AWS re:Invent

NET410

Deep dive on DNS in the hybrid cloud

Gavin McCullagh

Principal System Development Engineer
Amazon Route 53
Amazon Web Services

Agenda

Route 53 Resolver in VPCs

Hybrid clouds

Route 53 Resolver inbound endpoints

Route 53 Resolver outbound endpoints & rules

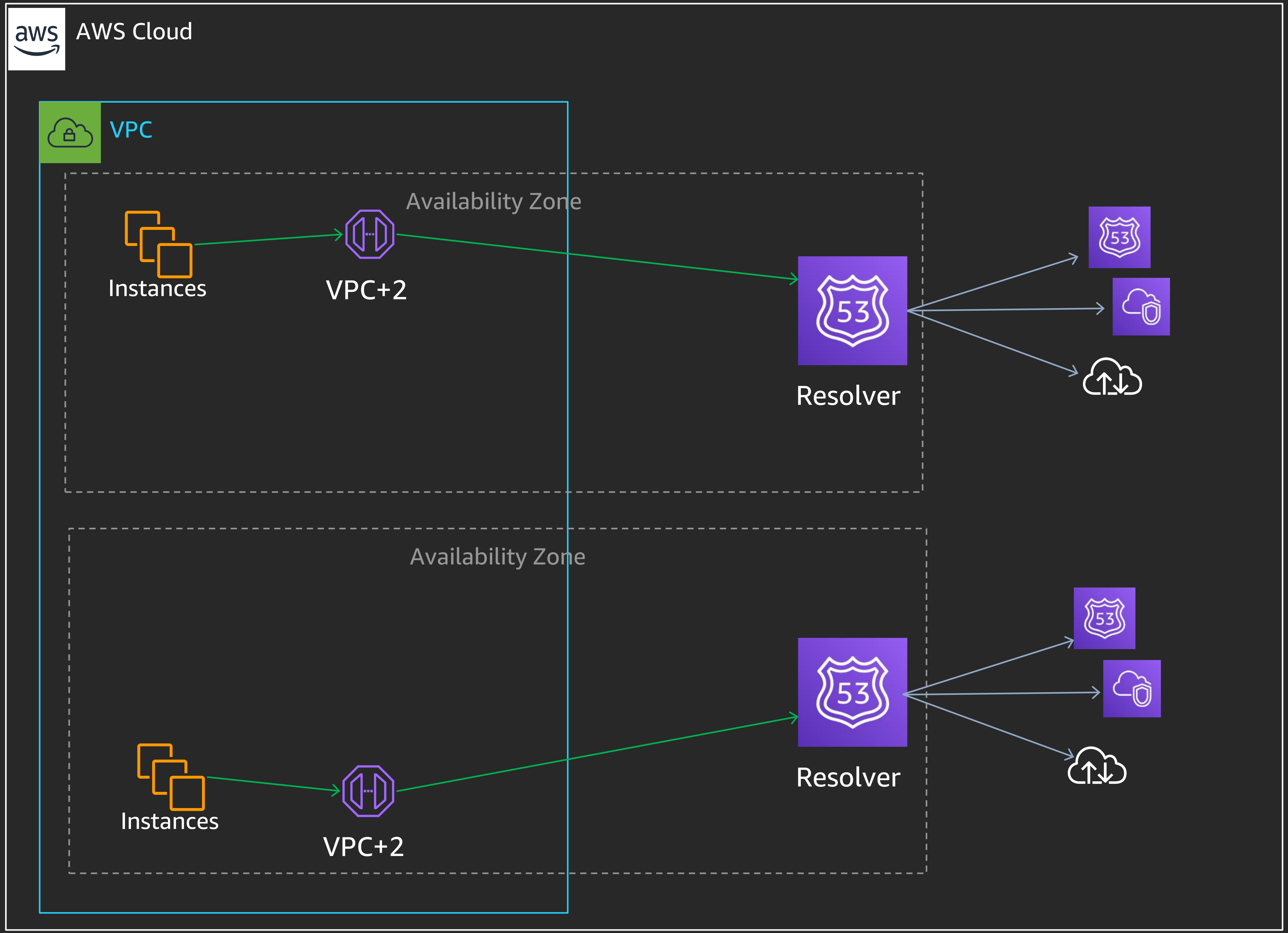
Route 53 Resolver & Active Directory

Managing DNS across many VPCs

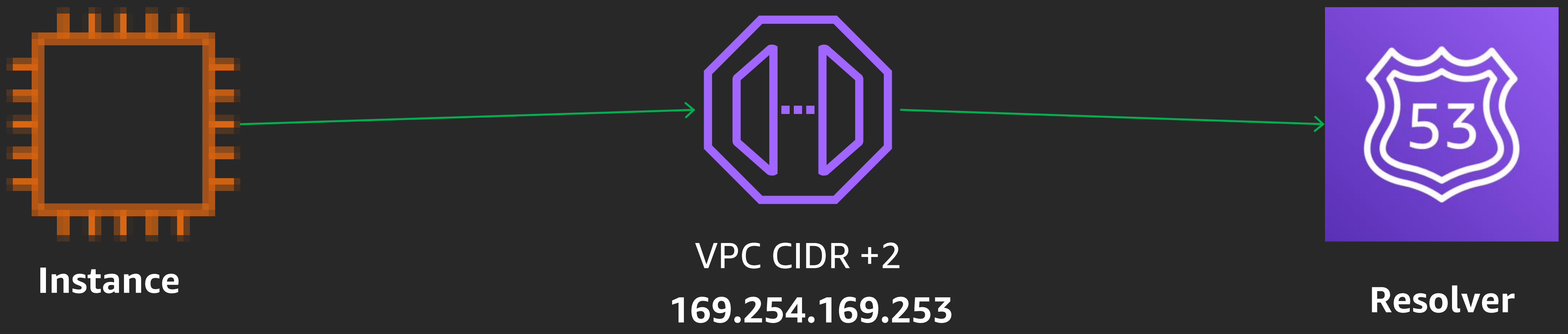
Route 53 Resolver

What is Route 53 Resolver?

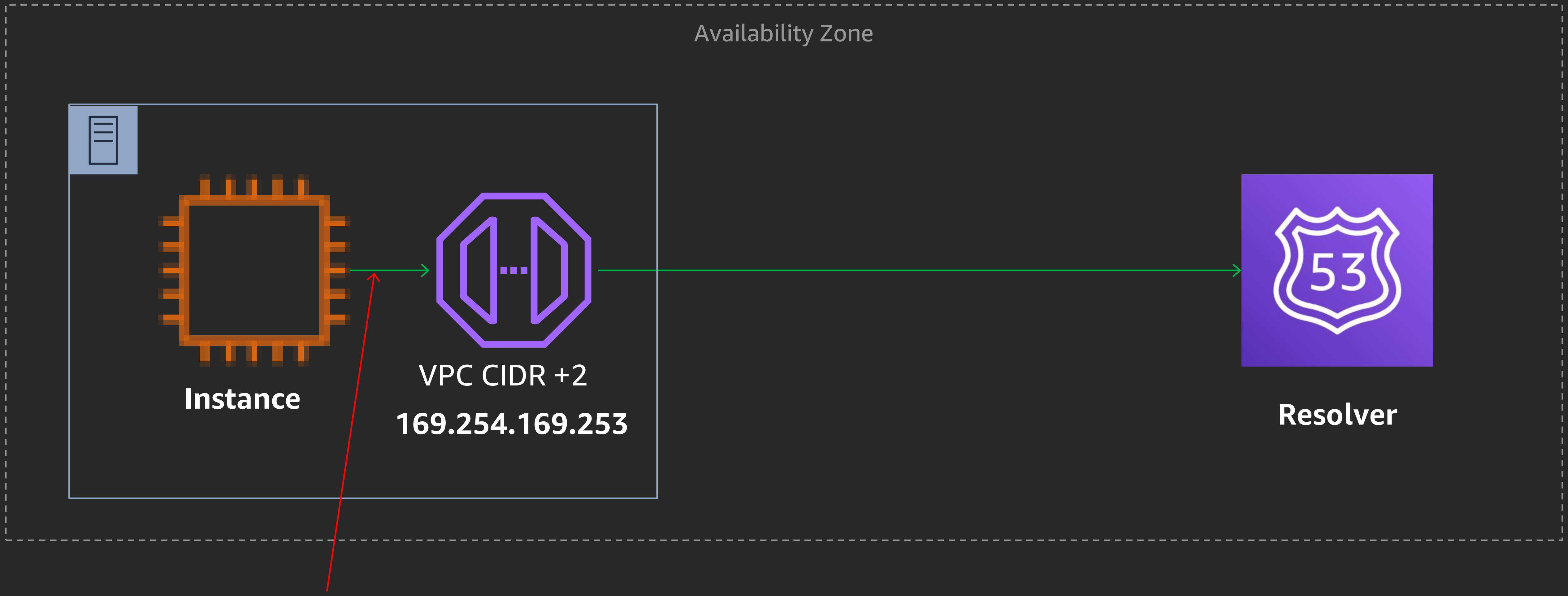
- The EC2 DNS Resolver needed an official name
- Route 53 Resolver is sometimes known as:
  - AmazonProvidedDNS
  - VPC Resolver
  - +2 Resolver
  - .2 Resolver
  - EC2 DNS Resolver
- New features in Q4 2018:
  - Resolver endpoints
  - Resolver forwarding rules


AWS Cloud
VPC
Availability Zone
Instances
VPC+2
Resolver
Availability Zone
Instances
VPC+2
Resolver

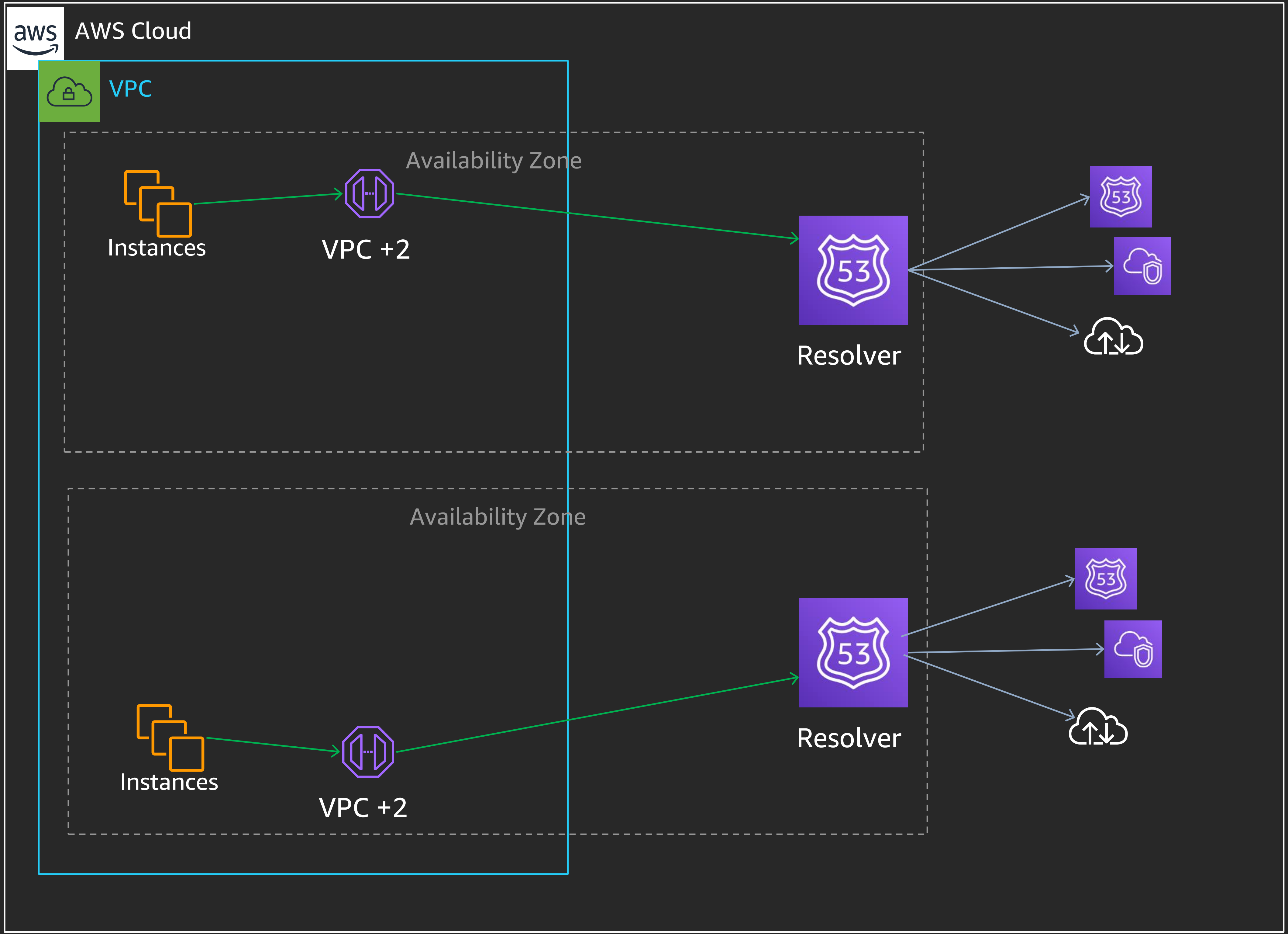
Route 53 Resolver

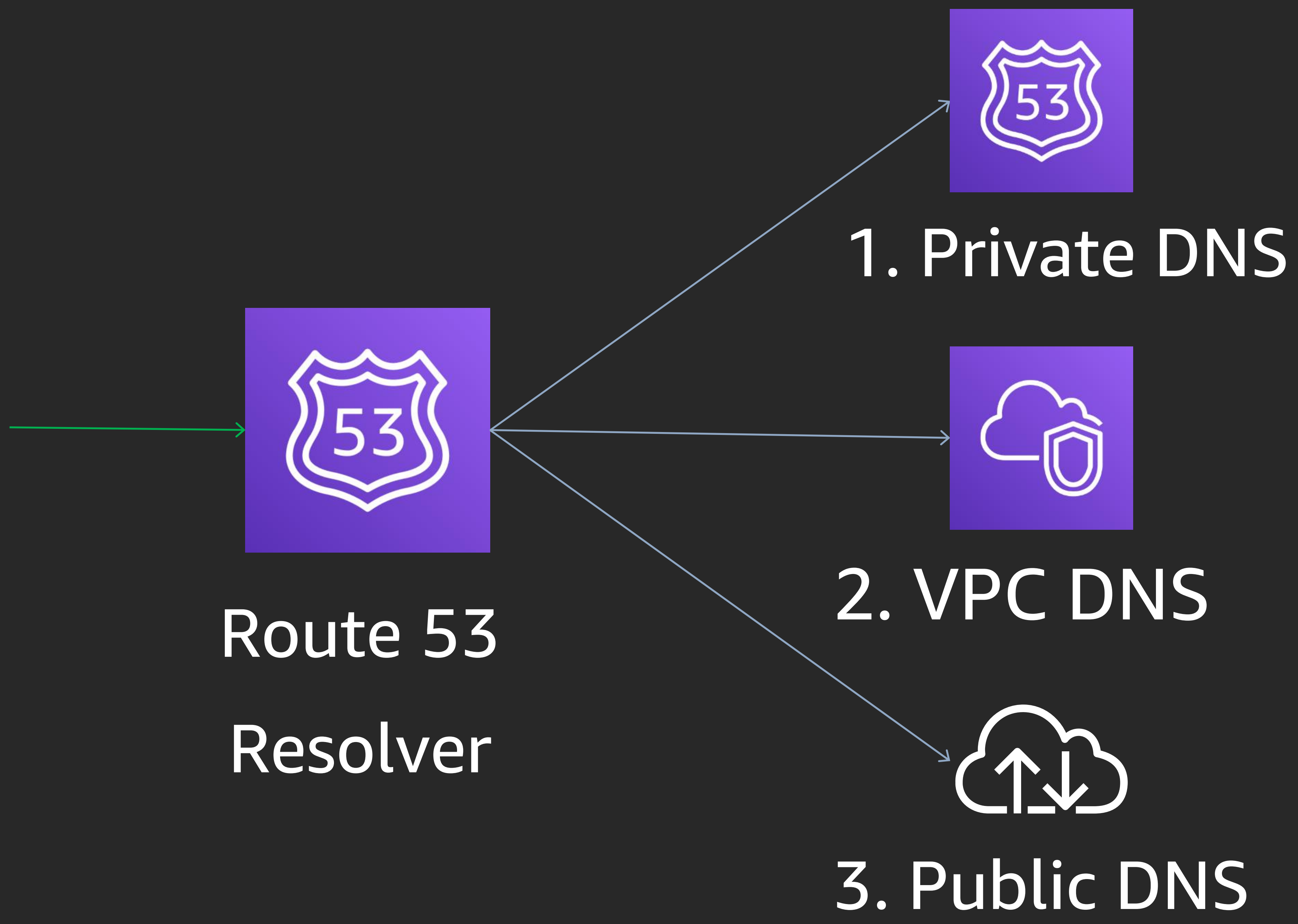


Route 53 Resolver



1024pps Limit Per ENI


AWS Cloud
VPC
Availability Zone
Instances
VPC +2
Resolver
Availability Zone
Instances
VPC +2
Resolver



1. Private DNS

Route 53

Resolver

2. VPC DNS

3. Public DNS

Route 53 Private DNS: How does it work?

1. Private DNS

Route 53 Resolver consumes Private Hosted Zone (PHZ) associations

If qname matches a PHZ, direct the query to Route 53 Private DNS

Private DNS takes higher priority than VPC DNS records

If you create a zone called “.”, all public and VPC DNS is overridden

Private DNS – Overlapping Zone Support

Launched November 2019!

Private DNS now supports overlapping Private Hosted Zones

e.g. mycompany.com and service.mycompany.com PHZs in one VPC

VPC DNS Names

2. VPC DNS

Defined special namespaces, e.g.:

- eu-west-2.compute.internal.
- 10.in-addr.arpa., 168.192.in-addr.arpa., {16..31}.172.in-addr.arpa.
- eu-west-2.compute.amazonaws.com.

```
ubuntu@ip-172-31-9-203:~$ dig SOA 1.16.172.in-addr.arpa @172.31.0.2  +noall +auth

; <<>> DiG 9.11.3-1ubuntu1.9-Ubuntu <<>> SOA 1.16.172.in-addr.arpa @172.31.0.2 +noall
+auth

;; global options: +cmd

in-addr.arpa. 60 IN SOA ns0.eu-west-2.compute.internal. hostmaster.amazon.com. 2012103100
3600 3600 3600 60
```

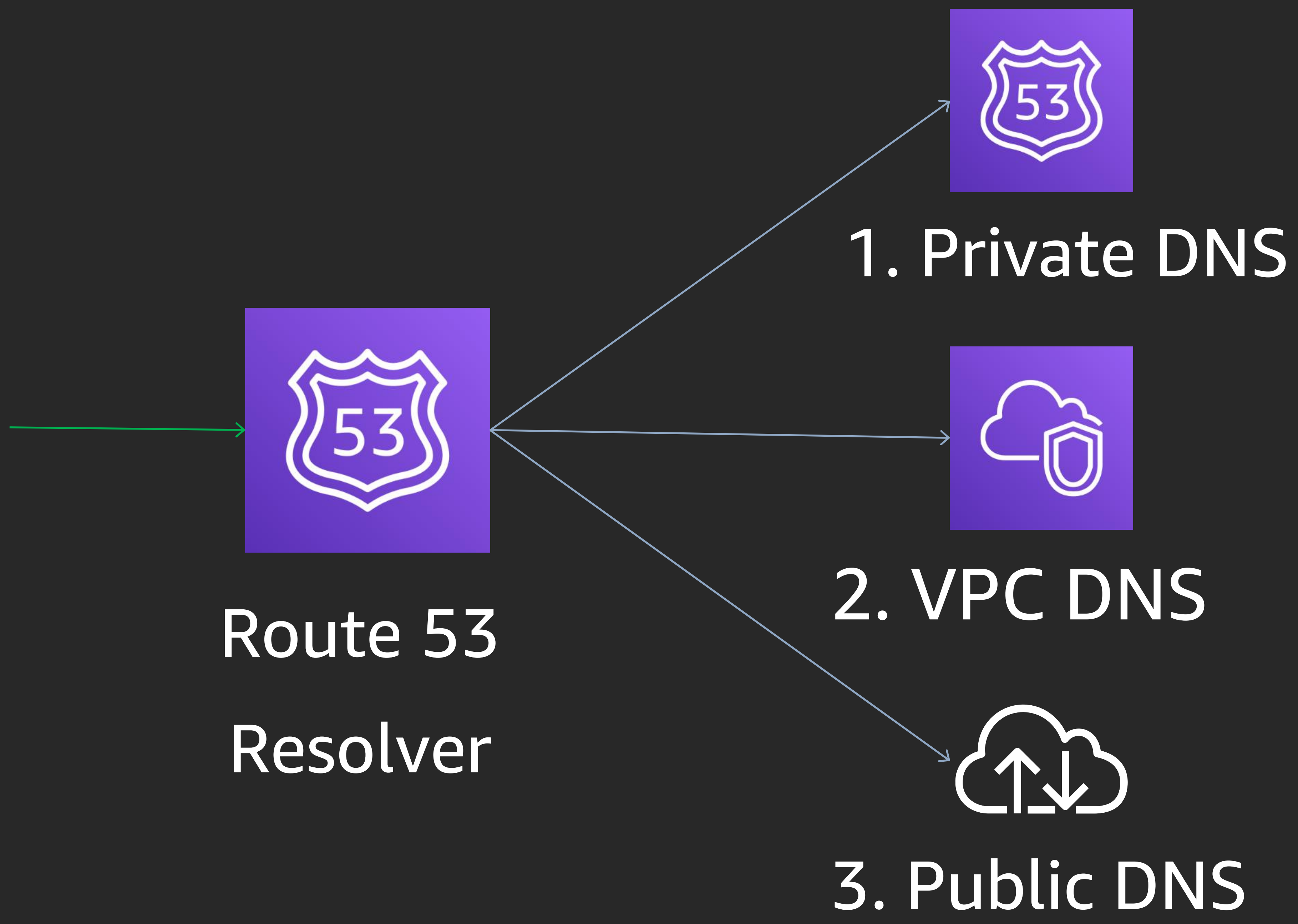
VPC DNS names

2. VPC DNS

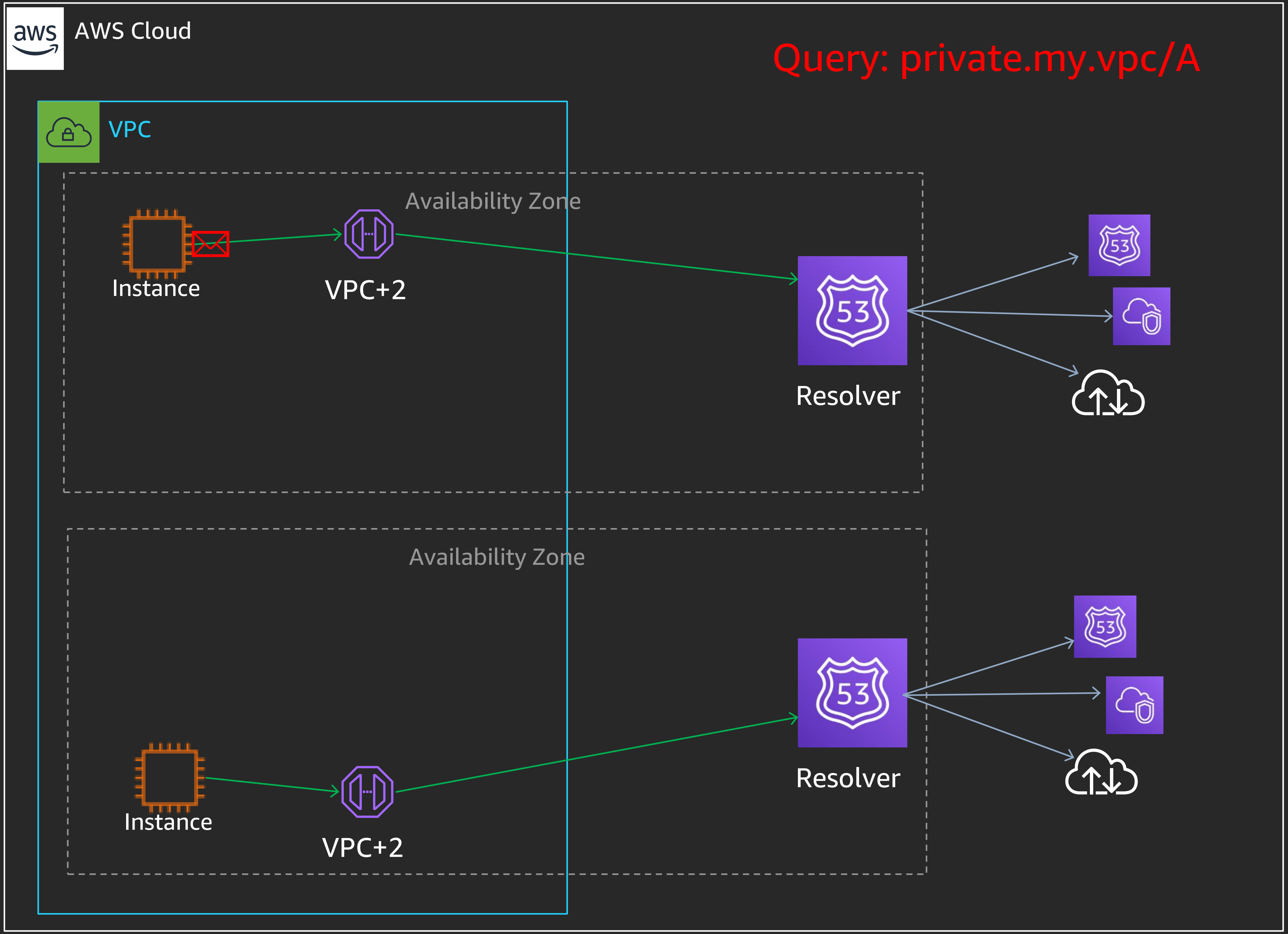
Defined special namespaces, e.g.:

