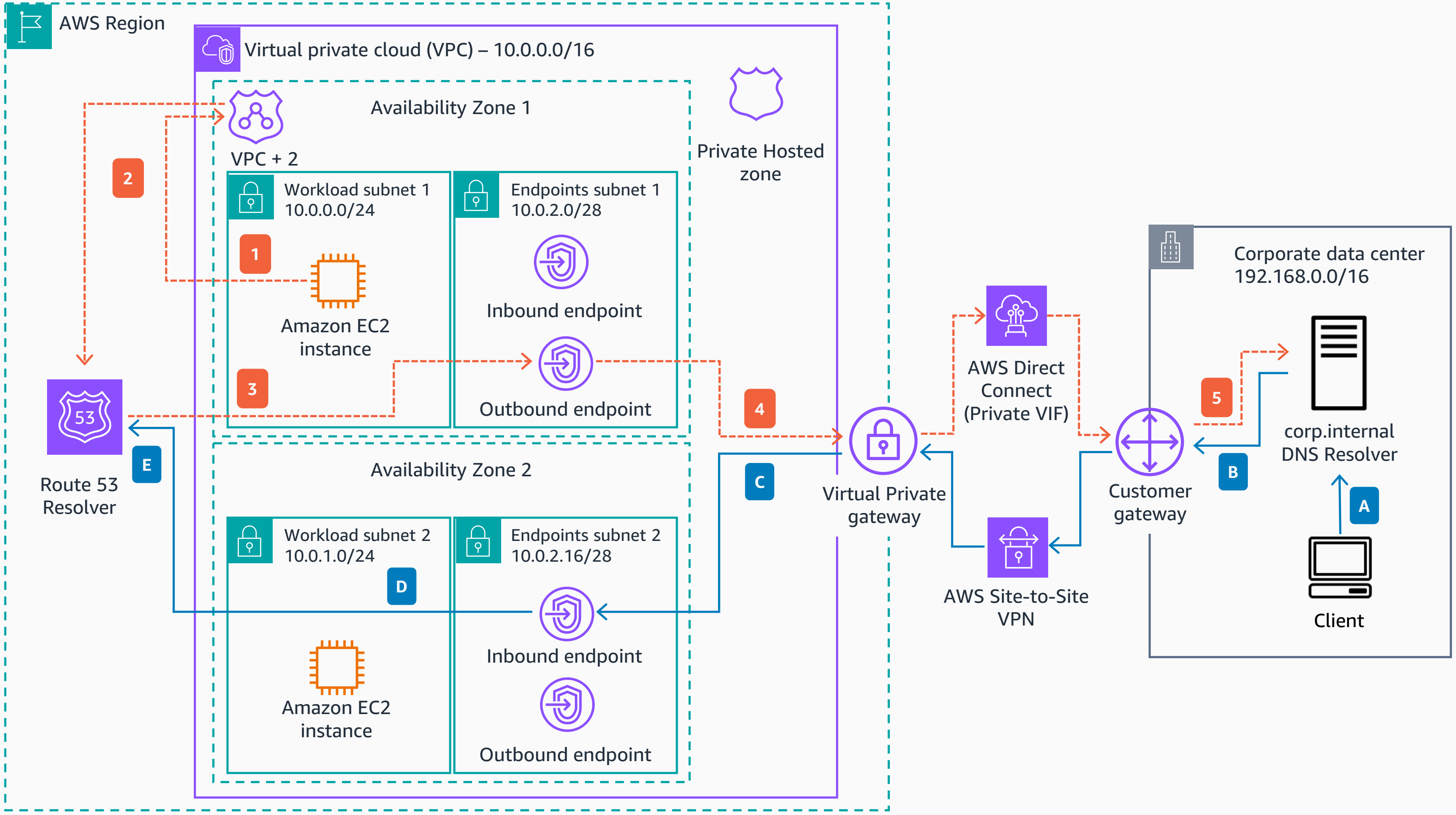
Hybrid DNS Resolution with Amazon Route 53 Resolver Endpoints



1 An **Amazon Elastic Compute Cloud (Amazon EC2)** instance needs to resolve the domain name "corp.internal". The authoritative domain name service (DNS) for this domain name is located at the corporate data center. The DNS query is sent to the virtual private cloud (VPC) + 2 resolver in the VPC.

2 An **Amazon Route 53** Forwarding rule is configured to forward any DNS query for "corp.internal" to the corporate data center.

3 The DNS query is sent to the **Route 53** Resolver outbound endpoint.

4 The **Route 53** Resolver outbound endpoint forwards the query to the on-premises DNS resolver with a private connection between AWS and the corporate data center – either using **AWS Direct Connect** or **AWS Site-to-Site VPN**.

5 DNS resolution for corp.internal domain names is carried out by the DNS resolver located in the corporate data center.

A A client located in the corporate data center needs to resolve an "amazonaws.com" domain name. It sends the query to an internal DNS resolver.

B The DNS resolver in the corporate data center has a forwarding rule that forwards any DNS query for "amazonaws.com" DNS domains to the **Route 53** Resolver inbound endpoint.

C The forwarded query arrives at the **Route 53** Resolver inbound endpoint through either **AWS Direct Connect** or an **AWS Site-to-Site VPN**.

D The **Route 53** Resolver inbound endpoint forwards the query to the **Route 53 Resolver**.

