Hybrid Connectivity to AWS Transit Gateway

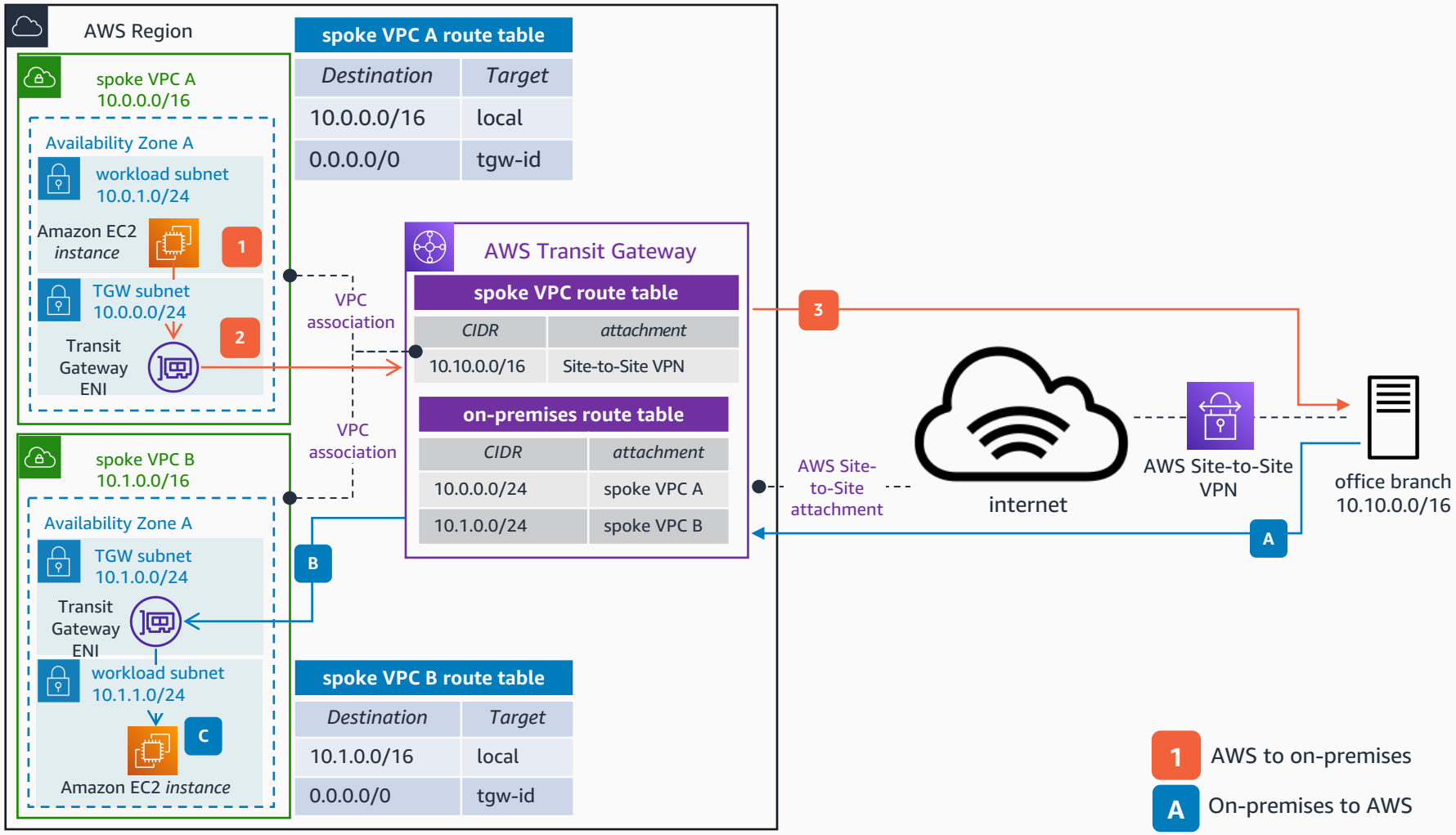
1. *Hybrid connectivity to AWS Transit Gateway with AWS Site-to-Site VPN*
2. *Hybrid connectivity to AWS Transit Gateway with AWS Direct Connect*
3. *AWS Site-to-Site VPN as primary and AWS Site-to-Site VPN as backup*
4. *AWS Direct Connect as primary and AWS Site-to-Site VPN as backup*
5. *AWS Direct Connect in active/passive configuration*
6. *AWS Site-to-Site VPN on top of AWS Direct Connect for traffic encryption*
7. *AWS Direct Connect and Transit Gateway Connect attachments*
8. *Hybrid connectivity with Private VIFs and inter-VPC with AWS Transit Gateway*

Reviewed for technical accuracy August 17, 2022

AWS Reference Architecture

Hybrid connectivity to AWS Transit Gateway with AWS Site-to-Site VPN

You can create a Site-to-Site VPN connection directly to a Transit Gateway. With this, you can take advantage of the benefits of a managed VPN solution, while connecting to several VPCs without having to add new connection. Take into account that it is recommended the use of a second VPN connection for high-availability.



1 Traffic initiated from an **Amazon Elastic Compute Cloud (Amazon EC2)** instance in the spoke VPC A and destined to the office branch is routed to the Transit Gateway elastic network interface (ENI) as per the spoke VPC A route table.

2 Traffic is forwarded to **AWS Transit Gateway (AWS TGW)**. As per the spoke VPC route table, the traffic is routed to the office branch via the **AWS Site-to-Site VPN** attachment.