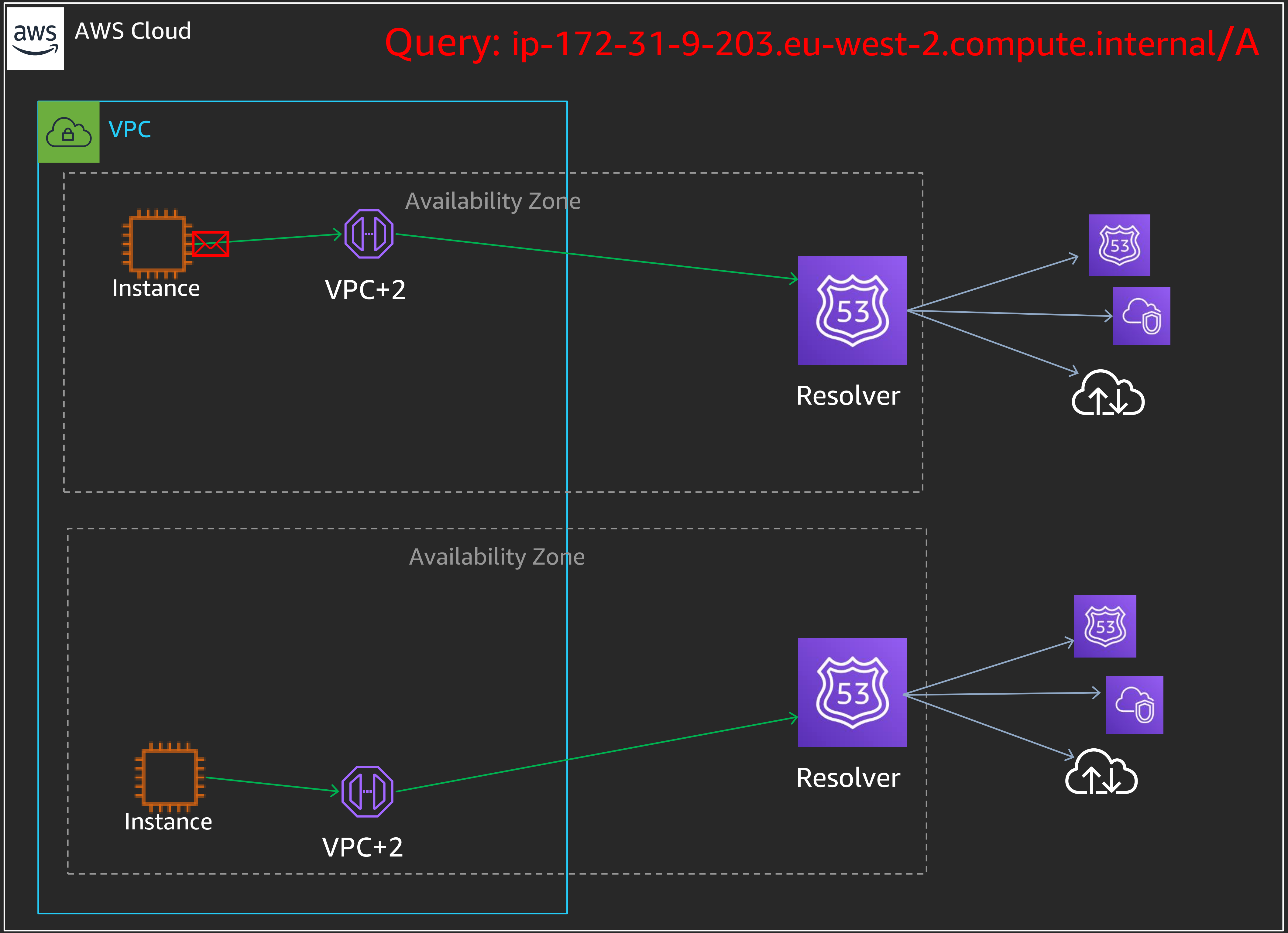
- eu-west-2.compute.internal.
- 10.in-addr.arpa., 168.192.in-addr.arpa., {16..31}.172.in-addr.arpa.
- eu-west-2.compute.amazonaws.com.

```
ubuntu@ip-172-31-9-203:~$ dig SOA 1.16.172.in-addr.arpa @172.31.0.2  +noall +auth

; <<>> DiG 9.11.3-1ubuntu1.9-Ubuntu <<>> SOA 1.16.172.in-addr.arpa @172.31.0.2 +noall
+auth

;; global options: +cmd

in-addr.arpa. 60 IN SOA ns0.eu-west-2.compute.internal. hostmaster.amazon.com. 2012103100
3600 3600 3600 60
```


Route 53
Resolver
1. Private DNS
2. VPC DNS
3. Public DNS

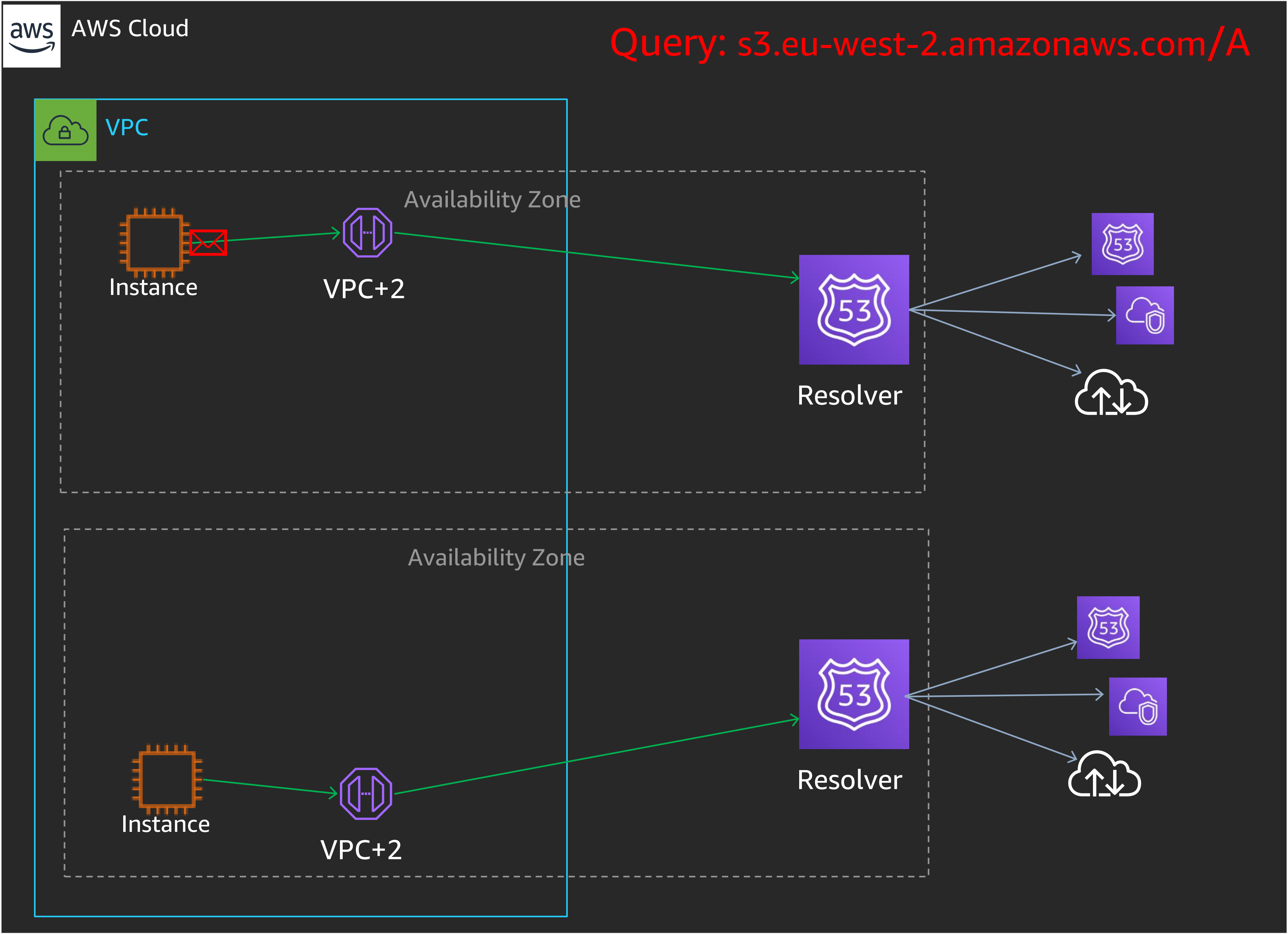
Query: private.my.vpc/A





Query: ip-172-31-9-203.eu-west-2.compute.internal/A

Query: s3.eu-west-2.amazonaws.com/A



Route 53 Resolver (VPC+2)

Simple

Just works

Easy to configure

Scalable

Grows with your VPC

Fault tolerance

Each AZ operates independently

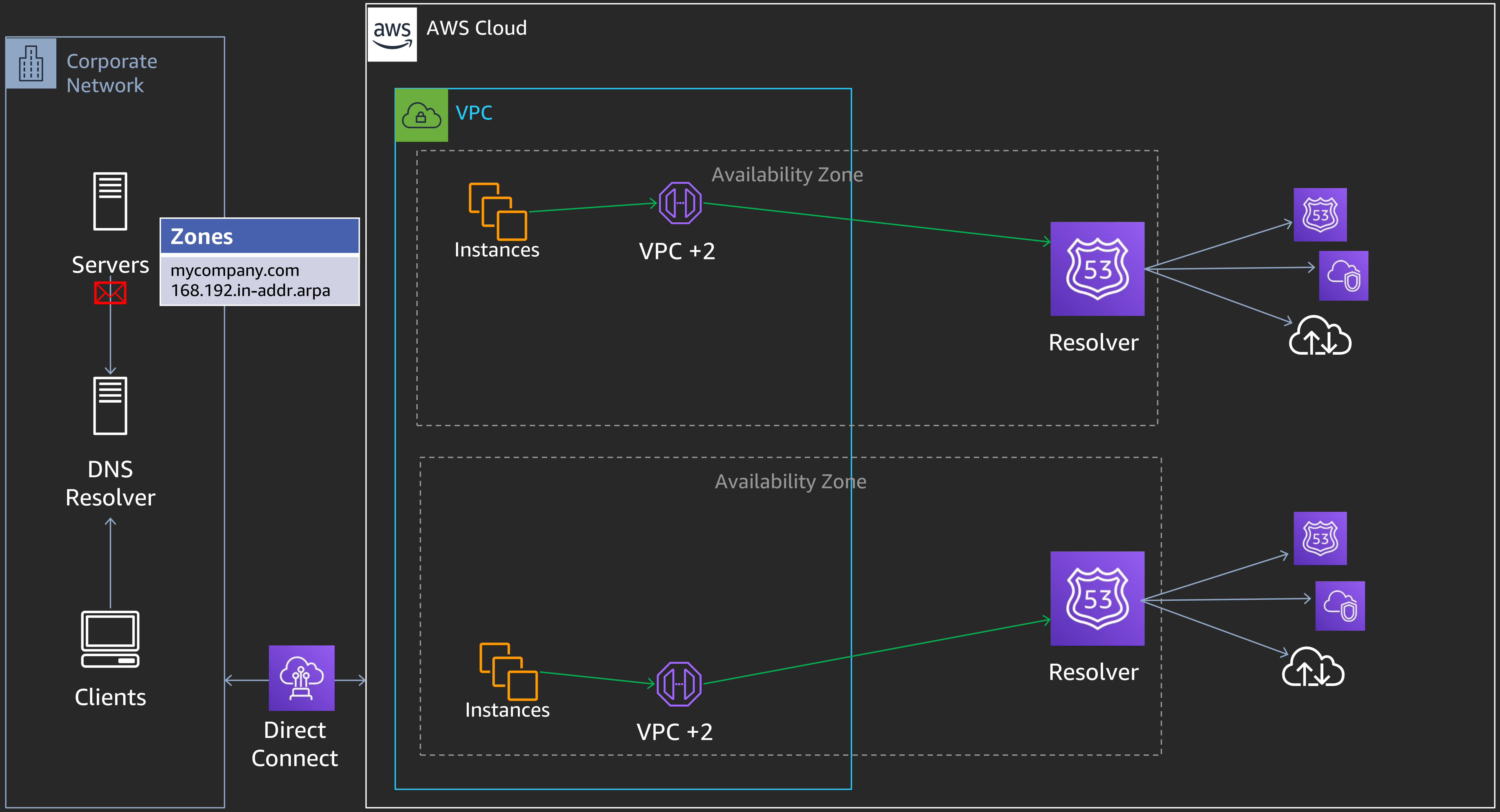
Performant

Caching improves latency

Low cost

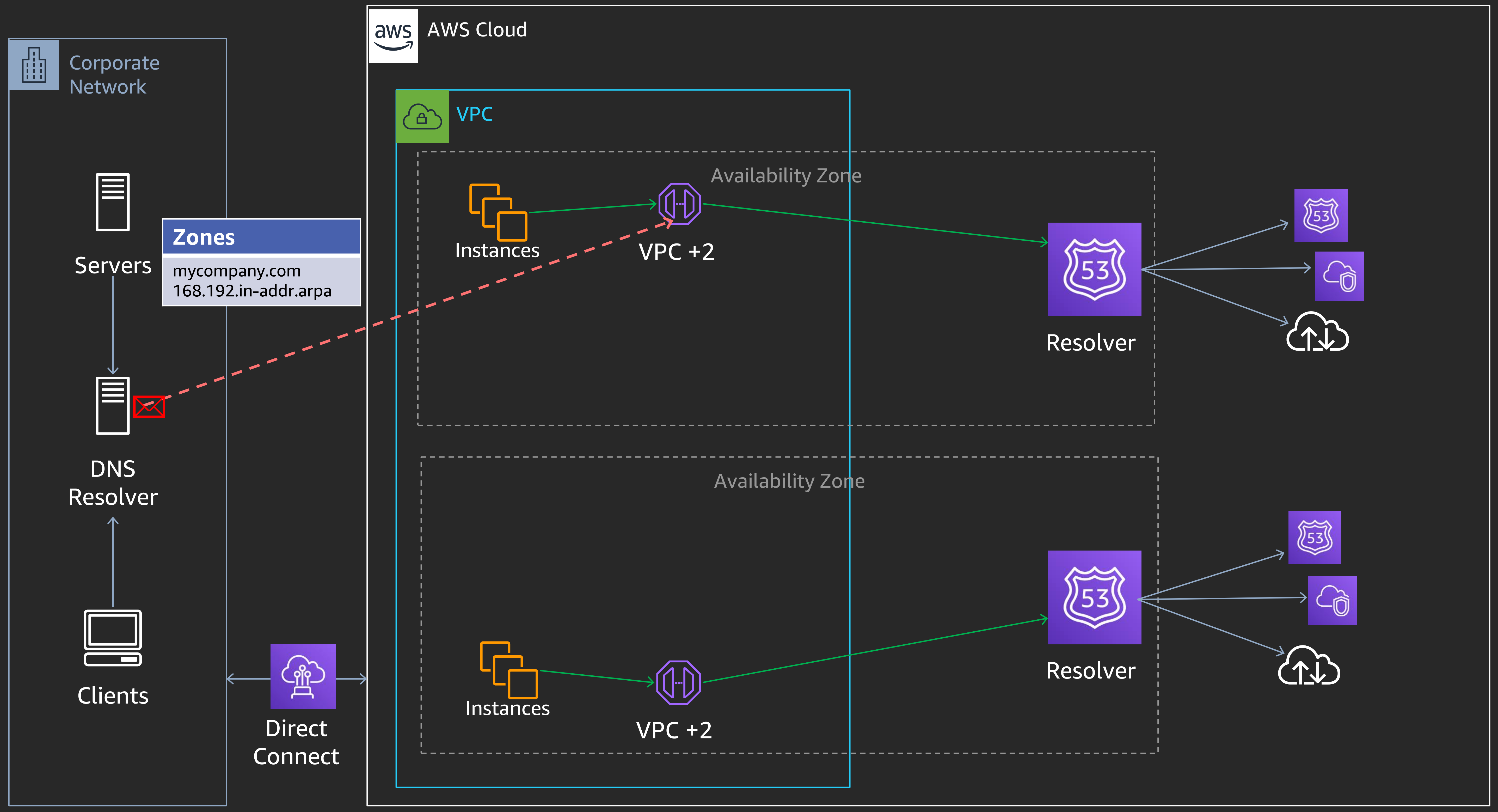
No query charges

Hybrid Cloud



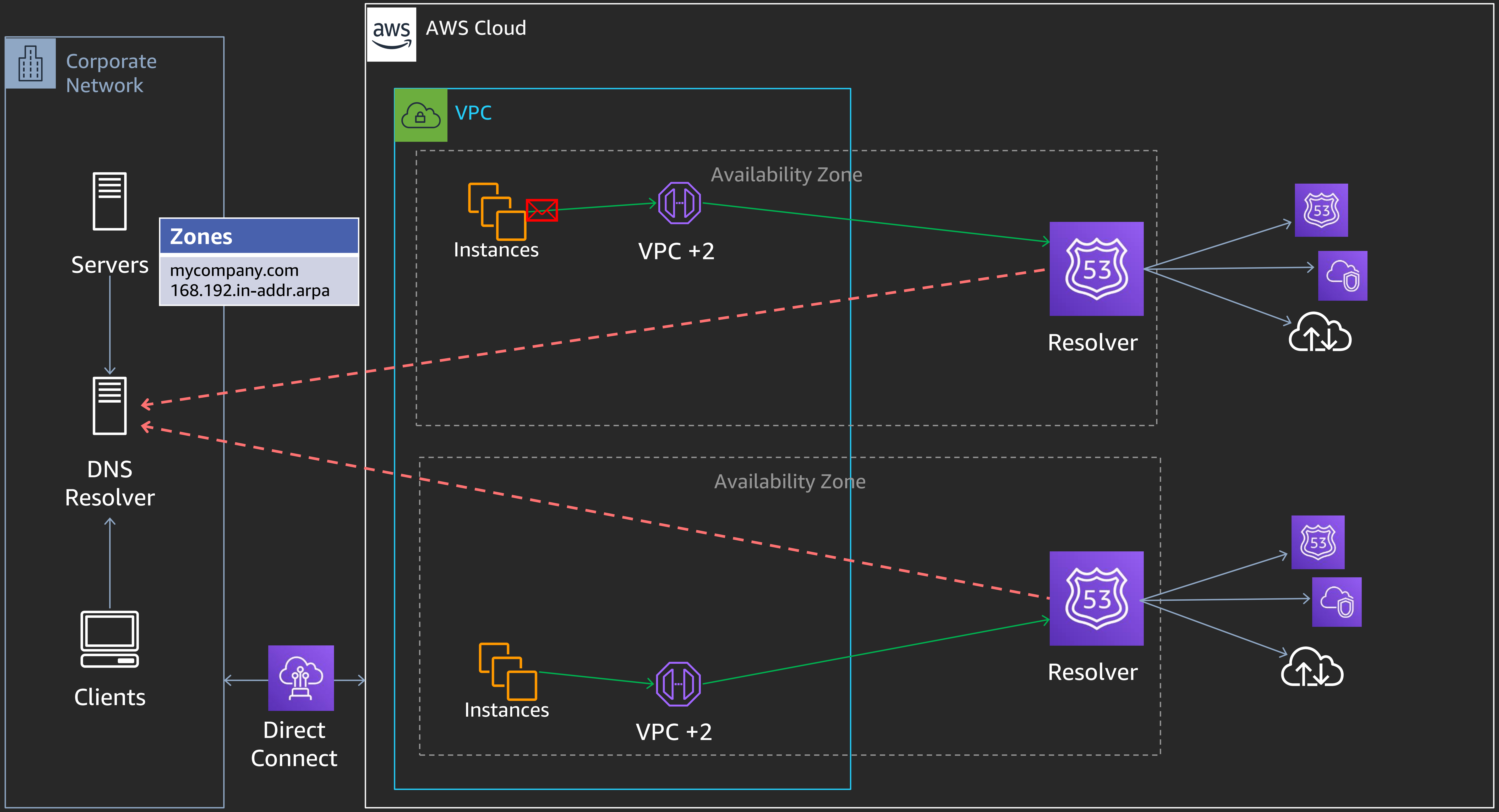
Zones

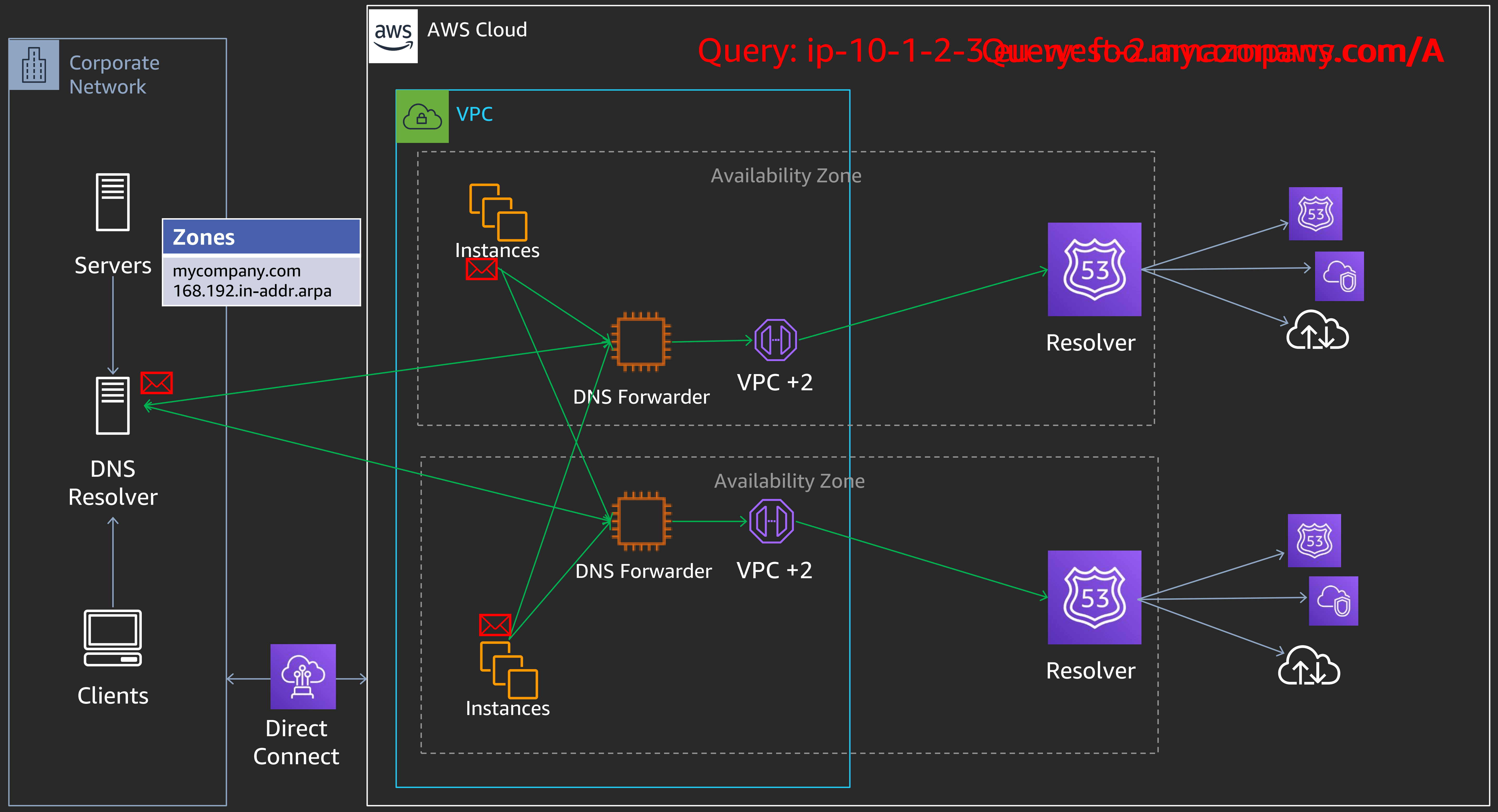
mycompany.com
168.192.in-addr.arpa



Zones

mycompany.com
168.192.in-addr.arpa

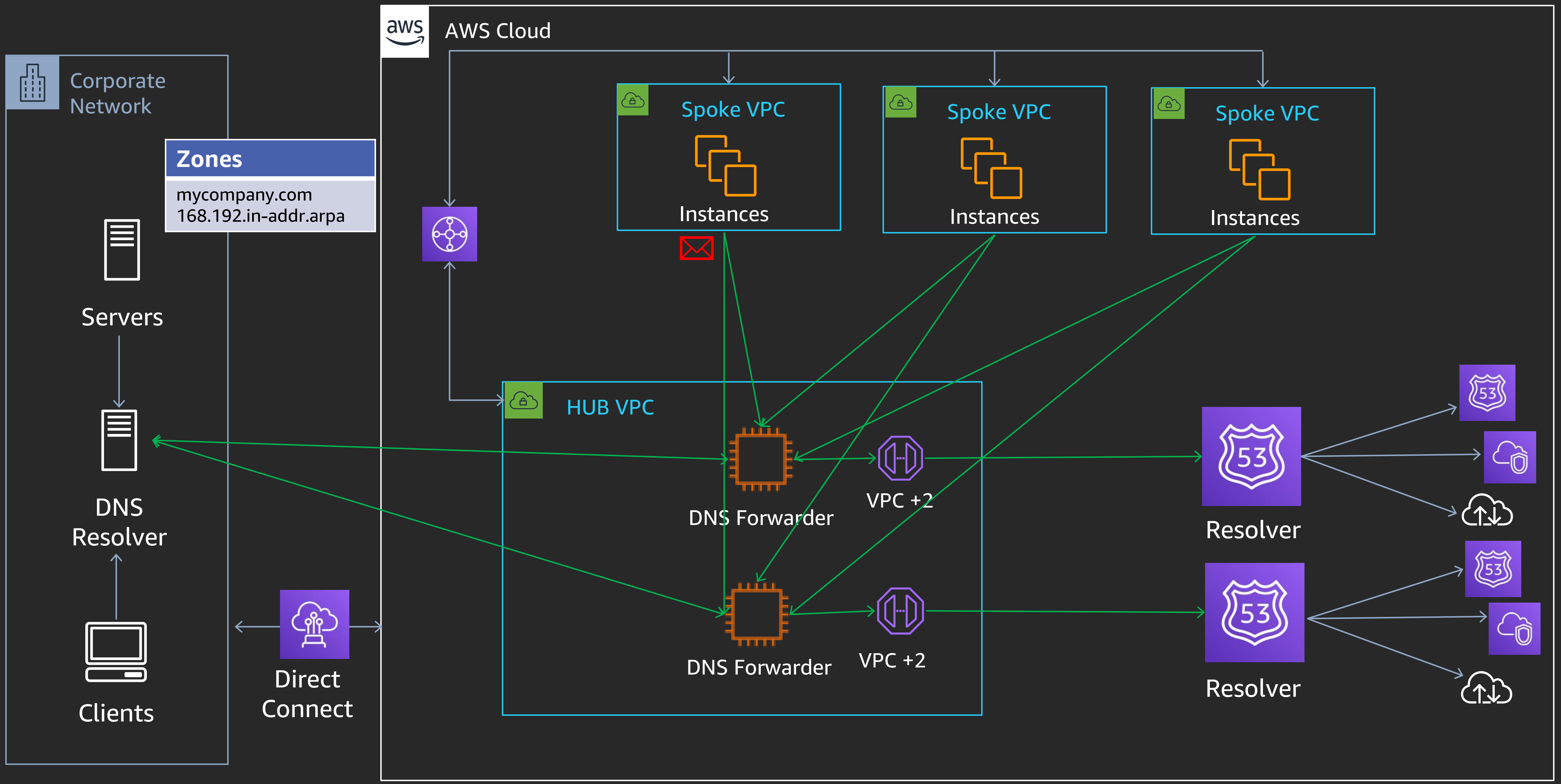

Corporate Network
Servers
Zones
mycompany.com
168.192.in-addr.arpa
DNS Resolver
Clients
Direct Connect
AWS Cloud
VPC
Availability Zone
Instances
VPC +2
Resolver
Availability Zone
Instances
VPC +2
Resolver


Corporate Network
Servers
Zones
mycompany.com
168.192.in-addr.arpa
DNS Resolver
Clients
Direct Connect
AWS Cloud
Query: ip-10-1-2-3
Query: test-2.mycompany.com/A
VPC
Availability Zone
Instances
DNS Forwarder
VPC +2
Resolver
Availability Zone
DNS Forwarder
VPC +2
Instances
Resolver

Hub and spoke

Query: s3-us-west-2.amazonaws.com/A

Query: foo.mycompany.com/A



Zones
mycompany.com 168.192.in-addr.arpa

Forwarding instances: The good

Works!

