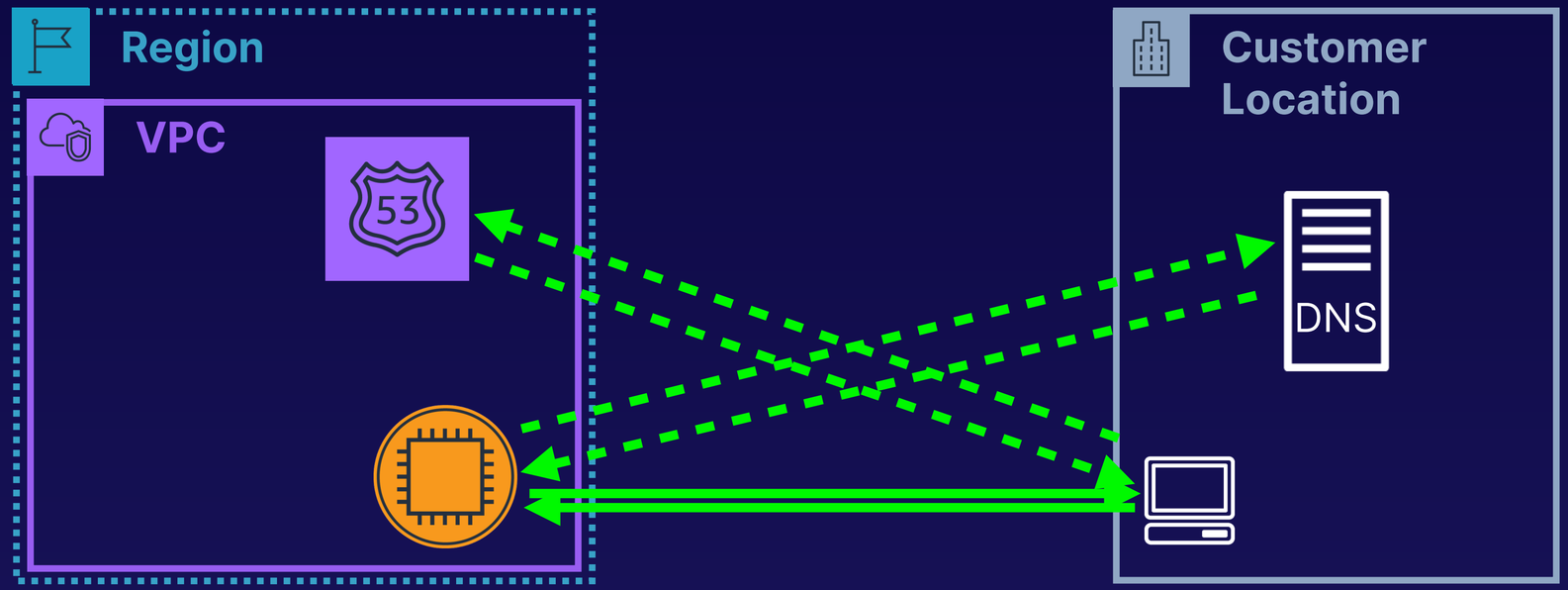
Hybrid DNS

Steven Moran
TECHNICAL INSTRUCTOR

What Is Hybrid DNS?



- Private DNS resolution across hybrid networks.
  - AWS resources are able to use on-prem DNS zones.
  - On-prem resources are able to use Route 53 private zones or VPC DNS.

Route 53 Resolver

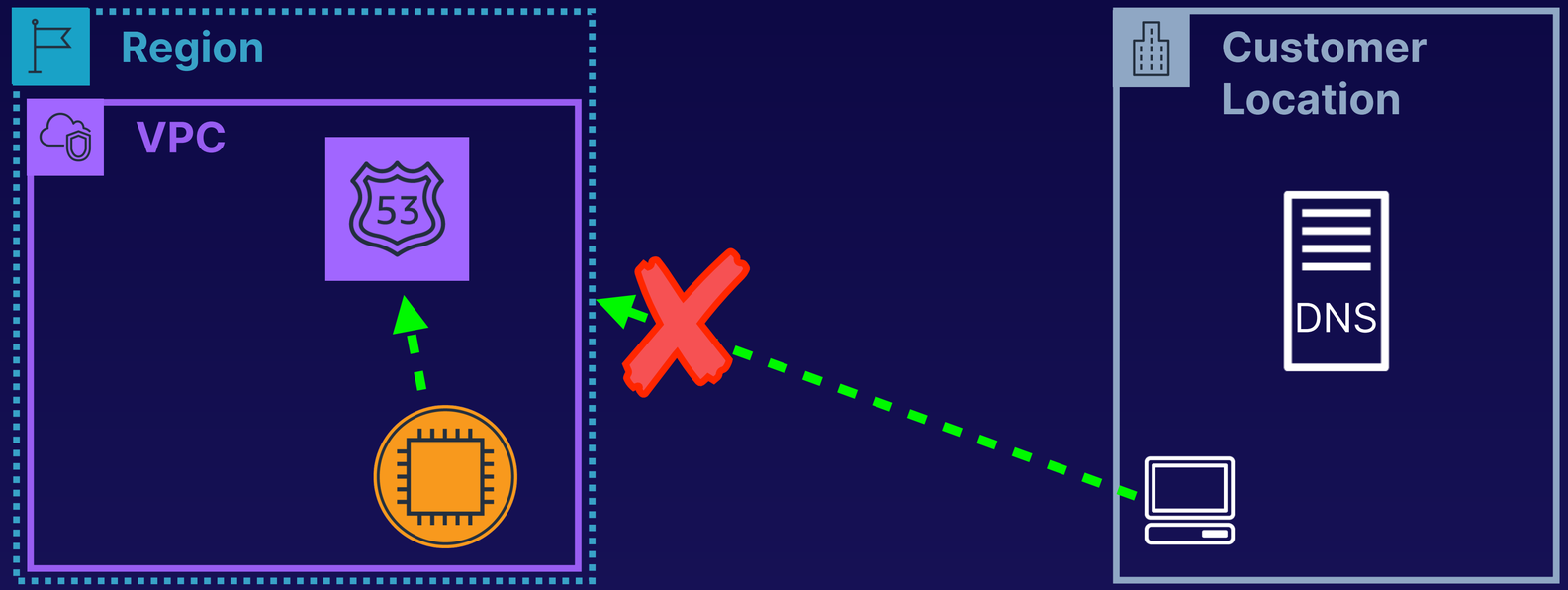
- Provides default DNS resolution within VPCs.
- “VPC +2” IP address.
- Part of EC2 service hardware.
  - Good availability and performance.
  - Only accessible from within AWS infrastructure.

Route 53 Resolver

- Route 53 Private Zones must be associated to VPCs.

