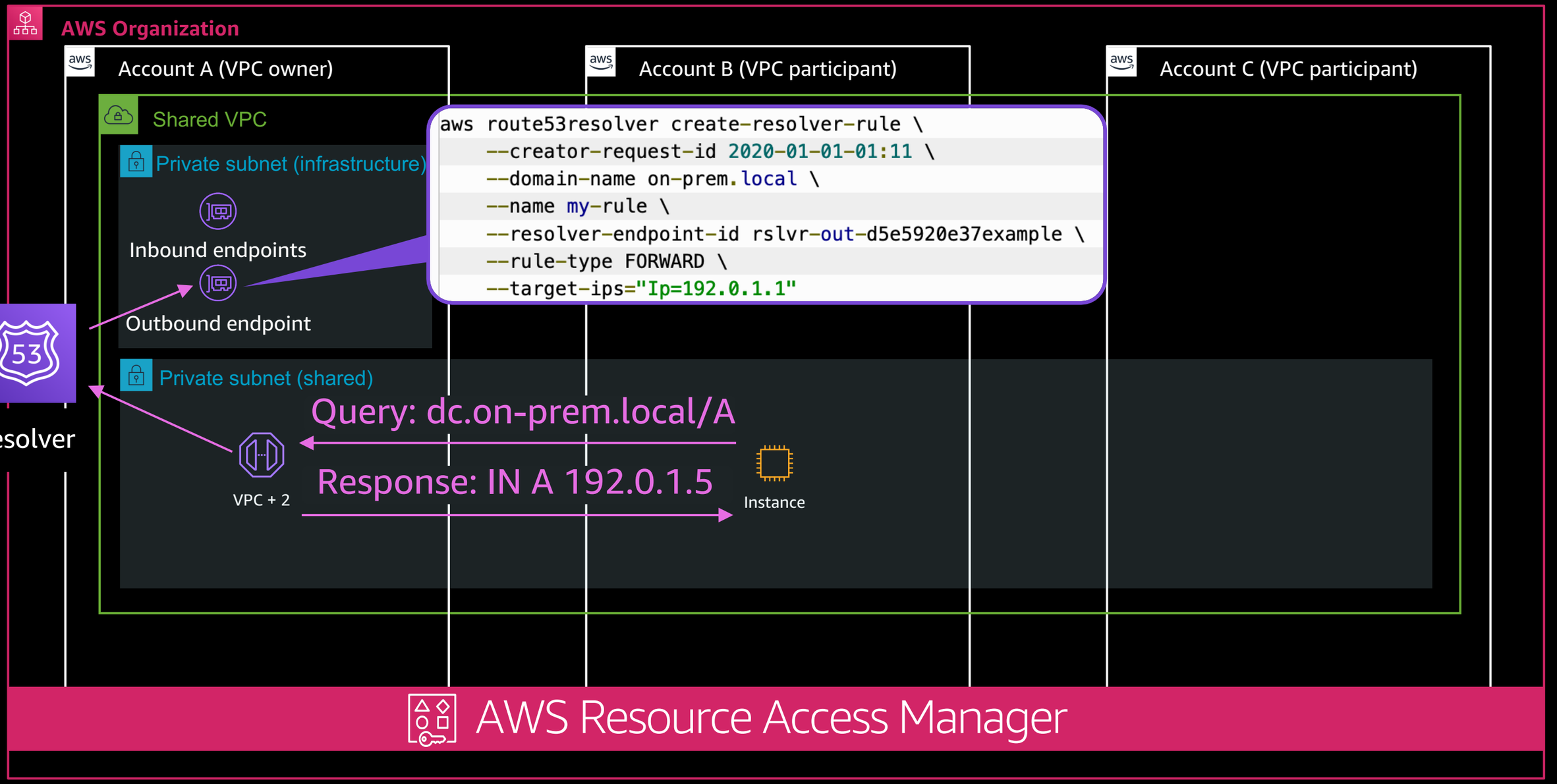
Every VPC participant inherits configuration



Zones

VPC participants can create their own hosted zones

Route 53 Resolver



Shared VPC size considerations



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Sizing considerations

	Great	Good	Avoid
# Participant accounts per VPC			

Sizing considerations

	Great	Good	Avoid
# Participant accounts per VPC	Up to 100	100–1,000	1,000+

Sizing considerations

	Great	Good	Avoid
# Participant accounts per VPC	Up to 100	100–1,000	1,000+
# of VPC subnets			

