
AWS
re:Invent

ENT401

AWS networking best practices in large-scale migrations

Gokul Bellala Kuppuraj

Sr. Solutions Architect, Migrations

AWS

AWS re:Invent

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

Story

This is regarding a customer journey to AWS. Example Corp. has 10 data centers globally and has decided to migrate their workloads to AWS. What are some of the major challenges they faced from a networking perspective as they migrate the first couple of datacenters to AWS and how did they address them using some of the AWS networking best practices?



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

Networking challenges in large migrations

- Hybrid connectivity
- Centralize networking
- Private DNS

Hybrid connectivity



AWS re:Invent

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

Why?

Migration takes time

Large volume of data

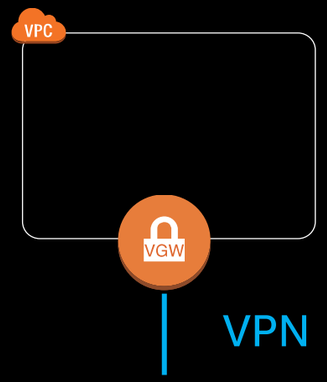
Limited cut-over window

Network latency

Replication requirements

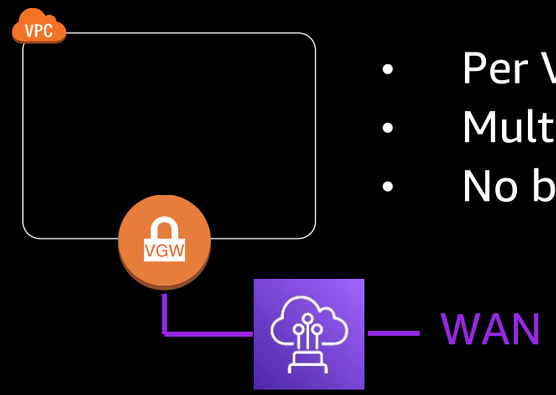
Hybrid connectivity options

AWS Site-to-Site VPN



- Per VPC
- 1.25 gbps per tunnel
- Encrypted in transit

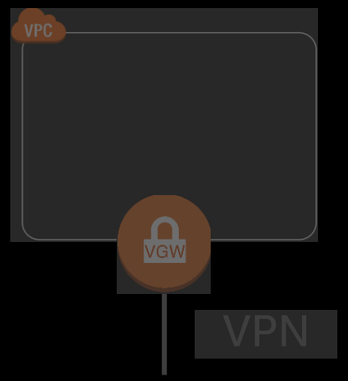
DX



- Per VPC (50-500 per port)
- Multiple VPCs with DX gateway
- No bandwidth restraint

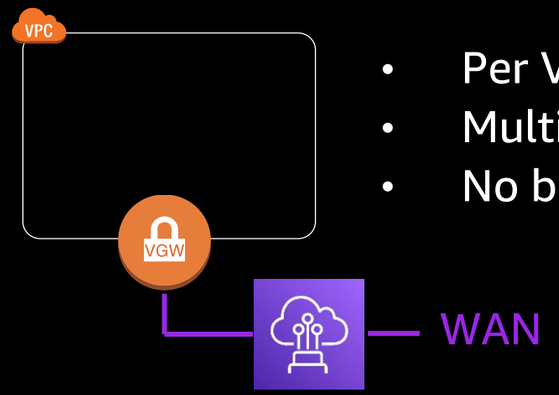
Connecting to on-premises at scale

VPN



- Per VPC
- 1.25 gbps per tunnel
- Encrypted in transit

DX



- Per VPC (50-500 per port)
- Multiple VPCs with DX gateway
- No bandwidth restraint

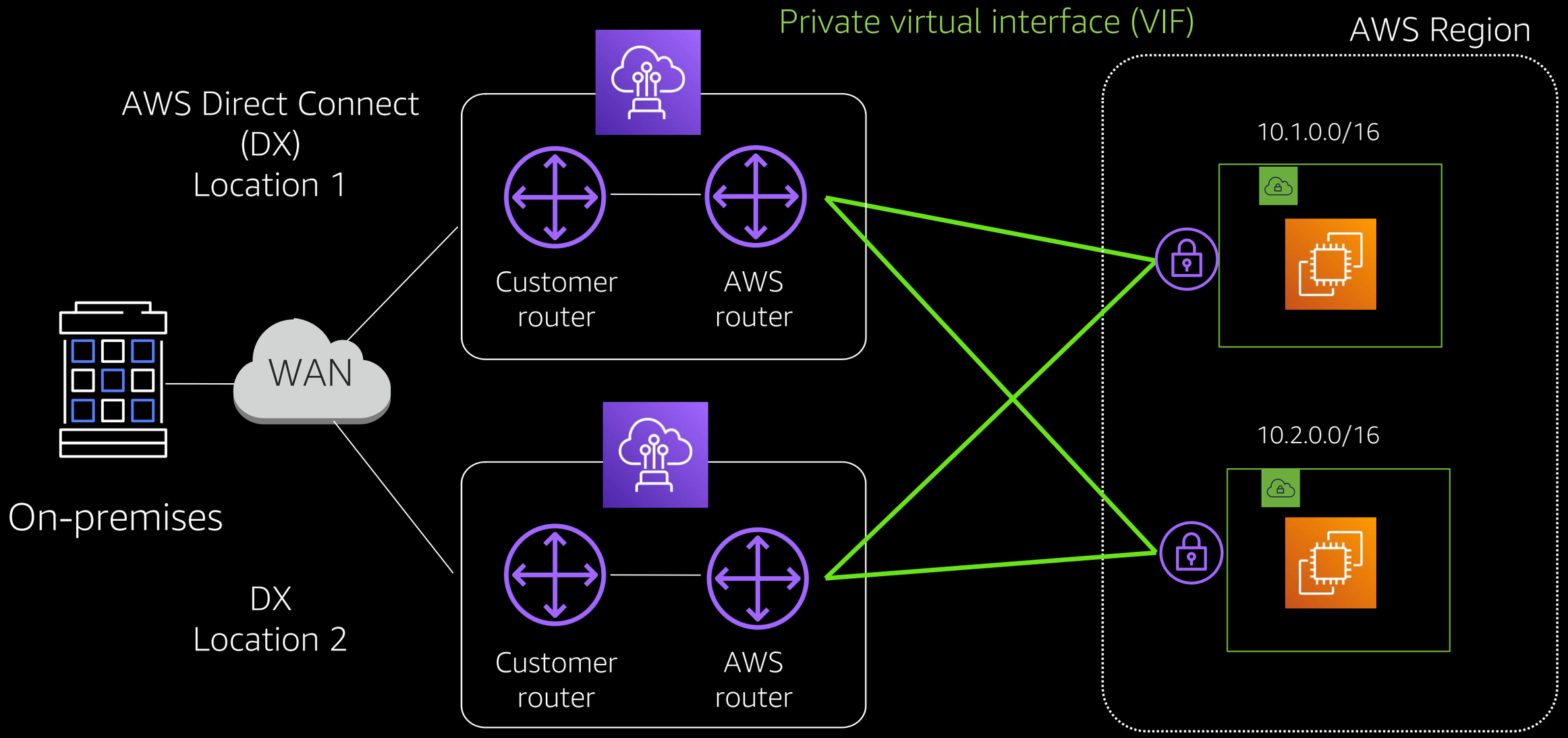
Dedicated network connection to AWS providing **consistent** performance and **reduced** bandwidth costs.

AWS Direct Connect – interface types

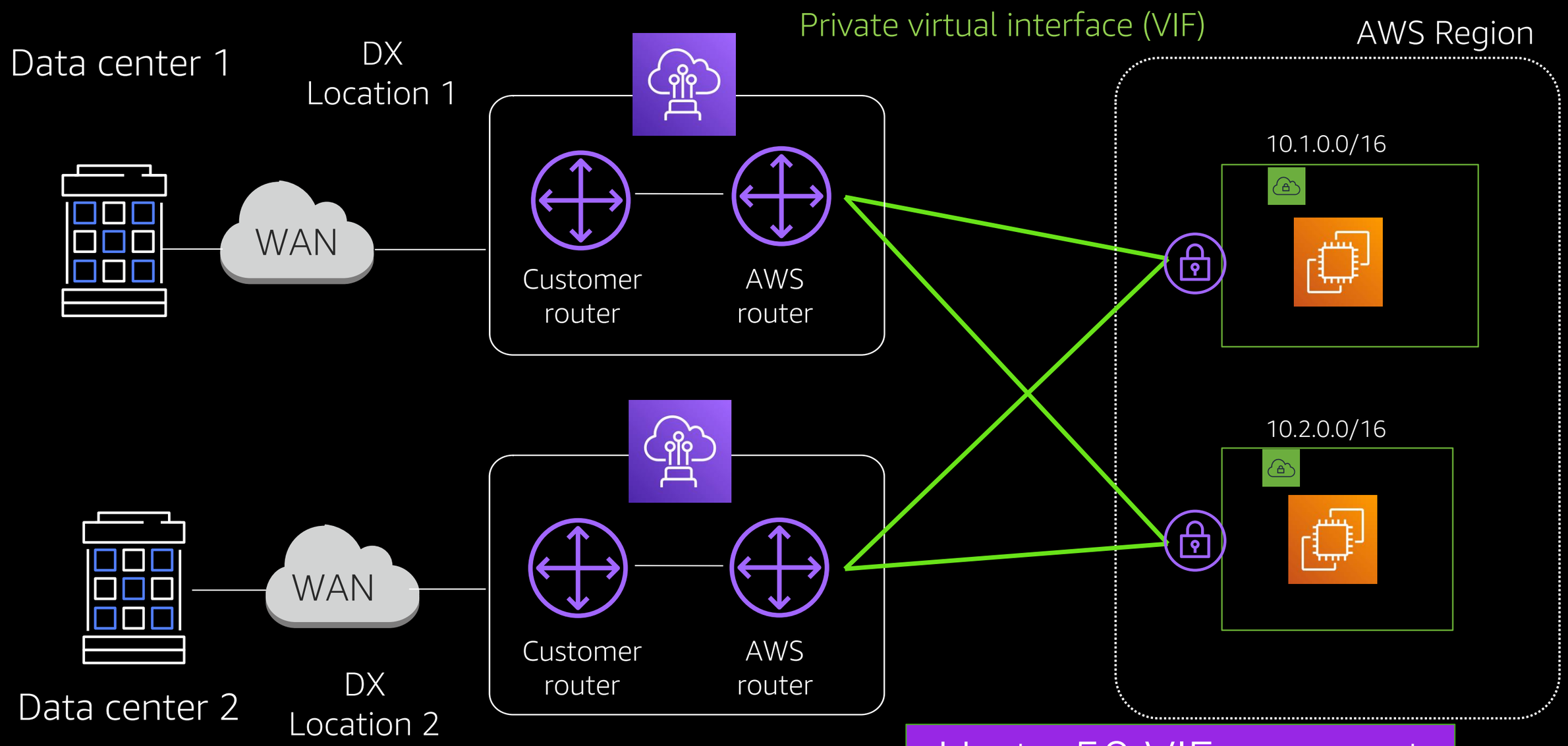
- **Public VIF** – used to access all AWS public services using public IP addresses, e.g., public endpoints for Application Discovery Service, Amazon Simple Storage Service, etc.
- **Private VIF** – used to connect to Amazon VPCs using private IP addresses; directly or via direct connect gateway
- **Transit VIF** – used to connect to transit gateways via direct connect gateway

