AWS re:Invent

NET411-R

Managing DNS across hundreds of VPCs

Matt Johnson
Solution Architect Manager
Amazon Web Services

Gavin McCullagh
Principal System Development Engineer
Route 53
Amazon Web Services

AWS re:Invent

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

aws

What are your challenges with VPC DNS?

Amazon Route 53 private DNS: Overlapping zone support

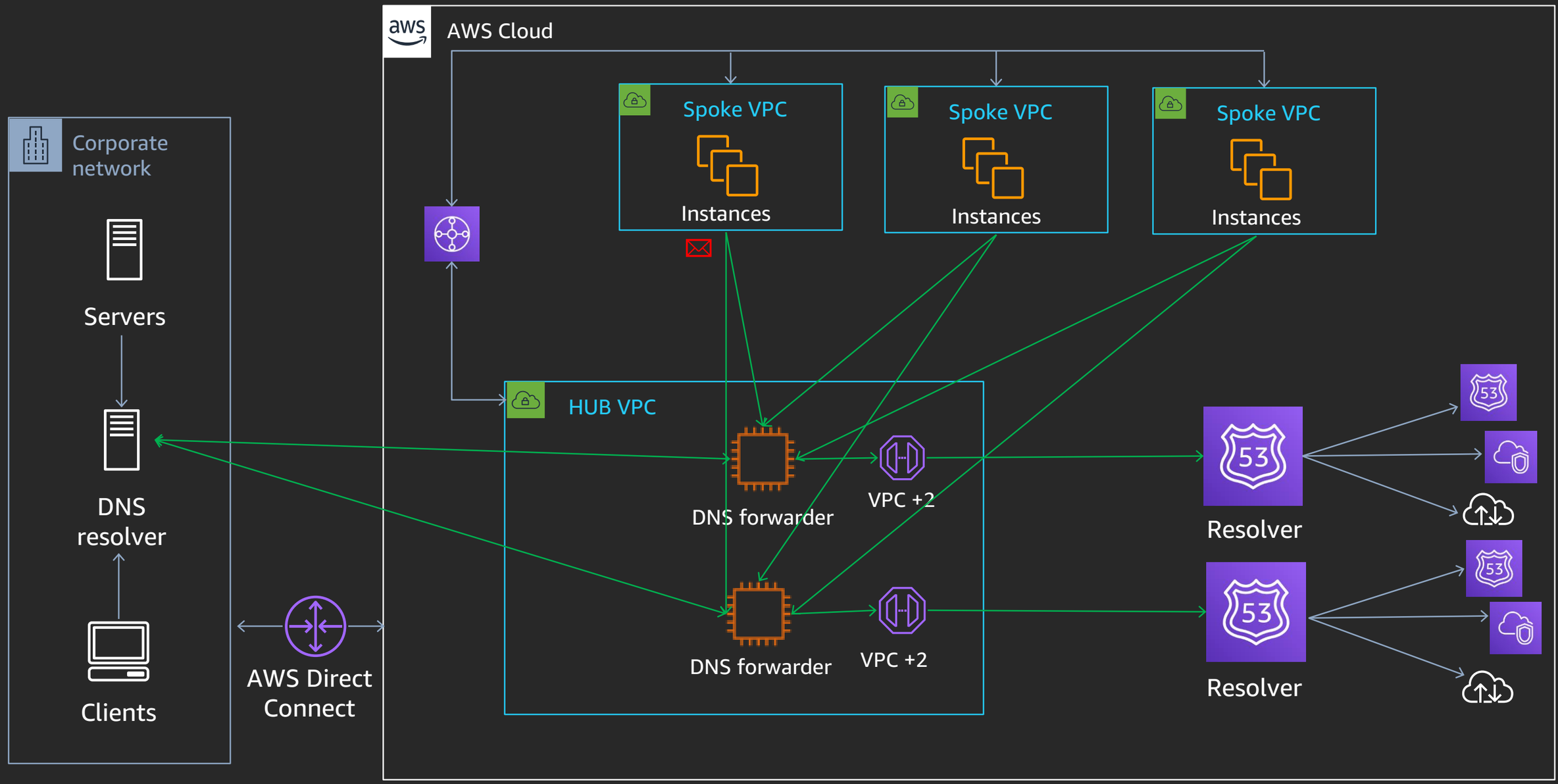
Launched November 2019

Private DNS now supports overlapping private hosted zones

Example: 1 VPC with

- example.com
- service1.example.com
