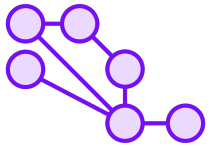
Amazon Route 53: Resolvers

Andru Estes
Principal Author
andru-estes

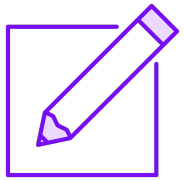
Hybrid DNS Overview

Hybrid DNS Overview



It is increasingly more common for organizations to have both on-premises resources and cloud-based resources for their workloads

Due to this, proper DNS name resolution is essential for both types of resources to function



This is where a Hybrid DNS configuration comes in

Benefits and Use Cases

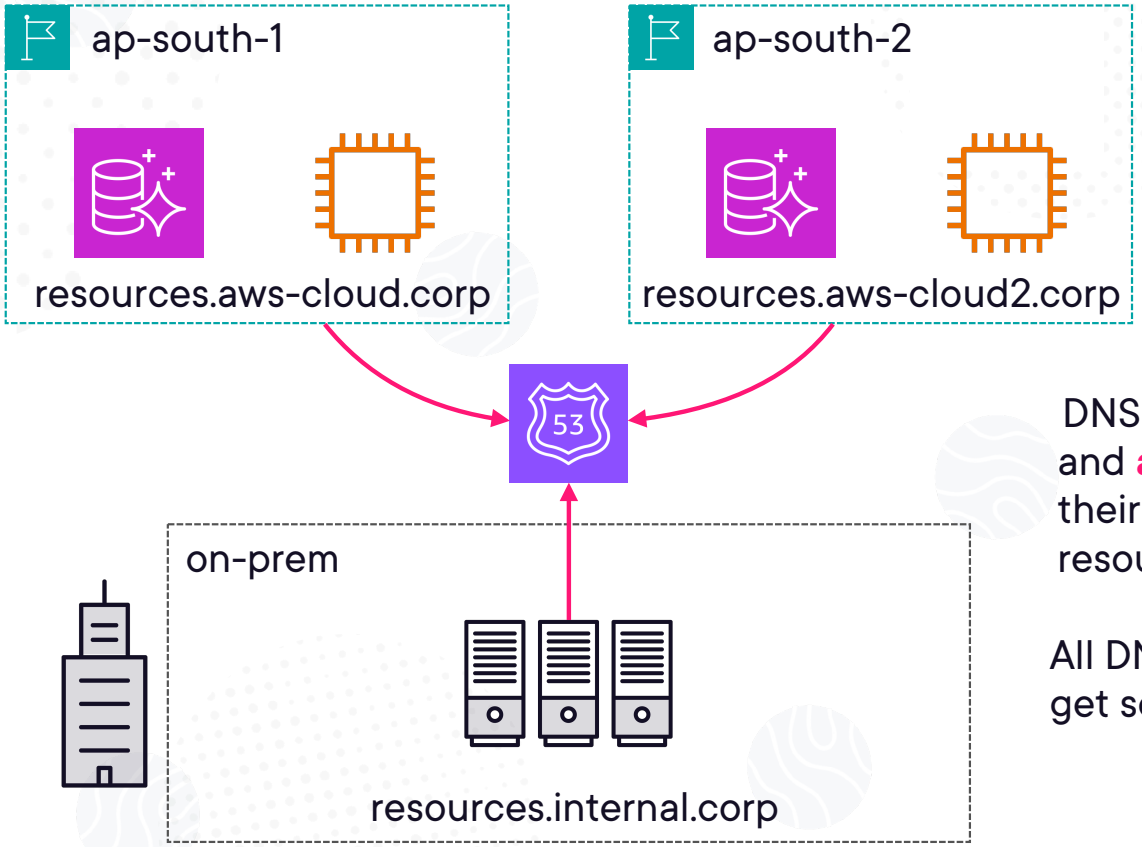
Benefits:

- You can manage DNS records for both on-premises and AWS resources from a central location (*Route 53*)
- Route 53's global infrastructure ensures high availability and scalability for your DNS resolution
- Easily connect your on-premises and AWS environments

Use Cases:

- Organizations with resources split between on-premises data centers and AWS
- Manage DNS during a phased migration to AWS
- Keep existing on-premises DNS infrastructure while utilizing AWS for new services

Simplified Architecture Diagram Example



DNS queries for **aws-cloud.corp** and **aws-cloud2.corp** get sent to their respective cloud-based resources and Regions

All DNS queries for **internal.corp** get sent to on-prem

Defining Hybrid DNS Rules with Route 53 Endpoints

The Amazon Route 53 Resolver

DNS resolver that responds recursively to DNS queries from AWS resources

VPCs connect to Route 53 Resolvers at a VPC+2 IP address and it is available by default in all VPCs!