3 The traffic is routed to the destination via the **Site-to-Site VPN** connection over the internet.

A Traffic from the office branch destined to the spoke VPC B is forwarded to the **Transit Gateway** via the **Site-to-Site VPN** connection.

B As per the **Transit Gateway** on-premises route table, the traffic is forwarded to the spoke VPC B attachment.

C The **Transit Gateway** ENI of the spoke VPC B forwards the traffic to the destination.

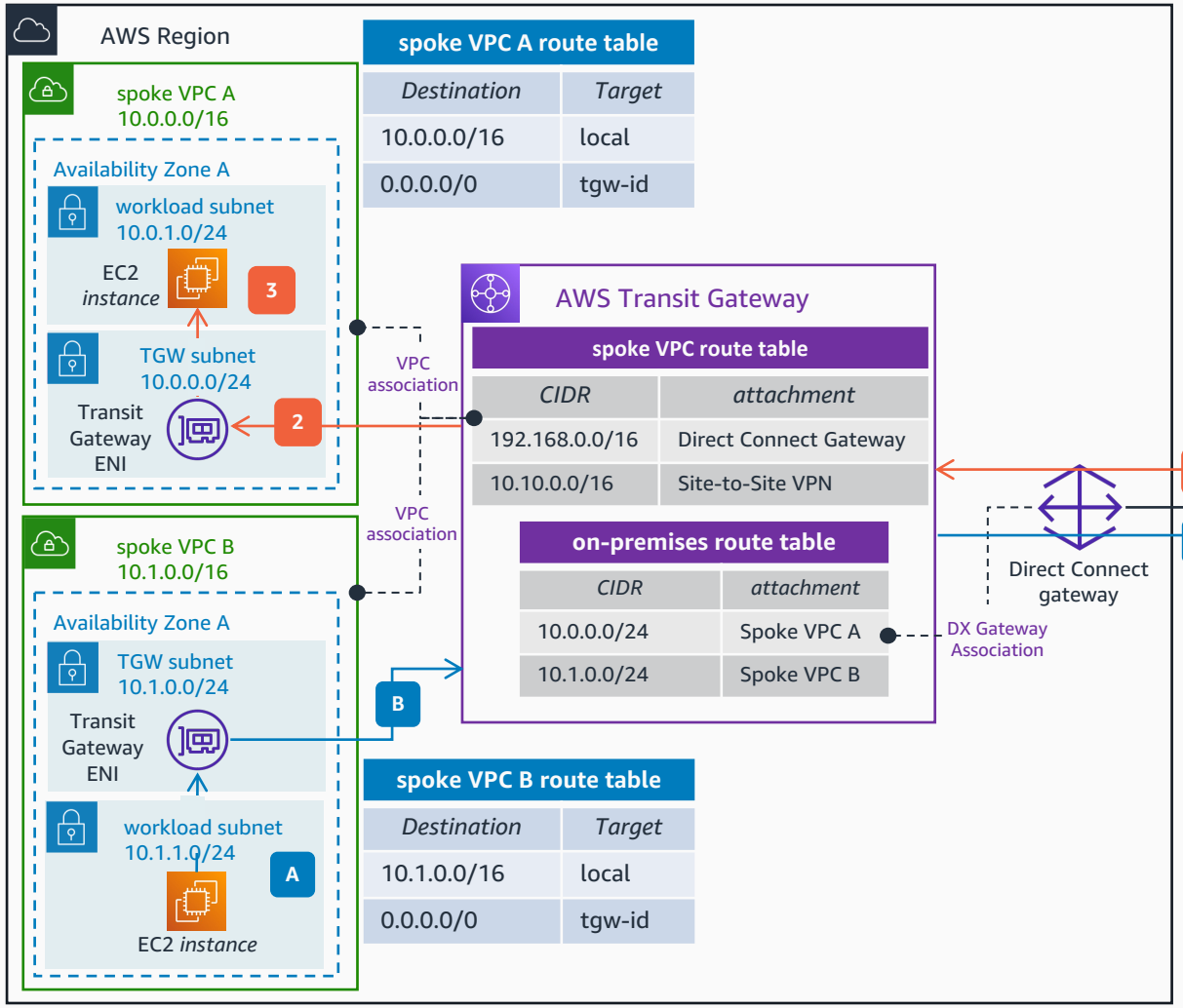
For more information about how to configure **AWS Site-to-Site VPN**, refer to:
[Getting started - AWS Site-to-Site VPN]

Reviewed for technical accuracy August 17, 2022

AWS Reference Architecture

Hybrid connectivity to AWS Transit Gateway with AWS Direct Connect

You can use a Transit VIF and a Direct Connect gateway to connect your on-premises environments to AWS. With this, you can benefit of the connectivity to multiple VPCs without the need of several Direct Connect connections. Take into account that it is recommended the use of a second connection (Direct Connect or VPN) for high-availability.



1 AWS to on-premises

A On-premises to AWS

1 Traffic from the corporate data center destined to the spoke VPC A is forwarded to **AWS Transit Gateway** via the **AWS Direct Connect (DX)** link. The **Transit Gateway** is connected to **Direct Connect** link by using a Transit virtual interface (VIF) and a **Direct Connect** Gateway.

2 As per the **Transit Gateway o**n-premises route table, the traffic is forwarded to the spoke VPC A attachment.

3 The **Transit Gateway** ENI of the spoke VPC A forwards the traffic to the destination.

A Traffic initiated from an **Amazon EC2** instance in the spoke VPC B and destined to the corporate data center is routed to the **Transit Gateway** ENI as per the spoke VPC B route table.