- service2.example.com

Hub and spoke strategy (forwarding instances)



Forwarding instances: The good



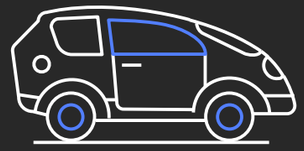
Works

Integrates VPC and on-premises DNS



Cost

Reusable across VPCs



Performant

Caching improves latency



Flexible

Configure logging, RPZ, AXFR, and so on

Forwarding instances: Challenges



Self-build

Build, maintain undiff. heavy lifting



Limits

ENI limit can be a bottleneck



Failures

Instance/AZ failure impacts entire VPC

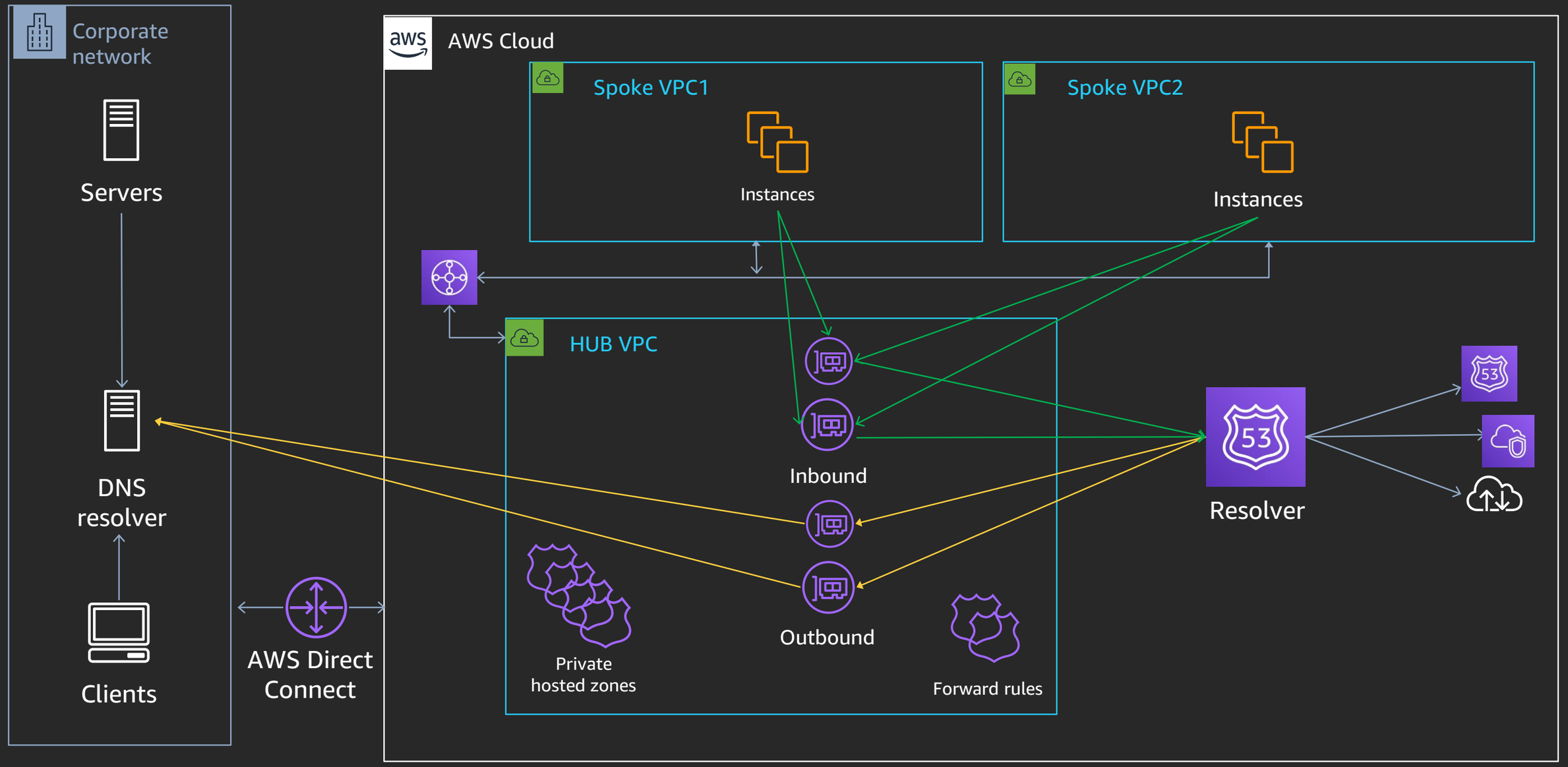
Hub and spoke strategies (Route 53 resolver)