Integrates VPC and on-premises DNS

Cost

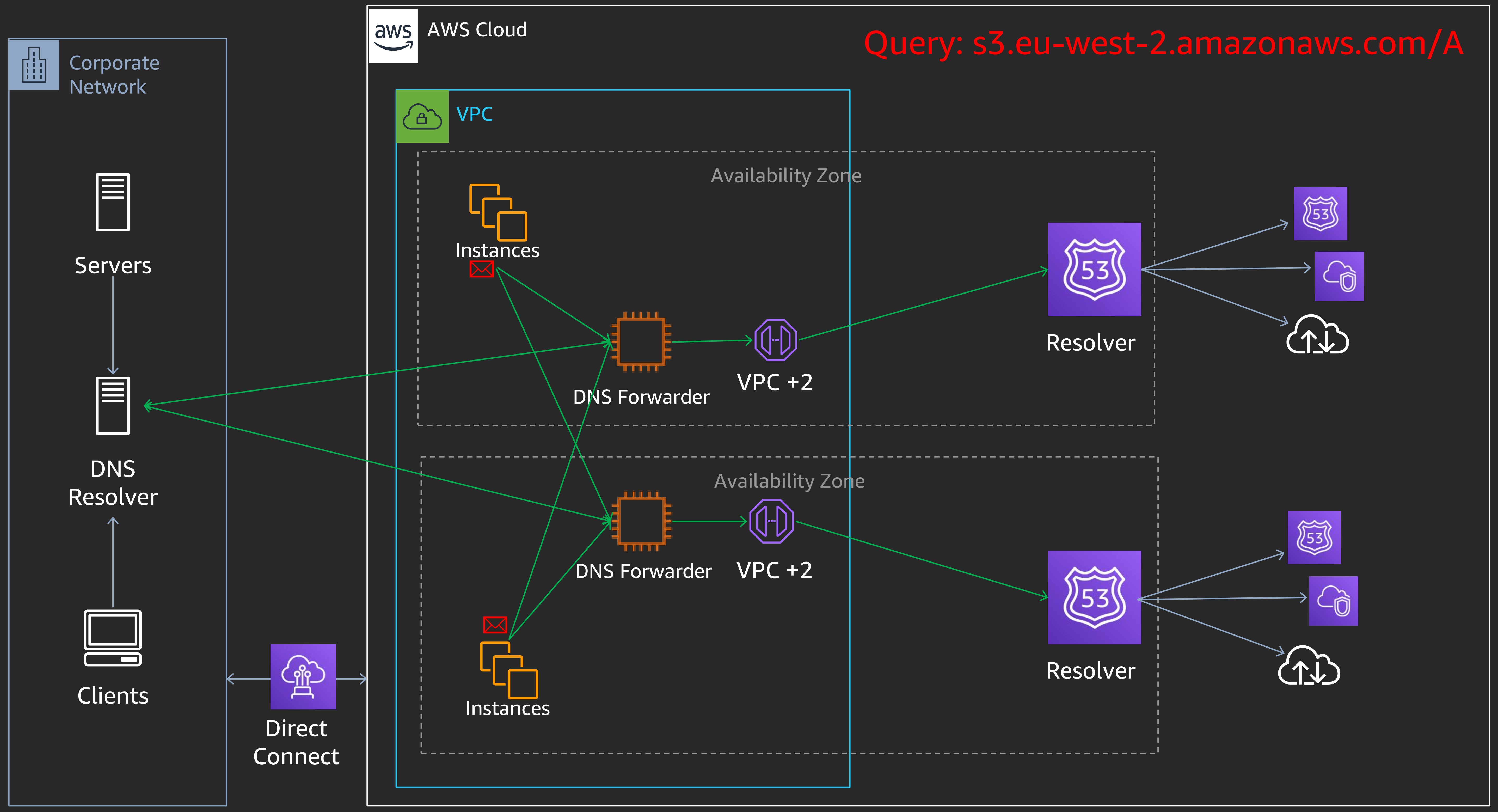
Reusable across VPCs

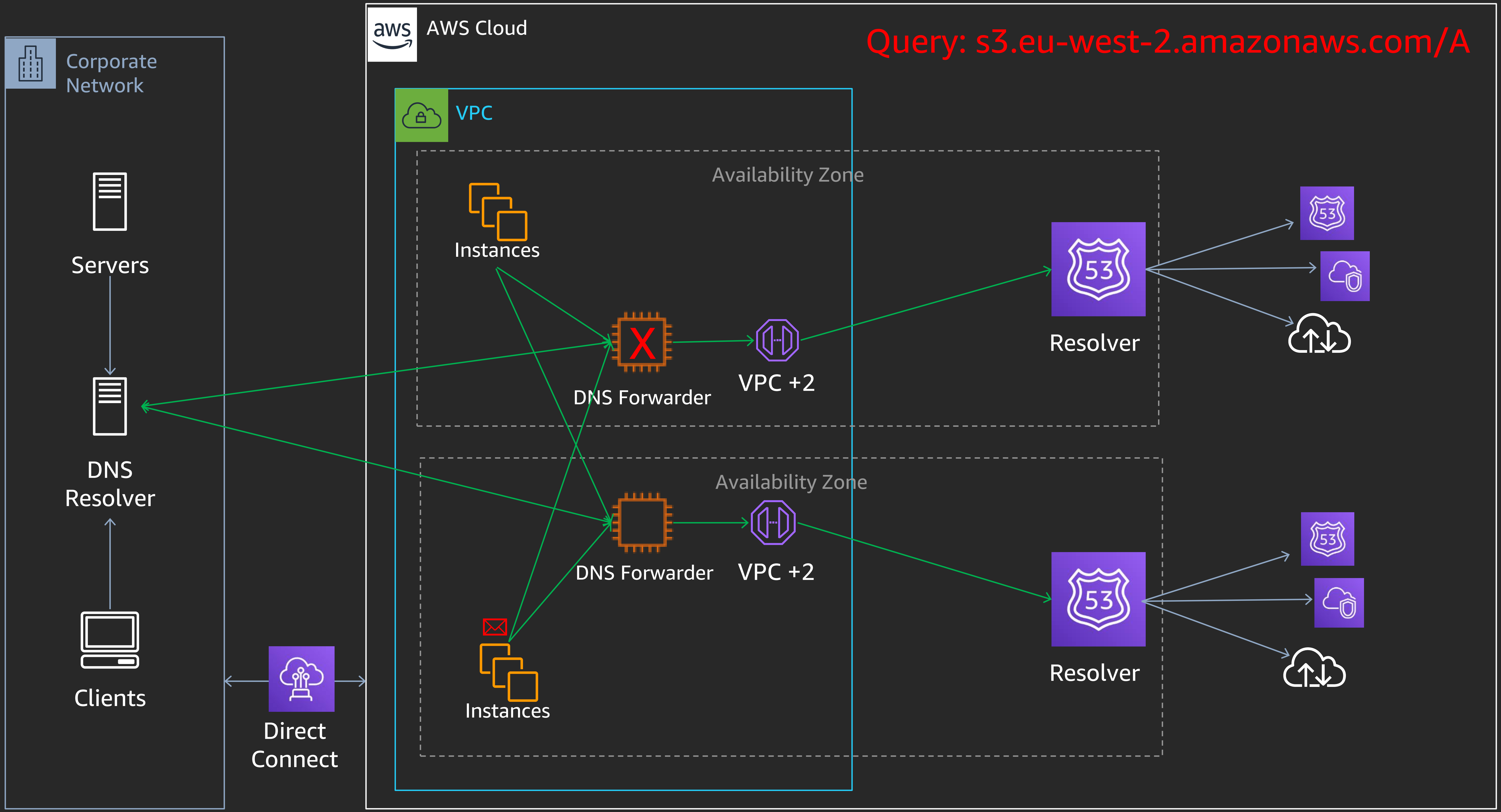
Performant

Caching improves latency

Flexible

Logging, RPZ, AXFR, etc.


Corporate Network
Servers
DNS Resolver
Clients
Direct Connect
AWS Cloud
Query: s3.eu-west-2.amazonaws.com/A
VPC
Availability Zone
Instances
DNS Forwarder
VPC +2
Resolver
Availability Zone
DNS Forwarder
VPC +2
Instances
Resolver



Query: s3.eu-west-2.amazonaws.com/A

Linux stub resolver

```
[ec2-user@ip-172-31-4-227 ~]$ cat /etc/resolv.conf

; generated by /usr/sbin/dhclient-script

search ap-southeast-2.compute.internal

options timeout:2 attempts:5

nameserver 172.31.4.10

nameserver 172.31.3.10
```

man resolv.conf:

“If there are multiple servers, the resolver library queries them in the order listed.”

Forwarding instances: 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

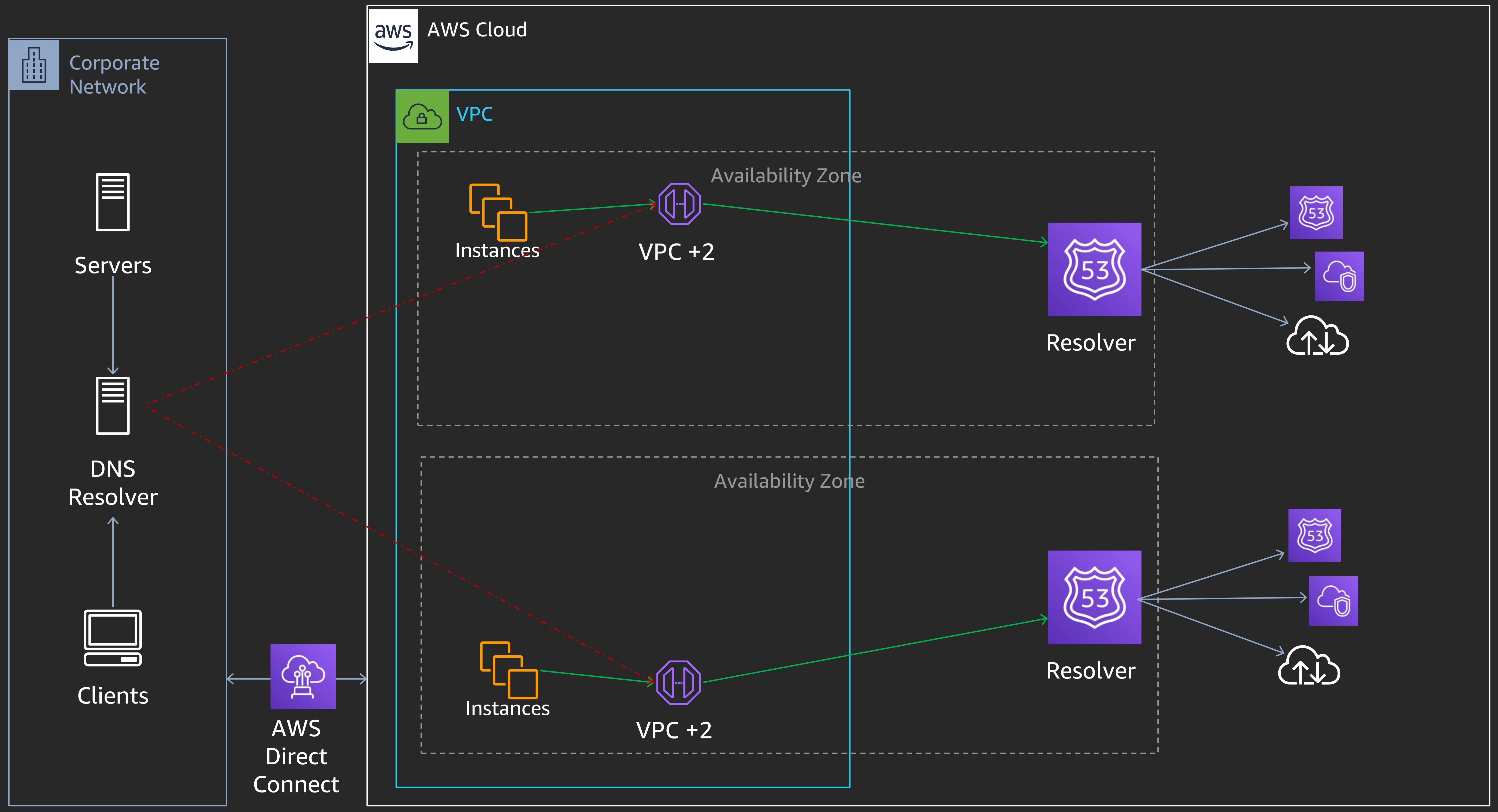
CIDR+2 vs. forward instances (2018)

	Managed	Limits	Caching	Cost	Blast Radius	On-premises integration	Flexibility
VPC +2 Resolver	**Fully Managed**	**1024x pps per ENI**	Yes	None	**Zonal**	No	Private DNS
Forwarding instances	Self Install	1024pps per forwarding instance	Yes	Per instance	Regional	**Yes**	**Local zones, logging, RPZ**

Route 53 Resolver Endpoints

Route 53 Resolver Inbound Endpoints

AWS re:Invent


Corporate Network
Servers
DNS Resolver
Clients
AWS Direct Connect
AWS Cloud
VPC
Availability Zone
Instances
VPC +2
Resolver
Availability Zone
Instances
VPC +2
Resolver

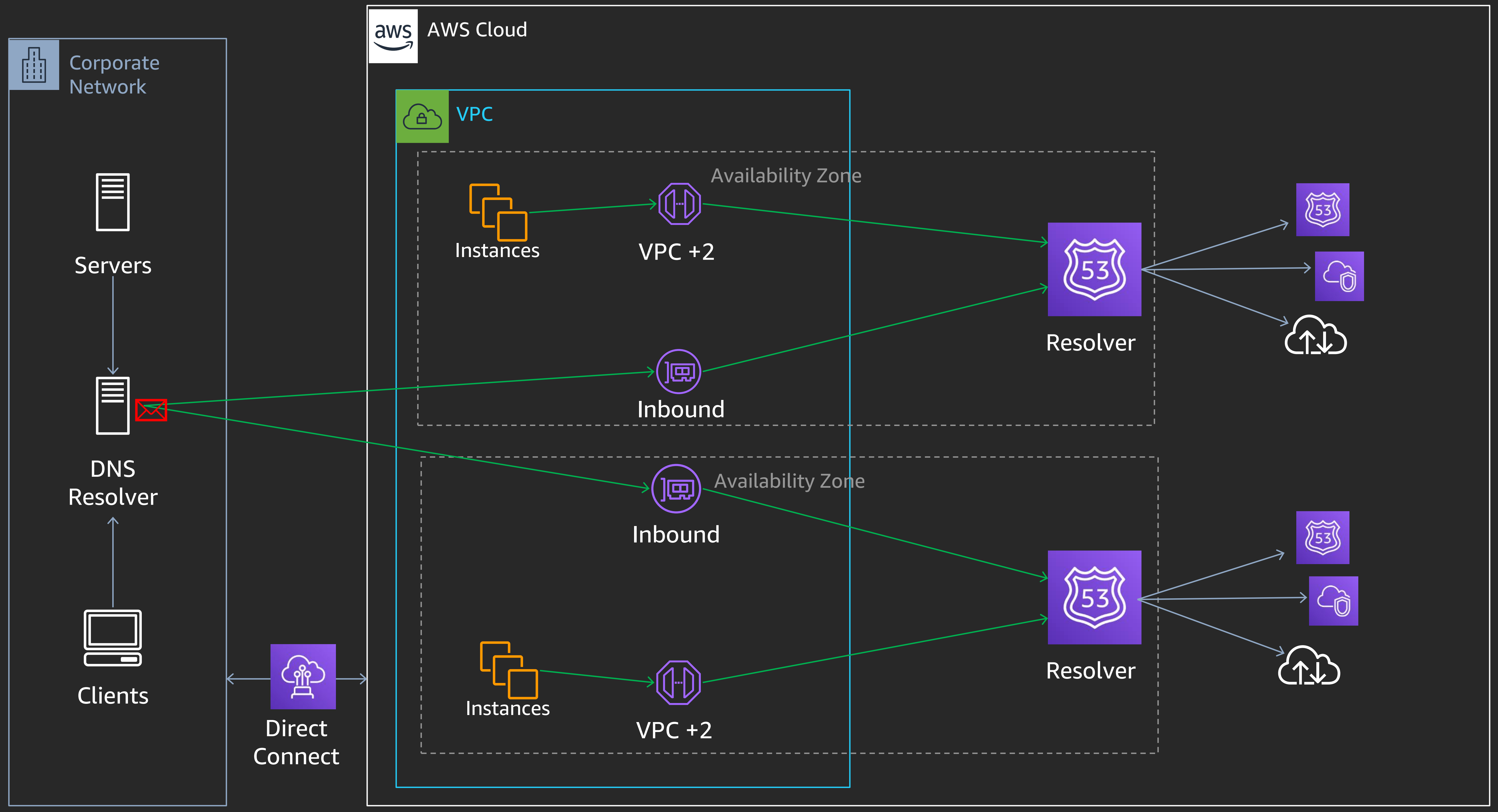
Route 53 Resolver: Inbound endpoints

Allow on-premises resolvers query Route 53 Resolver

Creates routable ENIs in VPC reachable over AWS Direct Connect or VPN

Nomenclature: one “endpoint” == multiple ENIs

Limit: 10,000 QPS per ENI


Corporate Network
Servers
DNS Resolver
Clients
Direct Connect
AWS Cloud
VPC
Availability Zone
Instances
VPC +2
Inbound
Resolver
Availability Zone
Inbound
Instances
VPC +2
Resolver
53
53
53
53

Inbound endpoints: Best practices

Use multiple ENIs in separate Availability Zones for high availability

Use a retrying DNS resolver on-premises

Specify your IPs

CloudWatch alarms on QPS

EC2 instances use VPC+2 Resolver not inbound endpoints

Inbound endpoints: Multiple VPCs

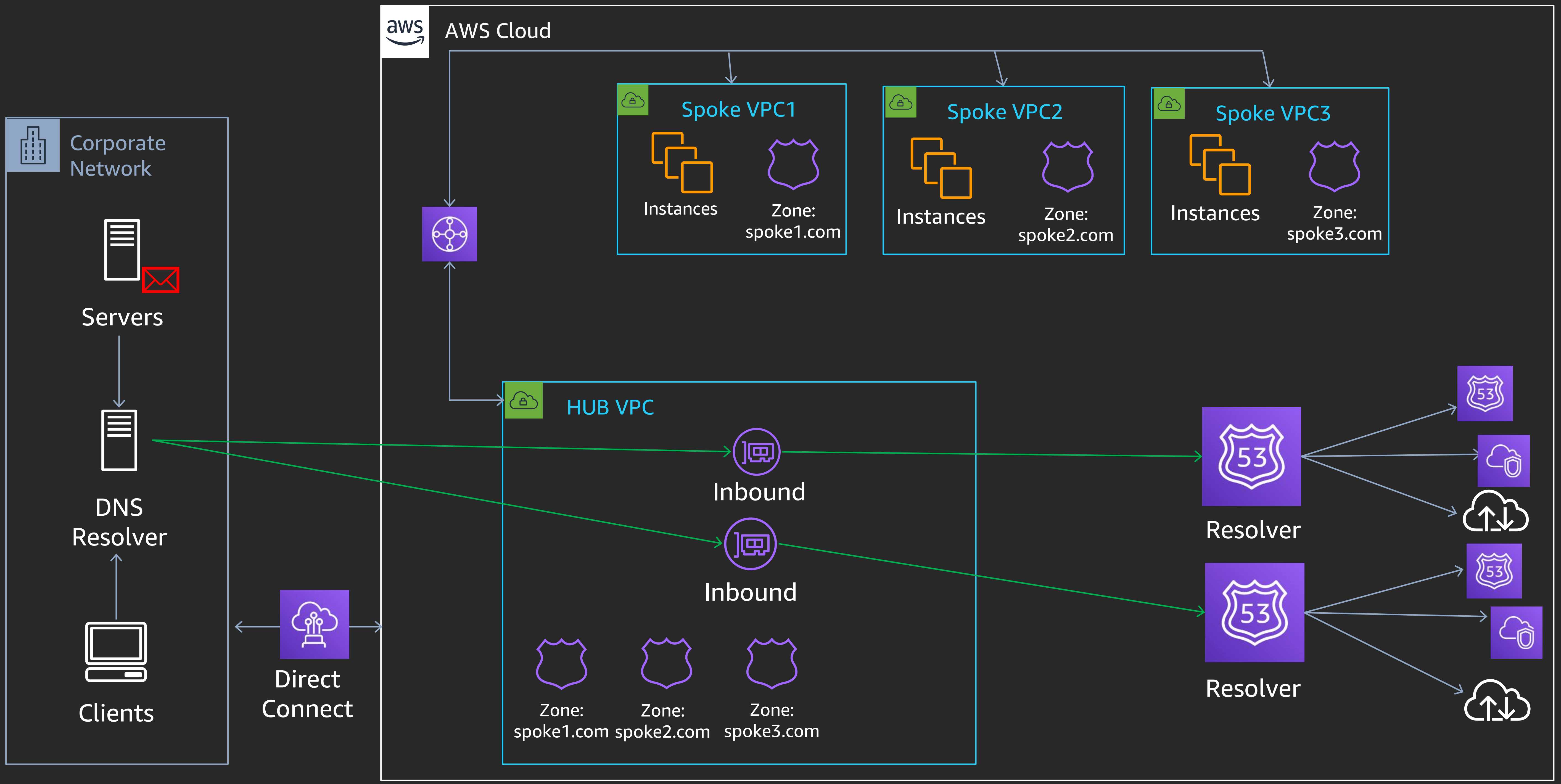
Do I need multiple endpoints for multiple VPCs?