All virtual Interfaces are 802.1Q VLANs with BGP peering

DX High Availability



DX High Availability – increased resiliency



Up to 50 VIFs per port

What if

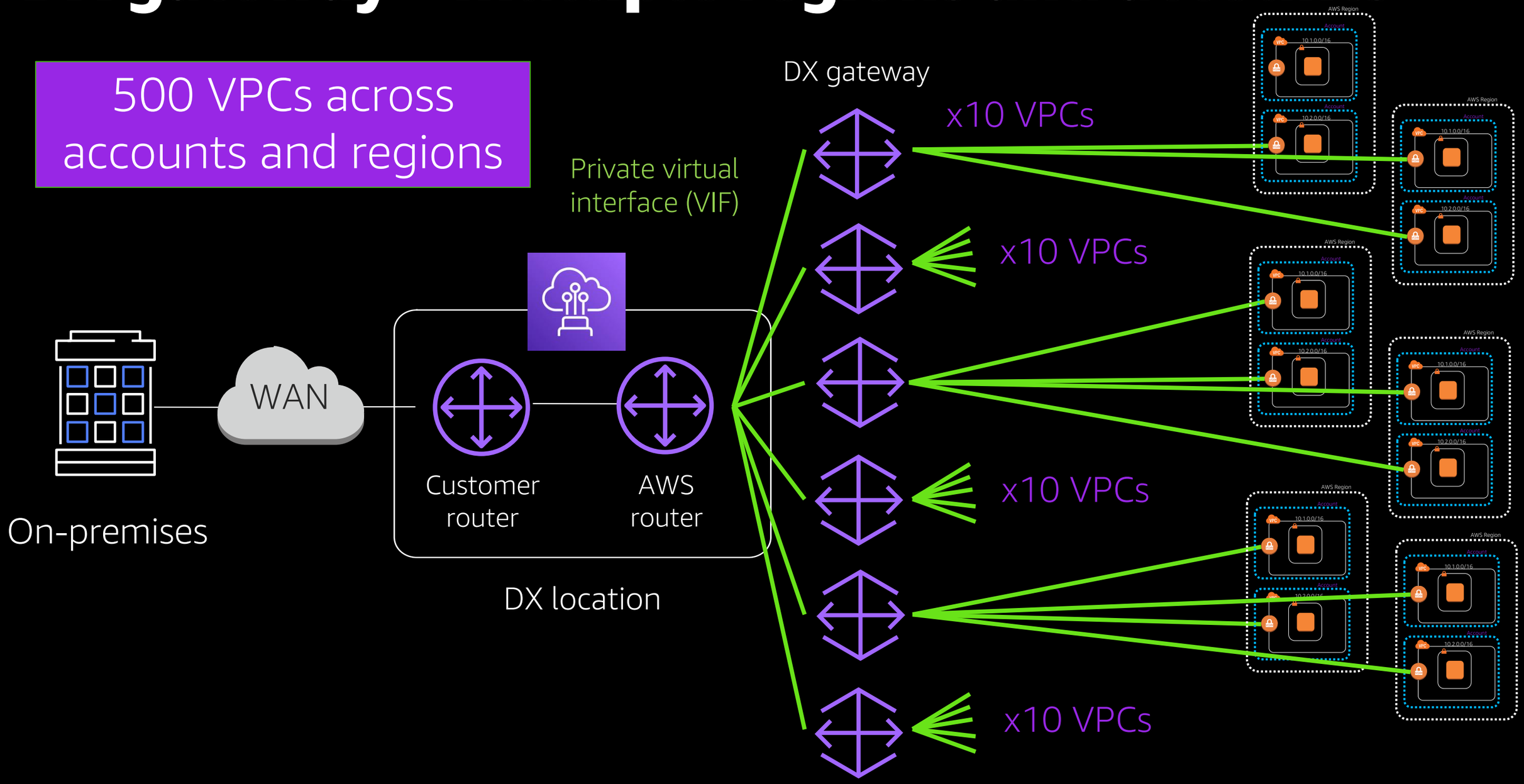
Connect > 50 VPCs

Leveraging multiple regions and accounts

Reduce number of BGP sessions

DX gateway – multiple regions and accounts

500 VPCs across accounts and regions



Traffic engineering



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

Amazon VPC and Direct Connect route selection



Amazon VPC

1. VPC local routes (preferred over more specific)
2. Longest prefix match (more specific)
3. Static routes
4. Dynamic routes (propagated) from VGW
    1. Prefer direct connect BGP routes
    2. VPN static routes
    3. VPN dynamic routes

Amazon VPC and Direct Connect route selection



AWS Direct Connect

1. Longest prefix – global
2. Local preference – global
3. AS-Path – direct connect location
    1. If AWS network “cost” is equal
    2. Requires local-pref for consistency
4. Equivalent – balance per flow

Private VIF communities: AWS egress local-pref



AWS Direct Connect

Community = metadata applied to a prefix during route advertisement that can later be acted upon

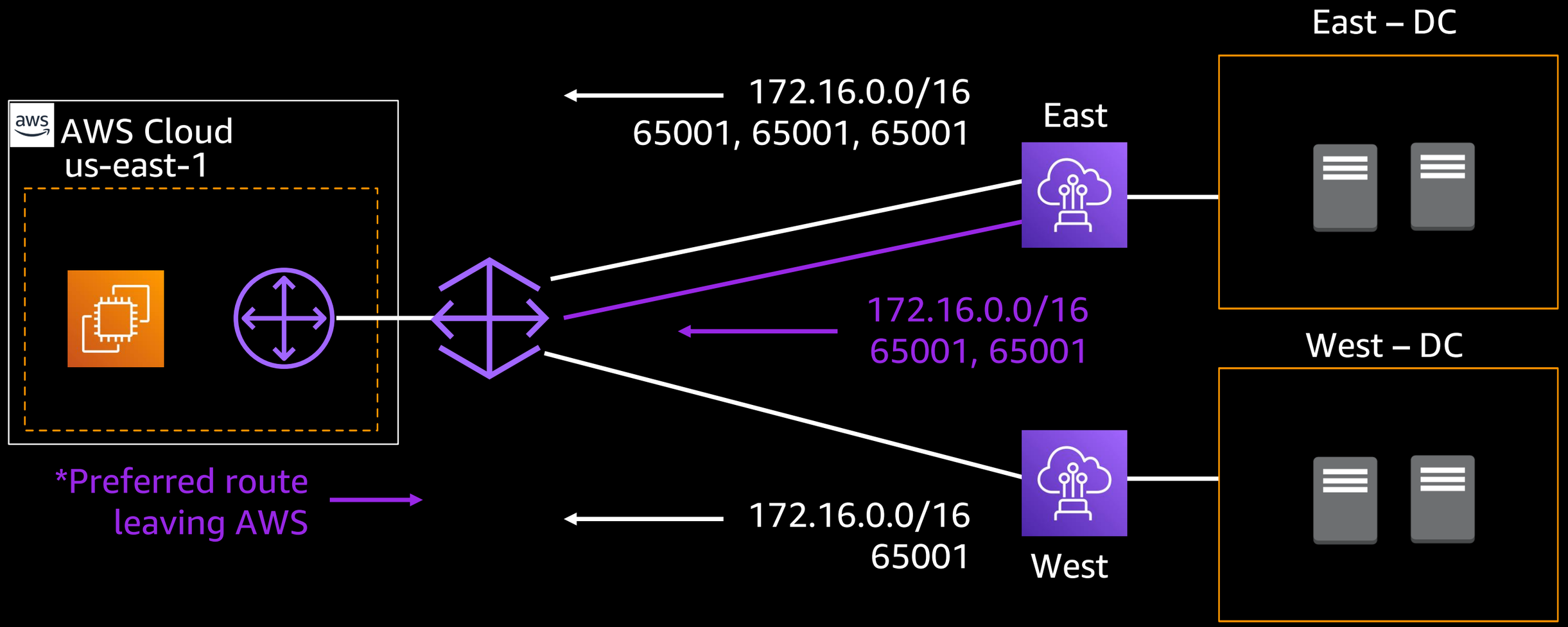
Private VIF – egress route manipulation (local-pref)