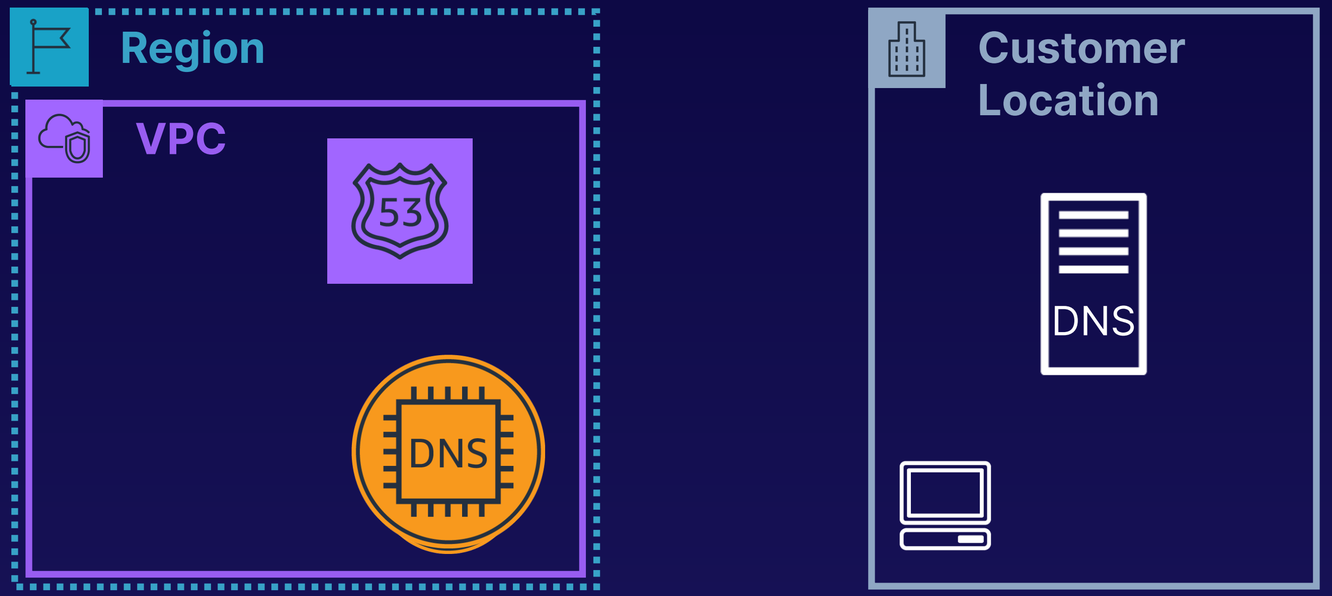
- Resolver search sequence:
  - Route 53 Private Zones.
  - VPC DNS domain.
  - Public DNS system.

The Hybrid DNS Challenge



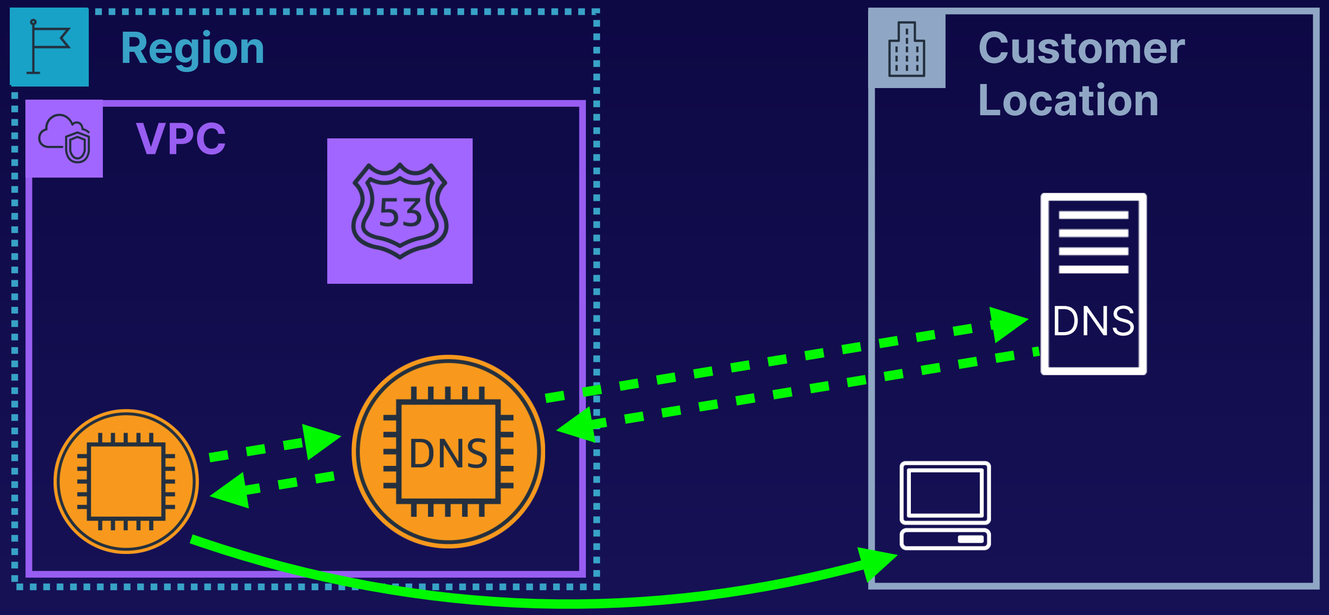
- EC2 instances always use Route 53 Resolver by default.
- On-prem systems cannot reach Route 53 Resolver.