The VPC+2 IP address connects to a Route 53 Resolver within an Availability Zone (*Remember the reserved IPs*)

Works for the following:

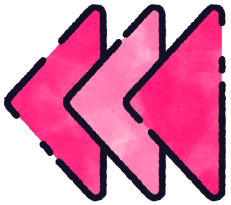
- Public records (*pluralsight.com*)
- Amazon VPC-specific DNS names (*ec2-10-0-2-144.compute-1.amazonaws.com*)
- Amazon Route 53 private hosted zones (*cloud.internal.corp*)

Image Source: http://unsplash.com

Remember DHCP Option Sets? This is what they mean when they list “AmazonProvidedDNS”.

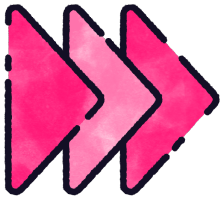
Resolver Endpoints and Rules

Resolver endpoints and conditional forwarding rules work together to allow you to resolve DNS queries between your on-premises resources and VPCs to create a hybrid cloud setup via a private connection (VPN or Direct Connection).



Inbound Resolver Endpoint

Allow DNS queries to your VPC from your on-premises network or another VPC



Outbound Resolver Endpoint

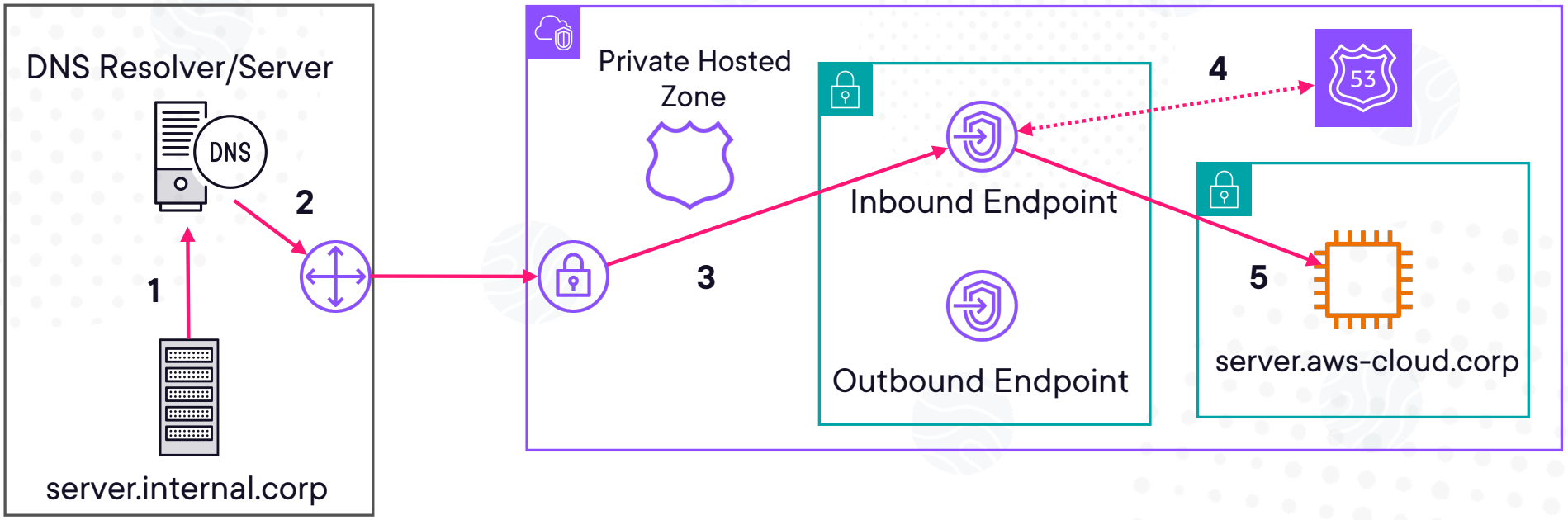
Allow DNS queries from your VPC to your on-premises network or another VPC