7224:7100 – low preference

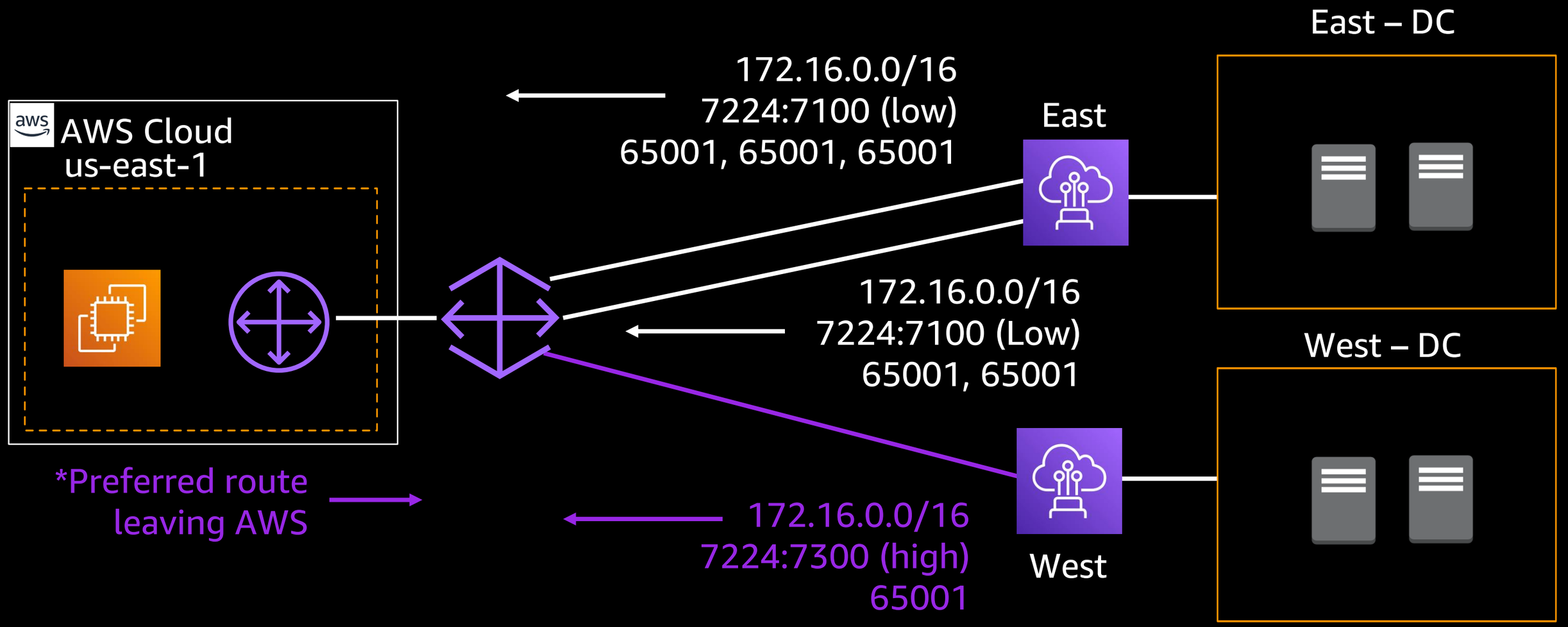
7224:7200 – medium preference

7224:7300 – high preference

Route selection



Route selection



Direct Connect best practices

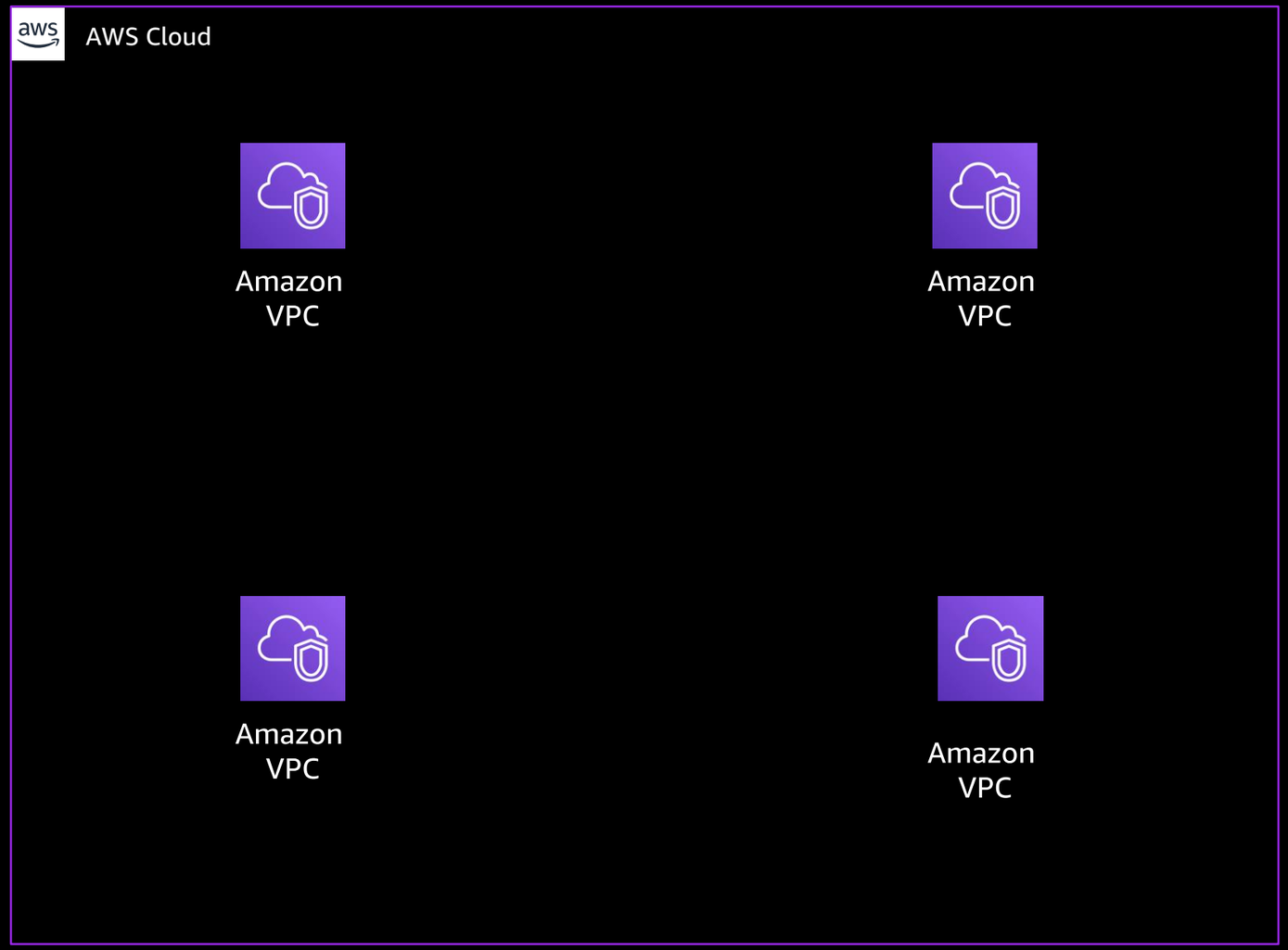
1. Leverage resiliency toolkit to order DX
2. Leverage DX gateway to scale and expand to different region
3. Option to leverage dedicated or hosted connection
4. Use multiple dynamically routed connections
5. Option to leverage VPN over DX for encryption

Centralized networking



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

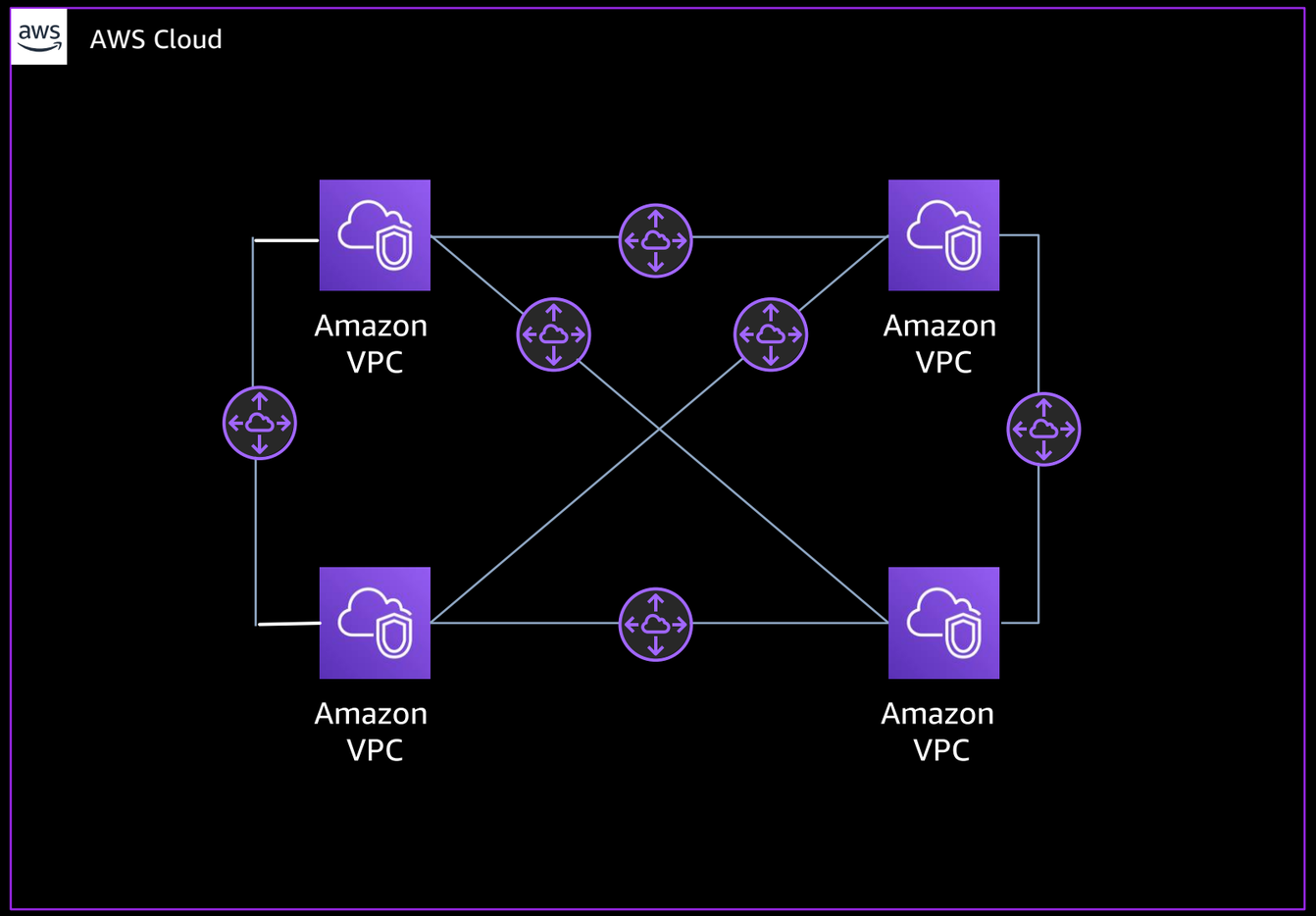
VPC-to-VPC connectivity



Amazon VPC peering

Pros

- Simple at small scale
- Referenceable security groups
- Intra and inter-region support
- Fully managed with redundancy



Cons

- Does not support transitive routing
- Complex management at scale

How many Amazon VPC peering connections do I need (full mesh)?