4 strategies have emerged in the community

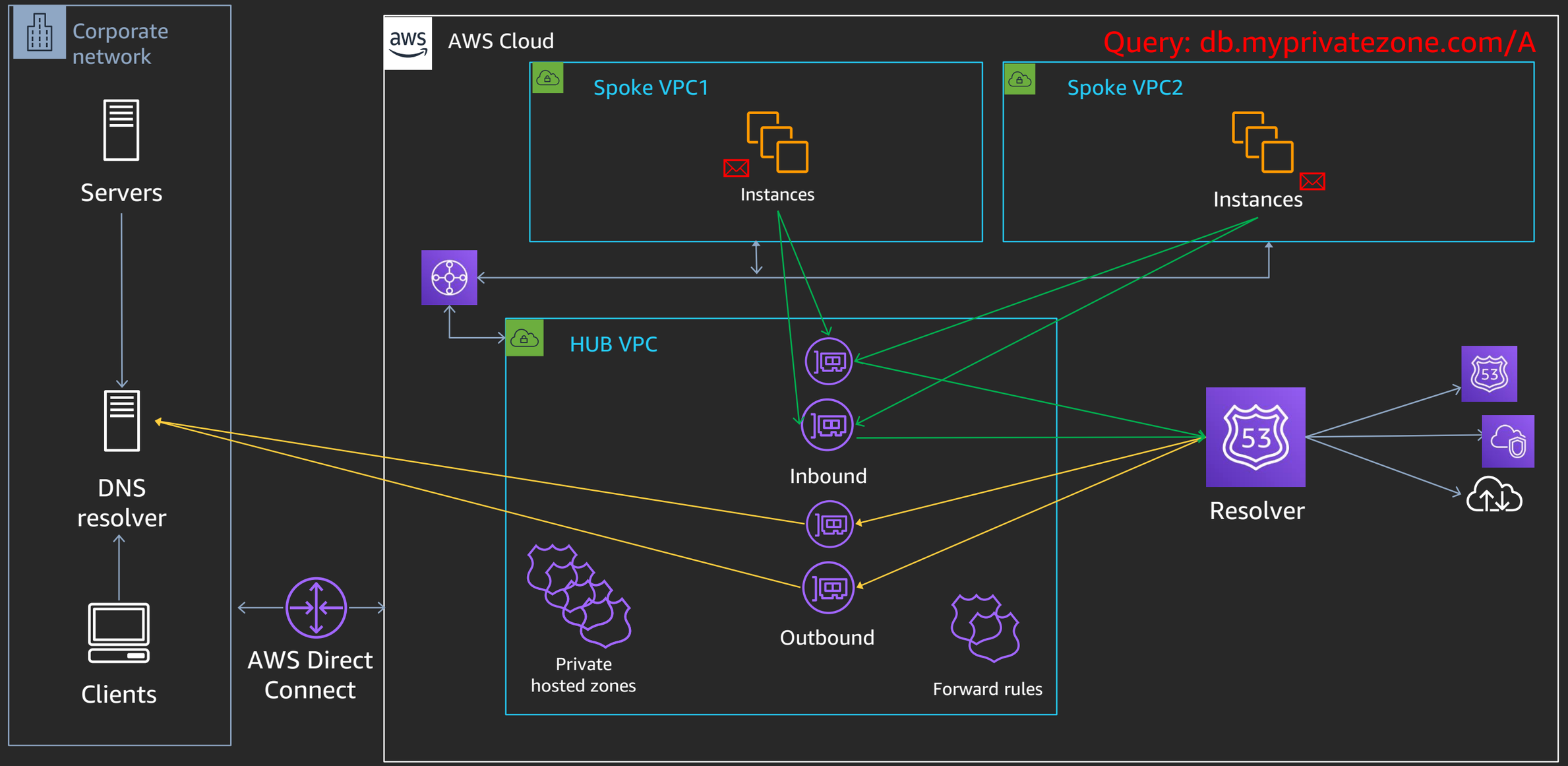
1. Manage hub DNS and change spoke DHCP nameservers
2. Manage hub DNS and forward queries using endpoints
3. VPC sharing
4. Share and associate private zones and resolver rules