B Traffic is forwarded to the **AWS Transit Gateway**. As per the spoke VPC route table, the traffic is routed to the office branch via the **AWS Direct Connect** Gateway attachment.

C The traffic is routed to the destination via the **AWS Direct Connect** link.

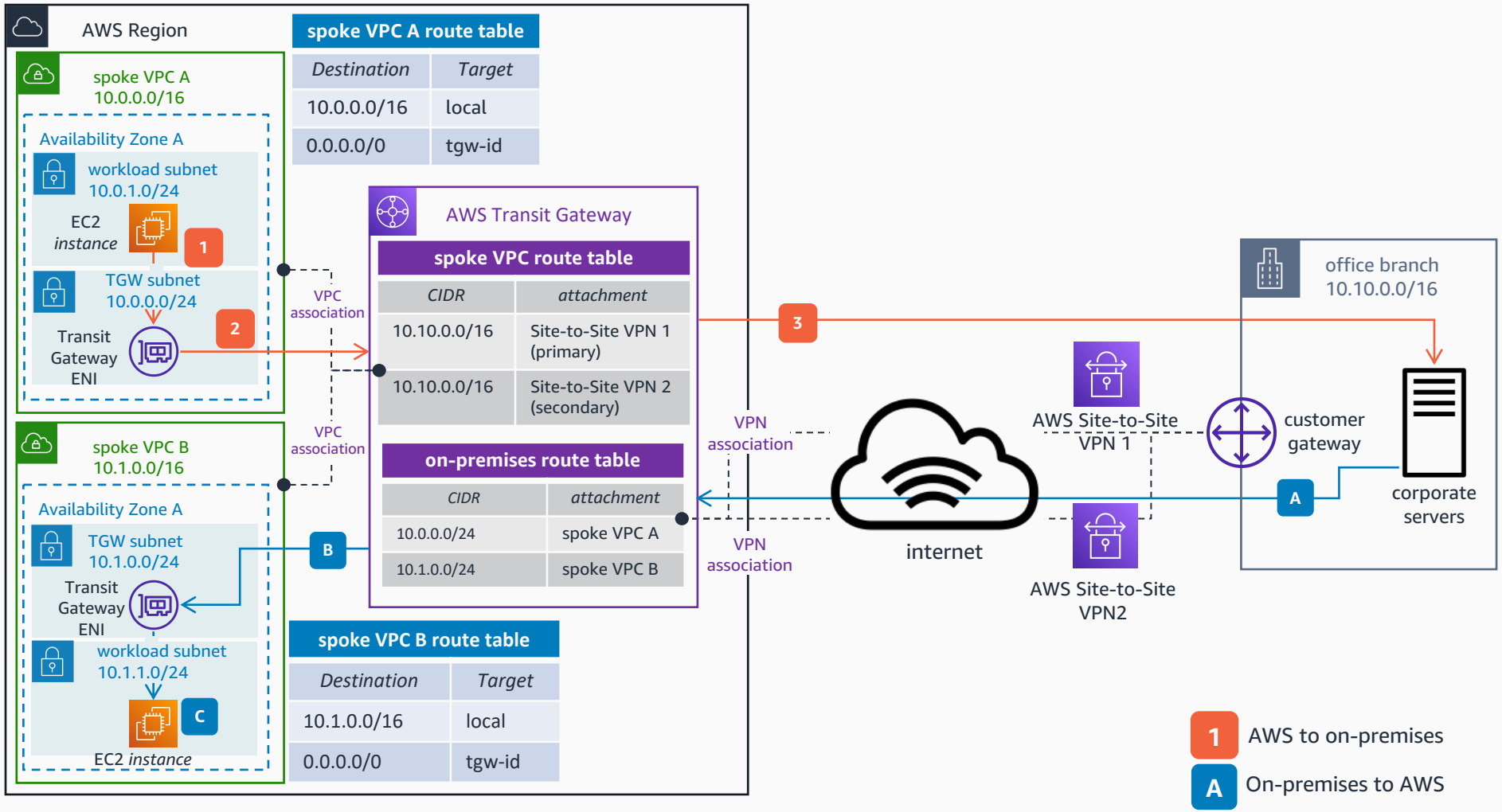
For more information about how to create an **AWS Direct Connect** connection, refer to: [Create a connection – AWS Direct Connect].

Reviewed for technical accuracy August 17, 2022

AWS Reference Architecture

AWS Site-to-Site VPN as primary and AWS Site-to-Site VPN as backup

You can create a Site-to-Site VPN connection directly to a Transit Gateway. With this, you can take advantage of the benefits of a managed VPN solution, while connecting to several VPCs without having to add new connection. Having a secondary VPN connection allows you to achieve high-availability in the hybrid setup.



1 AWS to on-premises

A On-premises to AWS

1 Traffic initiated from an **Amazon EC2** instance in the spoke VPC A and destined to the office branch is routed to the **Transit Gateway** ENI as per the spoke VPC A route table.

2 Traffic is forwarded to the **AWS Transit Gateway**. As per the spoke VPC route table, the traffic is routed to the office branch via the primary **AWS Site-to-Site VPN** attachment. To influence the choice of the primary tunnel you can advertise a shorter Border Gateway Protocol (BGP) AS_PATH from your preferred customer gateway.