1,225

VPC x 50

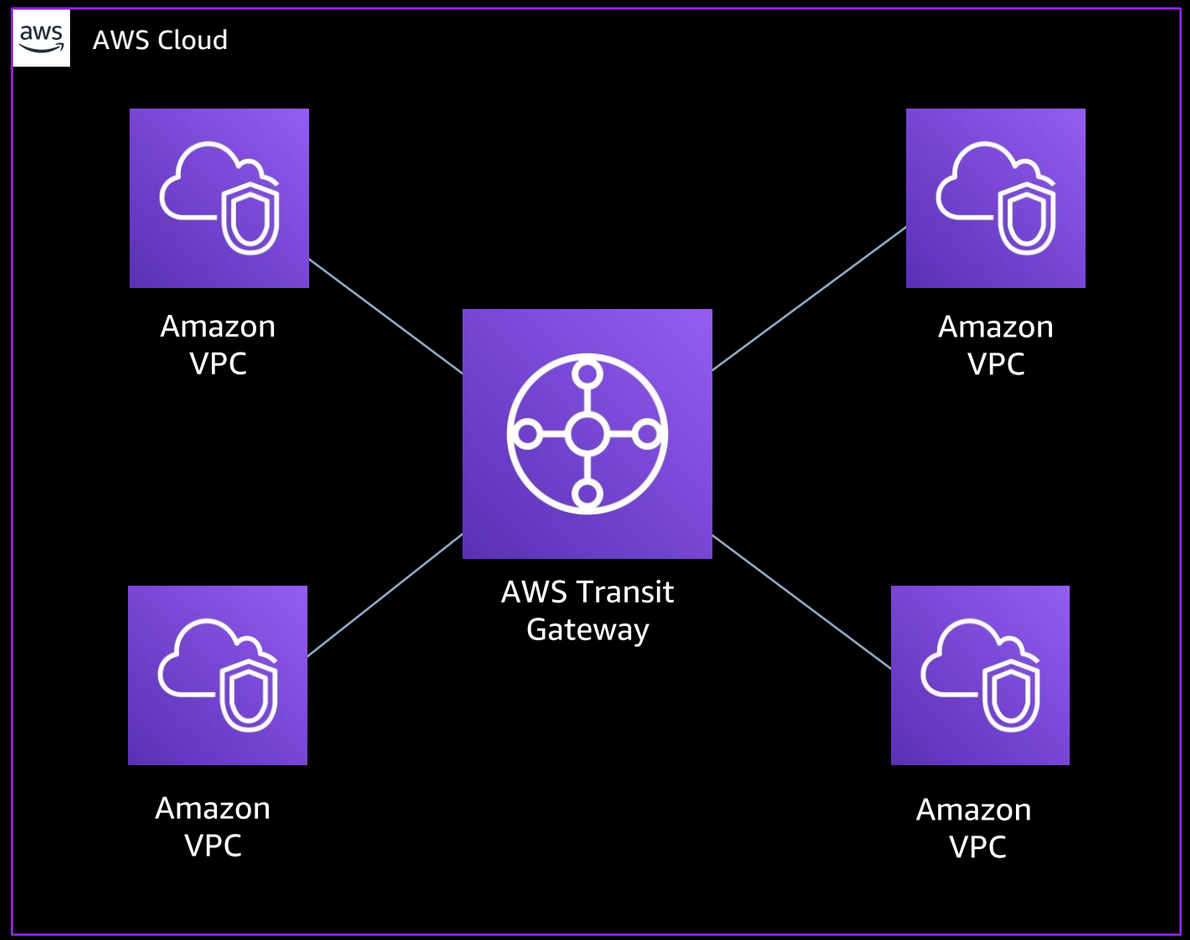
Amazon VPC peering connections per Amazon VPC

125

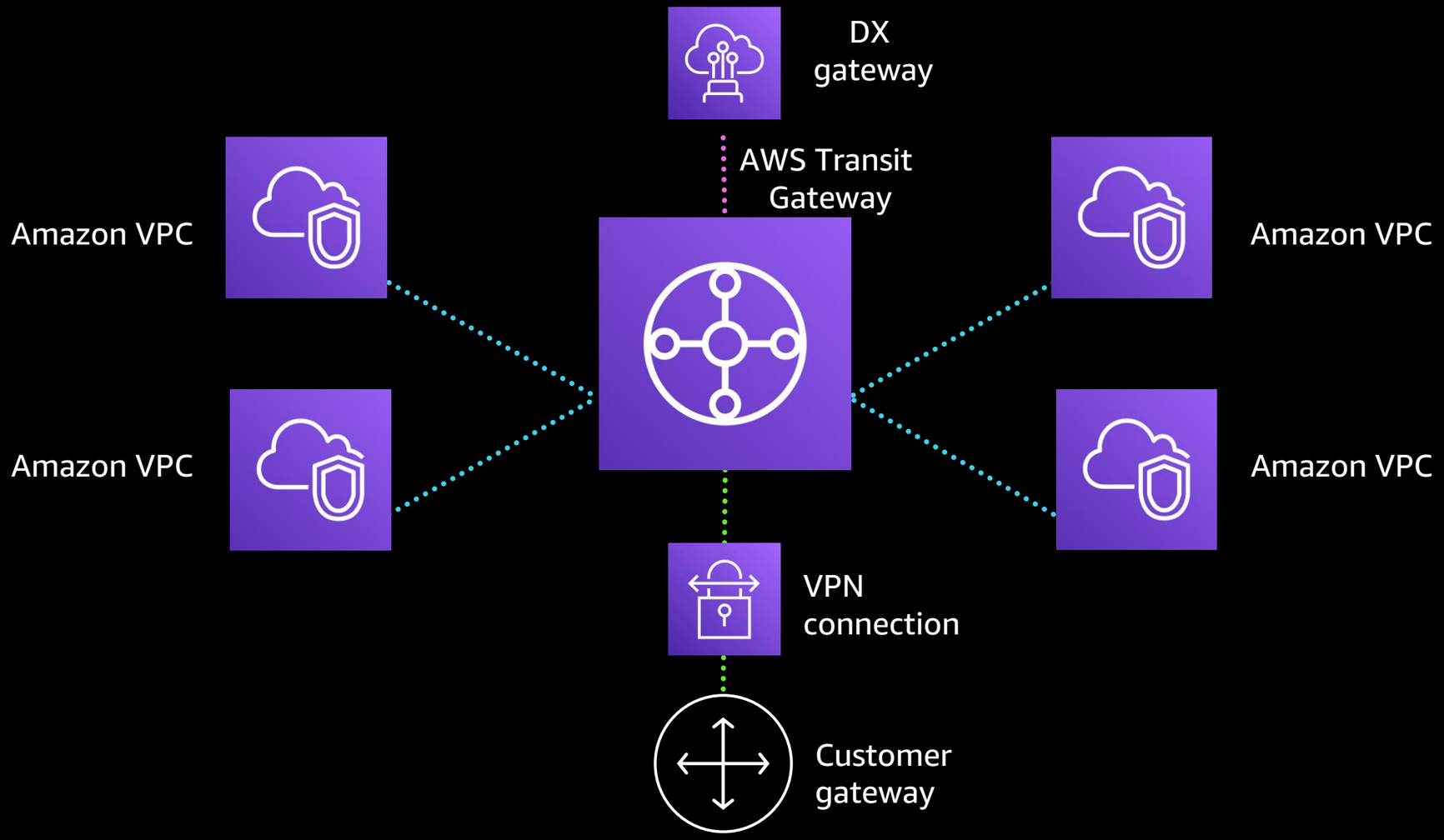
Static routes per Amazon VPC route table