How do they compare?

1. Manage hub DNS; change spoke DHCP



1. Manage hub DNS; change spoke DHCP



1. Manage hub DNS; change spoke DHCP

Pros

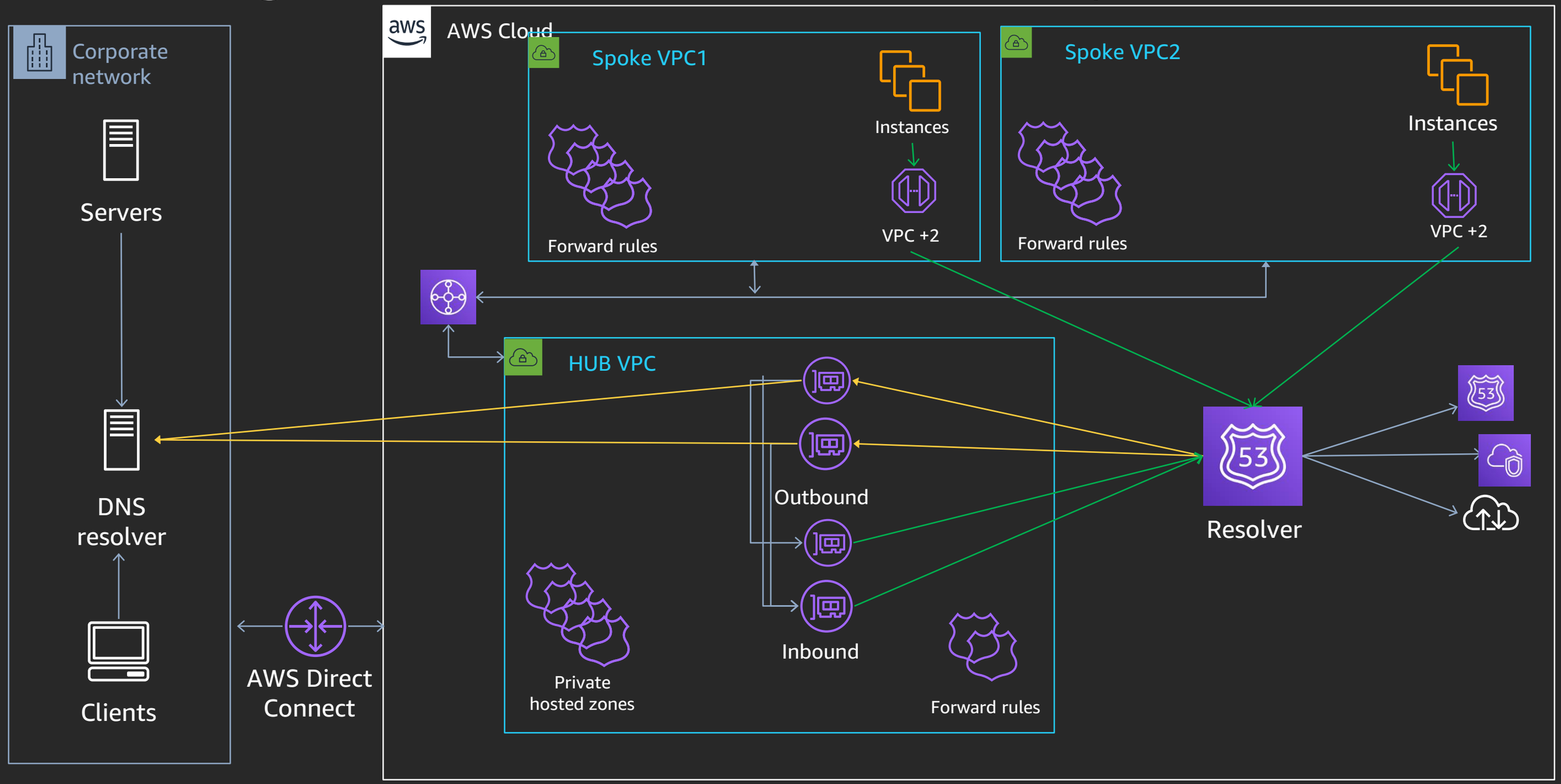
- Easier setup
- Familiar (like forwarding instances)

