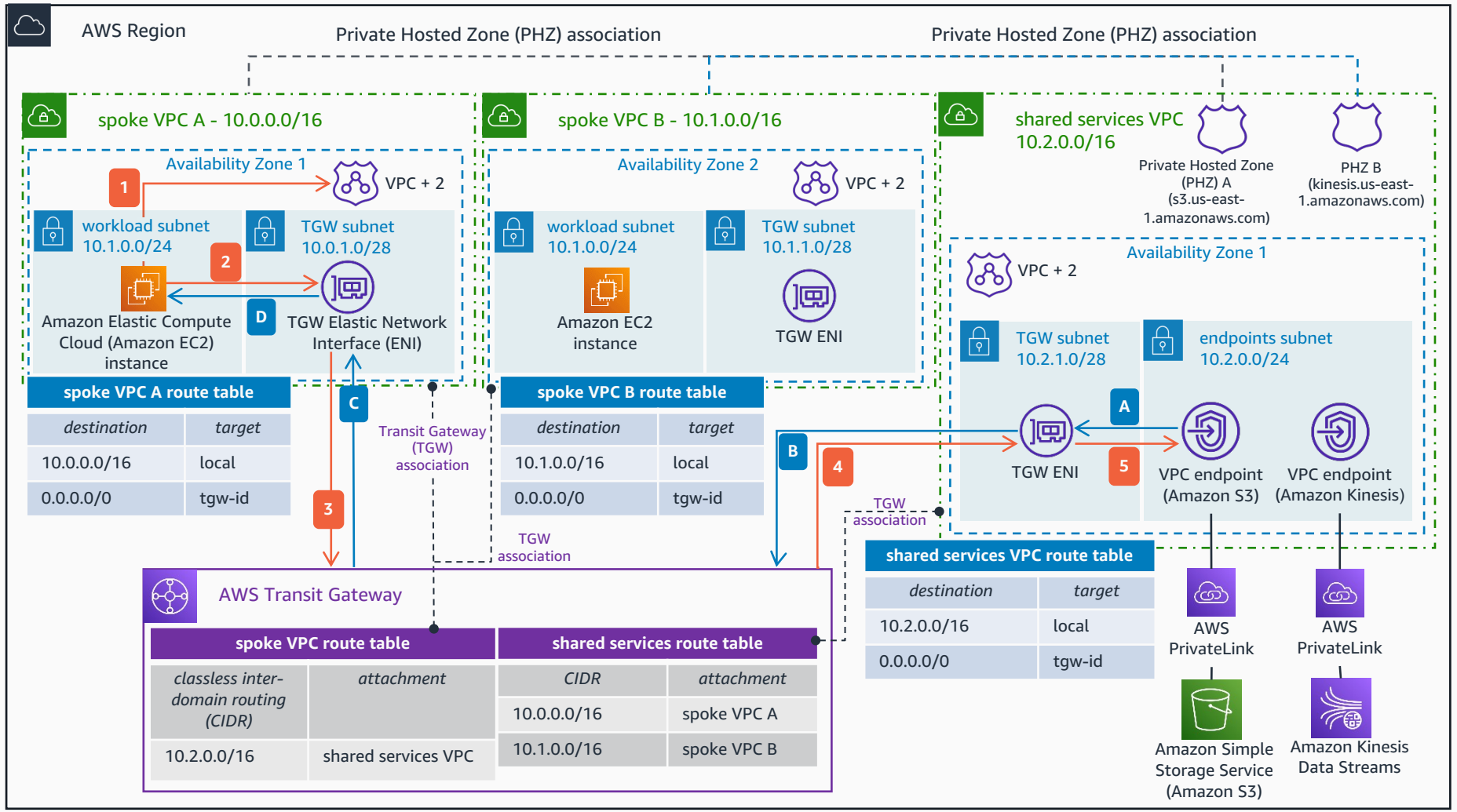
Centralizing VPC endpoints with AWS Transit Gateway

Reviewed for technical accuracy May 25, 2022

AWS Reference Architecture

Centralizing VPC Endpoint Access with AWS Transit Gateway

To achieve unified name resolution for your virtual private cloud (VPC) endpoints, you need to create custom Amazon Route 53 Private Hosted Zones (PHZs) and associate them to all the VPCs that need to consume the resources of these endpoints. Remember to disable private domain name system (DNS) on the VPC endpoints when creating them.



1. An **Amazon EC2** instance that needs to connect to **Amazon S3** via an interface endpoint located in the *shared services* VPC first needs to resolve the domain name by querying the VPC + 2 resolver. PHZ A is associated with the *spoke* VPC A to complete the domain resolution.
2. Once the instance knows the private IP to connect to, it sends the traffic to the TGW ENI as per the spoke VPC A route table.
3. The traffic is sent to the **Transit Gateway**.
4. As per the **Transit Gateway** spoke VPC route table, the traffic is forwarded to the shared services VPC.
5. The TGW ENI in the shared services VPC forwards the traffic to the corresponding interface endpoint – in this case, the one connecting to **Amazon S3**.

A. The response is sent back from the VPC endpoint to the TGW ENI.

B. The traffic is forwarded to the **Transit Gateway**.

C. As per the **Transit Gateway** shared services route table, the traffic is sent to the spoke VPC A.

D. The response is sent by the TGW ENI to the destination – an **Amazon EC2** instance.

* For more information about interface endpoints and AWS PrivateLink, refer to *Access an AWS service using an interface VPC endpoint*.