1,000

Connecting VPCs at scale – AWS Transit Gateway



AWS Transit Gateway – hybrid connectivity



Static routes per AWS Transit Gateway

10,000

AWS Transit Gateway attachments per transit gateway

5,000

AWS Transit Gateway

Regional service

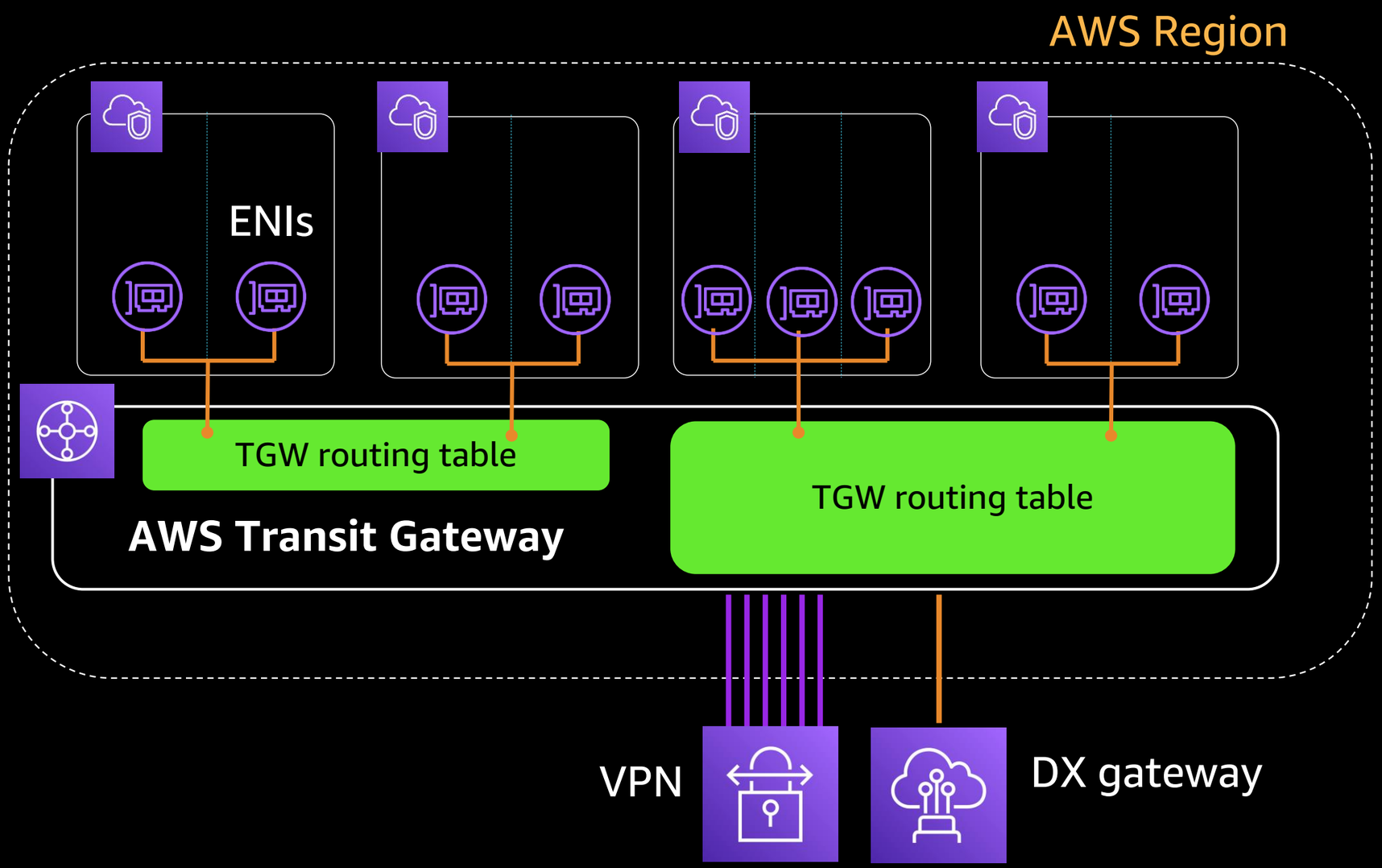
- Centralize VPN and DX gateway

Scalable

- Thousands of VPCs **across accounts**
- Spread traffic over many VPN connections

Flexible routing

- Network interfaces in subnets
- Control segmentation and sharing with TGW route tables



Considerations on using TGW route tables

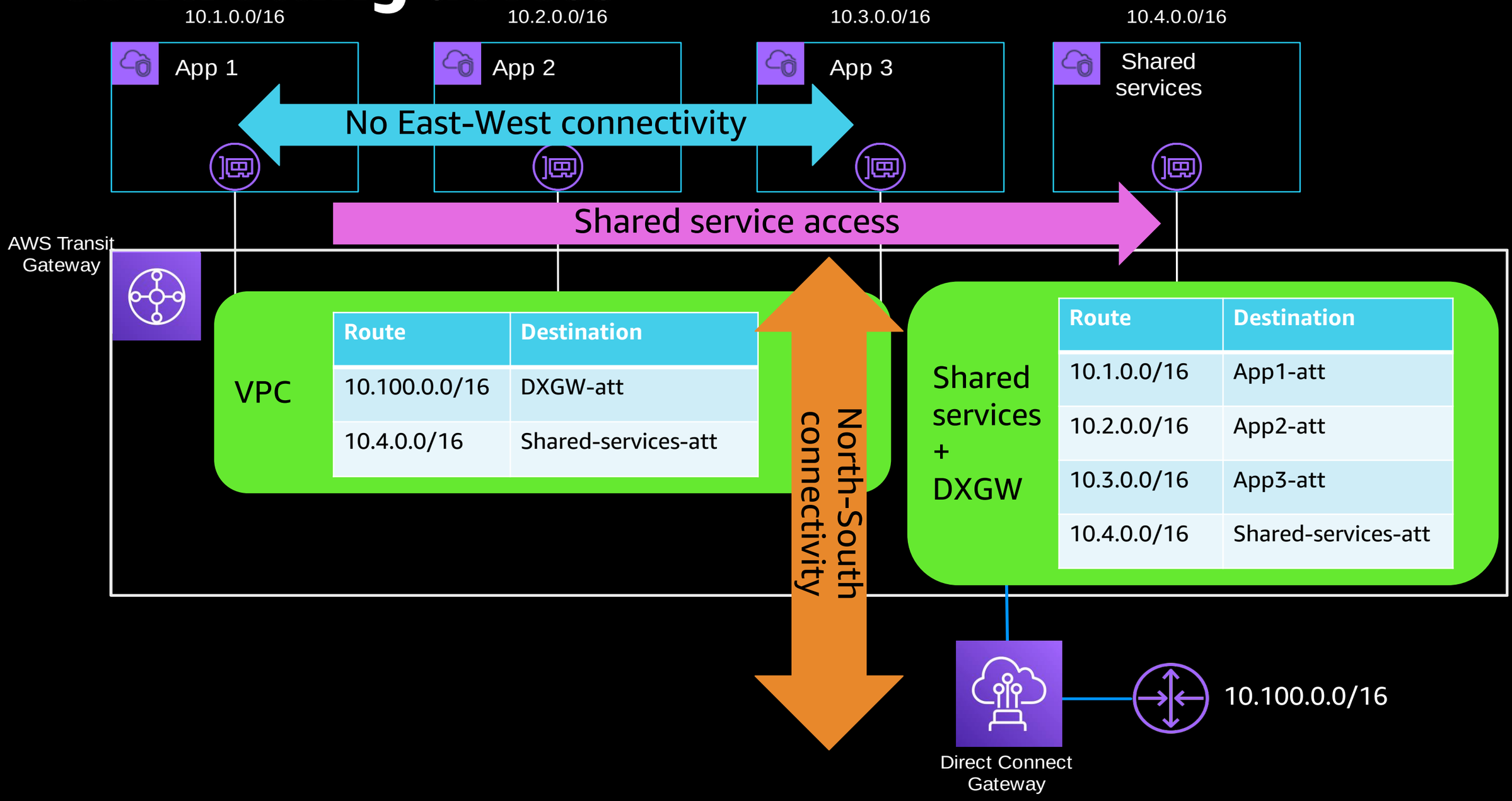
1. Group (associate) VPCs to TGW route tables that have the same connectivity requirements

2. VPCs associated to the same TGW route tables does not enable connectivity between other associated VPCs unless configured

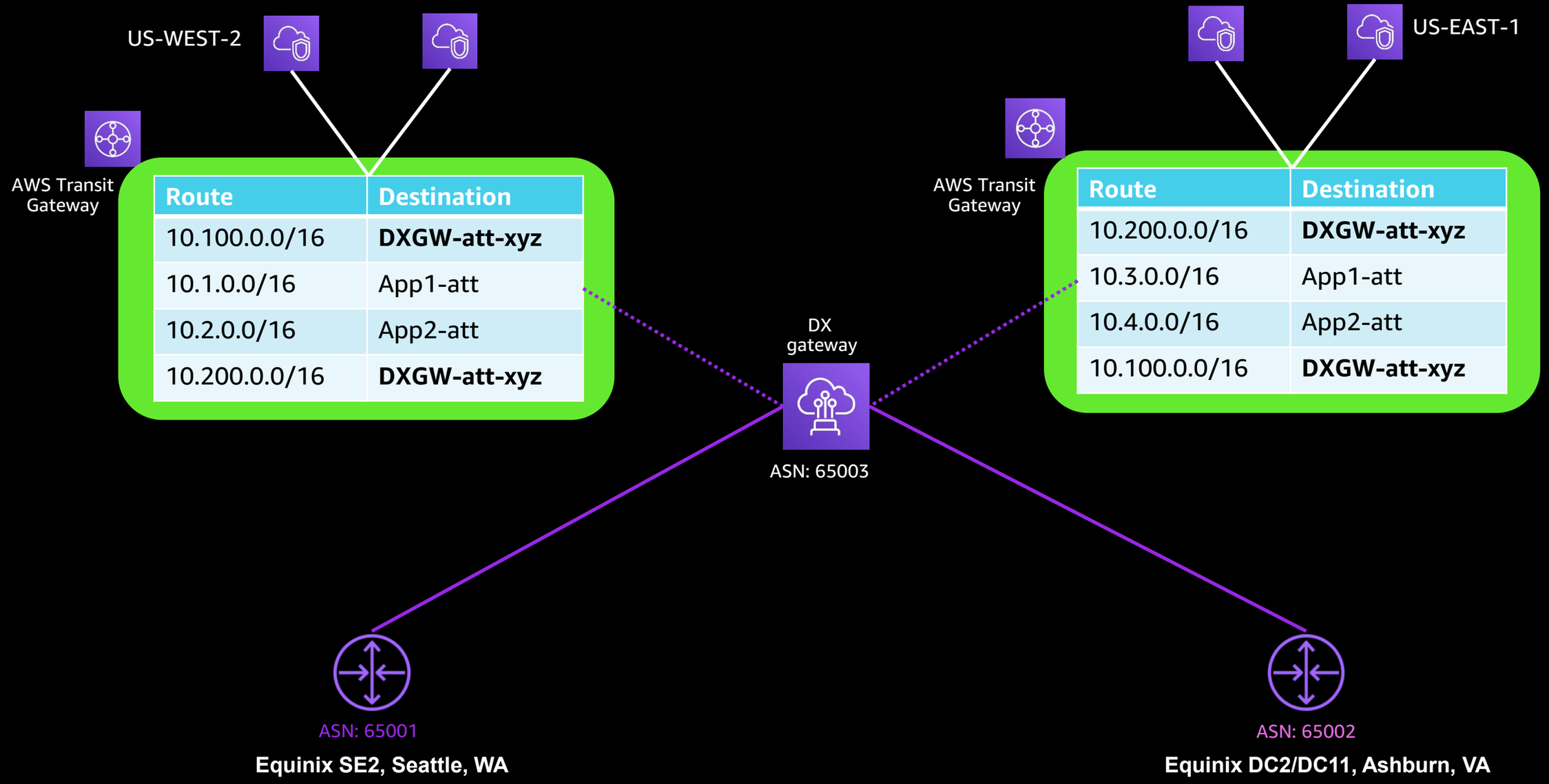
3. You can choose to enable VPC propagation or rely on static routes