Generally, no

- Associate all Private Hosted Zones to one VPC
- Internal Instance names resolve across all VPCs
- Public EC2 internal IPs resolve with peering/TGW

Hub and spoke

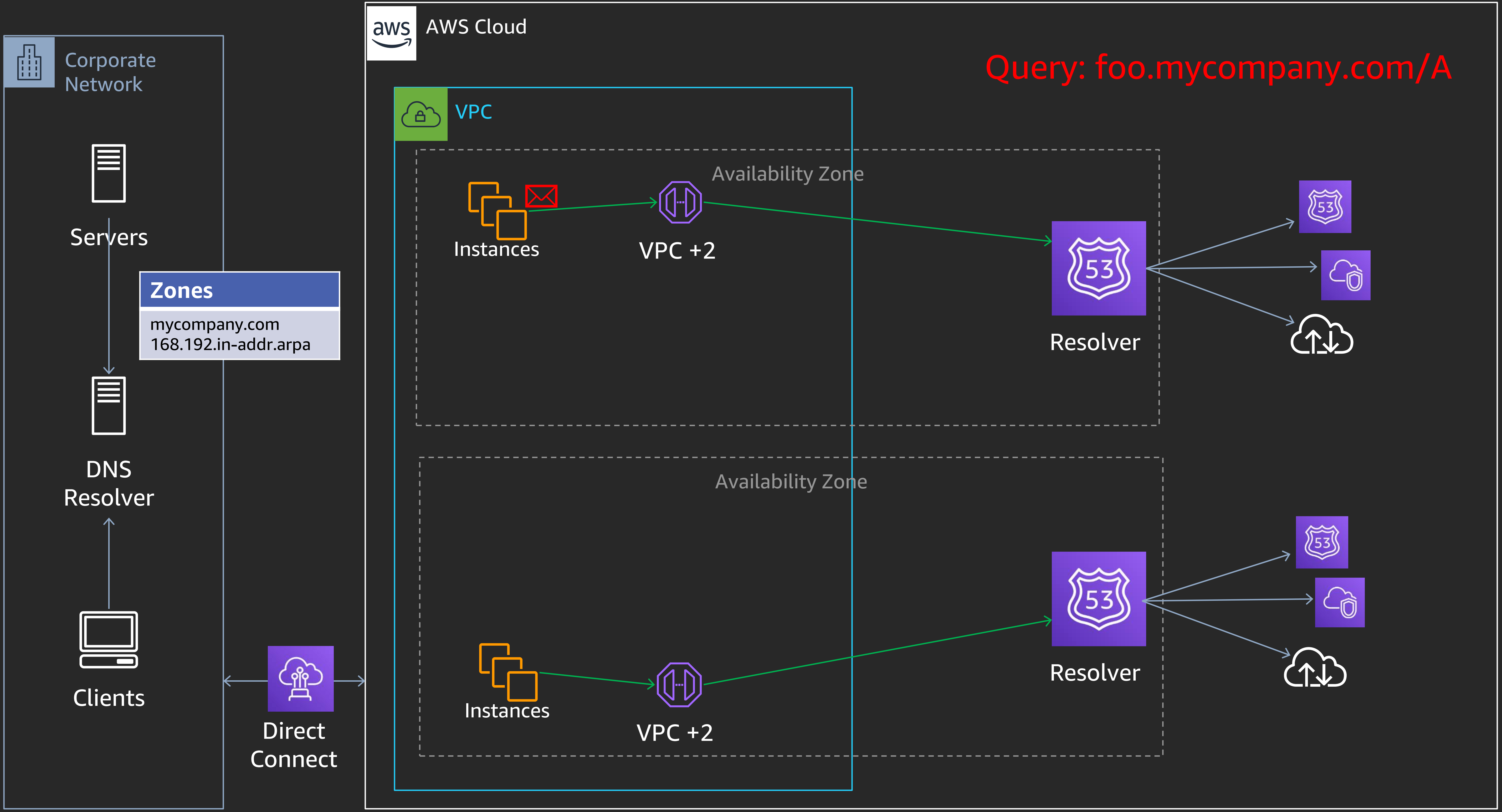
Query: foo.spoke2.com/A



Resolving EC2 domains from on-premises

	Managed	Limits	Caching	Cost	Blast Radius	Query Metrics
Inbound Endpoints	**Fully Managed**	**10K QPS per ENI**	At Resolver Service	$0.125 per hour per ENI	Zonal	Yes
Forwarding Instances	Self-Managed	1024 PPS per Forward Instance	Yes	EC2 Instance pricing	Zonal	No

Route 53 Resolver Outbound Endpoints & Rules


Corporate Network
Servers
Zones
mycompany.com
168.192.in-addr.arpa
DNS Resolver
Clients
Direct Connect
AWS Cloud
Query: foo.mycompany.com/A
VPC
Availability Zone
Instances
VPC +2
Resolver
Availability Zone
Instances
VPC +2
Resolver

Route 53 Resolver: Outbound endpoints

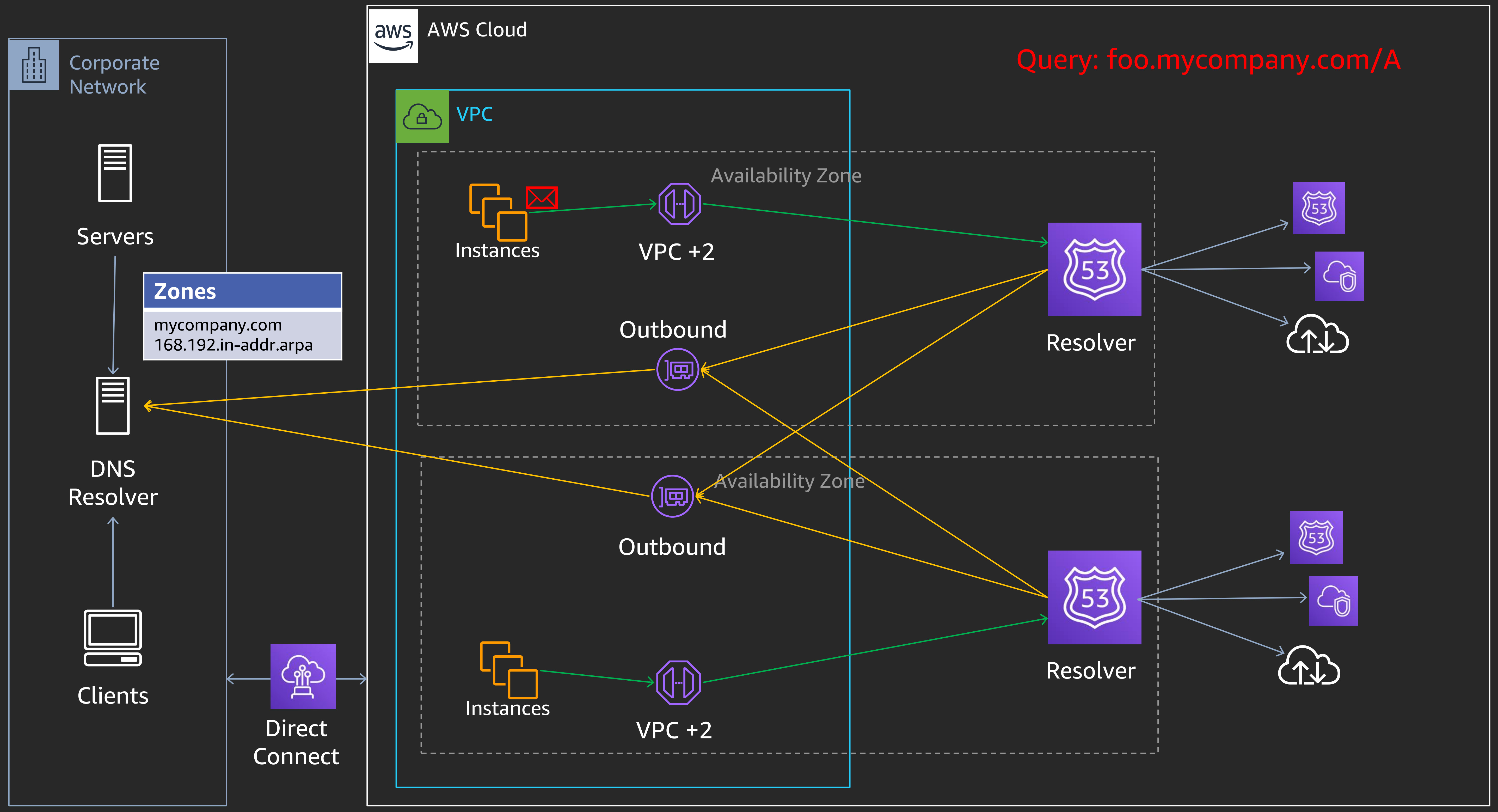
Path for the Route 53 Resolver to query your DNS Resolvers

Creates source ENIs in your VPC

Usable by many VPCs

Nomenclature: one “endpoint” == multiple ENIs

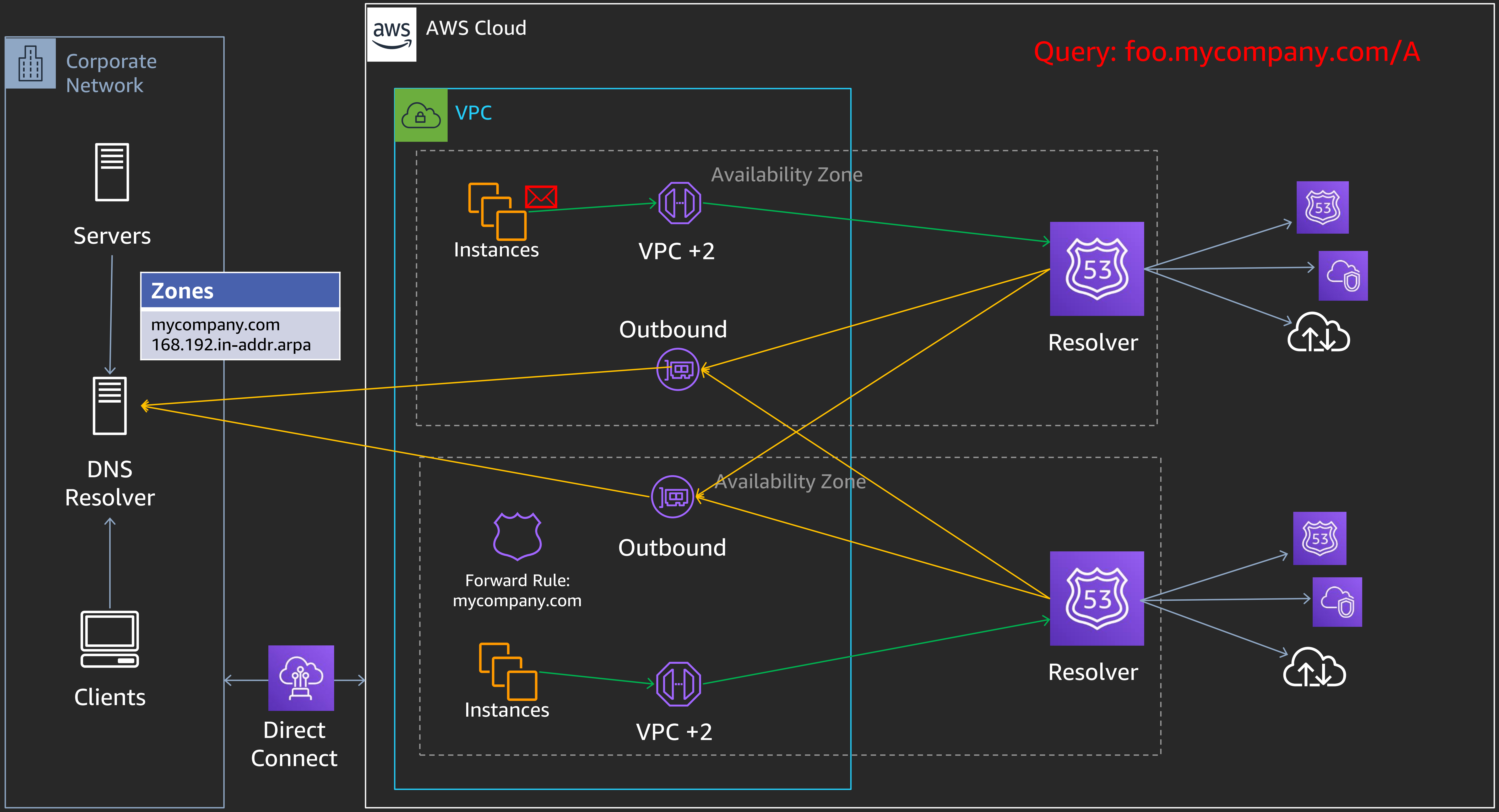
Limit: 10,000 QPS per ENI


AWS Cloud
Query: foo.mycompany.com/A
Corporate Network
VPC
Availability Zone
Servers
Zones
mycompany.com
168.192.in-addr.arpa
Instances
VPC +2
Resolver
Outbound
DNS Resolver
Availability Zone
Outbound
Resolver
Clients
Instances
VPC +2
Direct Connect

Route 53 Resolver – Resolver Rules

Configure how Route 53 Resolver makes queries

Two types: FORWARD and SYSTEM


Corporate Network
Servers
Zones
mycompany.com
168.192.in-addr.arpa
DNS Resolver
Clients
Direct Connect
AWS Cloud
Query: foo.mycompany.com/A
VPC
Availability Zone
Instances
VPC +2
Outbound
Resolver
Availability Zone
Outbound
Forward Rule:
mycompany.com
Instances
VPC +2
Resolver
53

Outbound Endpoints: Multiple VPCs

Do I need multiple outbound endpoints for multiple VPCs?

No. Share and associate rules to many VPCs.

Do I need to share Outbound Endpoints between VPCs/Accounts?

No. When you associate a rule, the endpoint is shared implicitly.

What if the VPCs are in different AWS accounts?

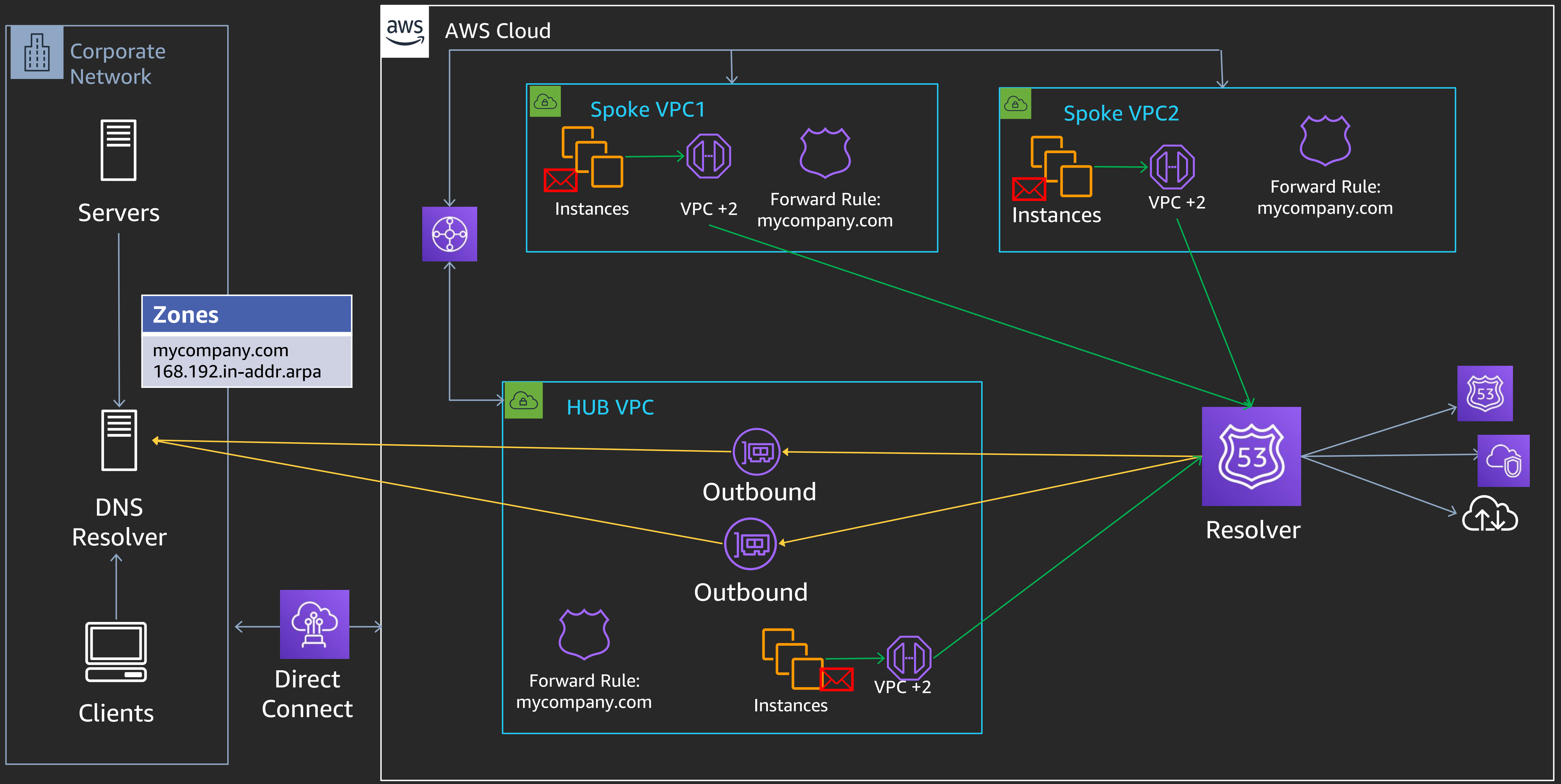
Resource Access Manager shares Resolver Rules cross-account.

Do I need VPC Peering or Transit Gateway?

No.

Hub and spoke

Query: foo.mycompany.com/A



Outbound Endpoints: Best practices

Use multiple ENIs in separate Availability Zone for high availability

Use forwarding sparingly

Maintain fixed IPs as targets

CloudWatch alarms on QPS

Resolving on-premises domains from EC2

	Managed	**Limits**	**Caching**	**Cost**	**Blast Radius**	**On-Premises Integration**	**Scope**
VPC+2 Resolver + Outbound Endpoints	**Fully Managed**	**1024 per ENI;** 10K QPS per Outbound	Local	$0.125 per hour per ENI	**Zonal**	**Yes**	Only Forwarded Queries
Forward Instances	Self-Install	Depends on Instance Size	Remote	EC2 Instance Pricing	Regional	Yes	All Queries

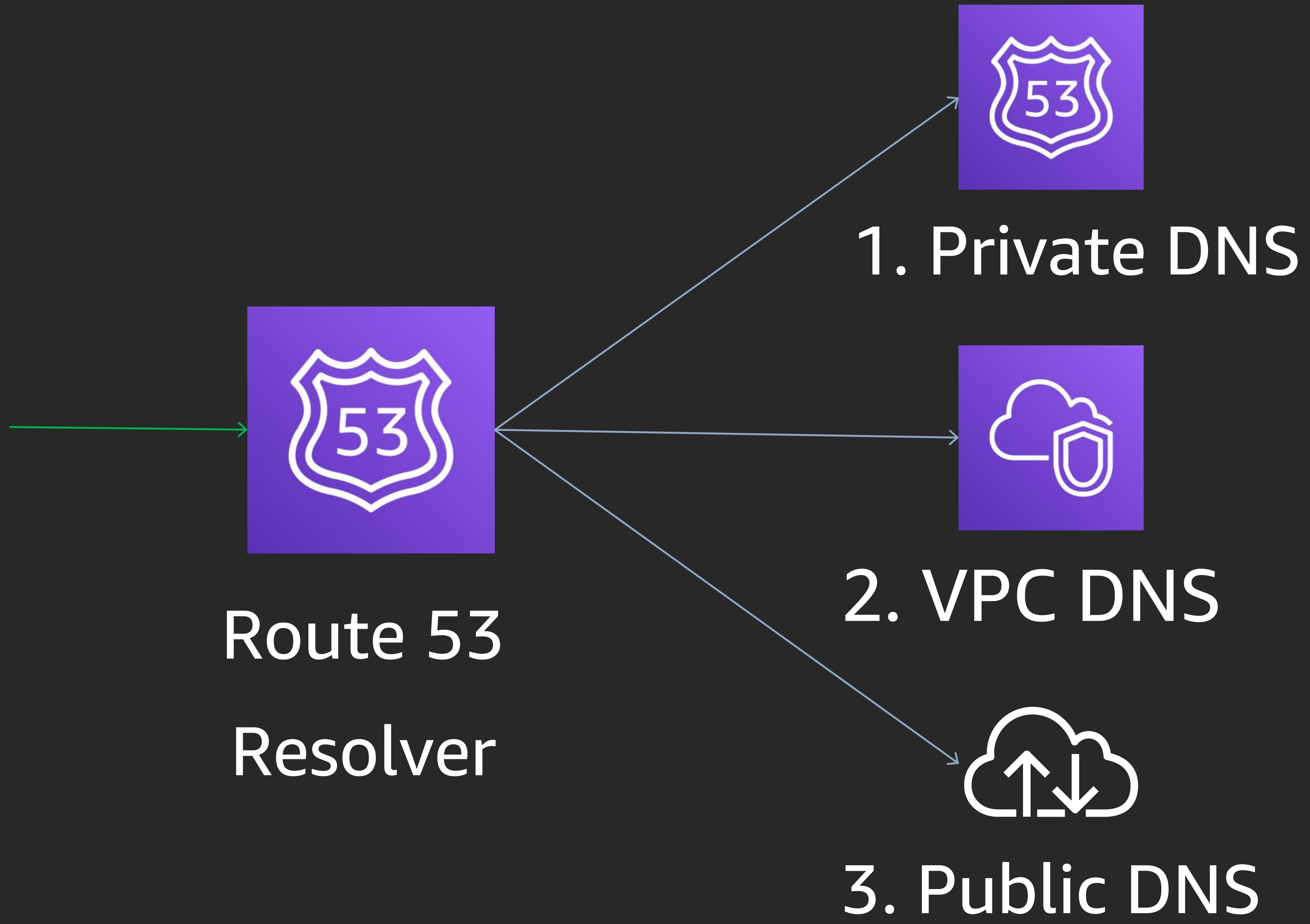
Resolver rules: How do they work?

What if I create rules that overlap?

Most specific matching rule wins

FORWARD wins over SYSTEM on same domain

How do these Rules interact with Private Hosted Zones and VPC DNS?



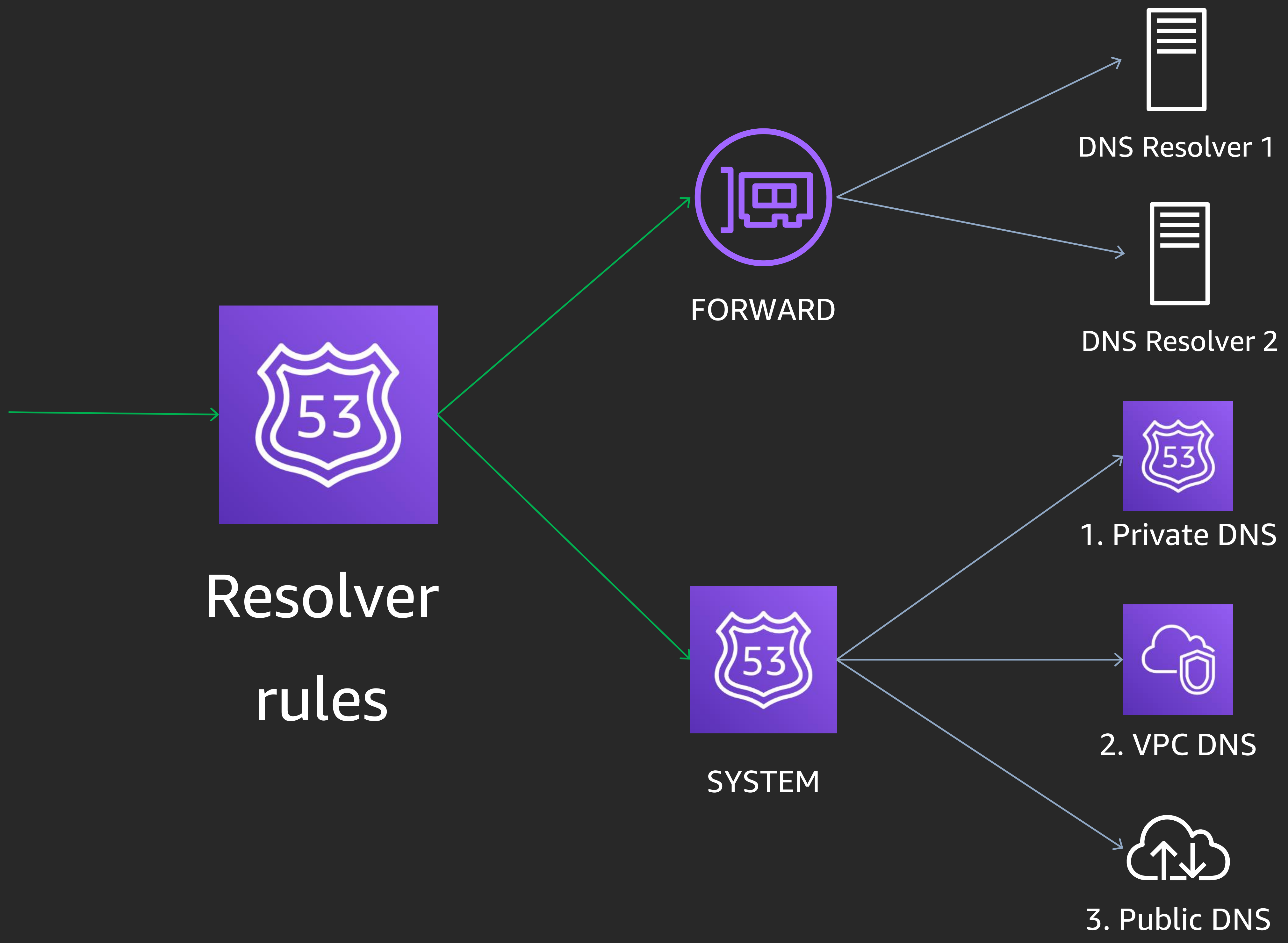
Route 53

Resolver

1. Private DNS

2. VPC DNS

3. Public DNS


Resolver rules
FORWARD
DNS Resolver 1
DNS Resolver 2
SYSTEM
1. Private DNS
2. VPC DNS
3. Public DNS

Autodefined system rules

Suppose we create a FORWARD rule on “.”

Would this override all VPC DNS and Private DNS?

Route 53 Resolver creates more specific “Autodefined System Rules”

Autodefined system rules

“.”