Customer-implemented DNS Resolvers



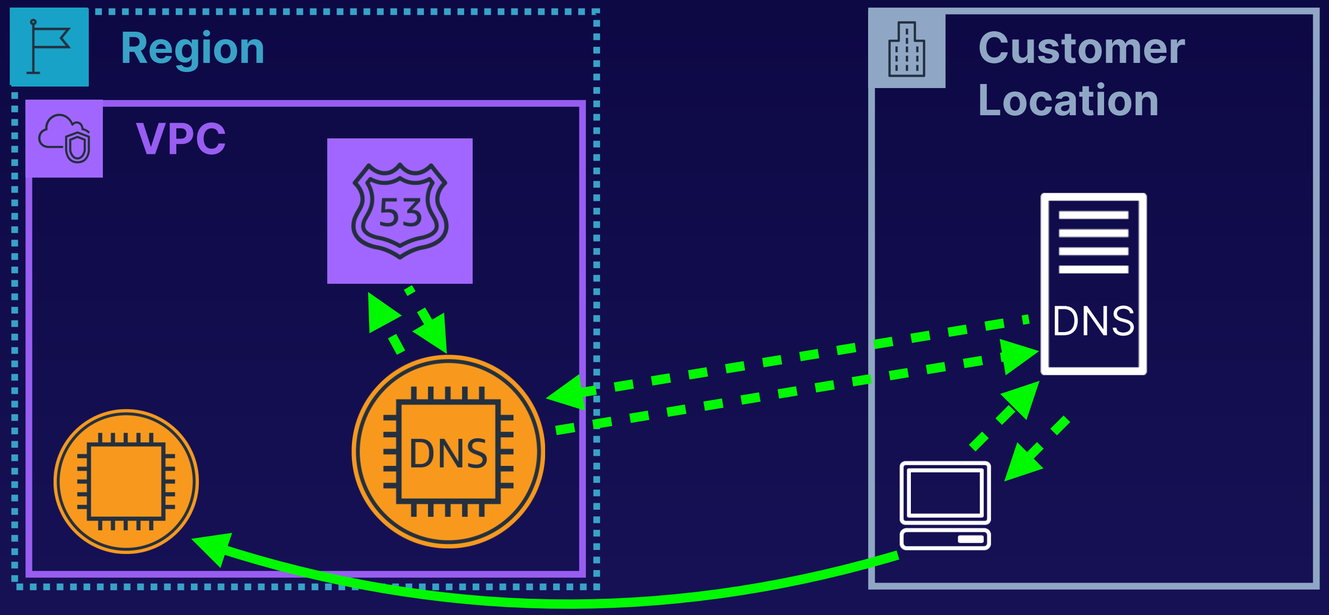
- EC2-hosted DNS resolvers are provisioned within VPC.

Customer-implemented DNS Resolvers



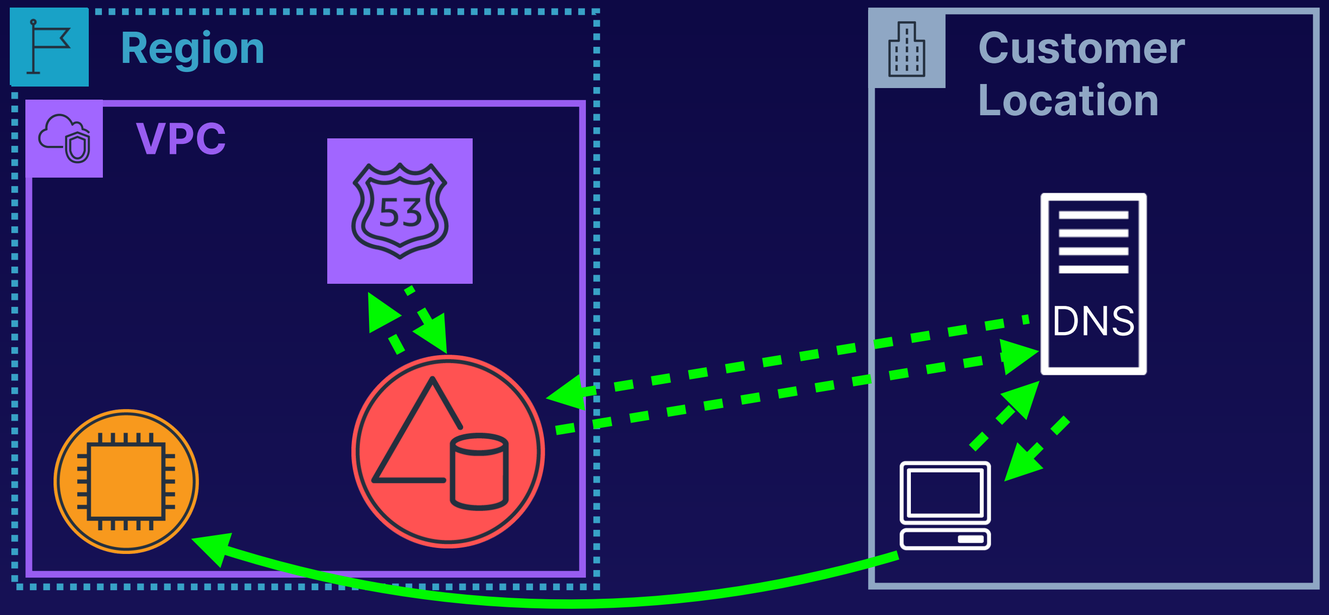
- EC2-hosted DNS resolvers are provisioned within VPC.
- VPC configured to use EC2 resolver instead of Route 53.
- Resolver forwards matching requests to on-prem DNS.

Customer-implemented DNS Resolvers



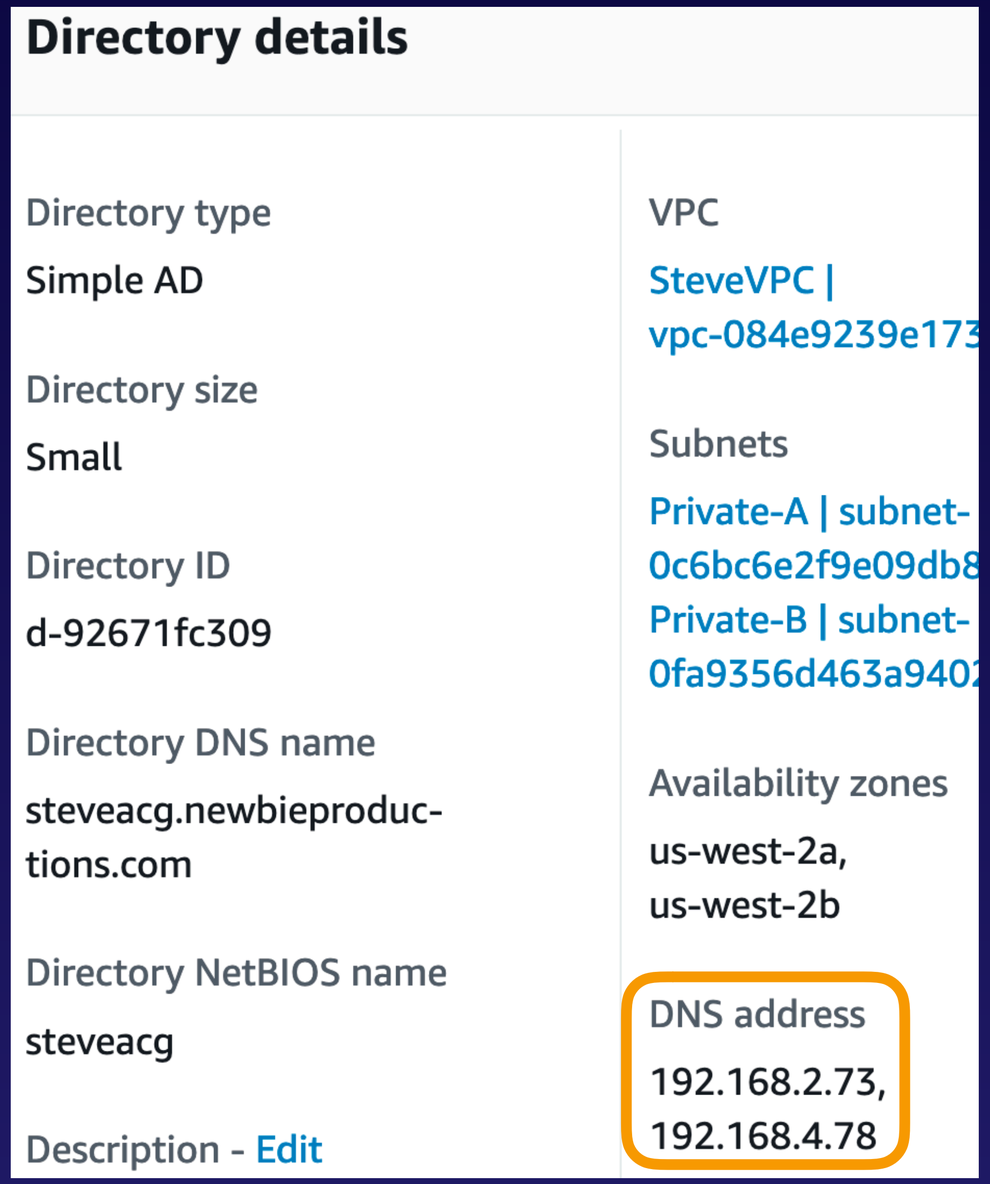
- EC2-hosted DNS resolvers are provisioned within VPC.
- VPC configured to use EC2 resolver instead of Route 53.
- Resolver forwards matching requests to on-prem DNS.
- On-prem DNS resolvers configured to forward matching requests to EC2 resolver.