3 The traffic is routed to the destination via the primary **Site-to-Site VPN** connection over the internet.

A Traffic from the office branch destined to the spoke VPC B is forwarded to the **Transit Gateway** via the primary **Site-to-Site VPN** connection. When advertising the same prefixes from both **Site-to-Site VPNs**, You can influence this choice by using BGP attributes, such as local preference.

B As per the **Transit Gateway** on-premises route table, the traffic is forwarded to the spoke VPC B attachment.

C The **Transit Gateway** ENI of the spoke VPC B forwards the traffic to the destination.

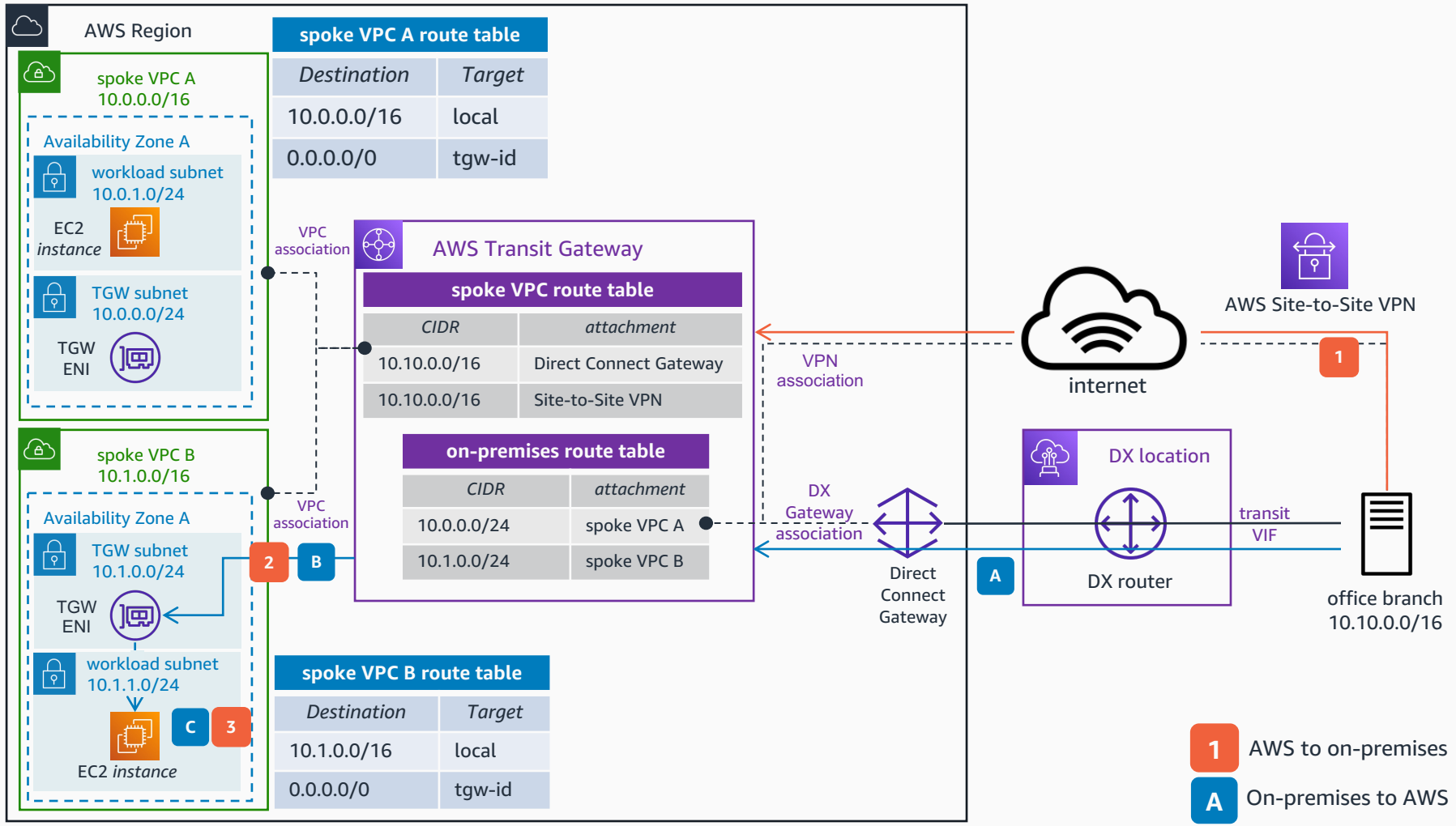
For more information about how to configure **AWS Site-to-Site VPN** to prefer one tunnel over the other, refer to:
[AWS Site-to-Site VPN - Configure tunnel preference]

Reviewed for technical accuracy August 17, 2022

AWS Reference Architecture

AWS Direct Connect as primary and AWS Site-to-Site VPN as backup

You can use a Transit VIF and a Direct Connect gateway to connect your on-premises environments to AWS. With this, you can benefit of the connectivity to multiple VPCs without the need of several Direct Connect connections. Having a VPN connection as backup line allows you to achieve high-availability in the hybrid setup.



A Traffic from the office branch destined to the Spoke VPC B is forwarded to the **Transit Gateway** via the **AWS Direct Connect** link, this behavior can be achieved by configuring the office branch devices with higher BGP local preference pointing to the DX peer. The **Transit Gateway** is connected to **Direct Connect** by using a Transit VIF and a **Direct Connect** Gateway.

B As per the **Transit Gateway o**n-premises route table, the traffic is forwarded to the spoke VPC B attachment.

C The **TGW** ENI of the spoke VPC B forwards the traffic to the destination.