VPC DNS:

- eu-west-2.compute.internal (London)
- eu-west-2.compute.amazonaws.com (London)
- 10.in-addr.arpa, 168.192.in-addr.arpa, [16-31].172.in-addr.arpa
- Rules for each /24 in VPC CIDR

Private DNS:

- All Private Hosted Zones associated with the VPC

Resolver rules example

Requirements:

- Forward all public DNS resolution via on-premises resolvers
- Route 53 Resolver should answer: amazonaws.com.
- Private Hosted Zone: mycloud.com.
- AWS PrivateLink: kinesis.eu-west-2.amazonaws.com.
- Corp office namespace: corp.mycloud.com
- VPC CIDR: 10.10.0.0/23
- On-premises CIDR range: 10.20.0.0/23

Resolver rules example

Domain	Type	Endpoint	Targets
“.”	SYSTEM (auto-defined)		

Resolver rules example

Domain	Type	Endpoint	Targets
“.”	SYSTEM (auto-defined)		
mycloud.com.	SYSTEM (auto-defined)		
kinesis.eu-west-2.amazon…	SYSTEM (auto-defined)		
eu-west-2.compute.internal.	SYSTEM (auto-defined)		
eu-west-2.compute.amaz….	SYSTEM (auto-defined)		

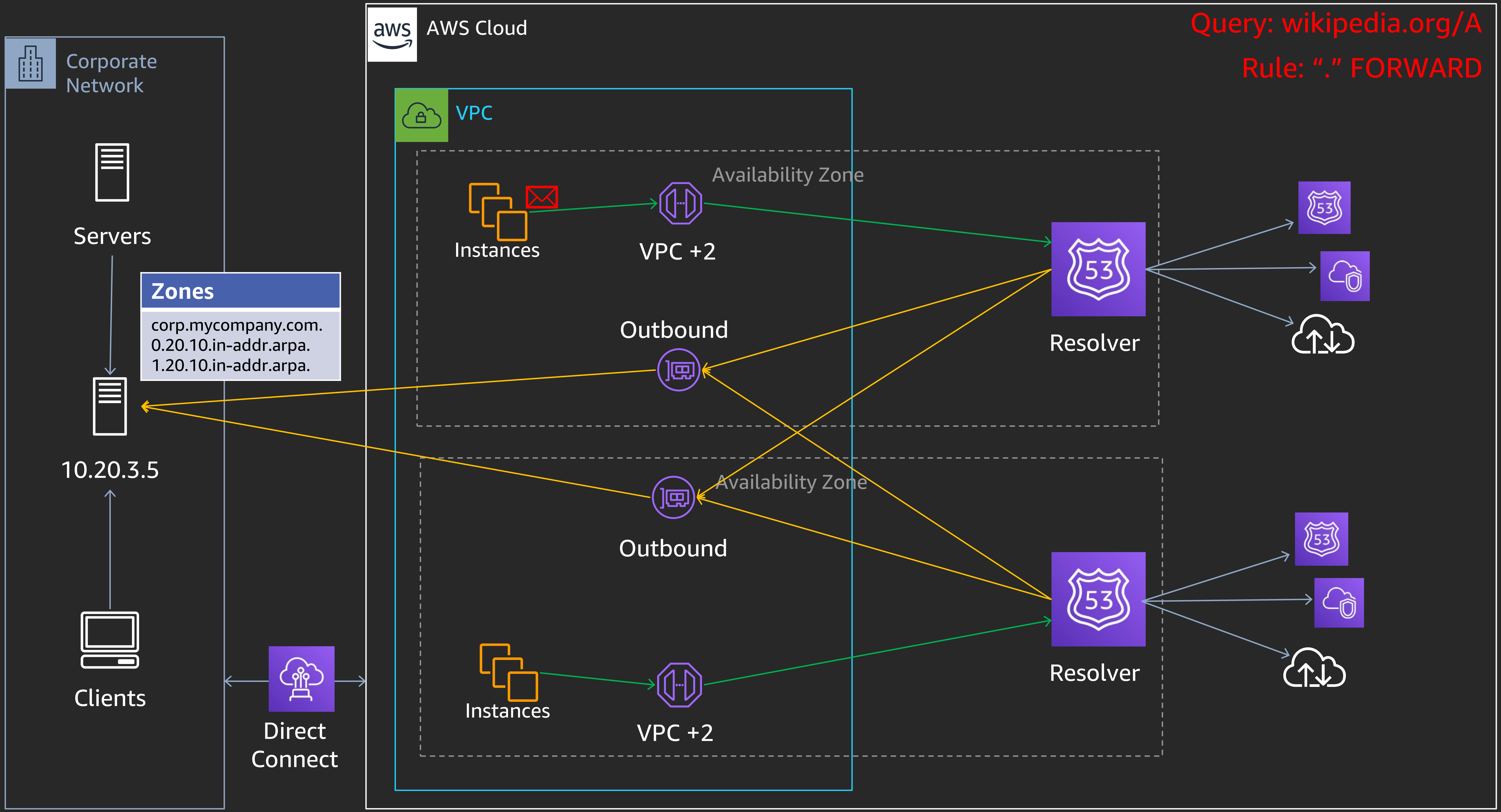
Resolver rules example

Requirements:

- Forward all public DNS resolution via on-premises resolvers
- Route 53 Resolver should answer: amazonaws.com.
- Private Hosted Zone: mycloud.com.
- AWS PrivateLink: kinesis.eu-west-2.amazonaws.com.
- Corp office namespace: corp.mycloud.com.
- VPC CIDR: 10.10.0.0/23
- On-premises CIDR range: 10.20.0.0/23

Resolver rules example

Domain	Type	Endpoint	Targets
“.”	SYSTEM (auto-defined)		
“.”	**FORWARD**	**rslvr-out-d085c56**	**10.20.3.4, 10.20.3.5**
mycloud.com.	SYSTEM (auto-defined)		
kinesis.eu-west-2.amazon…	SYSTEM (auto-defined)		
eu-west-2.compute.internal.	SYSTEM (auto-defined)		
eu-west-2.compute.amaz….	SYSTEM (auto-defined)		



Query: wikipedia.org/A

Rule: “.” FORWARD

Zones

corp.mycompany.com.
0.20.10.in-addr.arpa.
1.20.10.in-addr.arpa.

Resolver rules example

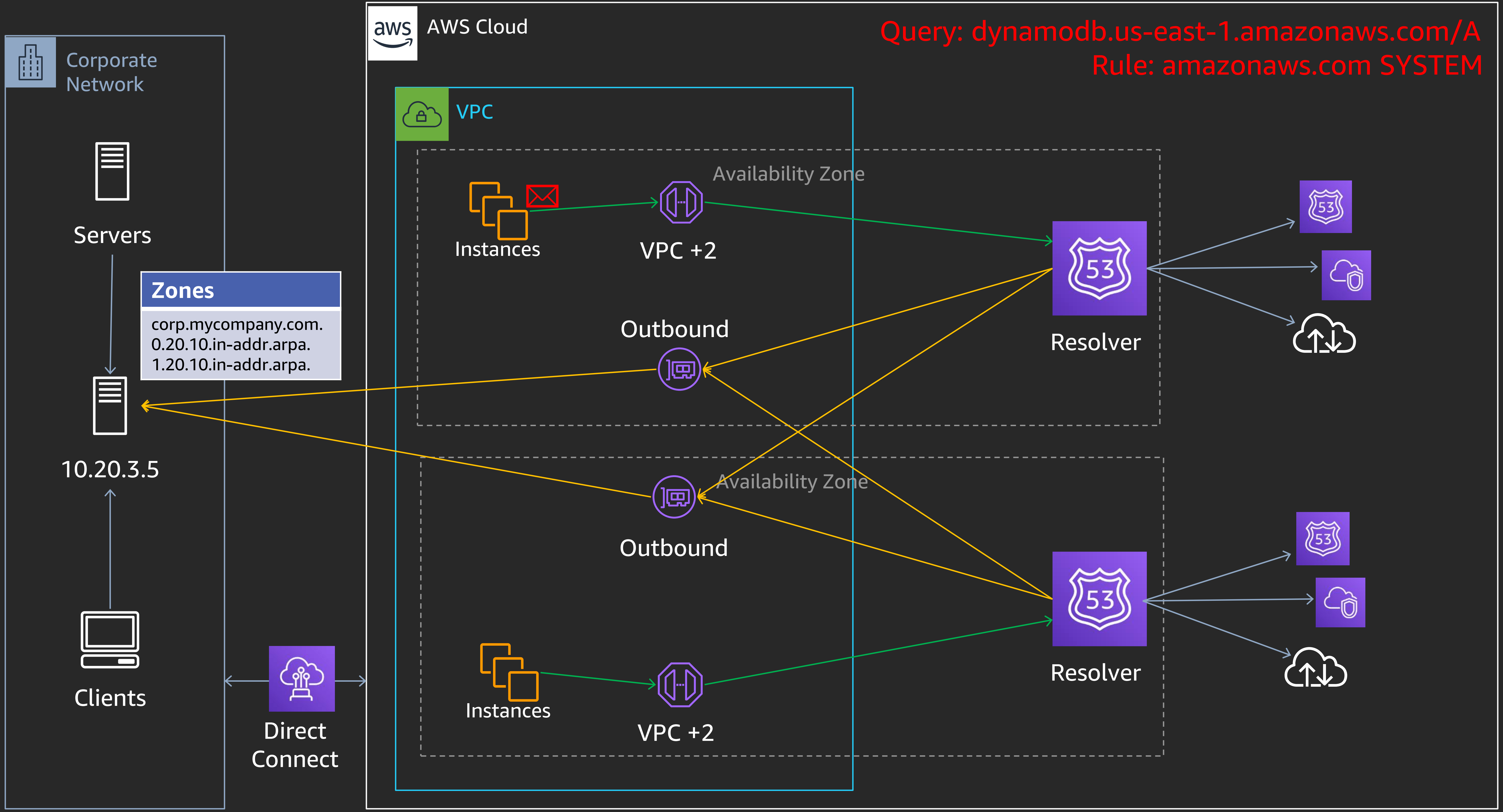
Requirements:

- Forward all public DNS resolution via on-premises resolvers
- Route 53 Resolver should answer: amazonaws.com.
- Private Hosted Zone: mycloud.com.
- AWS PrivateLink: kinesis.eu-west-2.amazonaws.com.
- Corp office namespace: corp.mycloud.com.
- VPC CIDR: 10.10.0.0/23
- On-premises CIDR range: 10.20.0.0/23

Resolver rules example

Domain	Type	Endpoint	Targets
“.”	SYSTEM (auto-defined)		
“.”	**FORWARD**	**rslvr-out-d085c56**	**10.20.3.4, 10.20.3.5**
amazonaws.com	**SYSTEM**		
mycloud.com.	SYSTEM (auto-defined)		
kinesis.eu-west-2.amazon…	SYSTEM (auto-defined)		
eu-west-2.compute.internal.	SYSTEM (auto-defined)		
eu-west-2.compute.amaz….	SYSTEM (auto-defined)		

Query: dynamodb.us-east-1.amazonaws.com/A
Rule: amazonaws.com SYSTEM



Corporate Network

Servers

Zones

corp.mycompany.com.
0.20.10.in-addr.arpa.
1.20.10.in-addr.arpa.

10.20.3.5

Clients

Direct Connect

AWS Cloud

VPC

Availability Zone

Instances

VPC +2

Outbound

Resolver

Availability Zone

Outbound

Instances

VPC +2

Resolver

Resolver rules example

Requirements:

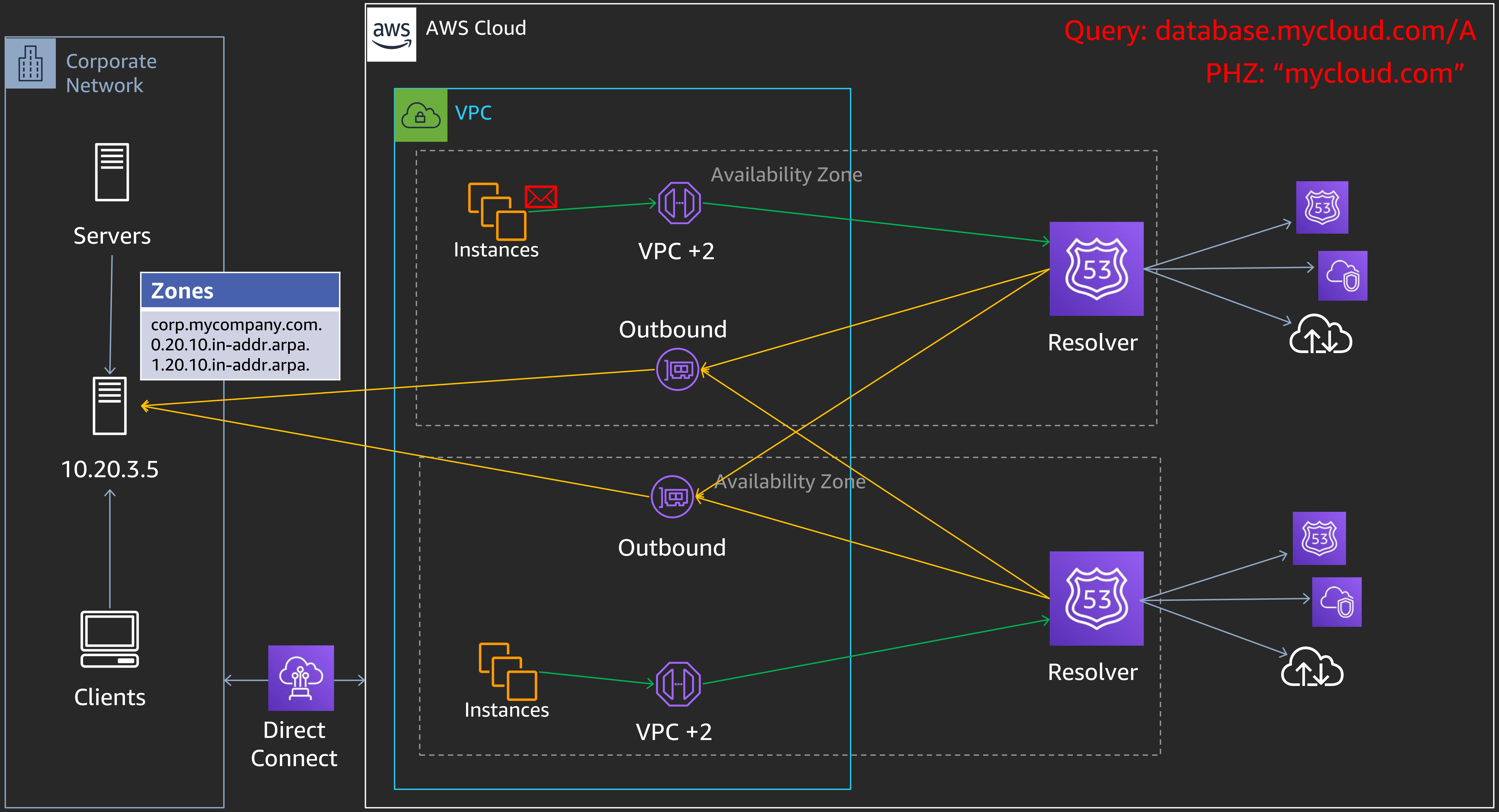
- Forward all public DNS resolution via on-premises resolvers
- Route 53 Resolver should answer: amazonaws.com.
- Private Hosted Zone: mycloud.com.
- AWS PrivateLink: kinesis.eu-west-2.amazonaws.com.
- Corp office namespace: corp.mycloud.com.
- VPC CIDR: 10.10.0.0/23
- On-premises CIDR range: 10.20.0.0/23

Resolver rules example

Domain	Type	Endpoint	Targets
“.”	SYSTEM (auto-defined)		
“.”	**FORWARD**	**rslvr-out-d085c56**	**10.20.3.4, 10.20.3.5**
amazonaws.com	**SYSTEM**		
mycloud.com.	SYSTEM (auto-defined)		
kinesis.eu-west-2.amazon…	SYSTEM (auto-defined)		
eu-west-2.compute.internal.	SYSTEM (auto-defined)		
eu-west-2.compute.amaz….	SYSTEM (auto-defined)		

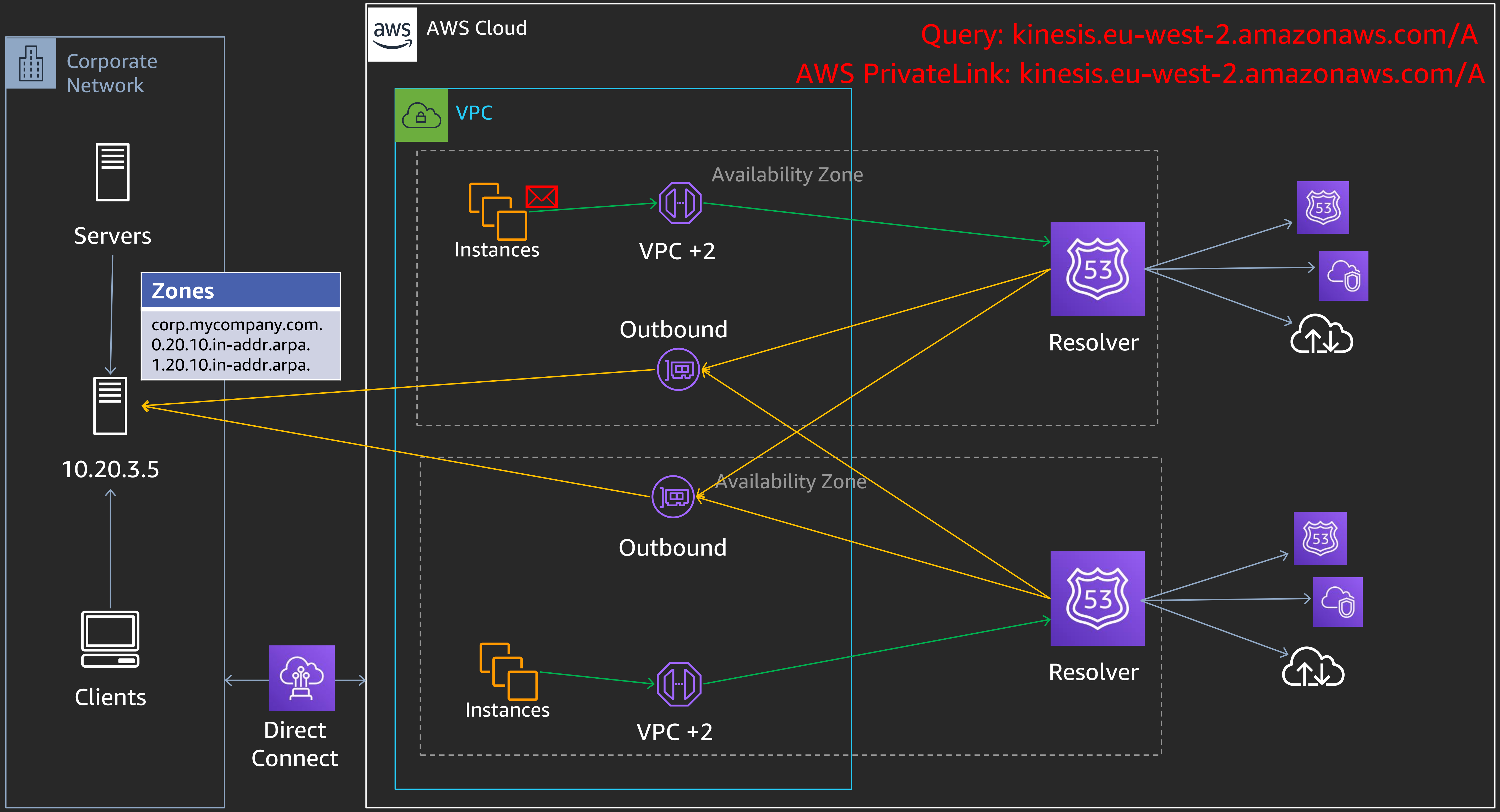
Query: database.mycloud.com/A

PHZ: “mycloud.com”



Zones

corp.mycompany.com.
0.20.10.in-addr.arpa.
1.20.10.in-addr.arpa.



Query: kinesis.eu-west-2.amazonaws.com/A

AWS PrivateLink: kinesis.eu-west-2.amazonaws.com/A

Zones

corp.mycompany.com.
0.20.10.in-addr.arpa.
1.20.10.in-addr.arpa.

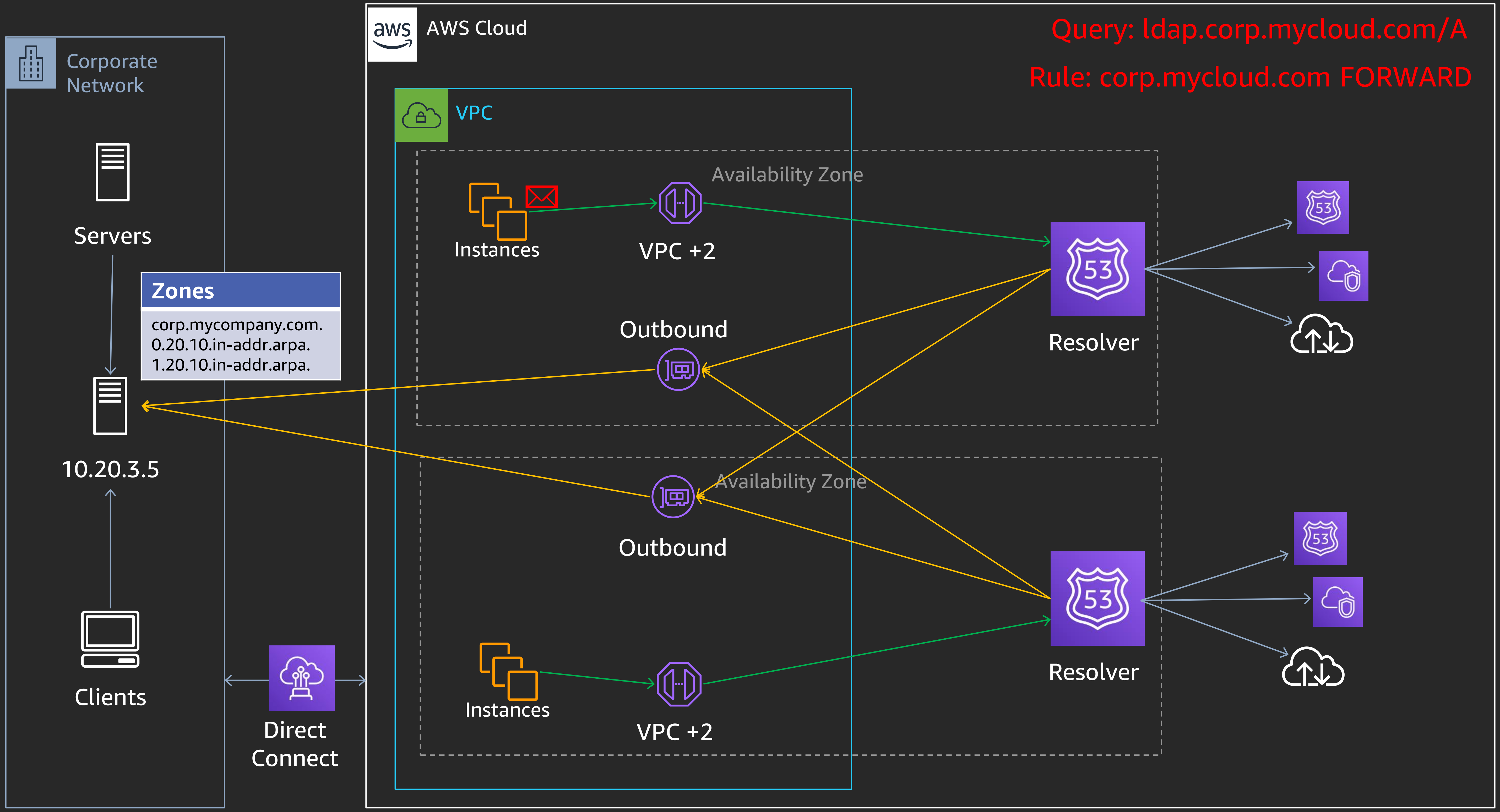
Resolver rules example

Requirements:

- Forward all public DNS resolution via on-premises resolvers
- Route 53 Resolver should answer: amazonaws.com.
- Private Hosted Zone: mycloud.com.
- AWS PrivateLink: kinesis.eu-west-2.amazonaws.com.
- Corp office namespace: corp.mycloud.com.
- VPC CIDR: 10.10.0.0/23
- On-premises CIDR range: 10.20.0.0/23

Resolver rules example

Domain	Type	Endpoint	Targets
“.”	SYSTEM (auto-defined)		
“.”	**FORWARD**	**rslvr-out-d085c56**	**10.20.3.4, 10.20.3.5**
amazonaws.com	**SYSTEM**		
mycloud.com.	SYSTEM (auto-defined)		
corp.mycloud.com.	**FORWARD**	**rslvr-out-d085c56**	**10.20.3.4, 10.20.3.5**
kinesis.eu-west-2.amazon…	SYSTEM (auto-defined)		
eu-west-2.compute.internal.	SYSTEM (auto-defined)		
eu-west-2.compute.amaz….	SYSTEM (auto-defined)		



Query: ldap.corp.mycloud.com/A

Rule: corp.mycloud.com FORWARD

Corporate Network

Servers

Zones

corp.mycompany.com.
0.20.10.in-addr.arpa.
1.20.10.in-addr.arpa.