4. You need a return path if the destination VPC requires a different connectivity pattern

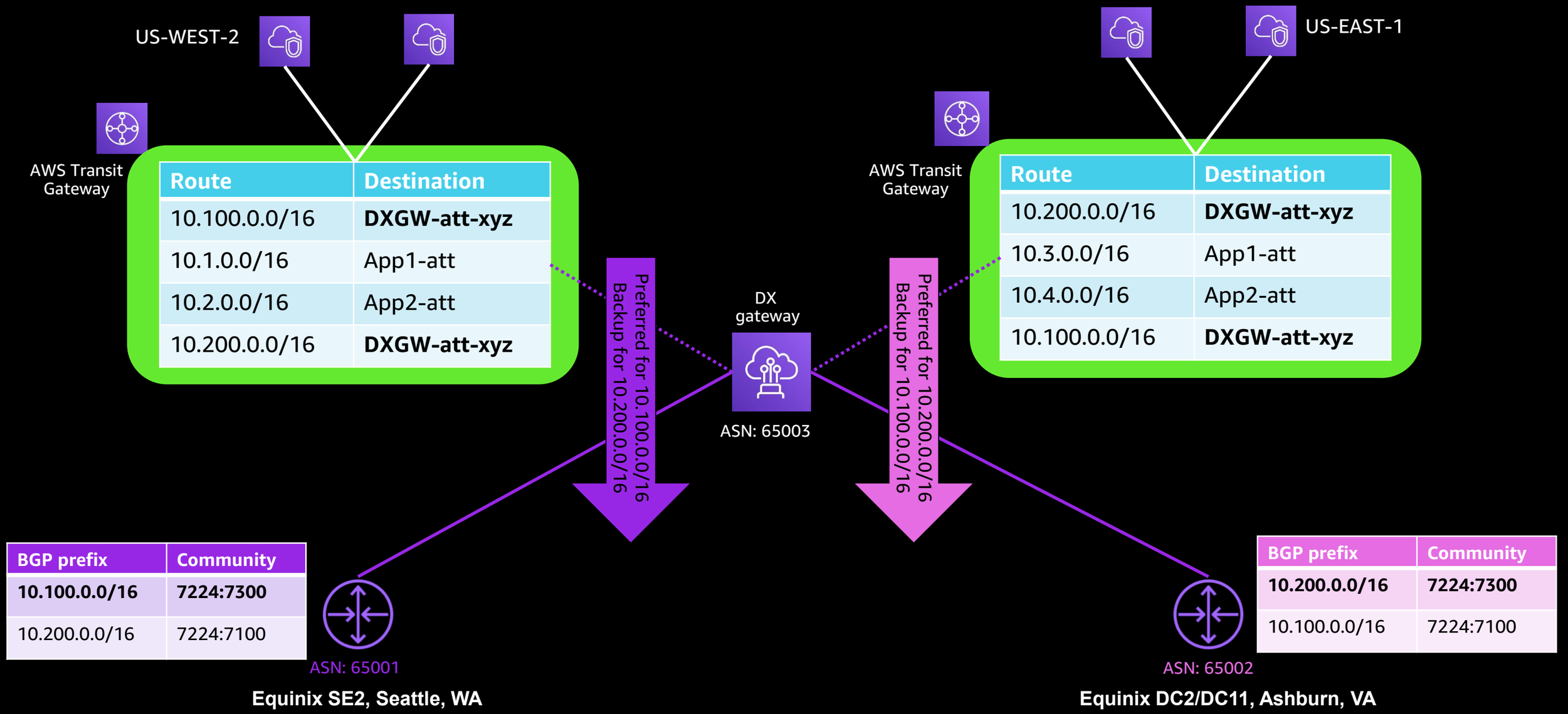
Controlling access



AWS Transit Gateway + DX gateway connectivity



AWS Transit Gateway + DX gateway connectivity



AWS Transit Gateway best practices

1. Use different ASNs per region for transit gateways

2. Do you have redundancy – device, location and application? Do you have AWS Transit Gateway attachments in multiple Availability Zones?

3. Use local-preference communities to ensure predictable active and backup paths

4. Limit the number of transit gateway route tables

Cost consideration example

AWS Transit Gateway costs (N. Virginia)

- $0.05/hour per attachment ~$36.50/month
- **$0.02 per GB data processed**

Direct connect costs

- 0.30/hour port-hour rate (all locations except Japan) ~216/month
- **$0 Data transfer IN**
- $0.02 data transfer out (From N. Virginia to any US DX location)