Sizing considerations

API call pagination is required

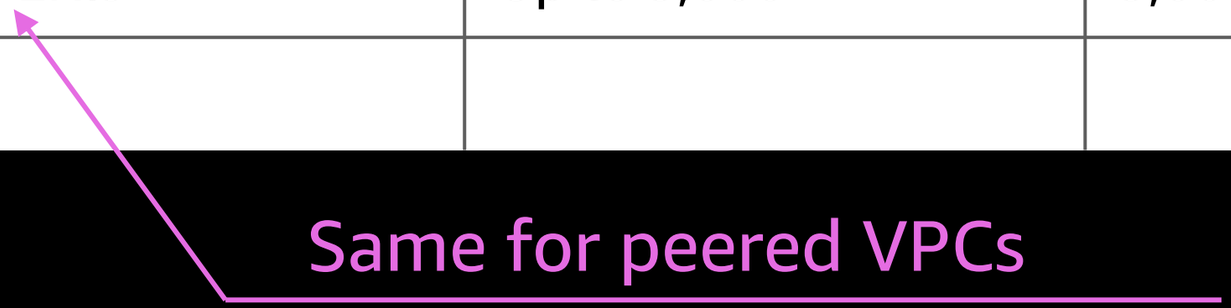
	Great	Good	Avoid
# Participant accounts per VPC	Up to 100	100–1,000	1,000+
# of VPC subnets	Up to 200	200–1,000	1,000+

Sizing considerations

	Great	Good	Avoid
# Participant accounts per VPC	Up to 100	100–1,000	1,000+
# of VPC subnets	Up to 200	200–1,000	1,000+
# of ENIs			

Sizing considerations

	Great	Good	Avoid
# Participant accounts per VPC	Up to 100	100–1,000	1,000+
# of VPC subnets	Up to 200	200–1,000	1,000+
# of ENIs	Up to 5,000	5,000–70,000	70,000+



Sizing considerations

	Great	Good	Avoid
# Participant accounts per VPC	Up to 100	100–1,000	1,000+
# of VPC subnets	Up to 200	200–1,000	1,000+
# of ENIs	Up to 5,000	5,000–70,000	70,000+
# of AWS Hyperplane ENIs*			

Sizing considerations

	Great	Good	Avoid
# Participant accounts per VPC	Up to 100	100–1,000	1,000+
# of VPC subnets	Up to 200	200–1,000	1,000+
# of ENIs	Up to 5,000	5,000–70,000	70,000+
# of AWS Hyperplane ENIs*			

* AWS Hyperplane ENIs are used by NLB, Interface VPC endpoints, EFS, NAT Gateways, Transit Gateways, Lambda in a VPC

Sizing considerations

	Great	Good	Avoid
# Participant accounts per VPC	Up to 100	100–1,000	1,000+
# of VPC subnets	Up to 200	200–1,000	1,000+
# of ENIs	Up to 5,000	5,000–70,000	70,000+
# of AWS Hyperplane ENIs*	Default service quota**		

* AWS Hyperplane ENIs are used by NLB, Interface VPC endpoints, EFS, NAT Gateways, Transit Gateways, Lambda in a VPC

Sizing considerations

	Great	Good	Avoid
# Participant accounts per VPC	Up to 100	100–1,000	1,000+
# of VPC subnets	Up to 200	200–1,000	1,000+
# of ENIs	Up to 5,000	5,000–70,000	70,000+
# of AWS Hyperplane ENIs*	Default service quota**		

* AWS Hyperplane ENIs are used by NLB, Interface VPC endpoints, EFS, NAT Gateways, Transit Gateways, Lambda in a VPC

** Each participant usage counts towards the quota; each resource in each AZ consumes one Hyperplane ENI

Sizing considerations

	Great	Good	Avoid
# Participant accounts per VPC	Up to 100	100–1,000	1,000+
# of VPC subnets	Up to 200	200–1,000	1,000+
# of ENIs	Up to 5,000	5,000–70,000	70,000+
# of AWS Hyperplane ENIs*	Default service quota**	Up to 1,000 ENIs per shared VPC	1,000+

* AWS Hyperplane ENIs are used by NLB, Interface VPC endpoints, EFS, NAT Gateways, Transit Gateways, Lambda in a VPC

** Each participant usage counts towards the quota; each resource in each AZ consumes one Hyperplane ENI

Summary



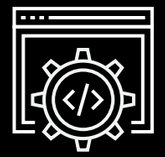
VPC sharing

Allows for a VPC to be shared by multiple AWS accounts within an AWS organization



Users

Many AWS users have deployed shared VPCs in production at large scale



Best practices

Use recommended architectures and guardrails



Scale

Scales with your cloud needs and can be combined with other AWS networking services



VPC sharing – a powerful tool for cloud scale networking

Thank you!



AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Please complete the session survey

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.