Cons

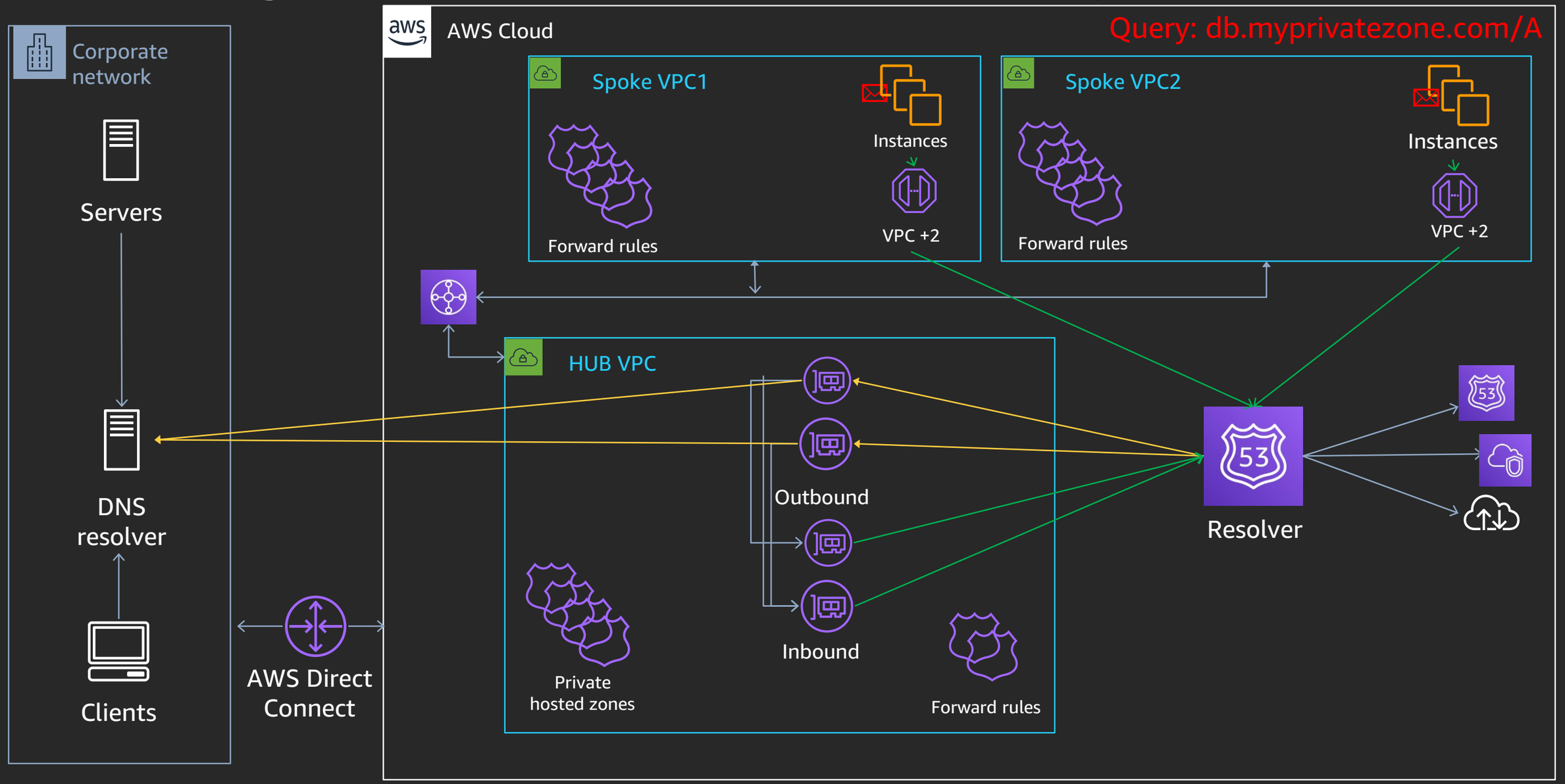
- No local cache
- All queries via 10K limit
- Most queries cross between AZs
- Expect hot-spotting on a single ENI
- Requires L3 connectivity between spokes and hub