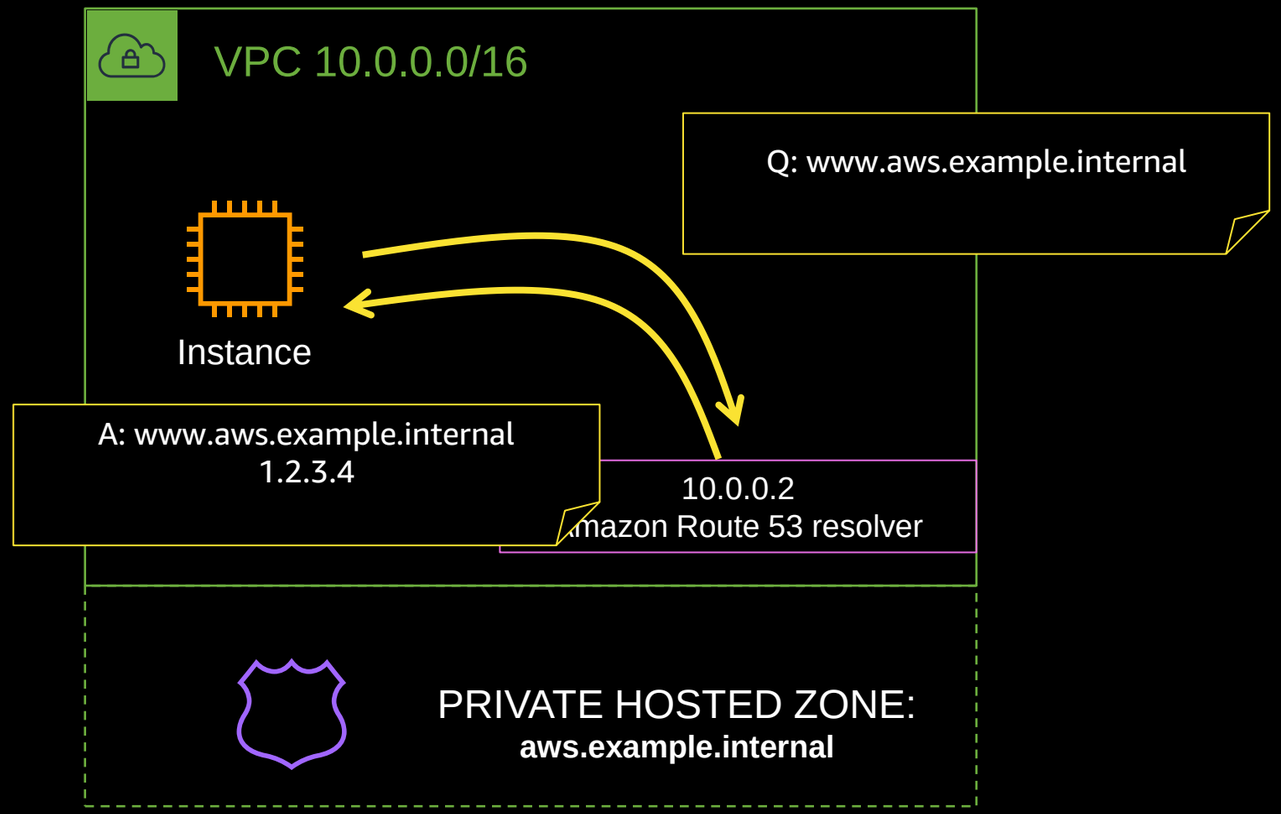
Scalable multi-VPC network architecture

Private DNS

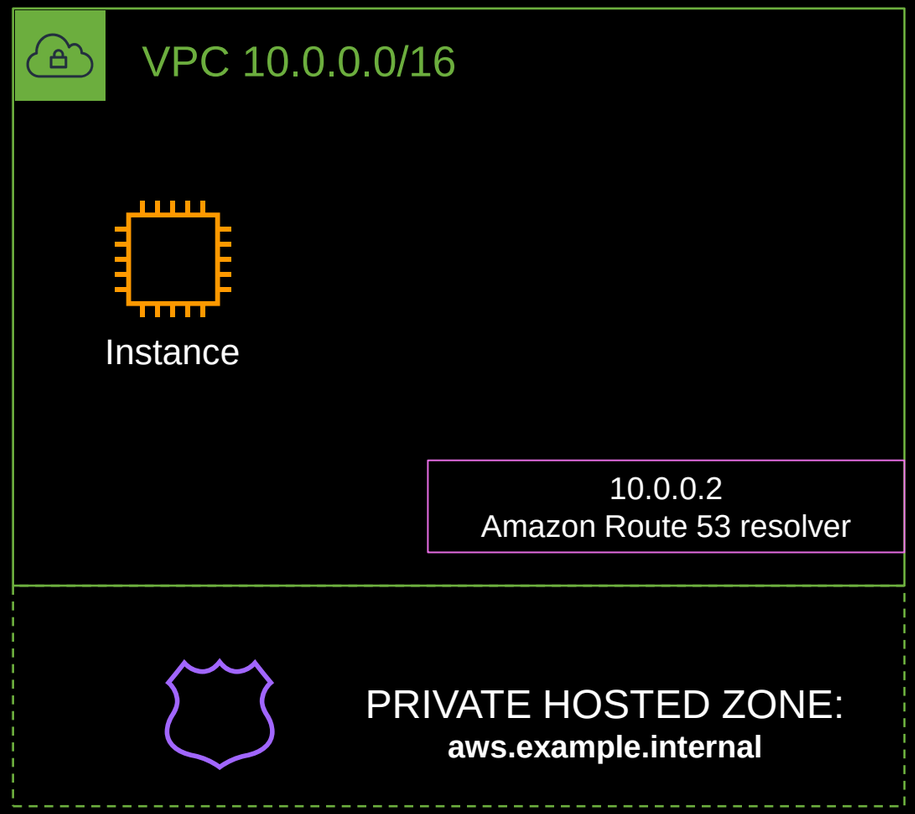


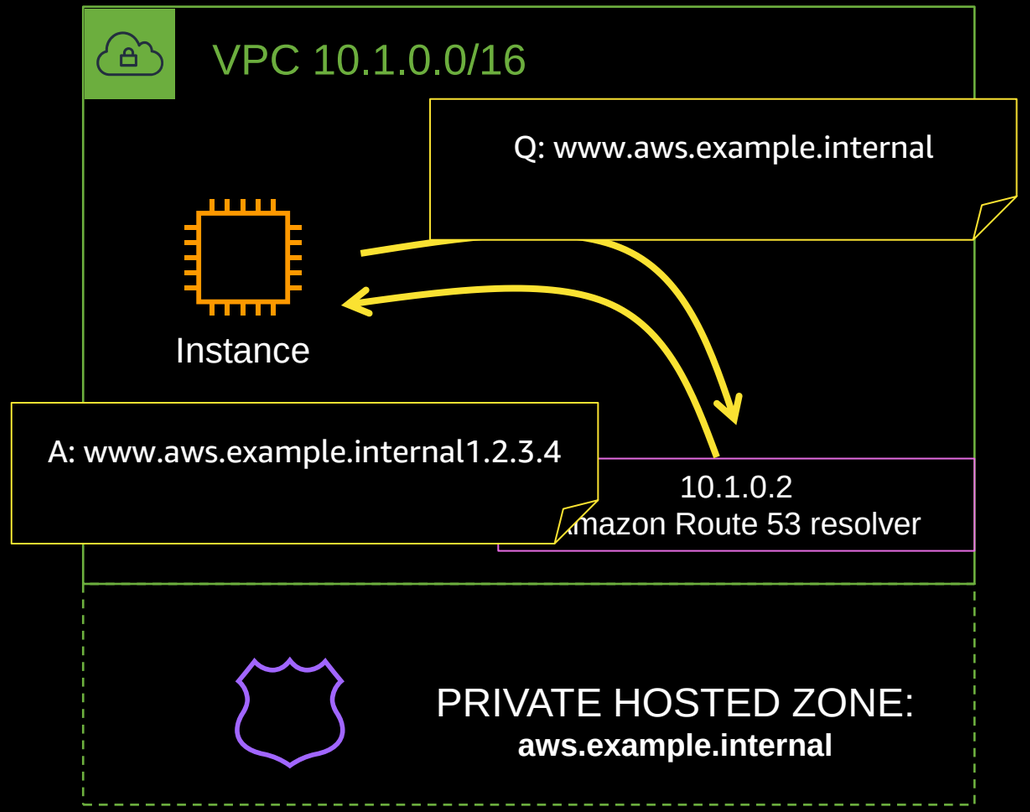
© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Resolving AWS domains within a VPC

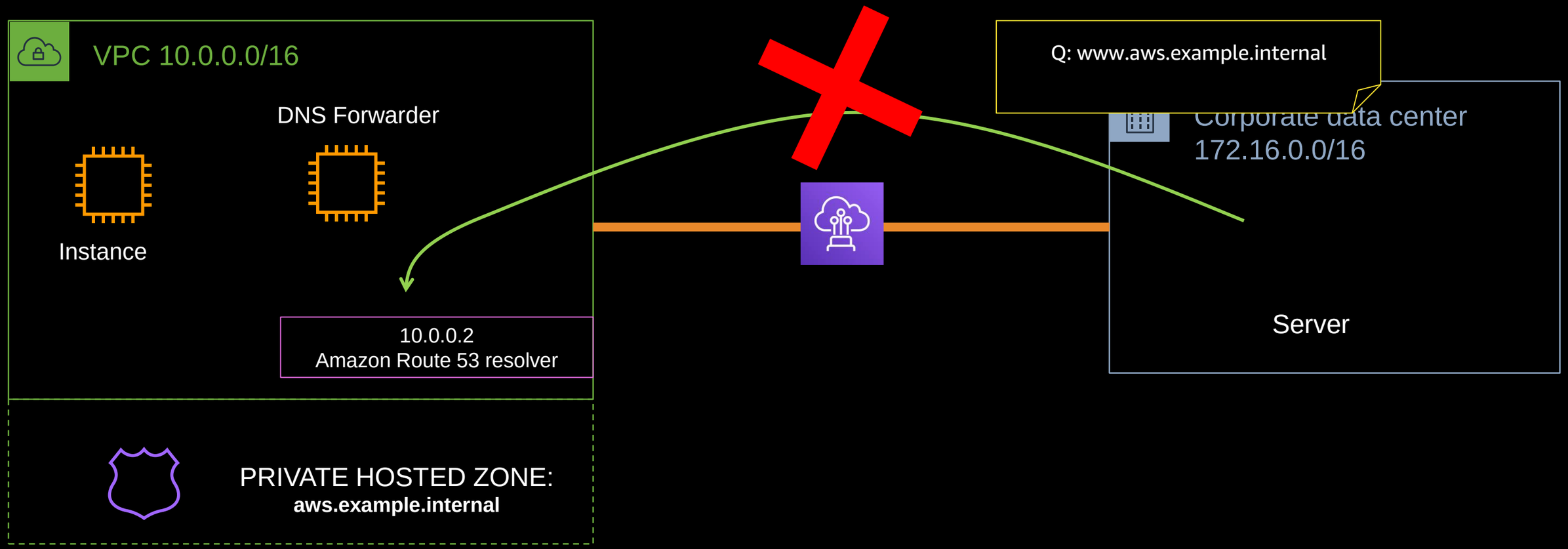


Associating AWS domains to other VPCs and AWS accounts





Resolving AWS domains in hybrid environments



Challenges



Self-build

Undifferentiated heavy lifting



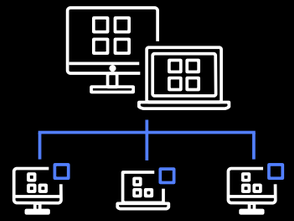
Limits

ENI limit can be a bottleneck



Failures

Instance failure impacts entire VPC



Isolation

AZ problem can impact entire VPC

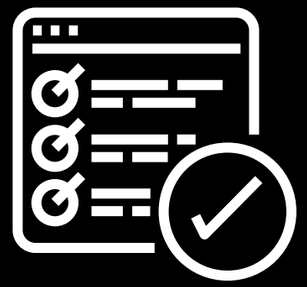
Route 53 resolver rules



Managed DNS resolver service from Route 53

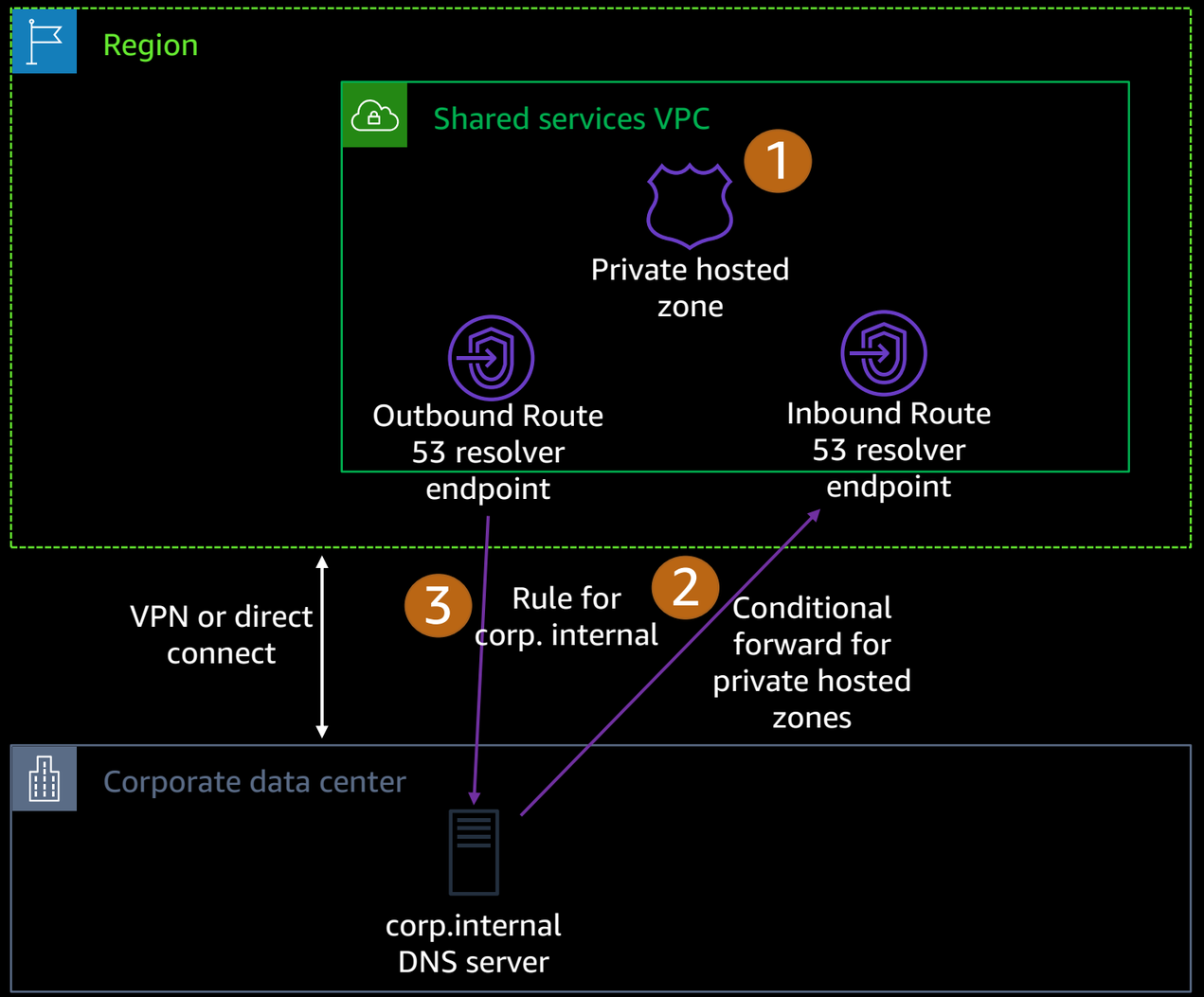


Enables hybrid DNS resolution over DX and managed VPN



Create conditional forwarding rules to re-direct query traffic

How does this work?