1 In the event of a **AWS Direct Connect** failure, traffic from the office branch destined to the spoke VPC B is forwarded to the **Transit Gateway** via the **AWS Site-to-Site VPN** connection.

2 As per the **Transit Gateway** on-premises route table, the traffic is forwarded to the spoke VPC B attachment.

3 The **TGW** ENI of the spoke VPC B forwards the traffic to the destination.

For more information about how to configure **AWS Direct Connect** with **AWS Site-to-Site VPN** as a backup, refer to:
Using a VPN connection as a backup to Direct Connect

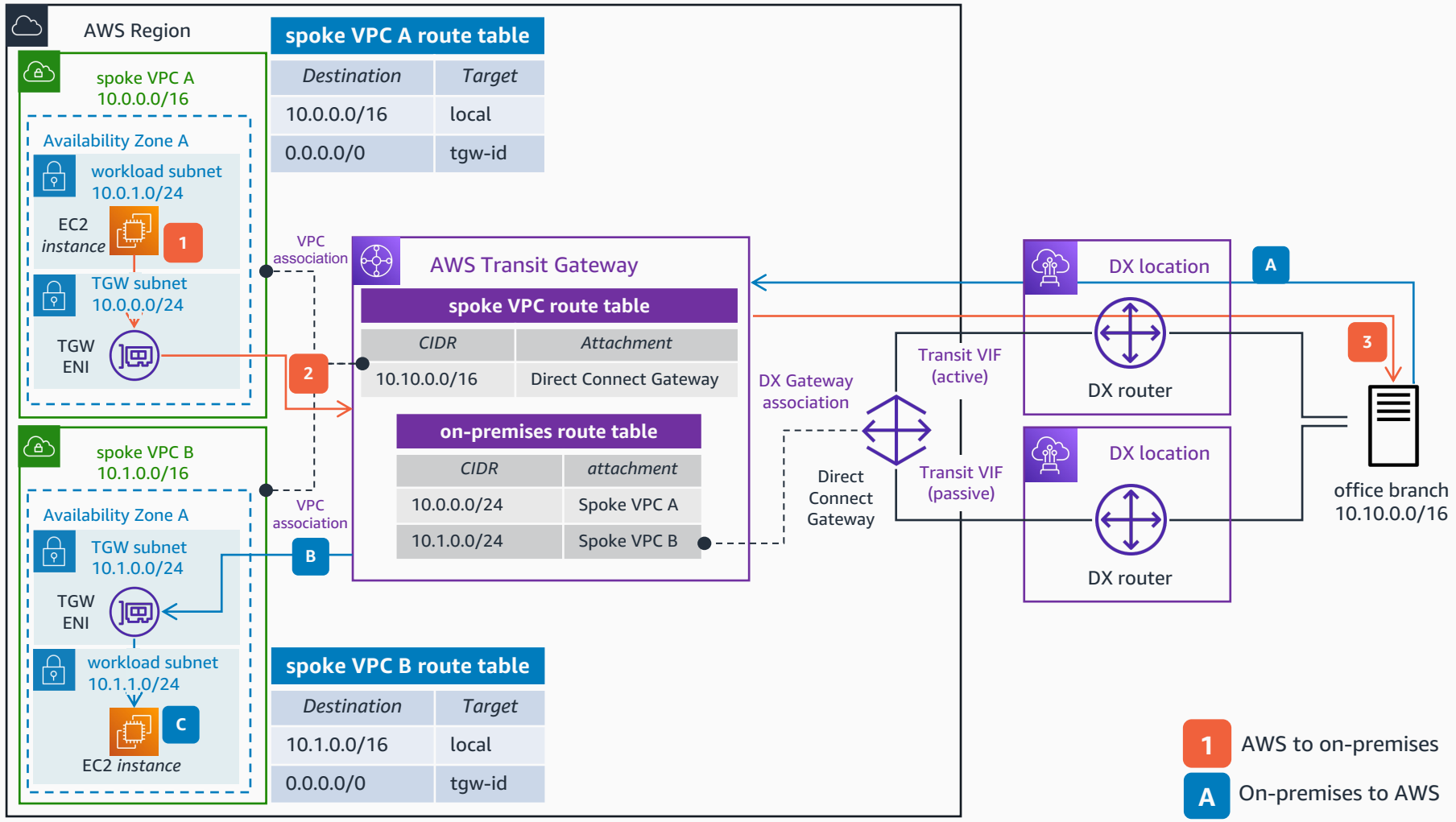
For more information about asymmetric routing, refer to:
Resolve asymmetric routing issues

Reviewed for technical accuracy August 17, 2022

AWS Reference Architecture

AWS Direct Connect in active/passive configuration (two connections)

You can use a Transit VIF and a Direct Connect gateway to connect your on-premises environments to AWS. With this, you can benefit of the connectivity to multiple VPCs without the need of several Direct Connect connections. Having a secondary Direct Connect connection as backup line allows you to achieve high-availability in the hybrid setup.



A Traffic from the office branch destined to the spoke VPC B is forwarded to the **Transit Gateway** via the active **AWS Direct Connect** link. The active/passive behavior in the **Direct Connect** links can be achieved by configuring the BGP configuration of each Transit VIF accordingly. The **Transit Gateway** is connected to **Direct Connect** by using a Transit VIF and a **Direct Connect** Gateway.

B As per the **Transit Gateway o**n-premises route table, the traffic is forwarded to the spoke VPC B attachment.

C The **TGW** ENI of the spoke VPC B forwards the traffic to the destination.