Verdict: Not recommended

2. Manage hub DNS; forward via endpoints



2. Manage hub DNS; forward via endpoints



2. Manage hub DNS; forward via endpoints

Pros

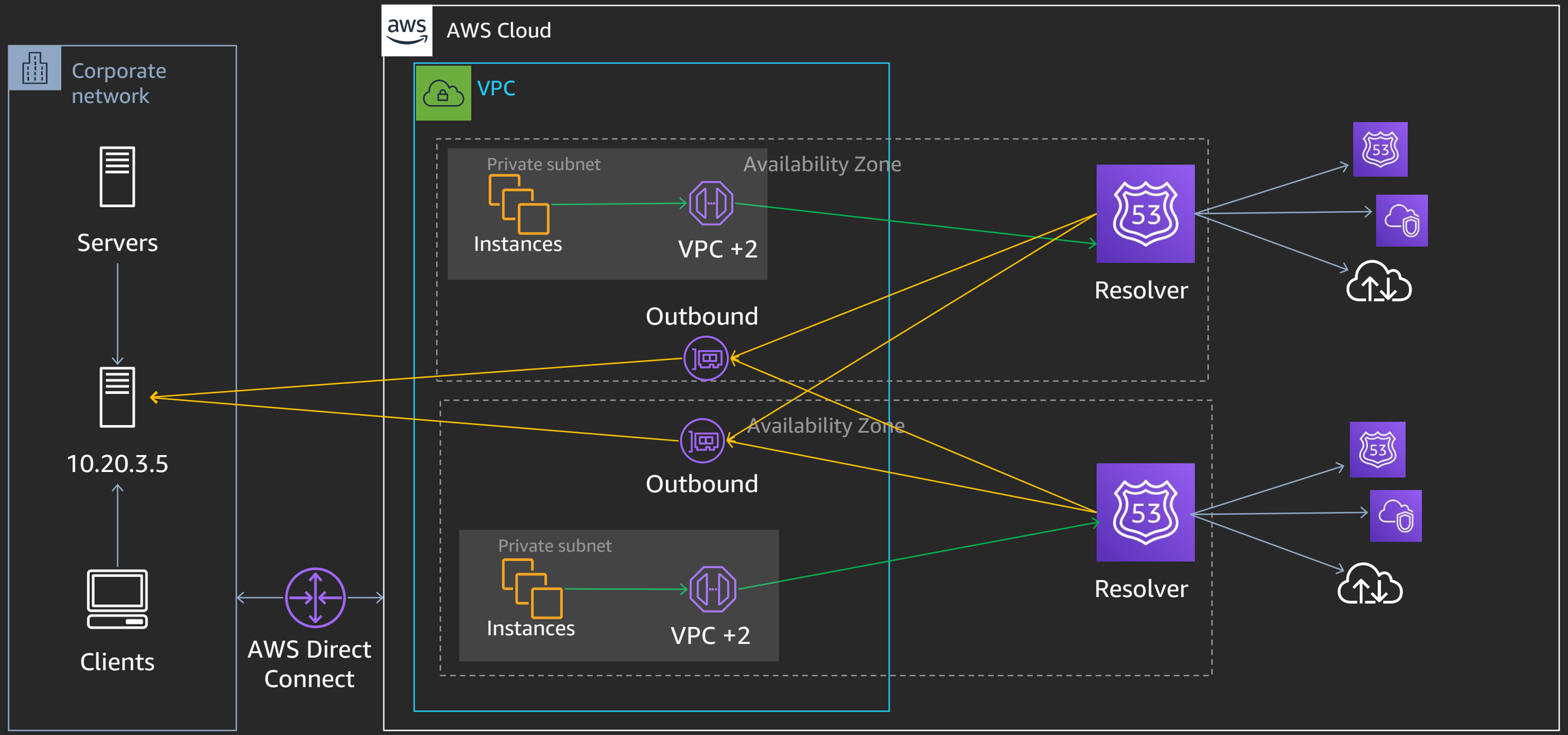
- Easier setup/maintenance
- Uses local +2 resolver, cache
- Nonforwarded queries use a scalable path

Cons

- Less Scalable (10K limit ×2)
- Each query crosses between AZs up to 4 times
- Not as resilient after failure