- Managed
- Increased resiliency
- 10K QPS per IP per Resolver endpoint
- Scalable

Common questions

1. Are Resolver endpoints regional?

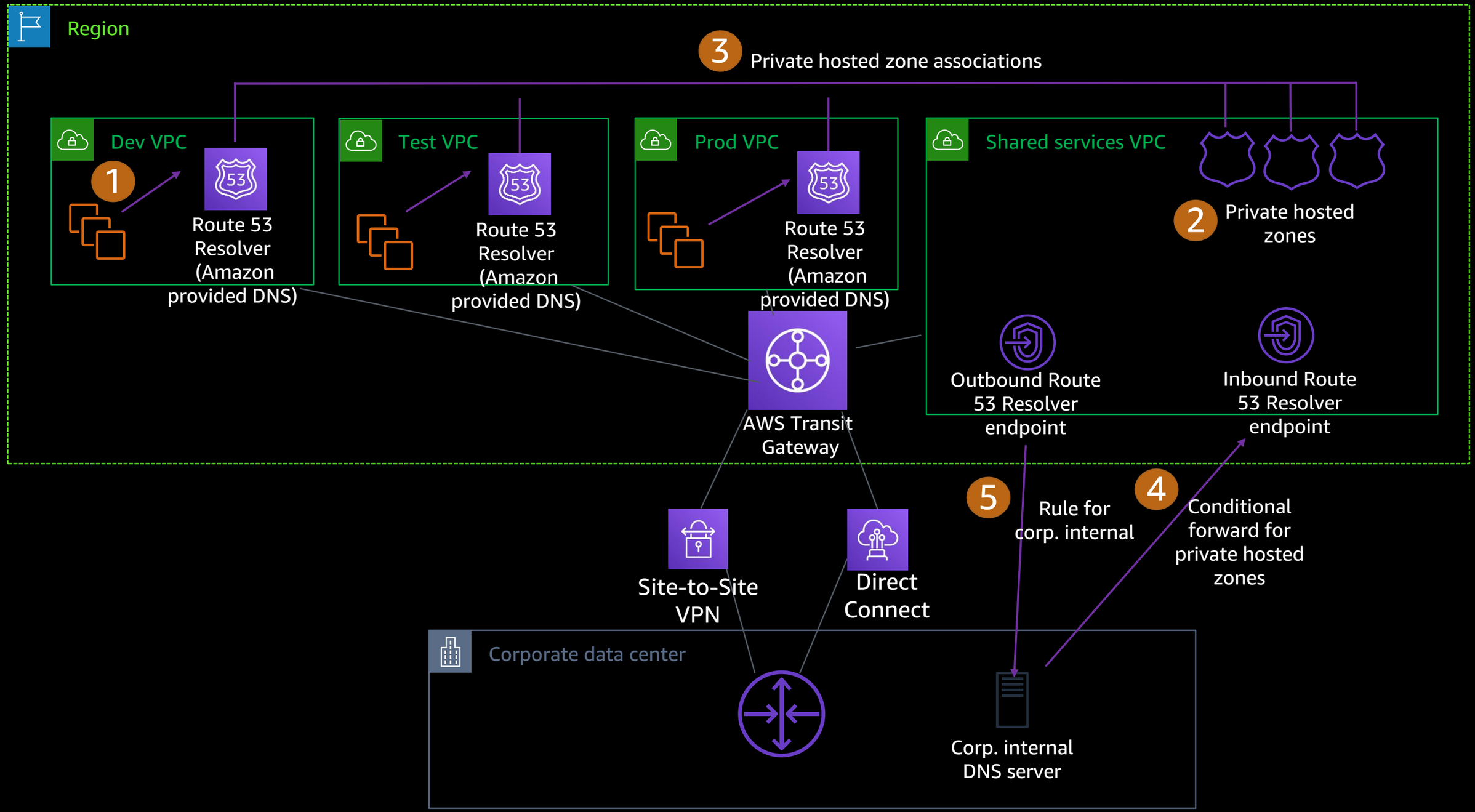
   Yes

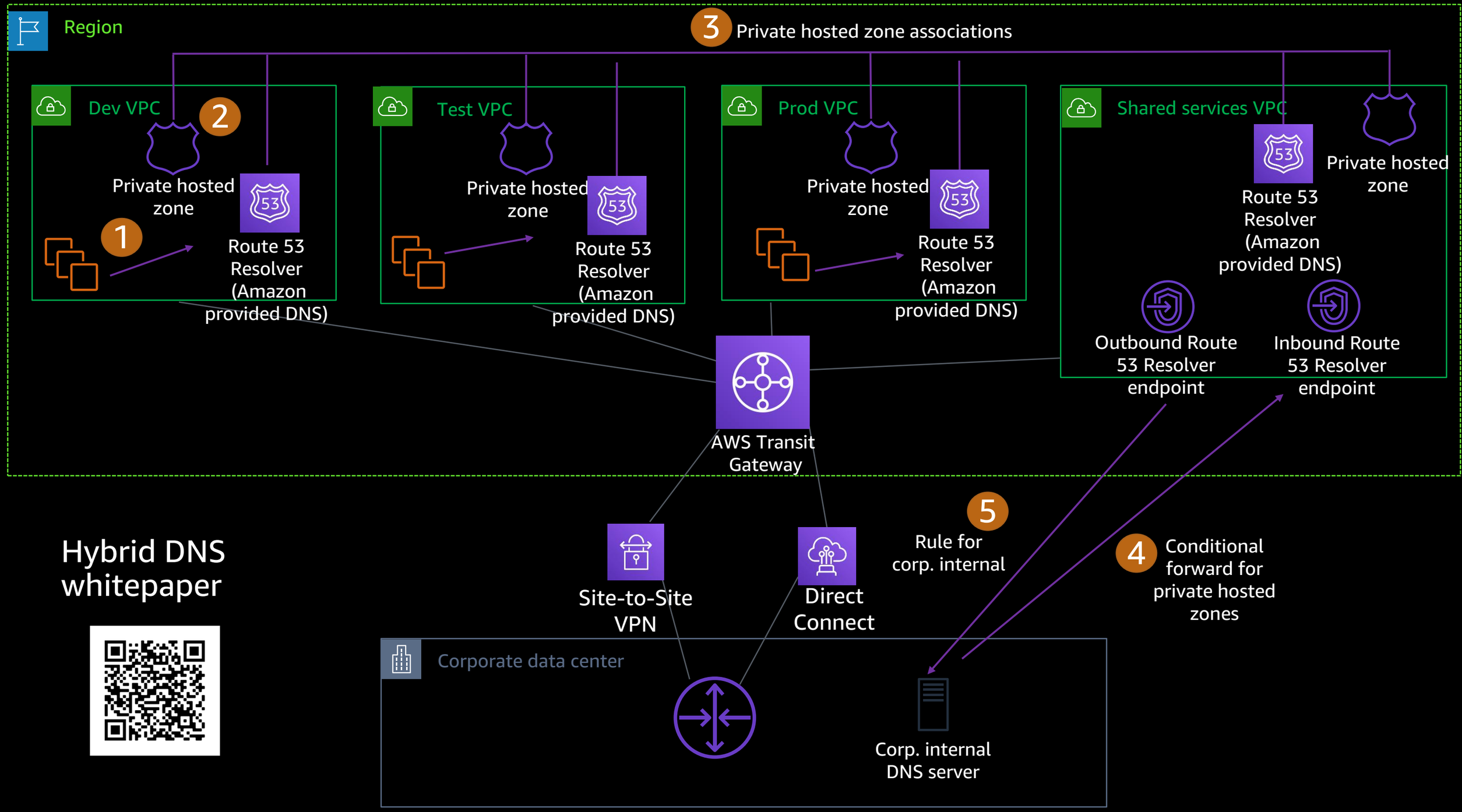
2. Unique endpoints for each VPC / Account?

   Not really

   Use Private Hosted Zone associations for inbound endpoints

   Use Resolver rule sharing via Resource Access Manager for outbound endpoints


Region
3
Private hosted zone associations
Dev VPC
1
Route 53 Resolver (Amazon provided DNS)
Test VPC
Route 53 Resolver (Amazon provided DNS)
Prod VPC
Route 53 Resolver (Amazon provided DNS)
Shared services VPC
2
Private hosted zones
AWS Transit Gateway
Outbound Route 53 Resolver endpoint
Inbound Route 53 Resolver endpoint
5
Rule for corp. internal
4
Conditional forward for private hosted zones
Site-to-Site VPN
Direct Connect
Corporate data center
Corp. internal DNS server


Region
3
Private hosted zone associations
Dev VPC
2
Private hosted zone
1
Route 53 Resolver (Amazon provided DNS)
Test VPC
Private hosted zone
Route 53 Resolver (Amazon provided DNS)
Prod VPC
Private hosted zone
Route 53 Resolver (Amazon provided DNS)
Shared services VPC
Route 53 Resolver (Amazon provided DNS)
Private hosted zone
Outbound Route 53 Resolver endpoint
Inbound Route 53 Resolver endpoint
AWS Transit Gateway
Hybrid DNS whitepaper
Site-to-Site VPN
Direct Connect
5
Rule for corp. internal
4
Conditional forward for private hosted zones
Corporate data center
Corp. internal DNS server

Route 53 resolver best practices

1. High availability
   a. Use resolver ENIs in multiple availability zones
2. Use forwarding sparingly
   a. Use Amazon provided DNS for Amazon EC2 instances
   b. Prefer associating private hosted zones / rules to all VPCs
   c. Keep queries within the local availability zone where possible
3. Monitoring
   a. Set Amazon CloudWatch alarms approaching QPS limits
4. DNS query logging
   a. For compliance, monitoring query behavior or spot DNS security threats

Takeaways and final thoughts

- Use services in combination to meet your specific requirements
- Be nimble with your architecture
- Design AWS private IP address ranges without overlapping CIDRs
- Test and validate

Resources

Cloud migration homepage: https://aws.amazon.com/cloud-migration/

Additional migration resources, AWS Prescriptive Guidance, AWS Enterprise Blog Collection: https://aws.amazon.com/cloud-migration/resources/

Migration Immersion Day: https://migration-immersionday.workshop.aws/en

All AWS workshops available here: https://www.workshops.aws/

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.