AWS Directory Servers as DNS Resolvers



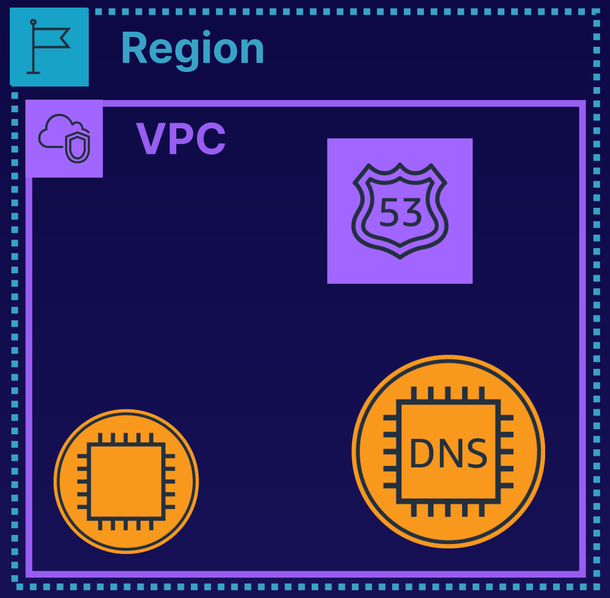
- AWS Directory Services Simple AD can provide the same functionality.

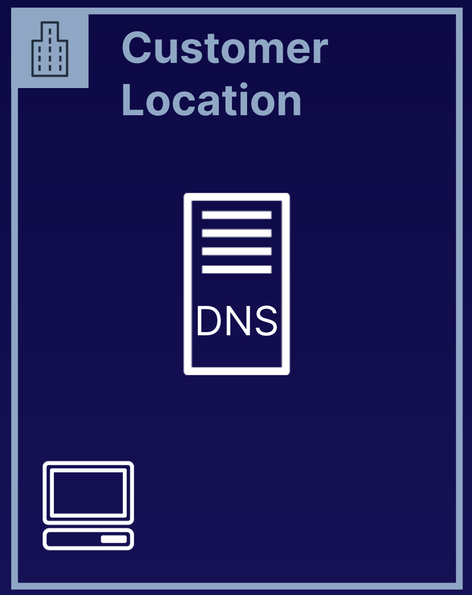
AWS Directory Servers as DNS Resolvers



- AWS Directory Services Simple AD can provide the same functionality.
- Configure on-prem DNS to forward to Simple AD DNS addresses.

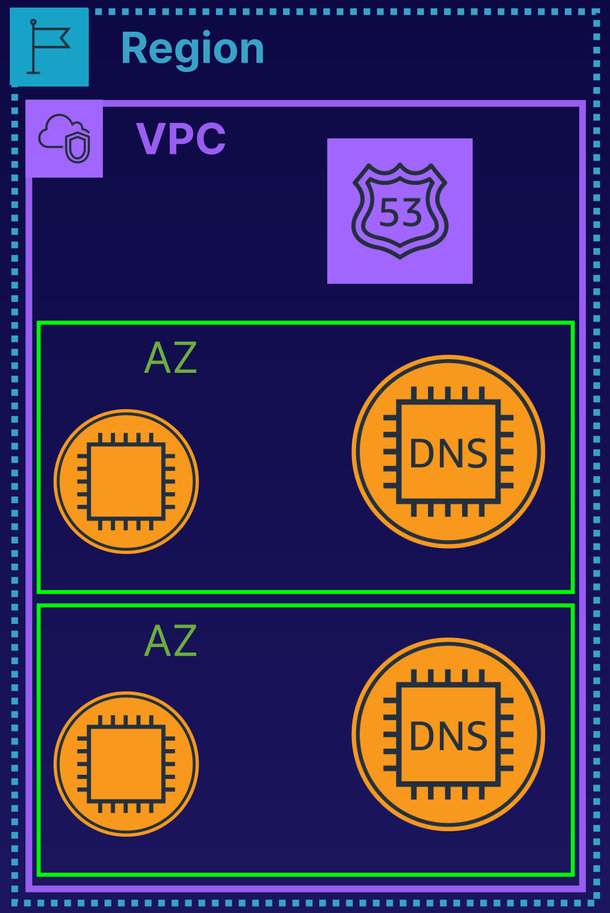
Customer-implemented DNS Resolvers – Problems

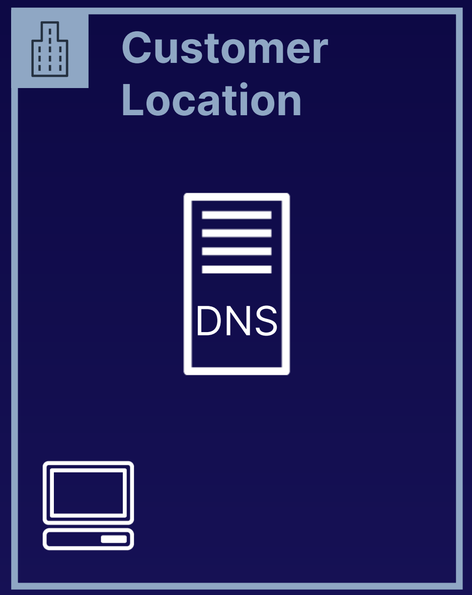




- Single EC2-ENI limited to 1,024 queries/second.