Resolver Rule

Forwarding rule for where you want to send inbound or outbound domain traffic

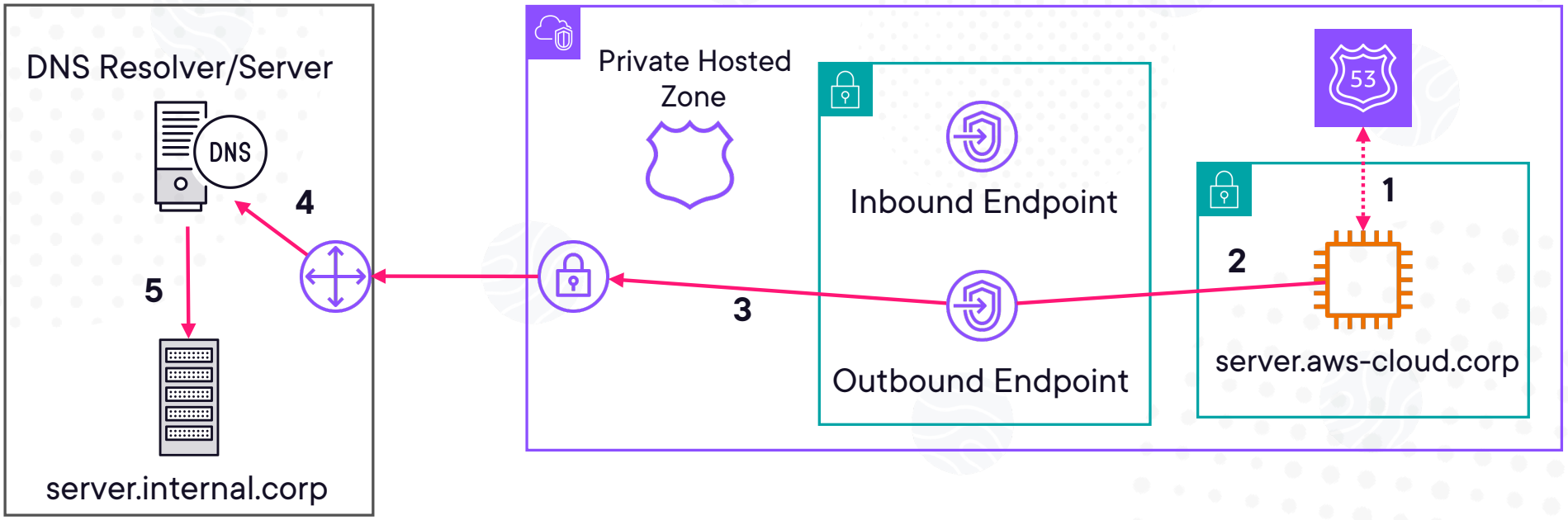
Resolver Rules are applied to VPCs and can be shared across multiple accounts using AWS Resource Access Manager (RAM)!

Simplified Inbound Architecture Diagram



1. On-prem server wants to resolve **server.aws-cloud.corp**, so it sends DNS query to on-prem DNS resolver
2. On-prem DNS resolver rule forwards query to the inbound endpoint in AWS VPC
3. DNS query is sent to the VPC over a private connection
4. The inbound endpoint queries the private hosted zone information for the resource via Route 53 Resolver
5. Traffic is then forwarded to the correct private IP address using private, hybrid DNS

Simplified Outbound Architecture Diagram

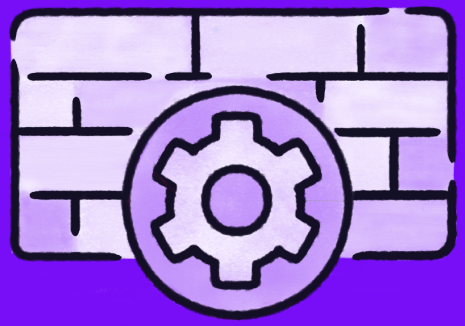


1. VPC server wants to resolve **server.internal.corp**, so it sends DNS query to the VPC+2 address
2. VPC+2 address has a resolver rule to forwards **internal.corp** traffic to on-prem via outbound endpoints
3. On-prem traffic is sent through the outbound endpoint over the private connection
4. Traffic on-prem is sent to the on-prem DNS resolver and server
5. Traffic is resolved and sent to the internal on-prem server

Exam Pro Tip: For Inbound Endpoints, think traffic coming inbound to a VPC

Exam Pro Tip: For Outbound Endpoints, think traffic sent outbound from a VPC

Protecting DNS Traffic with Resolver DNS Firewall



Route 53 Resolver DNS Firewall

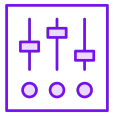
Allows you to control access to sites and block DNS-level threats for DNS queries going out from your VPC through the Route 53 Resolver

Route 53 Resolver DNS Firewall Concepts

Define domain name filter rules that you associate with your VPCs

You can specify lists of domain names to allow or block

You can customize the responses for the DNS queries that you block



You can even fine-tune the domain lists to allow certain query types

Important: This only filters on the domain name, it doesn't resolve the name

This is only for DNS traffic, and not for any other type of layer protocol (*HTTPS, HTTP, SSH, TLS, etc.*)!

Module Summary and Exam Tips

Hybrid DNS Review

Using hybrid DNS approaches allows you to easily connect your on-premises and AWS environments

You can centrally manage DNS in Route 53 and resolve traffic both ways

Remember some of the use Cases:

- Manage DNS during a phased migration to AWS
- Keep existing on-premises DNS infrastructure while utilizing AWS for new services

The Route 53 Resolver is the DNS resolver that responds recursively to DNS queries from AWS resources.

This is one of the 5 reserved IP addresses within your subnet CIDRs!

Resolver Endpoints Review

Inbound

Used for resolving DNS queries coming into your VPCs

Outbound

Used for resolving DNS queries going out of your VPCs

You can use the Route 53 Resolver DNS Firewall to filter outbound DNS traffic!