Verdict: Compromise but may be useful

3. VPC sharing



3. VPC sharing

Pros

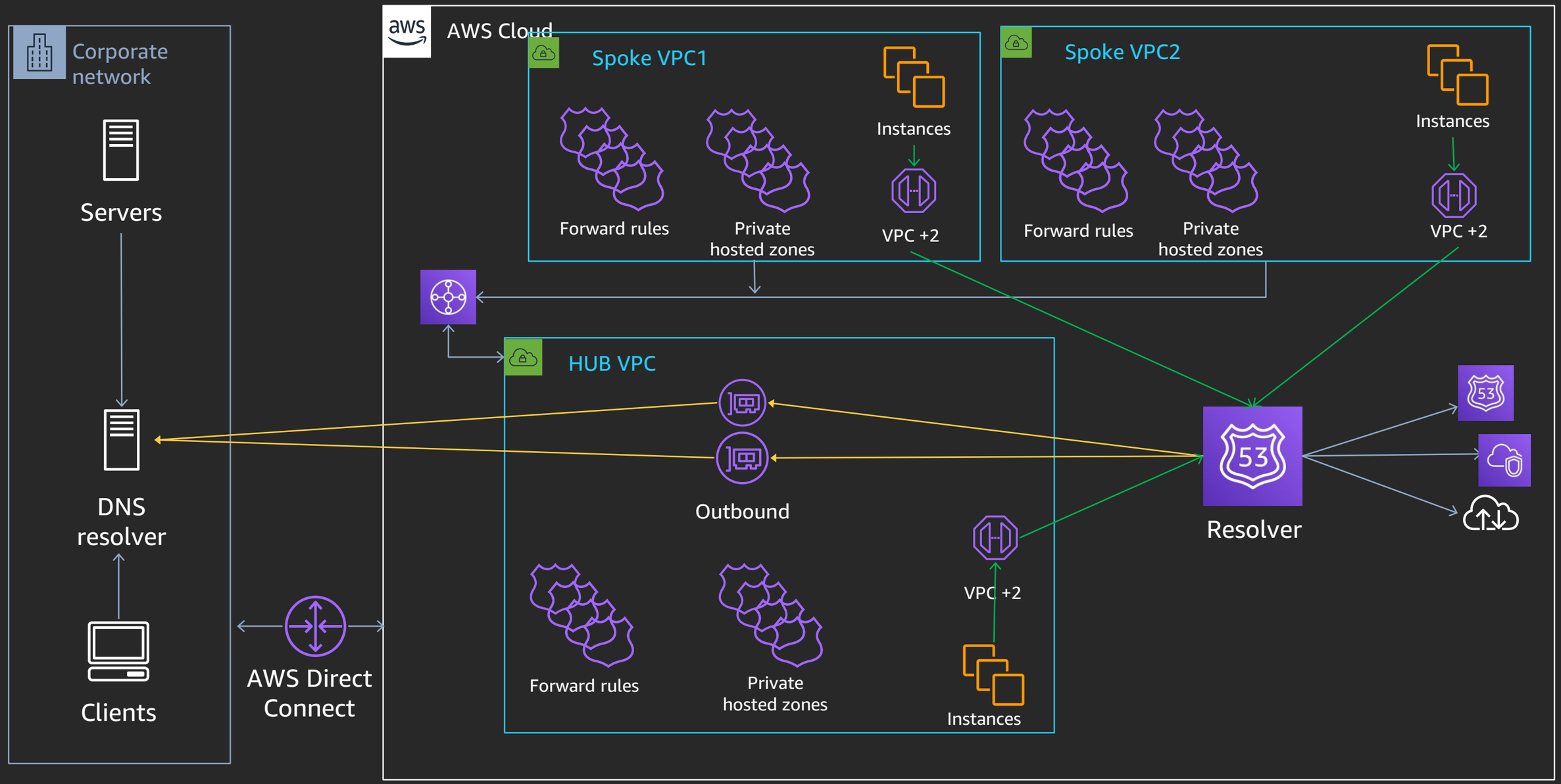
- Don’t have hundreds of VPCs
- Only 1 resolver; guaranteed consistent view of DNS
- Simplified networking

Cons

- Not 100% feature parity today
- Reduced autonomy for dev teams

Verdict: Best practice

4. Share and associate zones and rules



4. Share and associate zones and rules

Pros

- Most resilient and scalable
- Uses the VPC+2 endpoint, local caching, AZ isolation
- Minimal forwarding hops

Cons

- Management is cumbersome
- Limits on VPC associations per private hosted zone

Verdict: Best practice

Route 53 resolver best practices

1. Use resolver ENIs in multiple AZs
2. Use AmazonProvidedDNS for EC2 instances
3. Use forwarding, but only when necessary
4. Prefer associating private hosted zones to all VPCs
5. Keep queries within the local AZ wherever possible
6. Monitor limits on resolver endpoints

Managing DNS across many VPCs

Large customers often have:

- Central infrastructure team managing networking and DNS
- Many dev teams, separate AWS accounts, and VPCs
- Peering or AWS Transit Gateway interconnecting
- Hub and spoke network architecture
- Require a shared, coherent DNS view

Managing DNS centrally can be challenging

Thank you!

AWS re:Invent

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

aws



Please complete the session survey in the mobile app.

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.