1 Traffic initiated from an **Amazon EC2** instance in the spoke VPC A and destined to the office branch is routed to the **Transit Gateway** ENI as per the spoke VPC A route table.

2 As per the **Transit Gateway s**poke VPC route table, the traffic is forwarded to the **Direct Connect** gateway.

3 Because of the BGP configuration of both **Direct Connect** connections, the active link is the preferred one for the traffic from the **Transit Gateway** to the office branch.

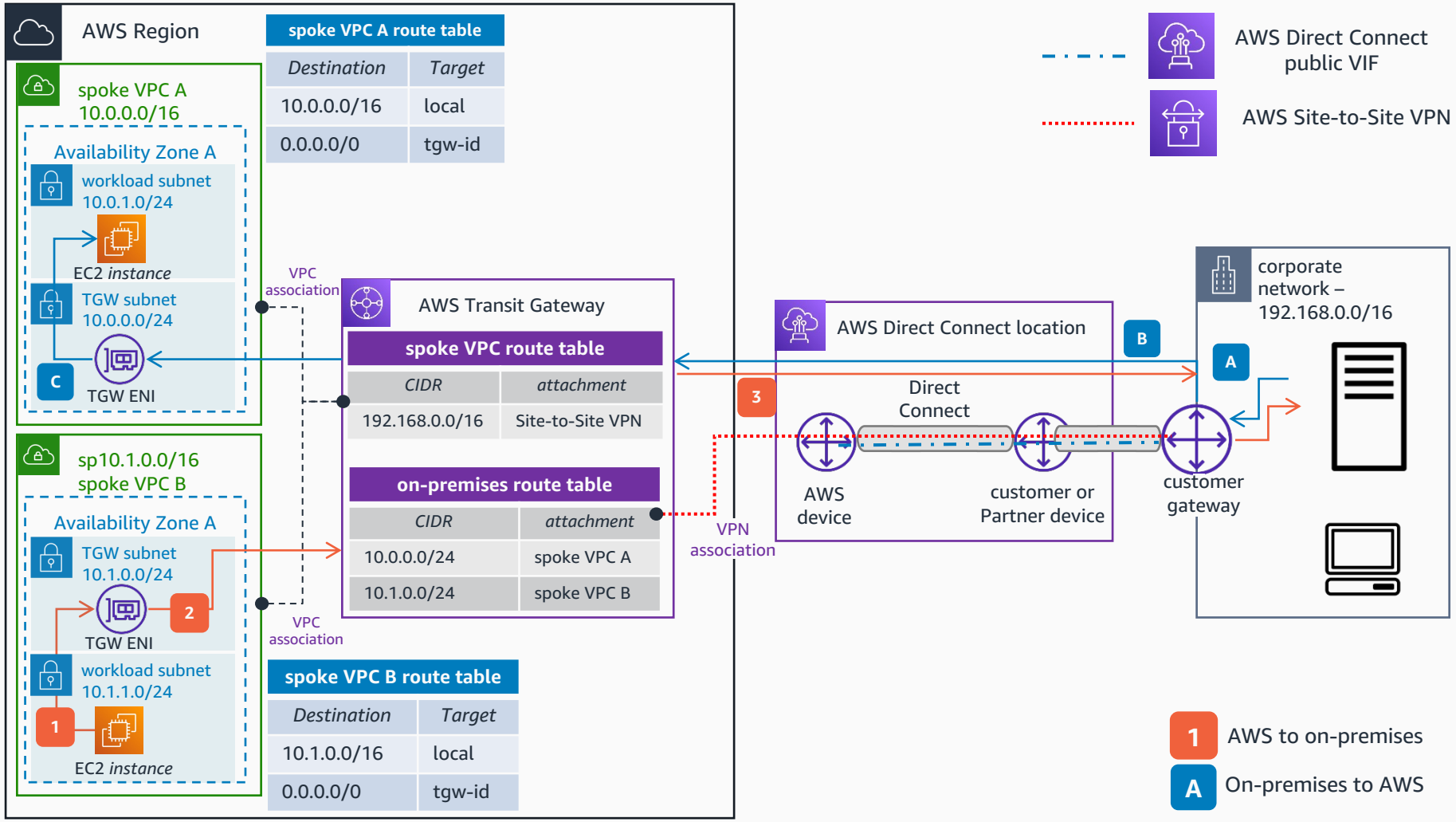
For more information about how to configure active/passive configurations with **AWS Direct Connect**, refer to: [Creating active/passive BGP connections over AWS Direct Connect].

Reviewed for technical accuracy August 17, 2022

AWS Reference Architecture

AWS Site-to-Site VPN on top of AWS Direct Connect for encryption

If you require traffic encryption in your AWS Direct Connect connection, one of the options to achieve is to create an AWS Site-to-Site VPN on top of the Direct Connect connection. You have two options: either by using a Public VIF to connect to the VPN public endpoint, or by creating a Private IP VPN on top of a Transit VIF to use private IPs.



A You can create an **AWS Site-to-Site VPN** on top of an **AWS Direct connect** link by using a public VIF. You will need to configure your customer gateway to bring up the VIF and create the VPN connection. Traffic from the corporate data center destined to the spoke VPC A will be routed via **the Site-to-Site VPN** connection.

B Traffic is sent to the **AWS Transit Gateway** via the **Site-to-Site VPN** connection, which is created over the **Direct Connect** link.

C As per the on-premises route table in the **Transit Gateway**, traffic is forwarded to the spoke VPC A attachment. The **TGW** ENI of the spoke VPC B forwards the traffic to the destination.