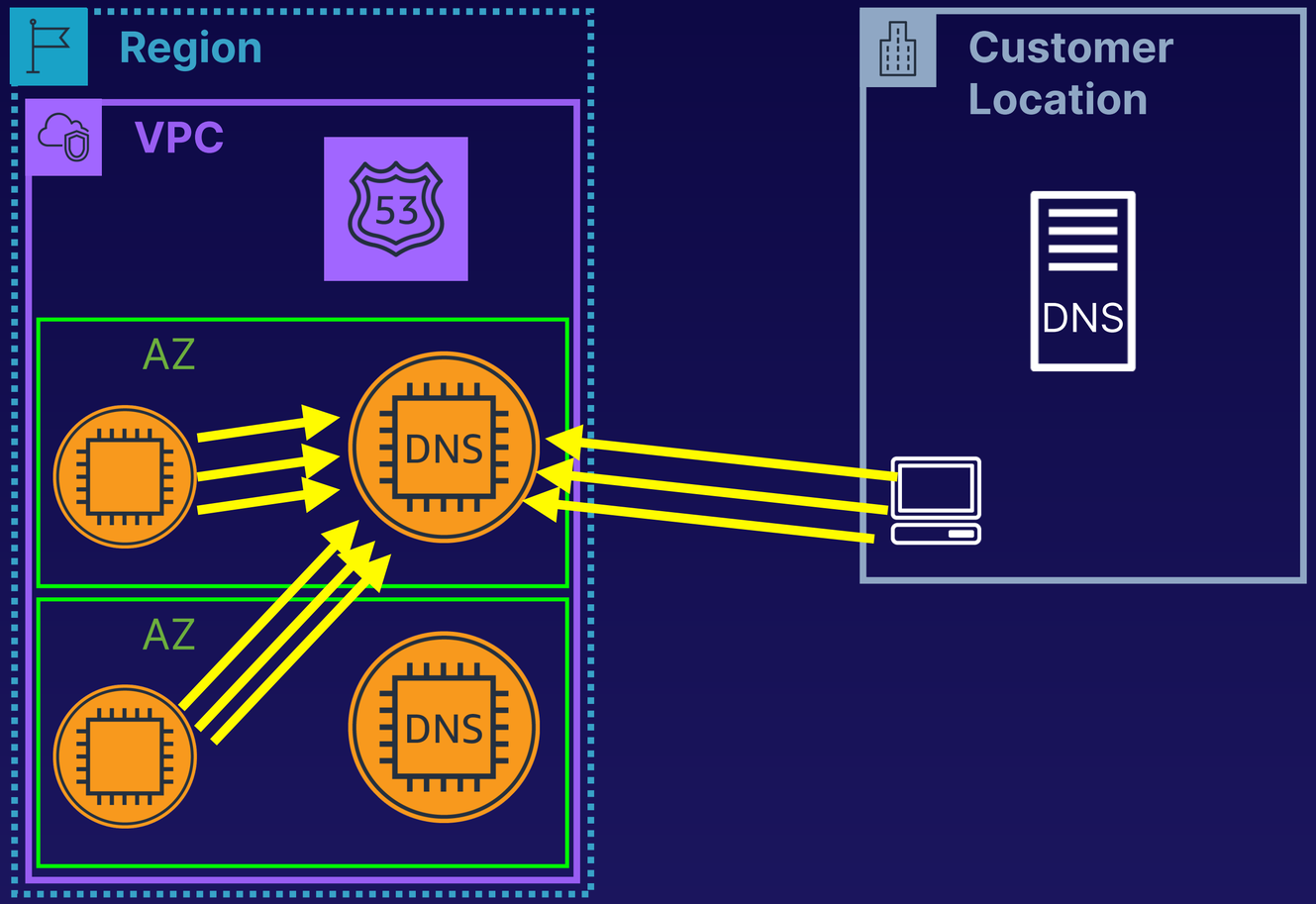
Customer-implemented DNS Resolvers – Problems





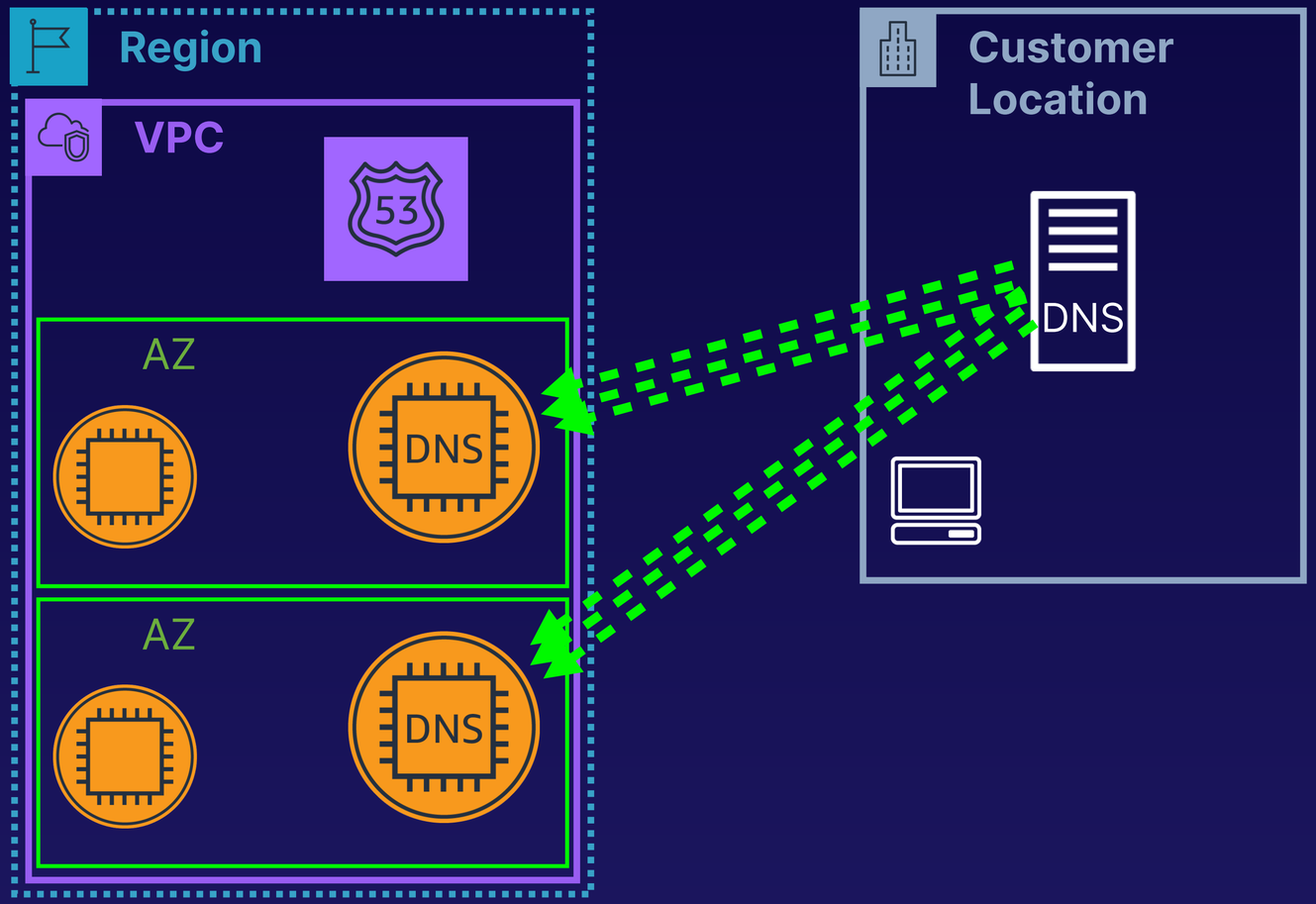
- Single EC2-ENI limited to 1,024 queries/second.
- Multi-AZ deployment needed for HA.