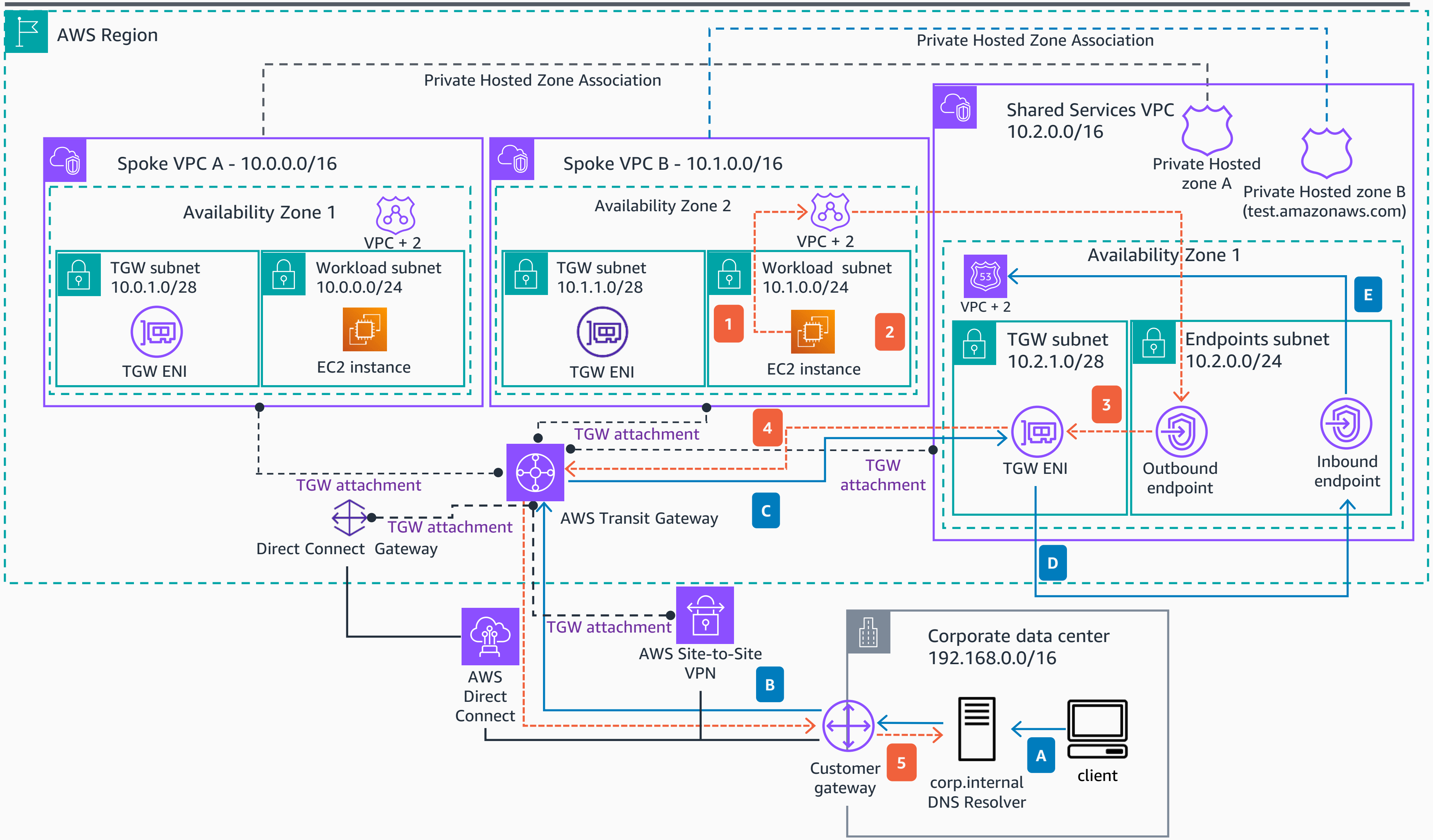
E The **Route 53 Resolver** resolves the DNS queries for "amazonaws.com" domain names.

Reviewed for technical accuracy October 4, 2023

AWS Reference Architecture

Multi-Account Hybrid DNS resolution

Private hosted zones (PHZs) can be centralized in a shared services virtual private cloud (VPC) for central DNS management or each VPC can have its own PHZs that are associated with a shared services VPC.



1. An **Amazon EC2** instance in the Spoke VPC B needs to resolve a “corp.internal” domain name, which needs to be resolved by the DNS resolver in the corporate data center.
2. The query is sent to the VPC + 2 resolver. A **Route 53** forwarding rule forwards the query to the **Route 53** Resolver outbound endpoint in the shared services VPC.
3. The **Route 53** Resolver outbound endpoint forwards the DNS query to the transit gateway elastic network interface (TGW ENI).
4. The DNS query arrives at the **Transit Gateway**. The **Transit Gateway** route table forwards the query to the corporate data center via **AWS Direct Connect** or **AWS Site-to-Site VPN**.
5. The DNS resolver resolves the “corp.internal” domain name.

A. A client located in the corporate data center needs to resolve a “test.amazonaws.com” domain name. It sends the query to its pre-configured DNS Resolver.

B. The DNS resolver in the corporate data center has a forwarding rule that points any DNS query for “test.amazonaws.com” DNS domains to the **Route 53** Resolver inbound endpoint.

C, D. The **Transit Gateway** forwards the query to the shared services VPC, which will land the DNS query at the **Route 53** Resolver inbound endpoint.

E. The **Route 53** Resolver inbound endpoint uses the VPC + 2 resolver. The private hosted zone B associated with the shared services VPC holds the DNS records for “test.amazonaws.com”, so the **Route 53** Resolver can resolve the query.

For more information about multi-account strategies with Route 53 Resolvers, refer to: Simplify DNS management in a multi-account environment with Route 53 Resolver.

Reviewed for technical accuracy October 4, 2023

AWS Reference Architecture