1 Traffic initiated from an **Amazon EC2** instance in the spoke VPC B and destined to the corporate data center is routed to the Transit Gateway ENI as per the spoke VPC A route table.

2 As per the **Transit Gateway** spoke VPC route table, the traffic is forwarded to the **AWS Site-to-Site VPN** attachment.

3 The traffic is sent to the corporate data center via the **Site-to-Site VPN** connection on top of the **Direct Connect** link.

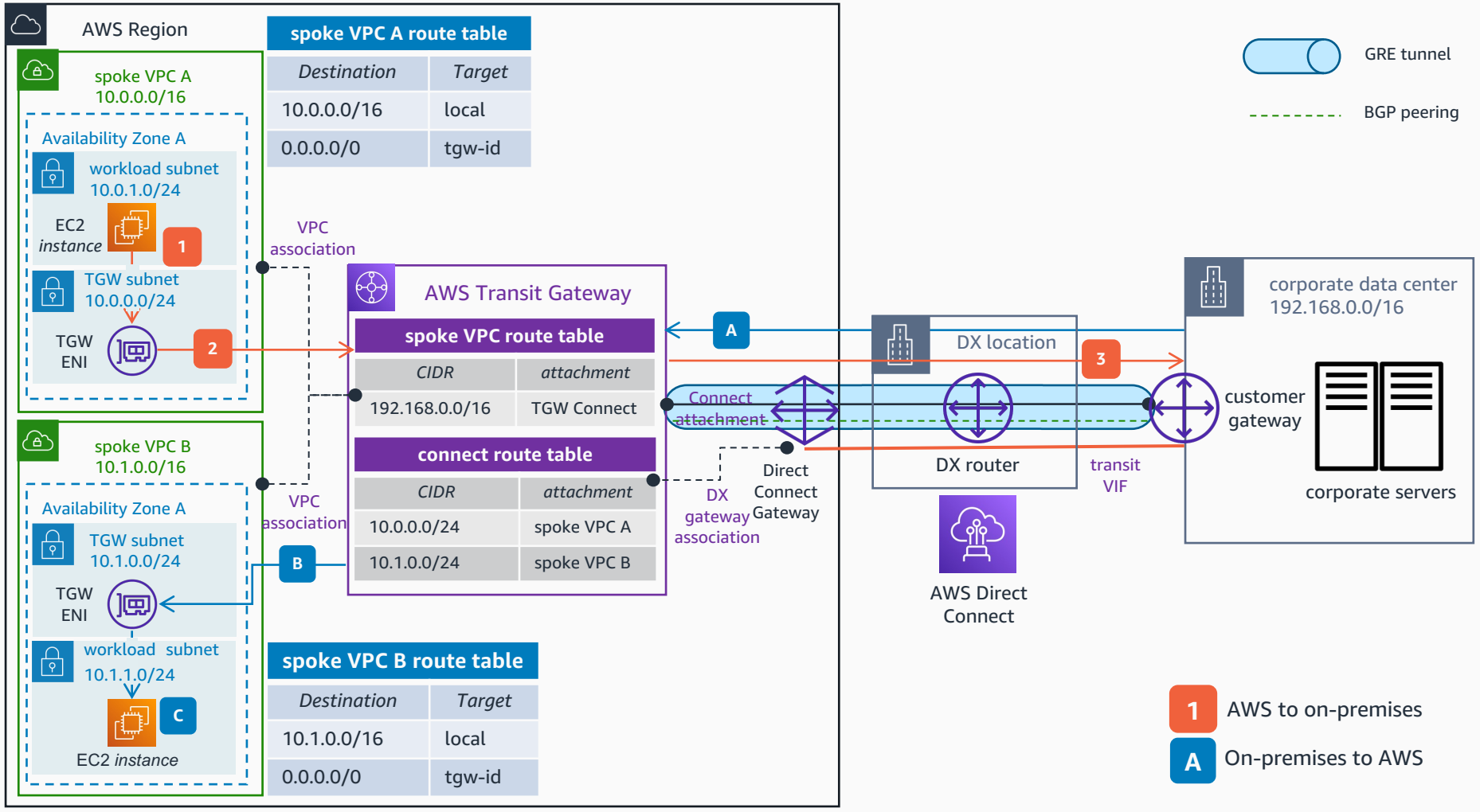
To know more about all the options to encrypt traffic in AWS Direct Connect, refer to: [Traffic Encryptions Options in AWS Direct Connect].

Reviewed for technical accuracy August 17, 2022

AWS Reference Architecture

AWS Direct Connect and Transit Gateway Connect attachments

Use AWS Transit Gateway Connect attachments to simplify your route management across hybrid cloud environments. This design allows the creation of several Connect attachments over the same AWS Direct Connect link to achieve the logical separation of traffic.



1. Traffic initiated from an instance in the spoke VPC A and destined to the corporate data center is routed to the **TGW** ENI as per the spoke VPC A route table.
2. Traffic is forwarded to the **Transit Gateway**. As per the spoke VPC route table, the traffic is routed to the corporate data center via the **Transit Gateway** Connect attachment.
3. The **Transit Gateway** Connect attachment uses the **Direct Connect** connection as transport, and connects the **Transit Gateway** to the corporate data center device using Generic Routing Encapsulation (GRE) tunneling and BGP.

A. Traffic from the corporate data center destined to the spoke VPC B is forwarded to the **Transit Gateway** via the GRE tunnel of the **Transit Gateway** Connect attachment – over the **Direct Connect** link.