Customer-implemented DNS Resolvers – Problems



- Single EC2-ENI limited to 1,024 queries/second
- Multi-AZ deployment needed for HA.
- Most DNS clients don’t load-balance across multiple servers.

Customer-implemented DNS Resolvers – Problems



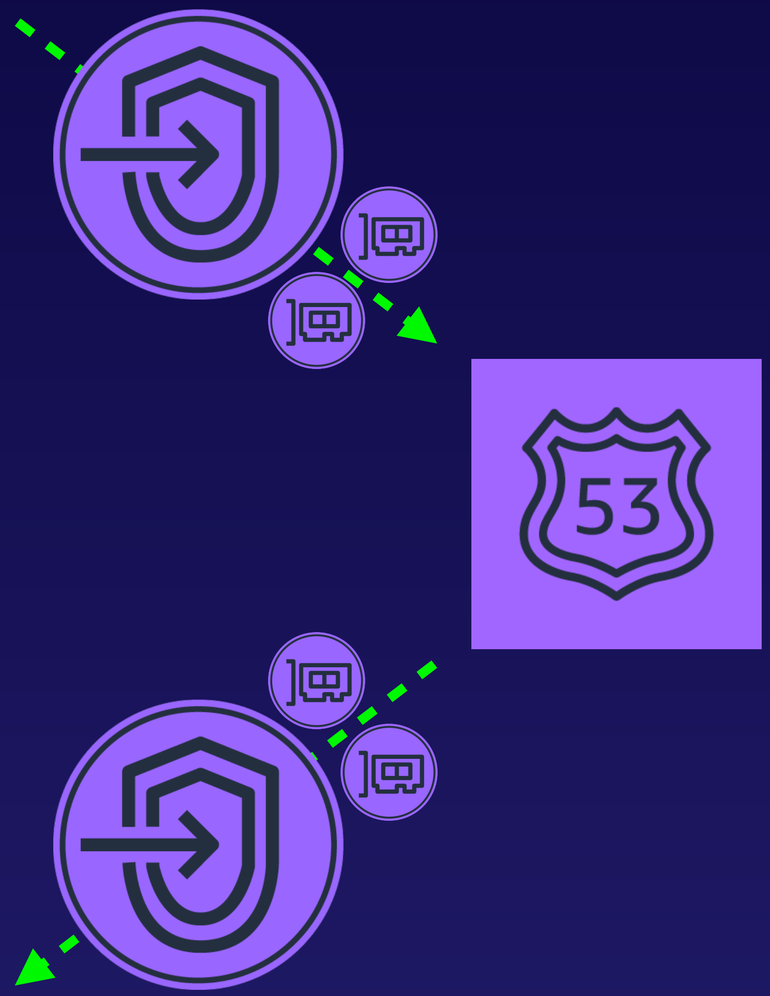
- Single EC2-ENI limited to 1,024 queries/second
- Multi-AZ deployment needed for HA.
- Most DNS clients don't distribute load across multiple servers.
- DNS resolver services can often load balance.

Route 53 Resolver Endpoints

- Provides IP accessible endpoints to the AWS Route 53 Resolver service.
- Endpoints support from 2 to 8 ENIs.
- Each ENI supports up to 10,000 queries/second.

Route 53 Resolver Endpoints

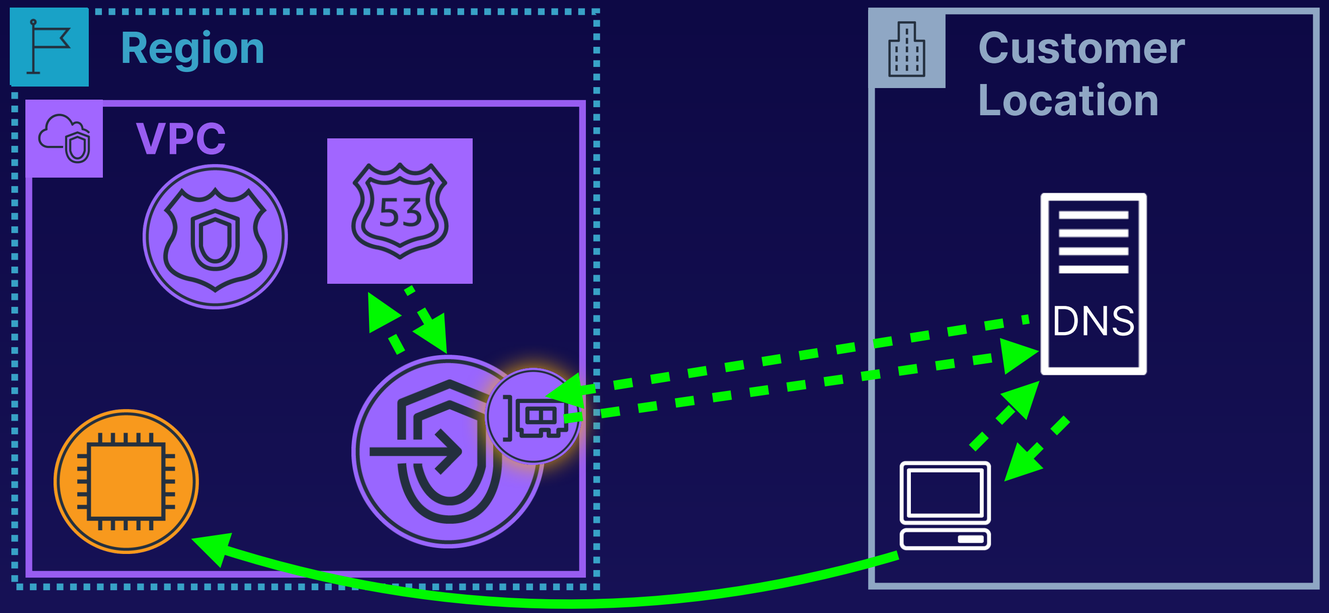
- Endpoints are created within a single VPC, but may be used by other VPCs in the same Region.
- Secured by a single VPC security group.
  - Group assignment cannot be changed after creation.
- Each endpoint can handle either inbound **or** outbound DNS requests.