10.20.3.5

Clients

Direct Connect

AWS Cloud

VPC

Availability Zone

Instances

VPC +2

Outbound

Resolver

Availability Zone

Outbound

Instances

VPC +2

Resolver

Resolver rules example

Requirements:

- Forward all public DNS resolution via on-premises resolvers
- Route 53 Resolver should answer: amazonaws.com.
- Private Hosted Zone: mycloud.com.
- AWS PrivateLink: kinesis.eu-west-2.amazonaws.com.
- Corp office namespace: corp.mycloud.com.
- VPC CIDR: 10.10.0.0/23
- On-premises CIDR range: 10.20.0.0/23

Resolver rules examples (reverse)

Domain	Type	Endpoint	Targets
“.”	SYSTEM (auto-defined)		
“.”	**FORWARD**	**rslvr-out-d085c56**	**10.20.3.4, 10.20.3.5**
10.in-addr.arpa.	SYSTEM (auto-defined)		
0.10.10.in-addr.arpa.	SYSTEM (auto-defined)		
1.10.10.in-addr.arpa.	SYSTEM (auto-defined)		

Resolver rules example

Requirements:

- Forward all public DNS resolution via on-premises resolvers
- Route 53 Resolver should answer: amazonaws.com.
- Private Hosted Zone: mycloud.com.
- AWS PrivateLink: kinesis.eu-west-2.amazonaws.com.
- Corp office namespace: corp.mycloud.com.
- VPC CIDR: 10.10.0.0/23
- On-premises CIDR range: 10.20.0.0/23

Resolver rules examples (reverse)

Domain	Type	Endpoint	Targets
“.”	SYSTEM (auto-defined)		
“.”	**FORWARD**	**rslvr-out-d085c56**	**10.20.3.4, 10.20.3.5**
10.in-addr.arpa.	SYSTEM (auto-defined)		
0.10.10.in-addr.arpa.	SYSTEM (auto-defined)		
1.10.20.in-addr.arpa.	SYSTEM (auto-defined)		
0.20.10.in-addr.arpa.	**FORWARD**	**rslvr-out-d085c56**	**10.20.3.4, 10.20.3.5**
1.20.10.in-addr.arpa.	**FORWARD**	**rslvr-out-d085c56**	**10.20.3.4, 10.20.3.5**

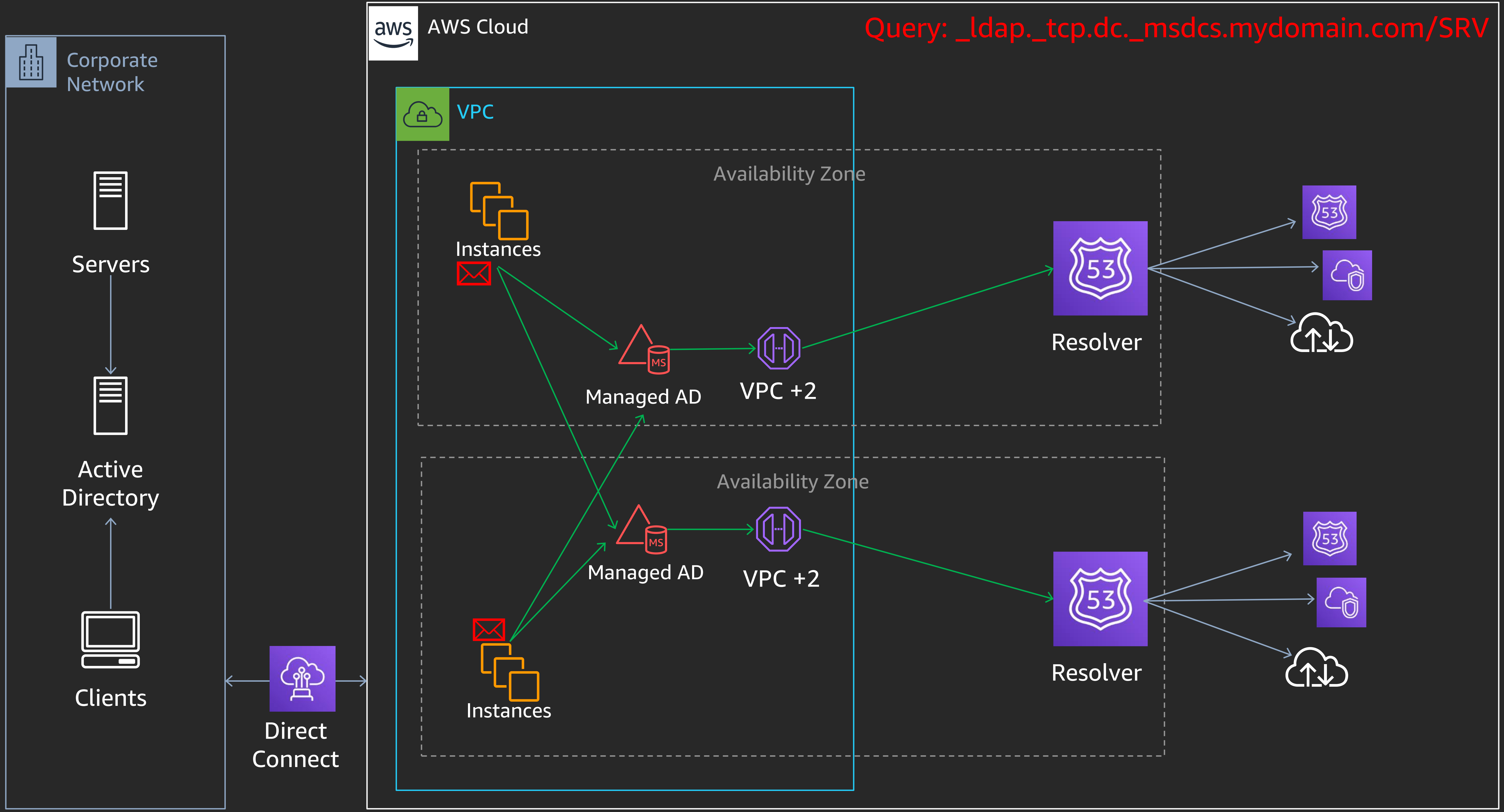
Resolver rules summary

- Most specific rule wins
- Private DNS, PrivateLink endpoints, and VPC DNS get autodefined rules
  - You can override them
- Best practice to allow SYSTEM resolve amazonaws.com.
- Don’t forget reverse records, e.g., for Kerberos
- VPC CIDR ranges get /24 rules (e.g., x.y.10.in-addr.arpa) autodefined
  - You can override them

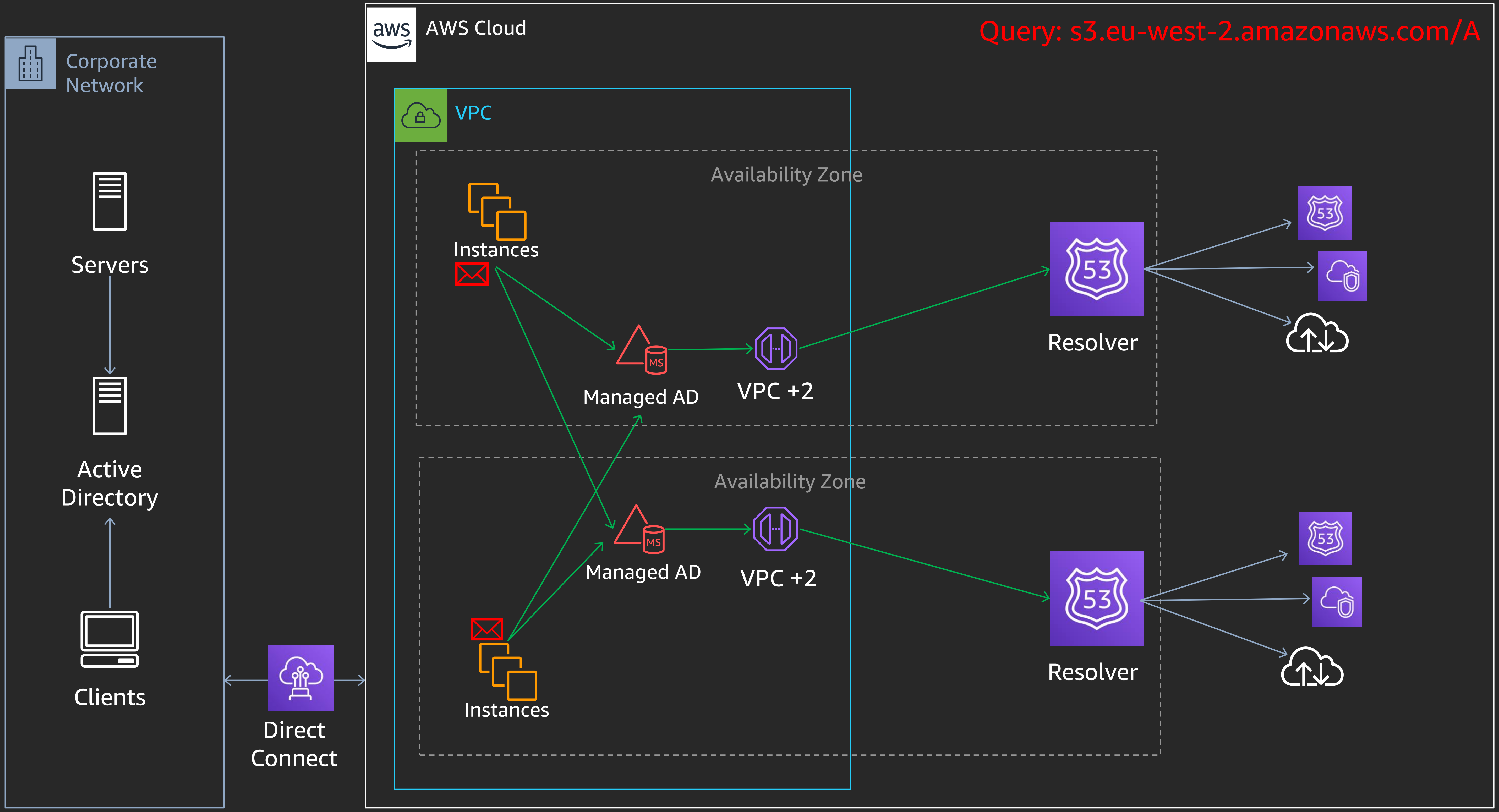
Route 53 Resolver and Active Directory

Active Directory in EC2

- AWS Managed Microsoft AD, Simple AD and self-install
- Active Directory manages Dynamic DNS for hosts on Active Directory domain
    - Forward and Reverse DNS are important (e.g. for Kerberos)
- Standard practice is to update DHCP to point at DCs for DNS
    - DCs answer for Active Directory domain and reverse records
    - DCs typically forward to Route 53 Resolver (+2) for all else



Query: _ldap._tcp.dc._msdcs.mydomain.com/SRV



Query: s3.eu-west-2.amazonaws.com/A

Active Directory in EC2

Like forward instances, this solution works well for many customers

Problems:

- Windows instances all tend to query the first name server in DHCP
- Scaling: 1024pps limit on VPC+2 applies
- Loss of Availability Zone isolation

Route 53 Resolver and Active Directory

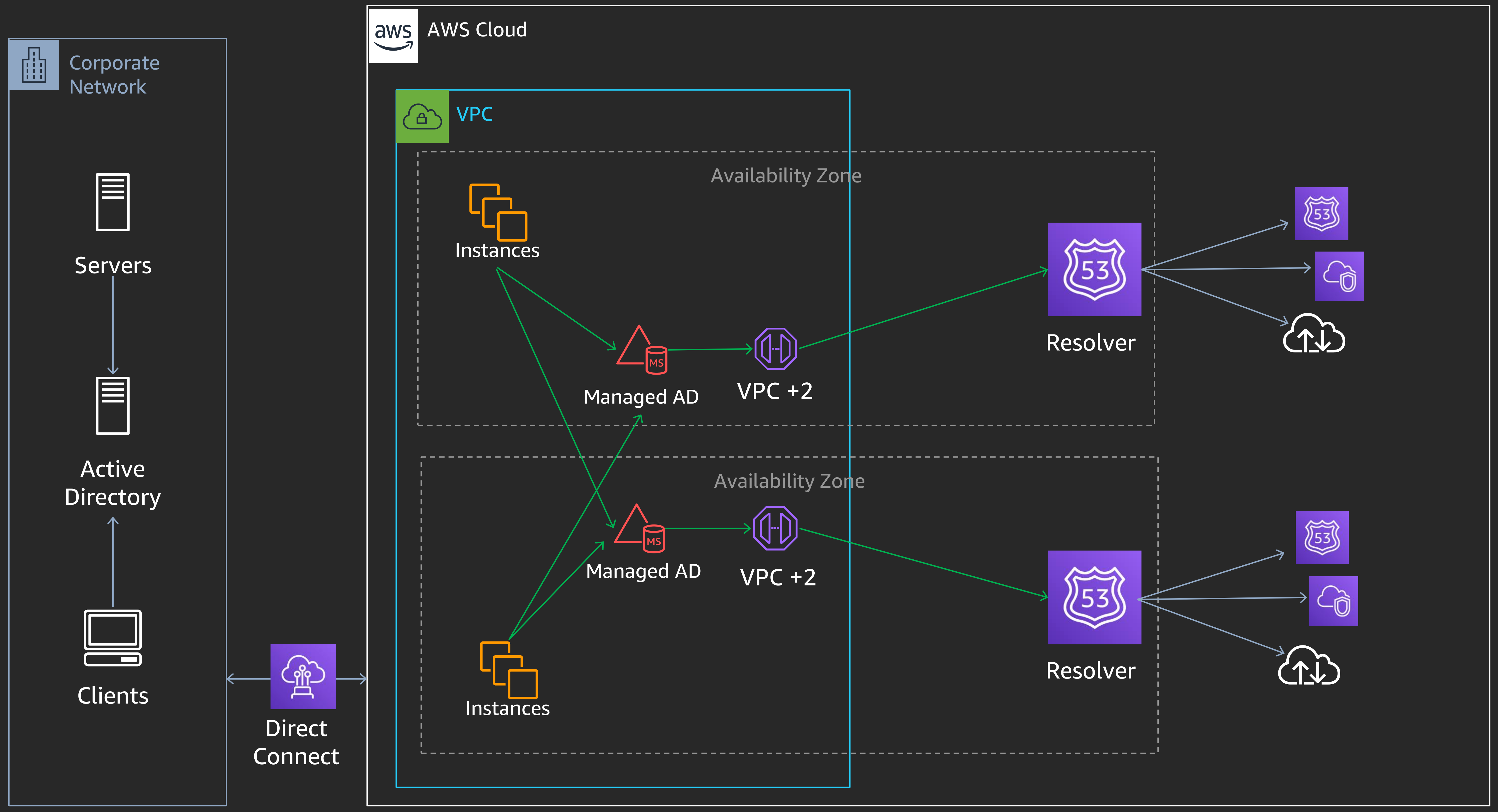
Steps:

1. Create Route 53 Resolver outbound endpoint
2. Create Resolver rules
    1. Forward Active Directory domain to AWS Managed Microsoft AD DNS addresses
    2. Forward VPC subnets to AWS Managed Microsoft AD DNS addresses, overriding each autodefined rule (/24 IP ranges)
3. Change DHCP domain-name-servers back to AmazonProvidedDNS

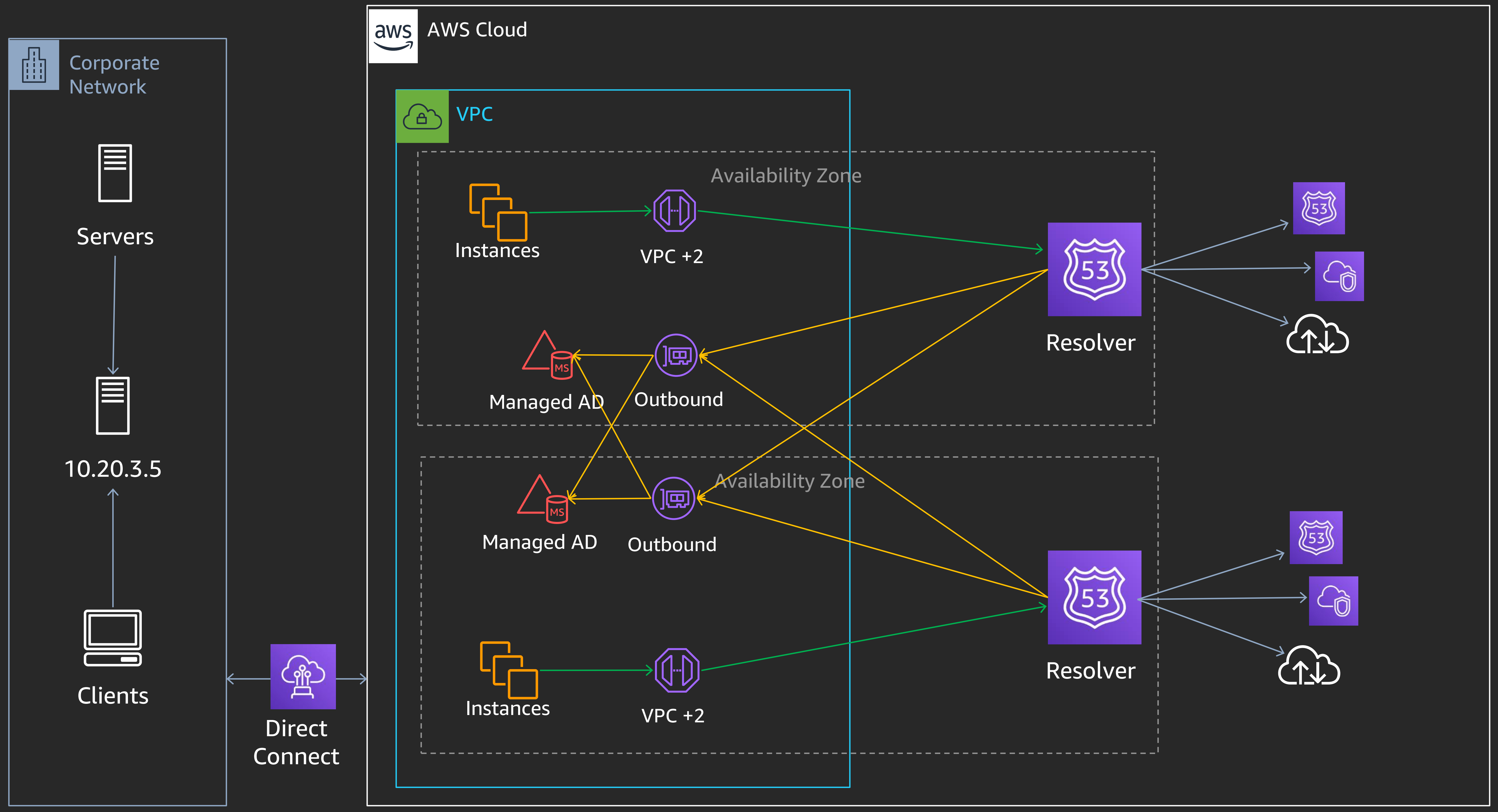
Active Directory in EC2

Requirements:

- Active Directory domain: mydomain.com
- VPC CIDR: 10.10.0.0/23



Corporate Network
Servers
Active Directory
Clients
Direct Connect
AWS Cloud
VPC
Availability Zone
Instances
Managed AD
MS
VPC +2
Resolver
53
Availability Zone
Managed AD
MS
VPC +2
Instances
Resolver
53

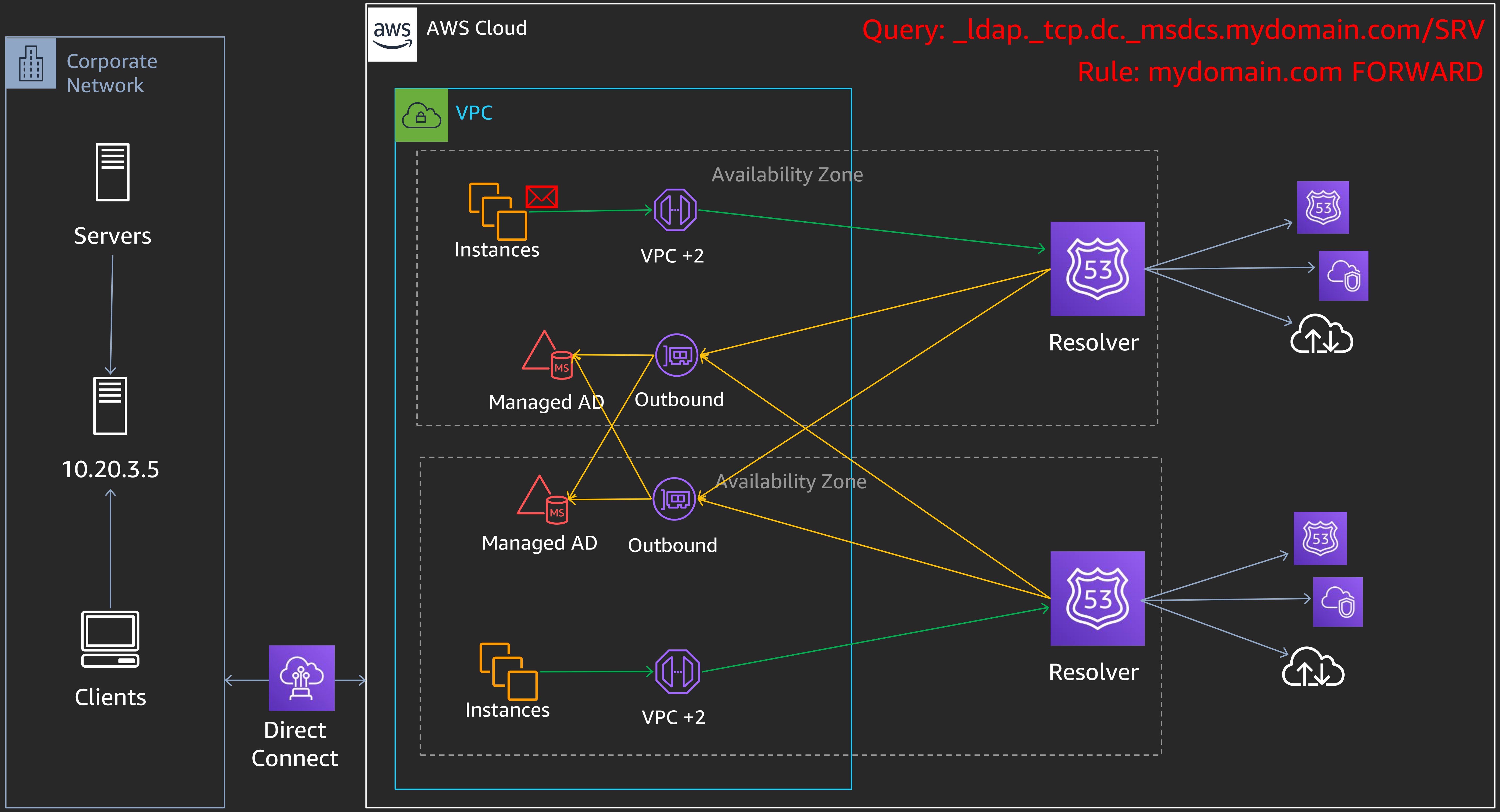

Corporate Network
Servers
10.20.3.5
Clients
Direct Connect
AWS Cloud
VPC
Availability Zone
Instances
VPC +2
Managed AD
Outbound
Resolver
53
MS
Availability Zone
Managed AD
Outbound
Instances
VPC +2
Resolver
53

Active Directory in EC2

Domain	Type	Endpoint	Targets
“.”	SYSTEM (auto-defined)		
mydomain.com.	**FORWARD**	**rslvr-out-d085c56**	**10.20.3.4, 10.20.3.5**
eu-west-2.compute.internal.	SYSTEM (auto-defined)		
eu-west-2.compute.amazonaws.com	SYSTEM (auto-defined)		

Active Directory in EC2 (reverse)

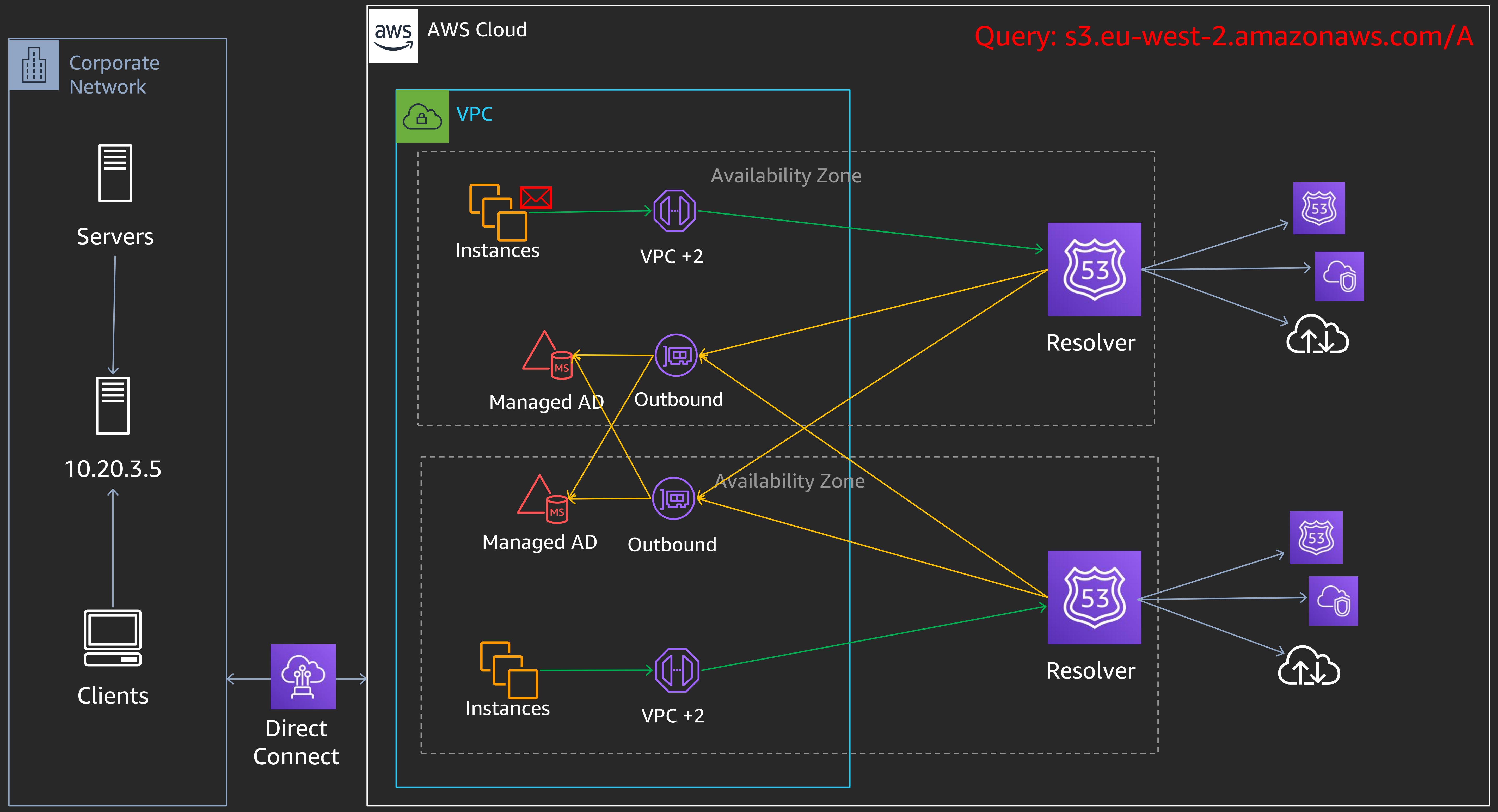
Domain	Type	Endpoint	Targets
"."	SYSTEM (auto-defined)		
"."	**FORWARD**	**rslvr-out-d085c56**	**10.20.3.4, 10.20.3.5**
10.in-addr.arpa.	SYSTEM (auto-defined)		
0.10.10.in-addr.arpa.	SYSTEM (auto-defined)		
1.10.20.in-addr.arpa.	SYSTEM (auto-defined)		
0.10.10.in-addr.arpa.	**FORWARD**	**rslvr-out-d085c56**	**10.20.3.4, 10.20.3.5**
1.10.10.in-addr.arpa.	**FORWARD**	**rslvr-out-d085c56**	**10.20.3.4, 10.20.3.5**