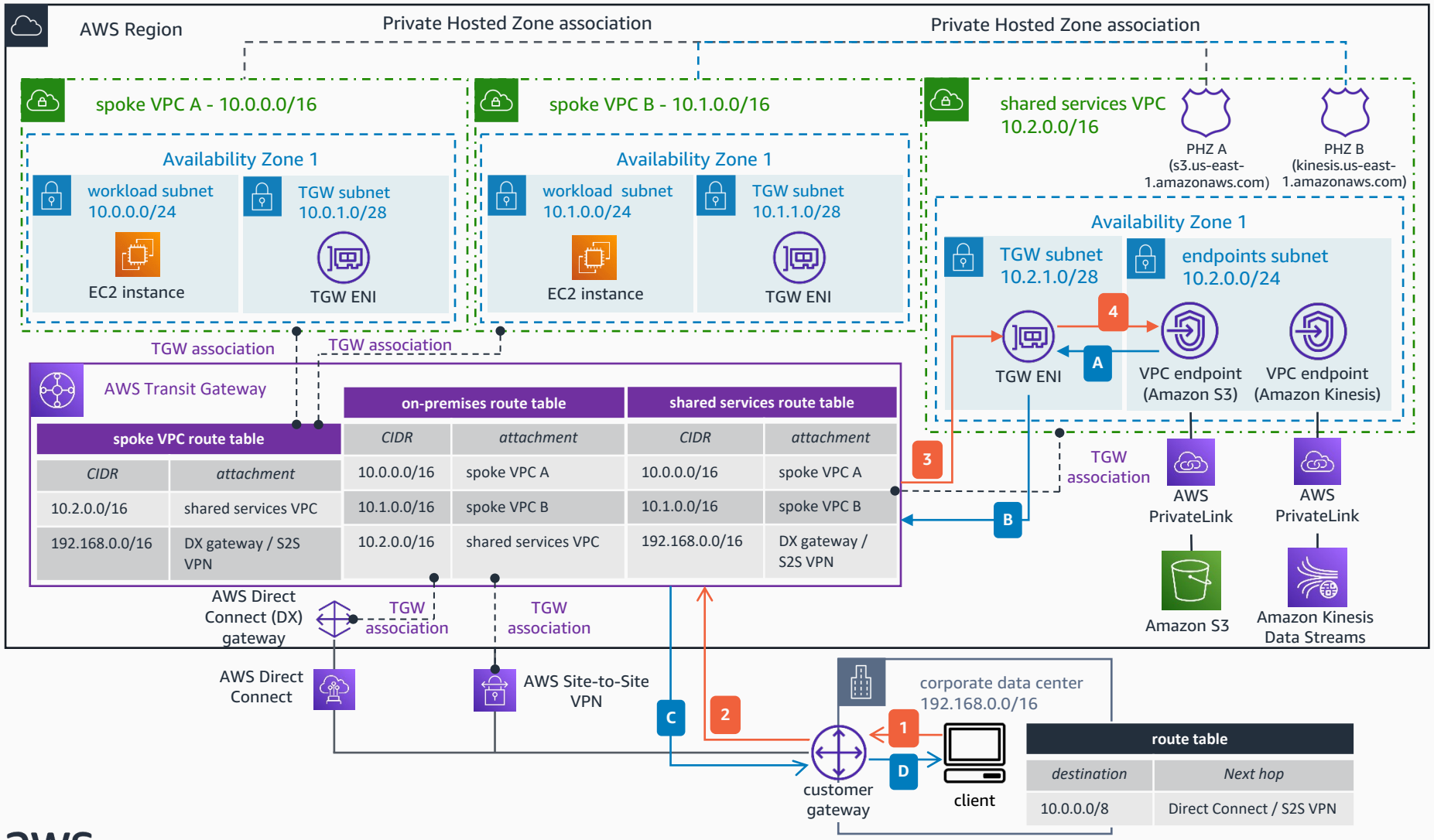
To see an example of this architecture in Terraform, refer to AWS Hub and Spoke Architecture with Shared Services VPC.

Reviewed for technical accuracy May 25, 2022

AWS Reference Architecture

Accessing VPC Endpoints from On-premises Environments

If you want to access AWS services from your on-premises environments without having to use the internet (or without using public endpoints), you can use AWS Transit Gateway to access Interface VPC endpoints by using AWS Direct Connect or AWS Site-to-Site VPN as transport between AWS and your corporate data centers.



1 Any client from the corporate data center that wants to connect to the VPC interface endpoints in the shared services VPC sends the request via the customer gateway. First it must resolve the DNS name to obtain the private IP address. This reference architecture diagram does not cover the DNS resolution.*

2 The traffic is sent to **AWS Transit Gateway** via an AWS Direct Connect link or an **AWS Site-to-Site VPN** connection.

3 As per the **Transit Gateway** on-premises route table, the traffic is forwarded to the shared services VPC.

4 The transit gateway ENI forwards the traffic to the VPC endpoint.

A The response is sent back from the VPC endpoint to the TGW ENI.

B The traffic is forwarded to **Transit Gateway**.

C As per the **Transit Gateway** shared services route table, the traffic is sent to the corporate data center via the **Direct Connect** link or the **Site-to-Site VPN** connection.

D The response is sent to the on-premises client.

* To learn how the Hybrid DNS resolution works with **Amazon Route 53** Resolver endpoints, refer to the following reference architecture.

For more information about centralizing **AWS PrivateLink** endpoints with **AWS Transit Gateway**, refer to the Integrating AWS Transit Gateway with AWS PrivateLink and Amazon Route 53 Resolver blog post.

Reviewed for technical accuracy May 25, 2022

AWS Reference Architecture