Route 53 Resolver Endpoints

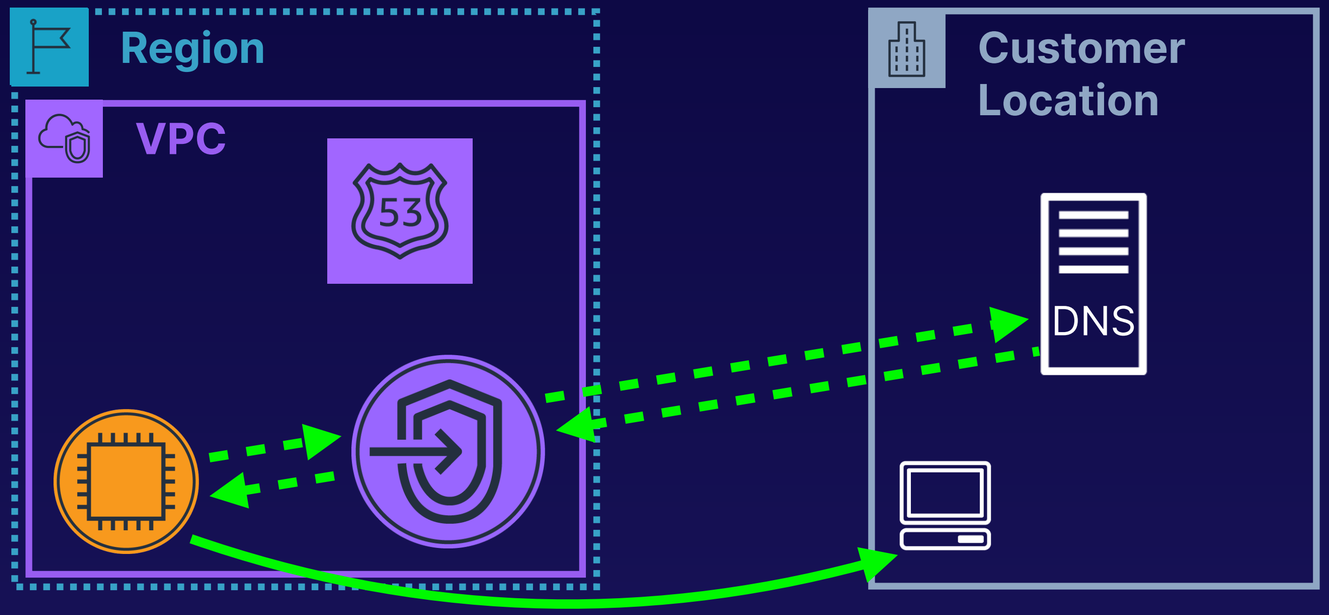
- Endpoint ENIs are AZ-scoped resources.
  - Place your endpoints in separate AZs for availability.
- ENIs use either dynamic or customer-assigned IP addresses.
- IP addresses are persistent for the lifetime of the endpoint.
- Pricing per ENI, per hour.

Inbound Endpoints



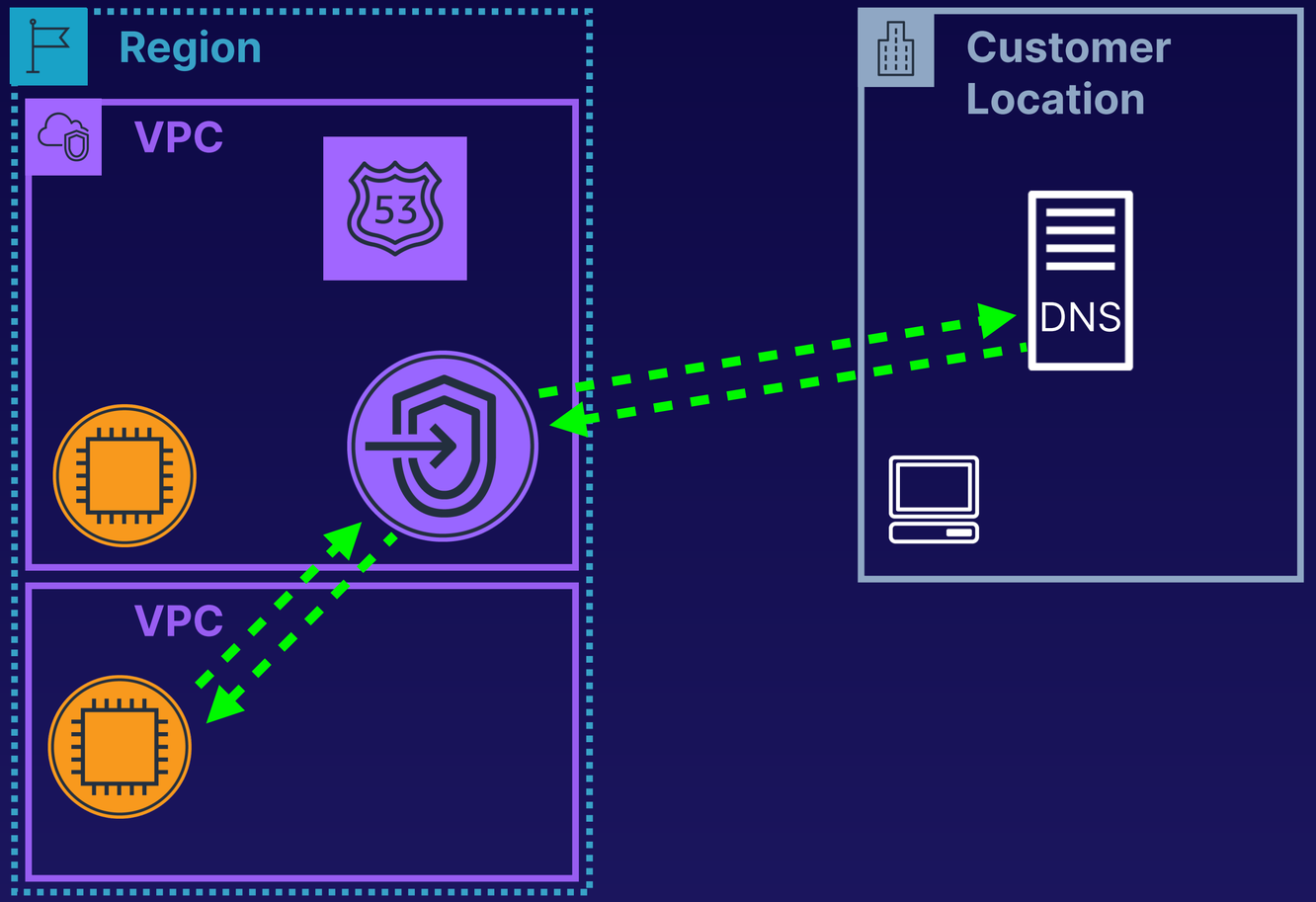
- Handles request forwarding from on-prem to AWS DNS resolver.
- Requests are sent to the IP address of an ENI.
- Request from on-prem DNS resolver instead of client for better performance.
- Private hosted zones must be associated to the VPC where resolver endpoints reside.