Query: _ldap._tcp.dc._msdcs.mydomain.com/SRV

Rule: mydomain.com FORWARD

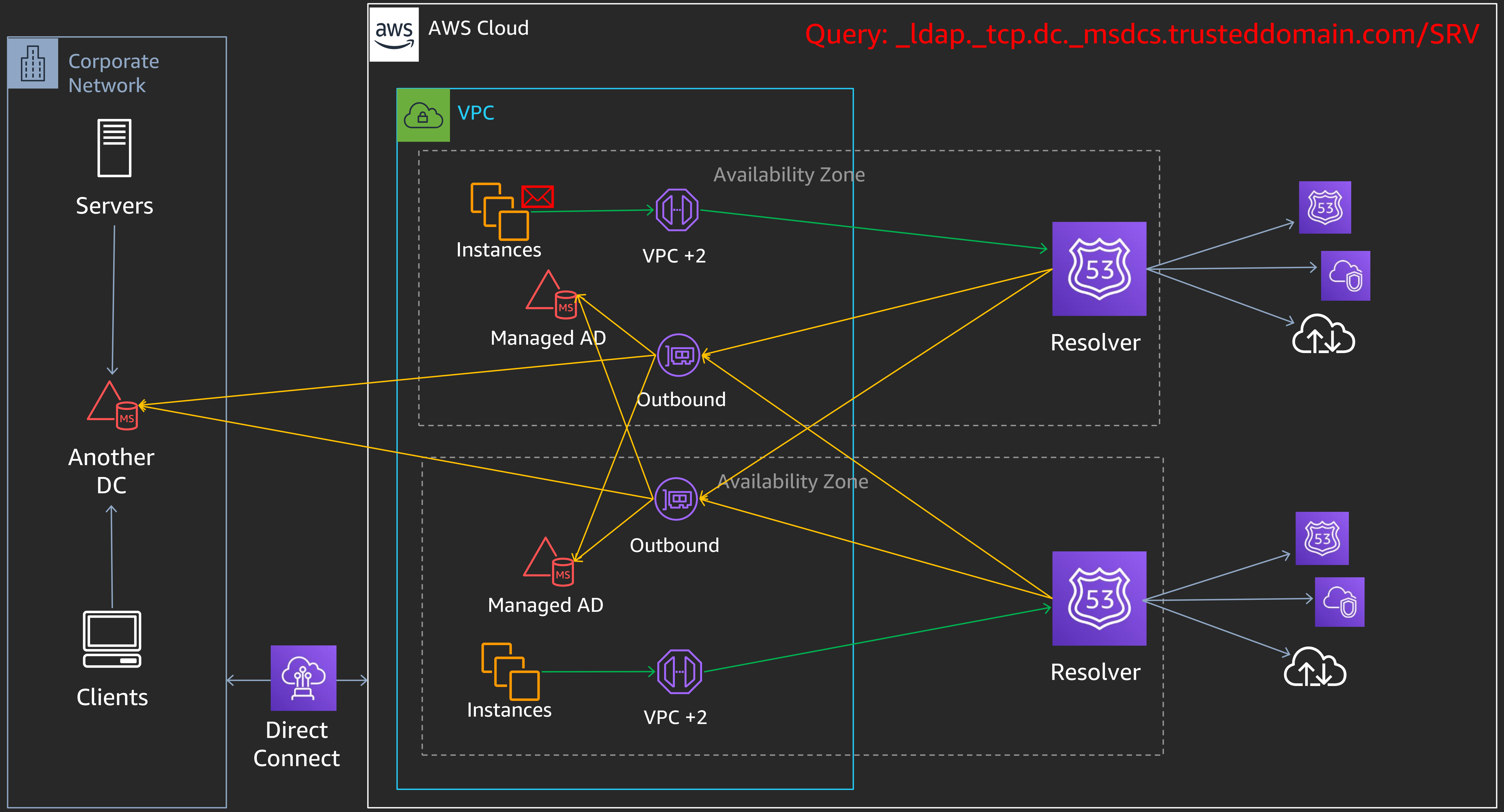
Query: s3.eu-west-2.amazonaws.com/A



Active Directory trusts

What if you have Active Directory trusts with an on-premises domain?

Typically prefer rules that forward direct to the trusted DC.



Query: _ldap._tcp.dc._msdcs.trusteddomain.com/SRV

Route 53 Resolver
Managing many VPCs

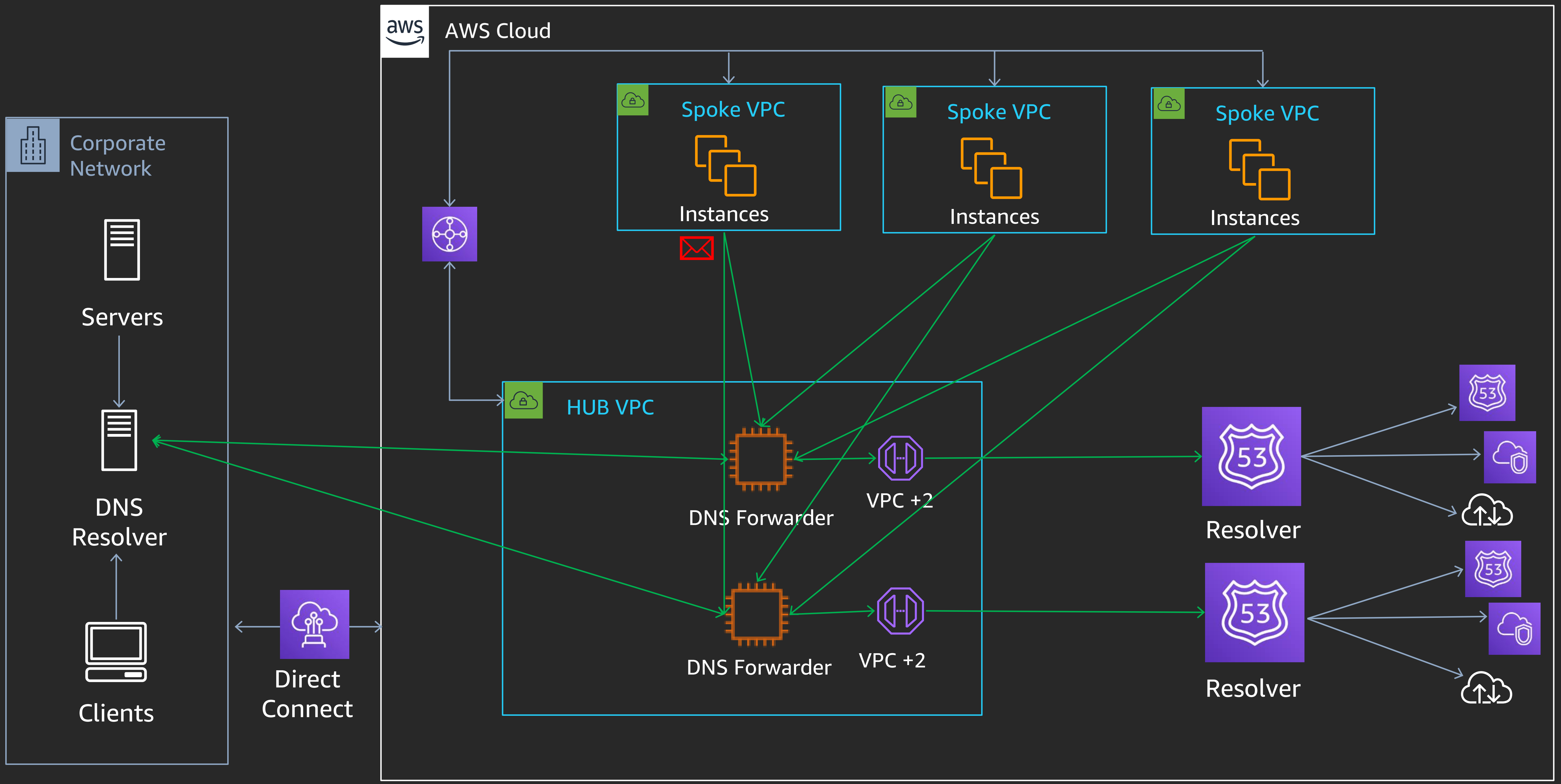
Managing DNS across many VPCs

Often large customers have:

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

Managing DNS centrally can be challenging.

Hub and spoke strategy (forwarding instances)



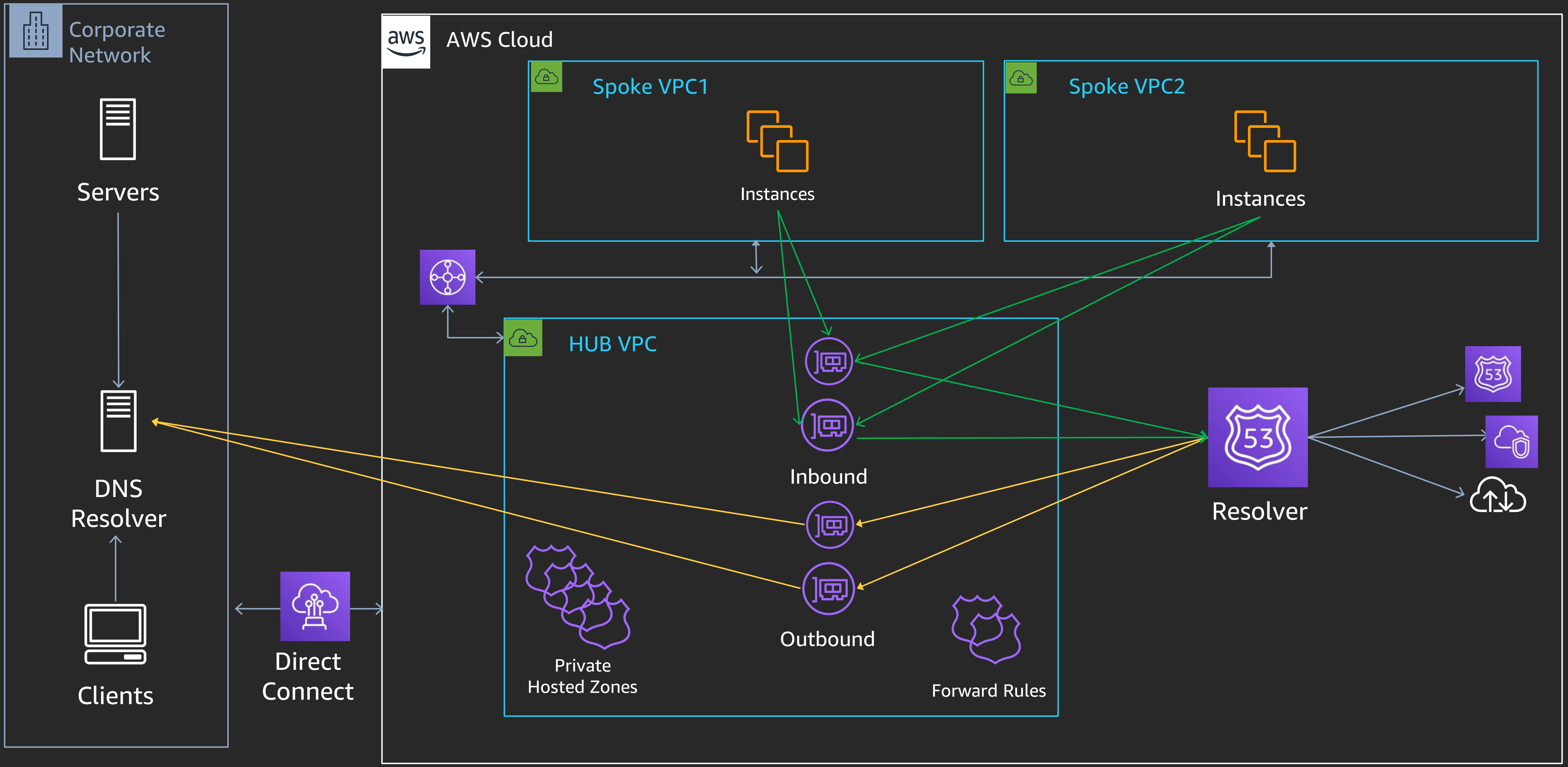
Hub and spoke strategies (Resolver Endpoints)

Four strategies have emerged in the community:

1. Manage hub DNS; change spoke DHCP domain-name-servers
2. Manage hub DNS; forward spoke queries to hub via endpoints
3. VPC sharing
4. Share and associate private hosted zones and resolver rules

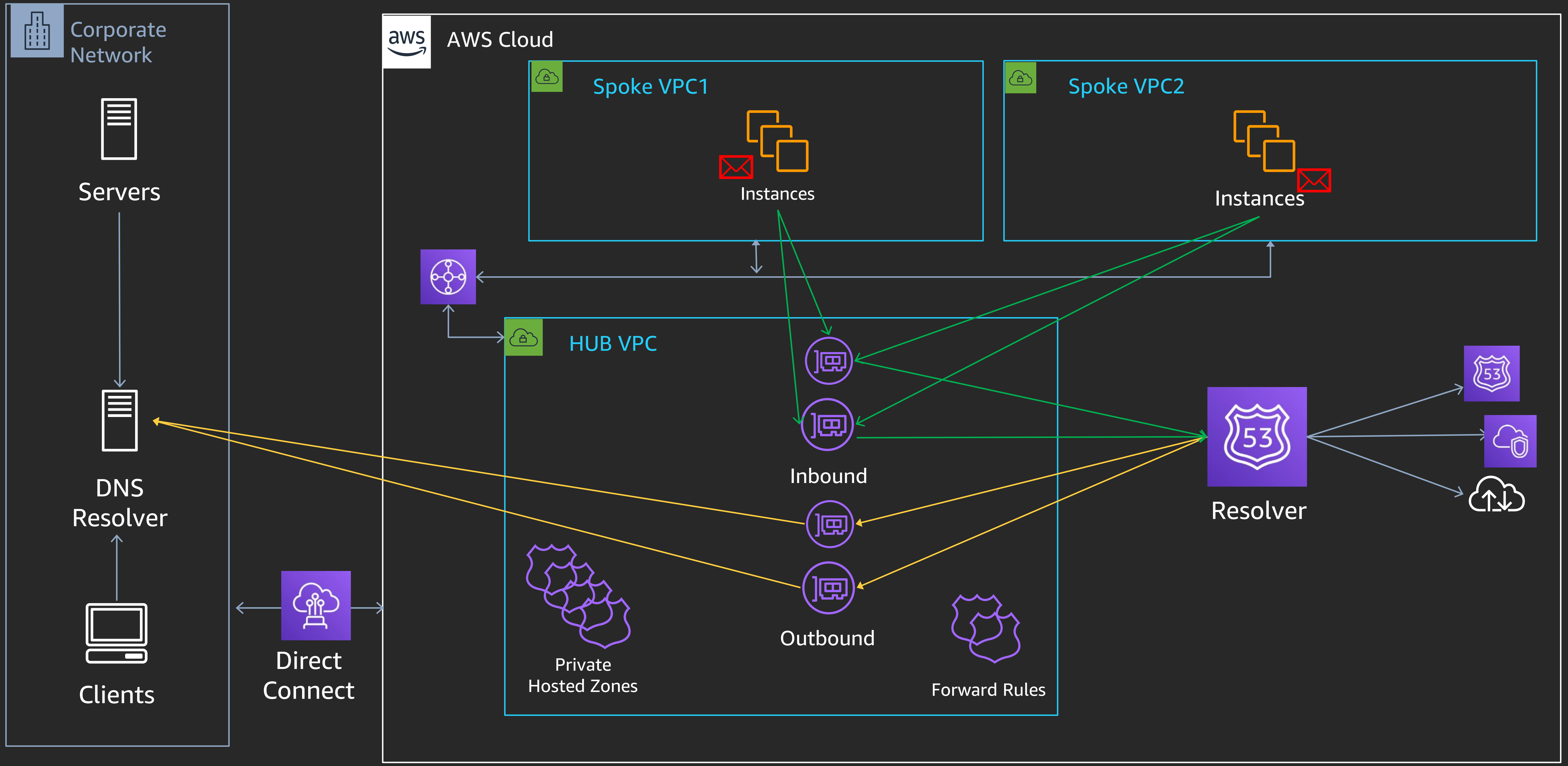
How do they compare?

1. Manage hub DNS; change DHCP



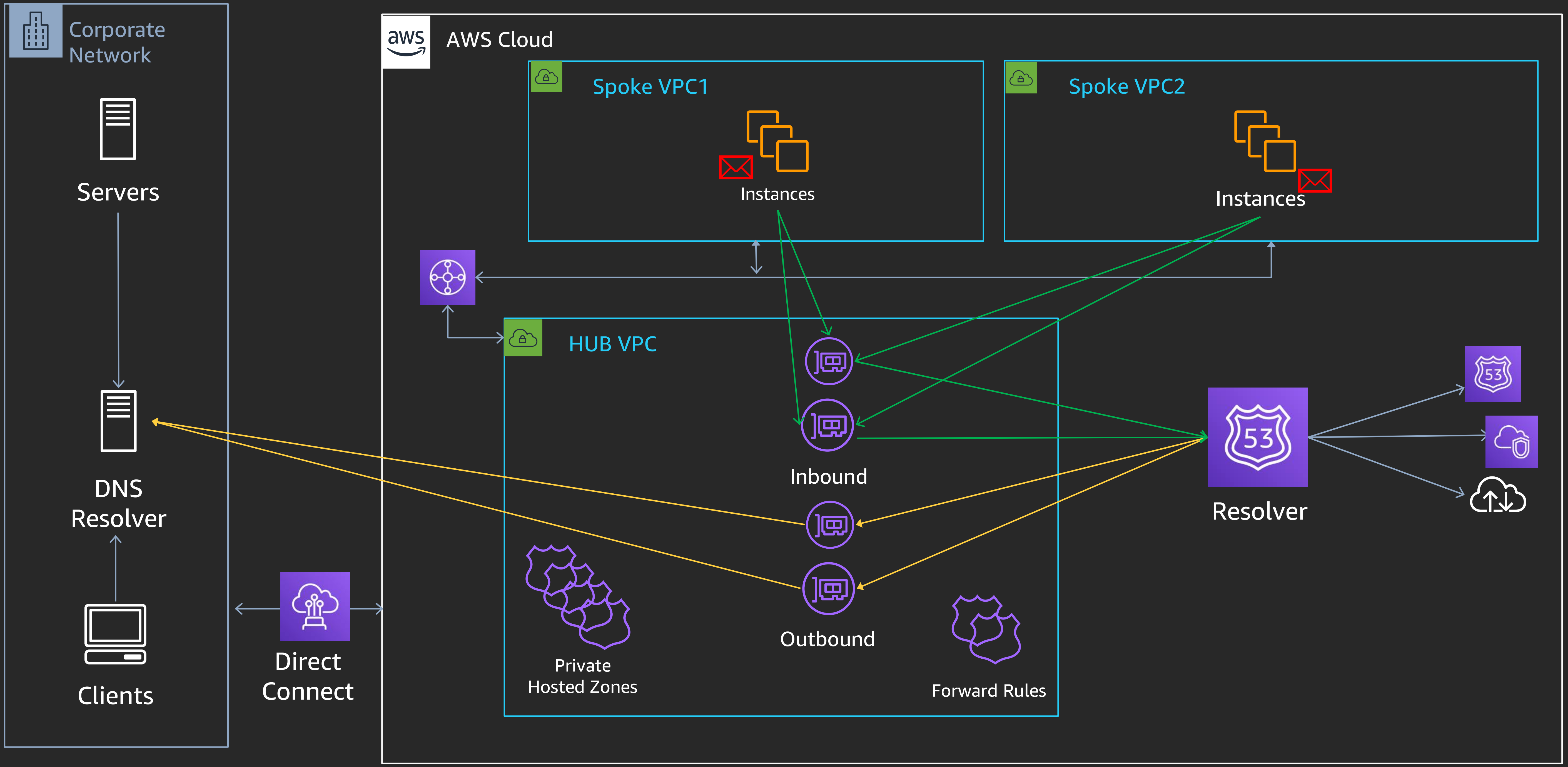
1. Manage hub DNS; change DHCP

Query: db.myprivatezone.com/A



1. Manage hub DNS; change DHCP

Query: corp.mydomain.com/A



1. Manage hub DNS; change DHCP

Pros:

- Familiar model (like Forwarding Instances)

Cons:

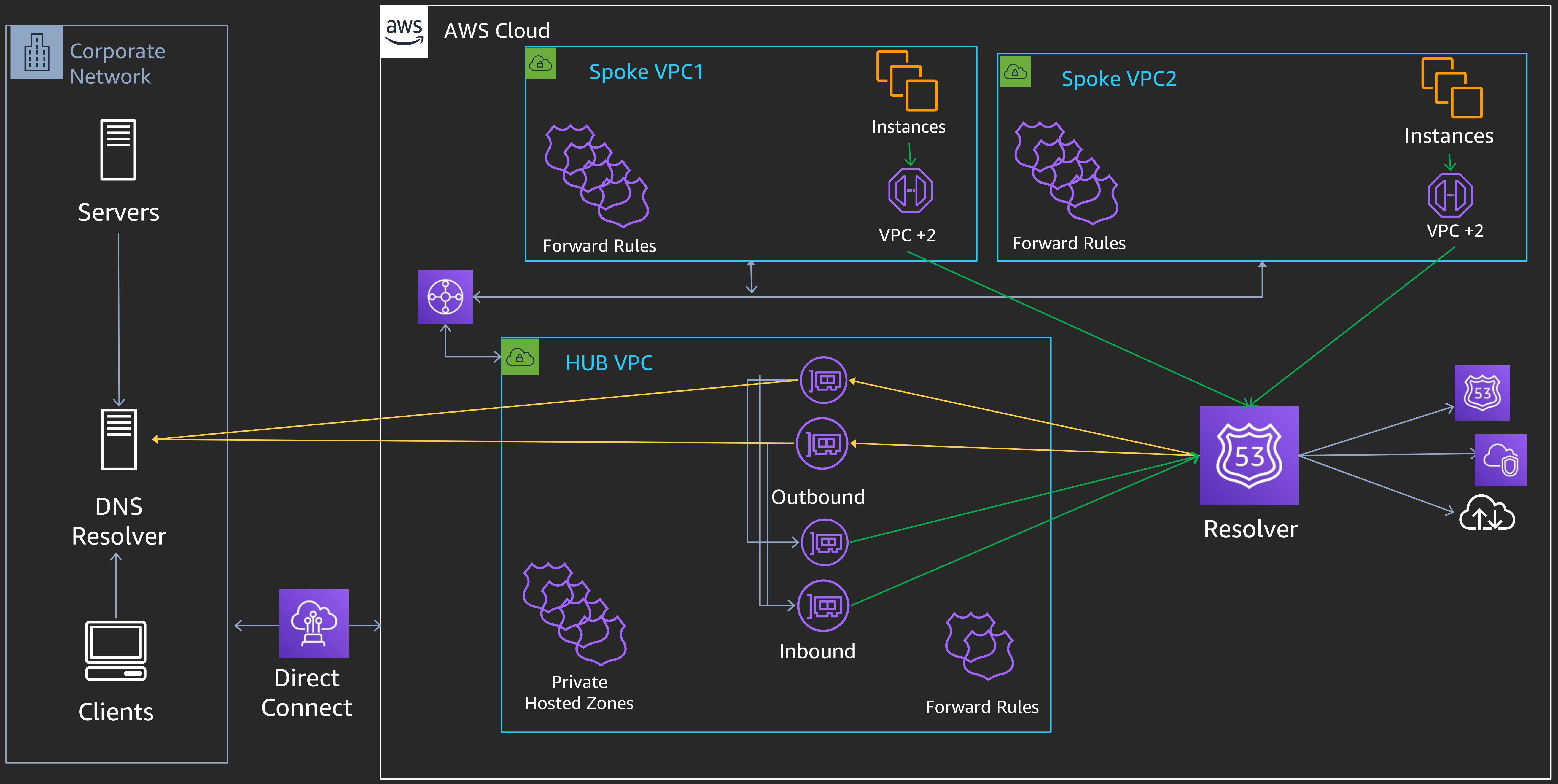
- Expect hot-spotting on single inbound ENI
- Not very fault tolerant
- No local instance cache
- All queries via 10K query/sec ENI limit
- Up to 4x inter-AZ hops per query
- Requires L3 connectivity between spokes and hub
- Higher query costs