B. As per the **Transit Gateway** Connect route table, the traffic is forwarded to the spoke VPC B attachment.

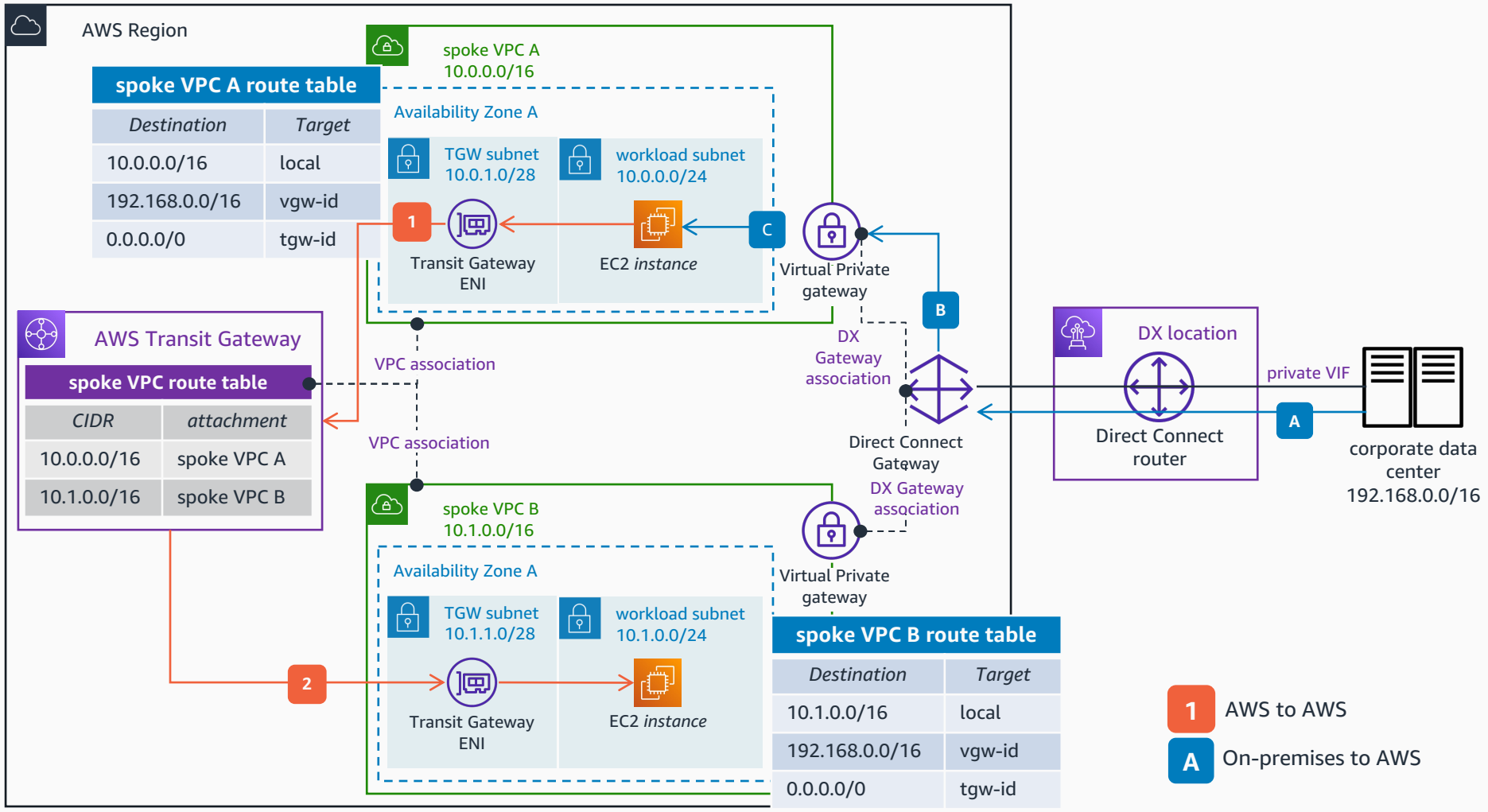
C. The **TGW** ENI of the spoke VPC B forwards the traffic to the destination.

Reviewed for technical accuracy August 17, 2022

AWS Reference Architecture

Hybrid connectivity with AWS Direct Connect Private VIFs and inter-VPC connection with AWS Transit Gateway

When transitivity communication is not needed in the connection between on-premises and AWS, you can be cost-effective by using VIFs and Direct Connect Gateway to connect your corporate data center to your VPCs, and use AWS Transit Gateway only for inter-VPC communication.



1 Traffic initiated from an **Amazon EC2** instance in the spoke VPC A and destined to spoke VPC B is routed to the **Transit Gateway** ENI as per the spoke VPC A route table. Traffic is forwarded to the **AWS Transit Gateway**.

2 As per the **AWS Transit Gateway** spoke VPC route table, the traffic is routed to spoke VPC B. The **Transit Gateway** ENI in spoke VPC B forwards the traffic to the destination.

A Traffic from the corporate data center destined to the spoke VPC A is forwarded to AWS via the **AWS Direct Connect** link. The corporate data center can communicate with both VPCs using one single private VIF thanks to the **Direct Connect** Gateway.

B For this specific use case, the traffic is forwarded to the Virtual Private Gateway of the spoke VPC A.

C As per the spoke VPC A route table, traffic is forwarded to the destination **Amazon EC2** instance.

Reviewed for technical accuracy August 17, 2022

AWS Reference Architecture