Outbound Endpoints



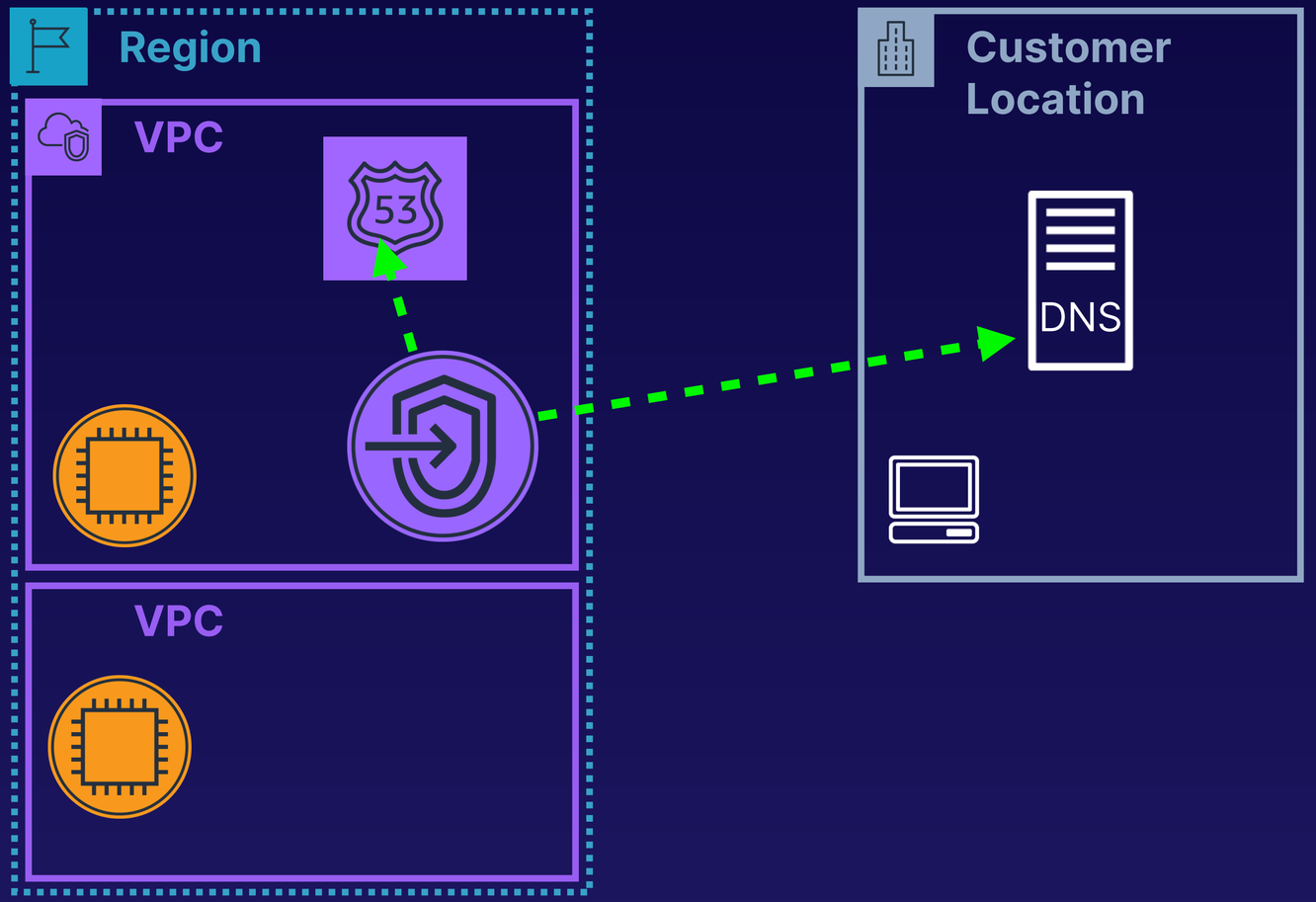
- Handle forwarding for requests originating within AWS.

Outbound Endpoints



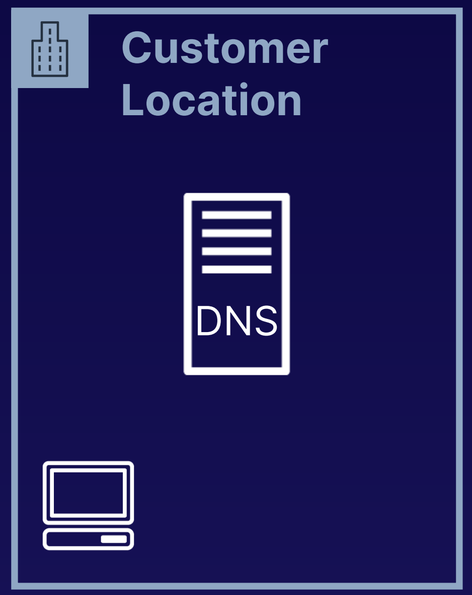
- Handle forwarding for requests originating within AWS.
- Can be associated with multiple VPCs in a Region.

Outbound Endpoint Traffic Rules



- Specify forwarding action for requests matching defined FQDN Patterns.
- **Forward** rules forward requests to IPv4 address of on-prem DNS.
- **System** rules forward requests to Route 53 Resolver.

Outbound Endpoint Traffic Rules



- System rules are automatically created for:
  - Private hosted zones
  - VPC domain names
  - Publicly reserved domain names
- If rules conflict, resolver prefers:
  - Most specific FQDN
  - **Forward** rules over **system** rules

Fast Takeaways

The default Route 53 Resolver cannot be accessed outside of a VPC.

Customer-implemented DNS resolvers have a number of limitations.

Route 53 Resolver endpoints are a managed alternative to custom resolvers.