Verdict: Not recommended

2. Manage hub DNS; forward via endpoints

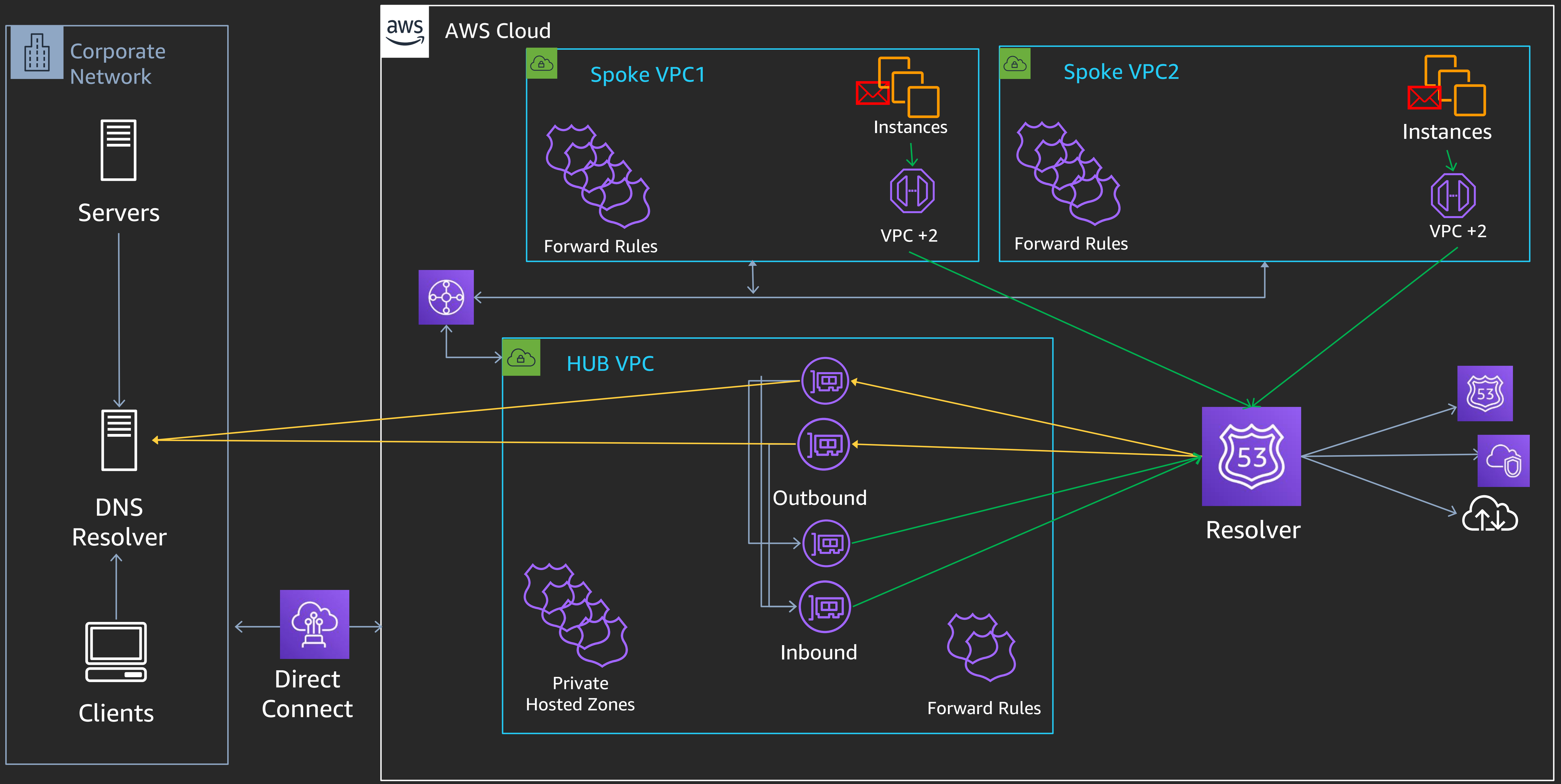
- Associate private hosted zones to hub VPC
- Outbound and inbound endpoint in hub VPC
- Rules forward from outbound endpoint through inbound endpoint to resolver for private hosted zones
- Additional rules forward to on-premises
- Share and associate rules to spoke VPCs

2. Manage hub DNS; forward via endpoints

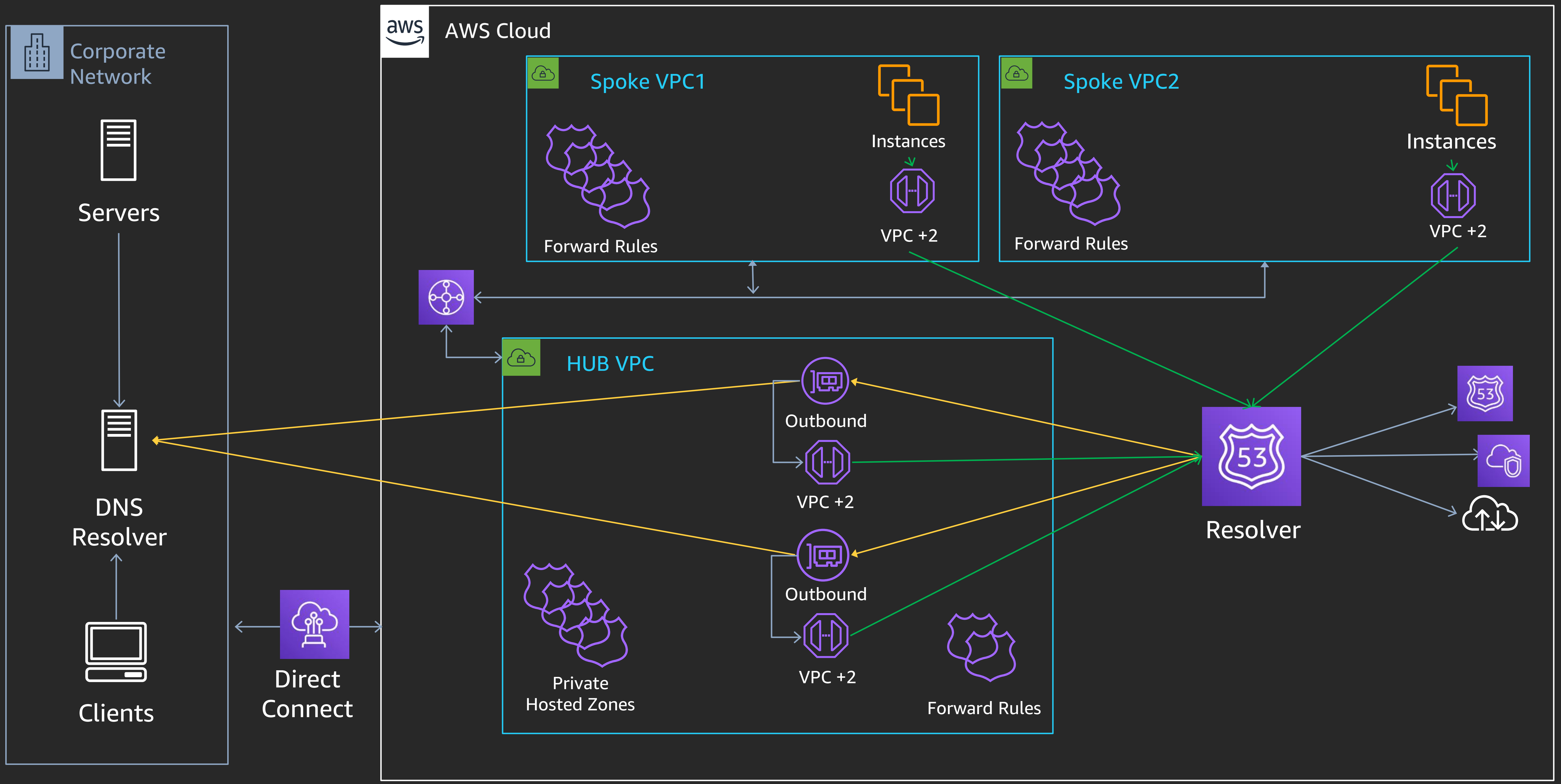


2. Manage hub DNS; forward via endpoints

Query: db.myprivatezone.com/A



2. Manage hub DNS; forward via endpoints



2. Manage hub DNS; forward via endpoints

Pros:

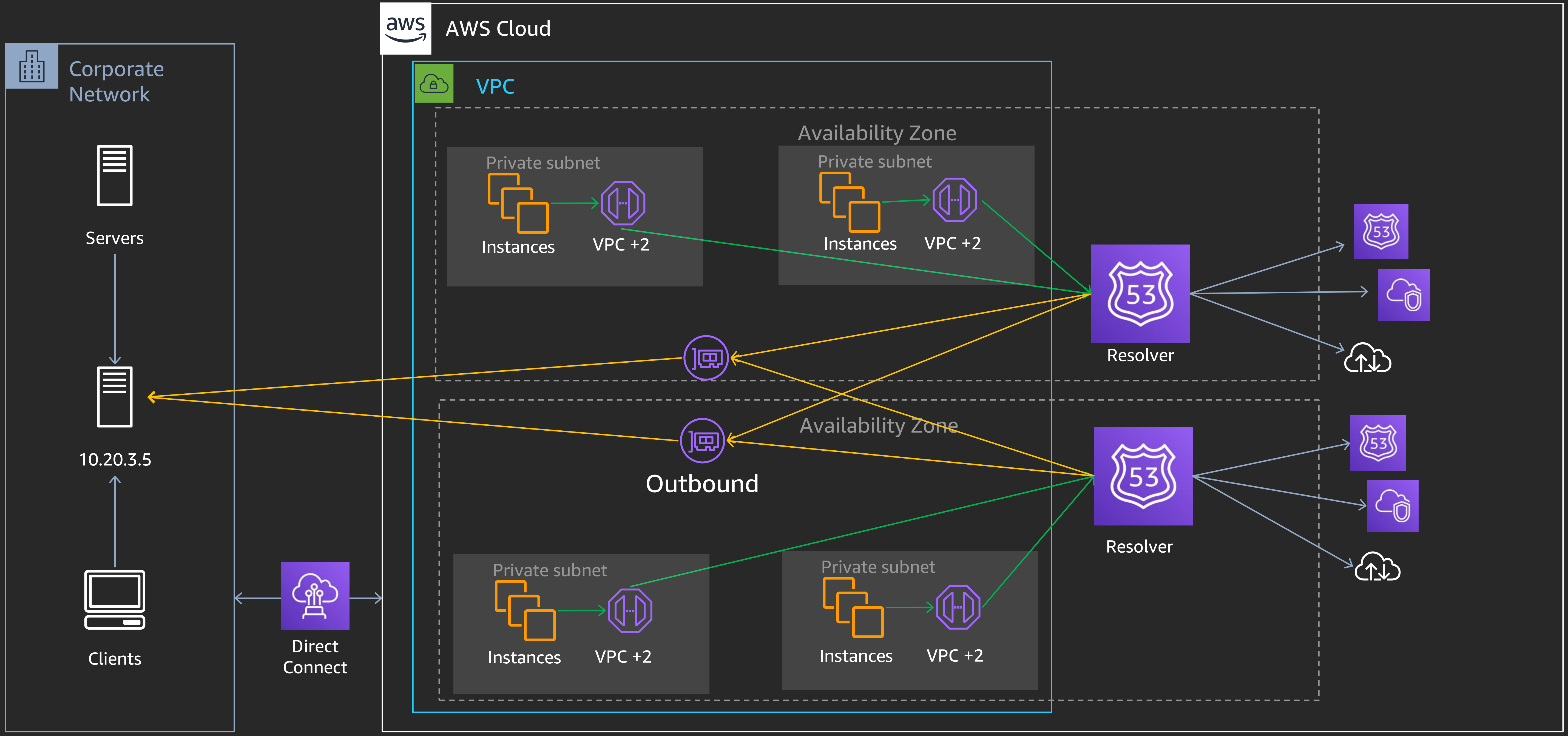
- Easier setup/maintenance
- Uses local +2 Resolver, cache
- Non-forwarded queries use scalable path

Cons:

- Less scalable (10K query/sec Limit; 1024pps if VPC+2)
- Each query crosses between Availability Zone up to four times
- Not as failure resilient
- Query costs

Verdict: Compromise but may be useful

3. VPC sharing



3. VPC sharing

Pros:

- Don’t need 100s of VPCs!
- One VPC, guaranteed consistent view of DNS
- Simplified networking

Cons:

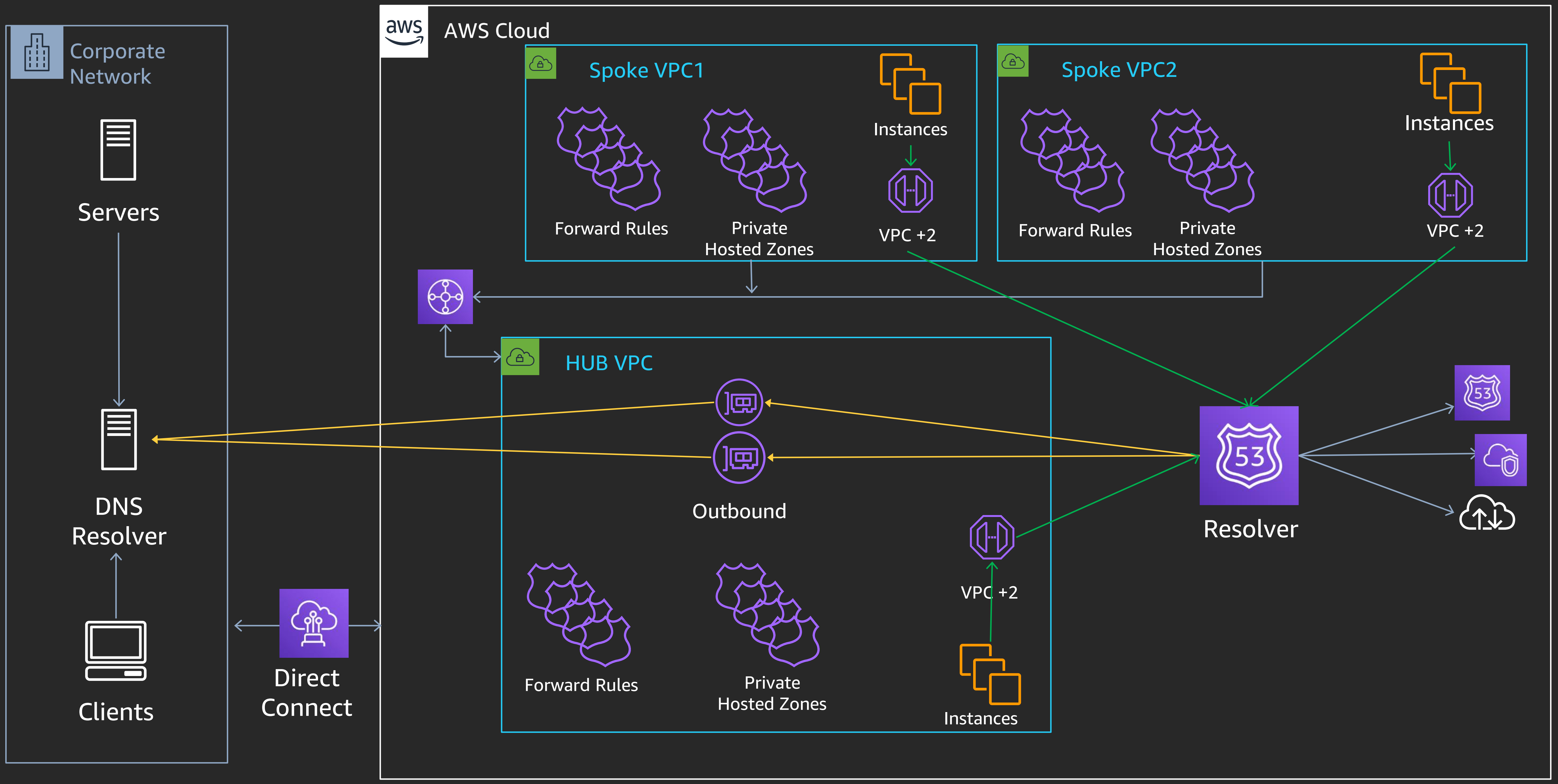
- Some feature gaps today
- Some reduced autonomy/isolation for dev teams

Verdict: Best practice

4. Share and associate

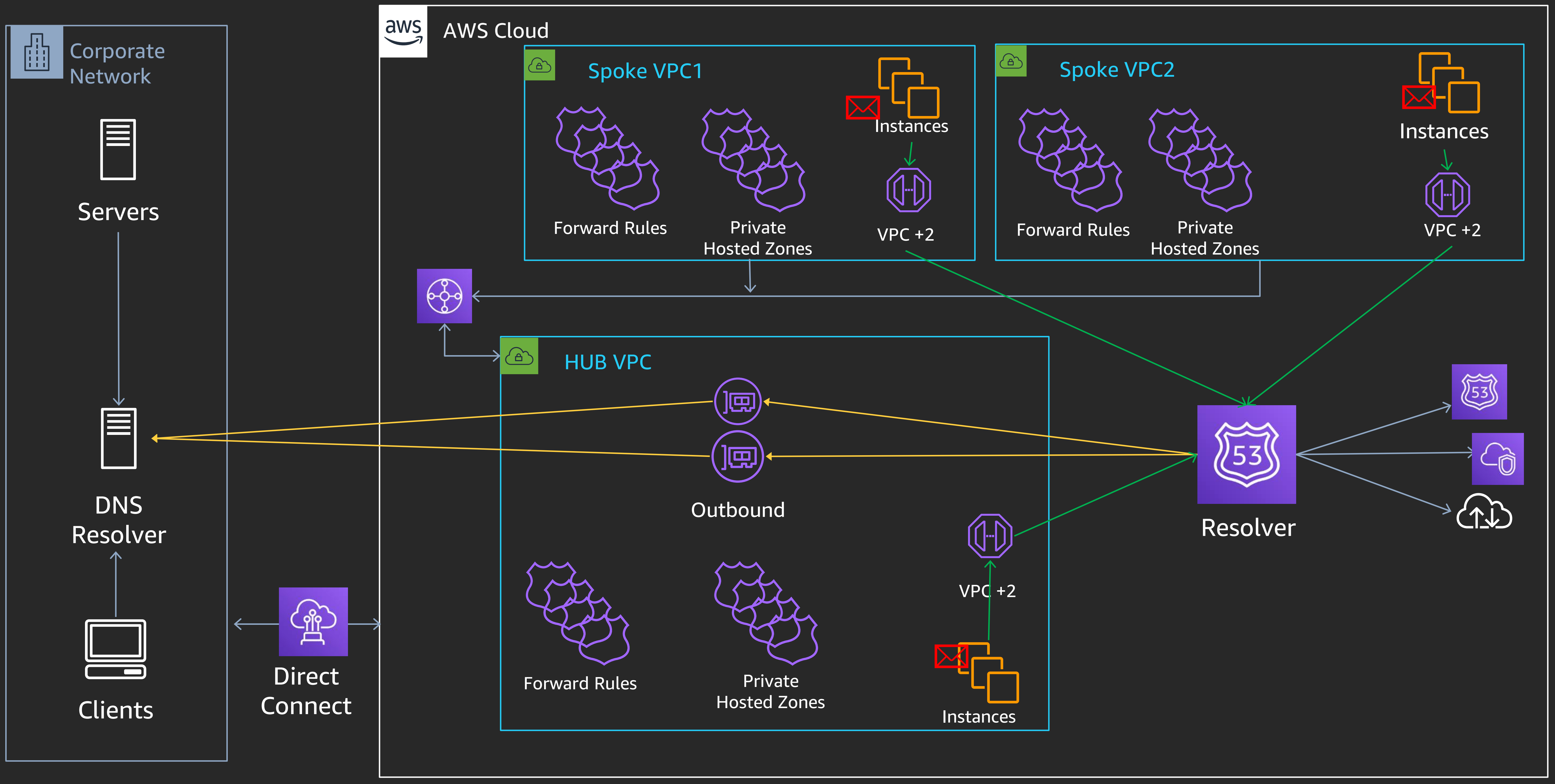
- Ensure that each VPC has correct view of DNS
- Share private hosted zones and rules
- Associate all private hosted zones and rules to every VPC
- Outbound/inbound endpoints only for on-premises resolution

4. Share and associate

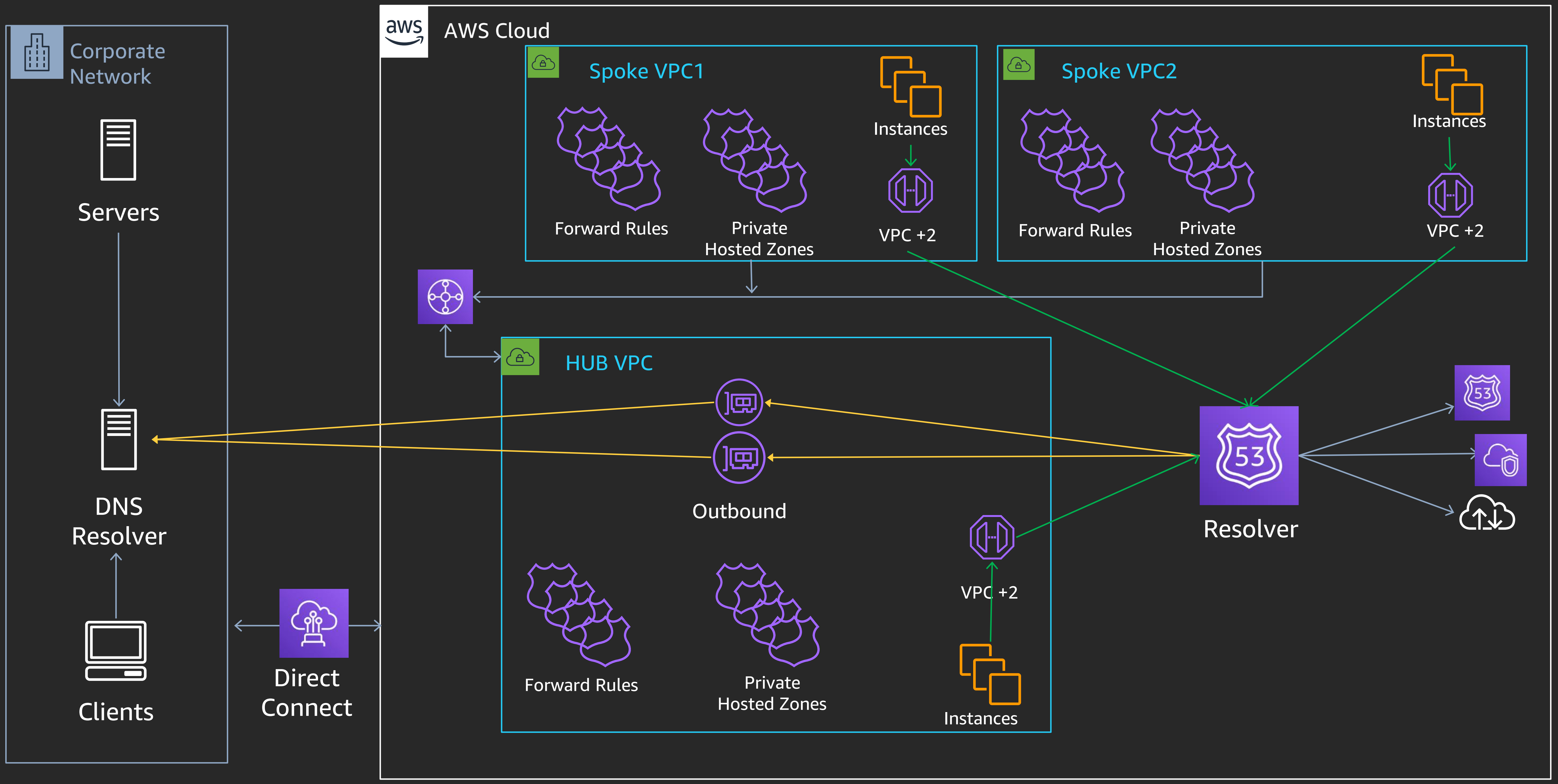


4. Share and associate

Query: db.myprivatezone.com/A



4. Share and associate



4. Share and associate

How do we handle PrivateLink endpoints between VPCs?

Create a sharable private hosted zone with an alias

- Private zone called **ssm.eu-west-2.amazonaws.com**
- **ssm.eu-west-2.amazonaws.com** A (ALIAS) **vpce-xxx….vpce.amazonaws.com.**

Blog: “**Integrating AWS Transit Gateway with AWS PrivateLink and Amazon Route 53 Resolver**”

4. Share and associate zones and rules

Pros:

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

Cons:

- PHZ Sharing is cumbersome and CLI/API only
- Limits on VPC Associations per Private Hosted Zone

Verdict: Best practice

Route 53 Resolver Best Practices

AWS re:Invent

aws

Route 53 Resolver best practices

1. High availability
   1. Always use resolver ENIs in multiple Availability Zones
2. Use forwarding sparingly
   1. Use AmazonProvidedDNS for EC2 instances
   2. Prefer associating private hosted zones/rules to all VPCs
   3. Keep queries within the local Availability Zone where possible
3. Monitoring
   1. Set CloudWatch alarms on resolver endpoints approaching QPS limits

Related Sessions

NET411-R – Managing DNS across hundreds of VPCs

NET411-R1 – Managing DNS across hundreds of VPCs

NET204-R - Hybrid connectivity on AWS

NET204-R1 - Hybrid connectivity on AWS

NET321 - AWS PrivateLink deployments: DNS mechanisms for routing & resiliency

NET336-R - Amazon Route 53 Resolver: Centralized DNS management of hybrid cloud

NET336-R1 - Amazon Route 53 Resolver: Centralized DNS management of hybrid cloud

NET336-R - Amazon Route 53 Resolver: Centralized DNS management of hybrid cloud

Learn networking with AWS Training and Certification

Resources created by the experts at AWS to help you build and validate networking skills

Free digital courses cover topics related to networking and content delivery, including Introduction to Amazon CloudFront and Introduction to Amazon VPC

Validate expertise with the **AWS Certified Advanced Networking - Specialty** exam

Visit aws.amazon.com/training/paths-specialty

aws training and certification

Thank you!

Gavin McCullagh

Amazon Route 53

!

Please complete the session survey in the mobile app.

AWS re:Invent

aws