Reference Architectures for Implementing SD-WAN Solutions on AWS

1. SD-WAN connectivity with AWS Transit Gateway Connect attachments

2. SD-WAN connectivity with AWS Site-to-Site VPN

3. SD-WAN connectivity with VPC attachments

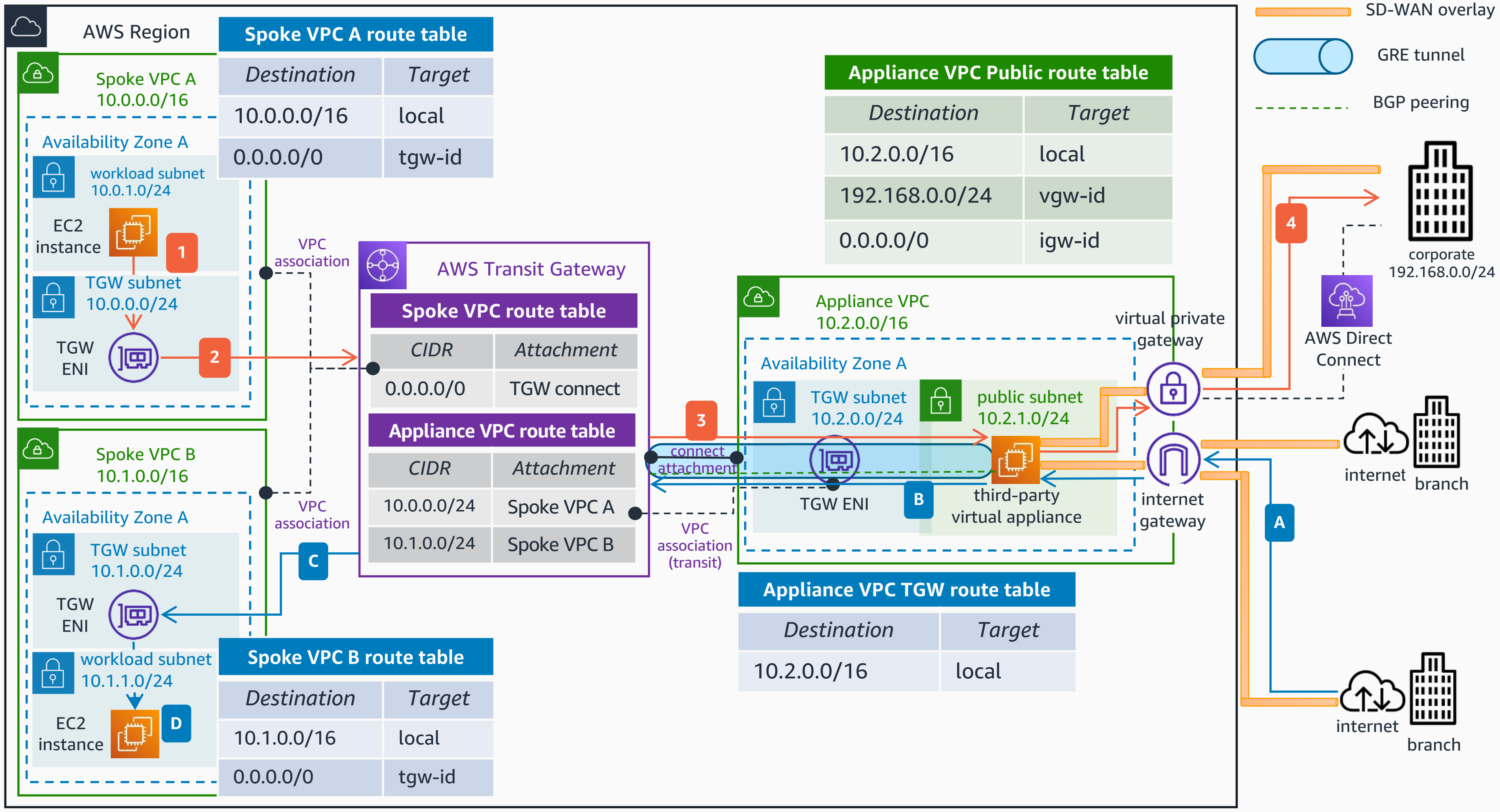
4. SD-WAN devices integration with AWS Transit Gateway and AWS Direct Connect

Reviewed for technical accuracy April 27, 2022

AWS Reference Architecture

SD-WAN Connectivity with AWS Transit Gateway Connect

Use AWS Transit Gateway Connect attachments to connect your software defined-wide area network (SD-WAN) to Transit Gateway, and simplify your route management across hybrid cloud environments. The SD-WAN headend peers with the Transit Gateway over a Generic Routing Encapsulation (GRE) tunnel, allowing this design to take advantage of the higher border gateway protocol (BGP) prefix limit of Transit Gateway. Additionally, with a single Transit Gateway Connect attachment, you will be able to scale horizontally the bandwidth of your connection up to 20 Gbps.



Spoke VPC A route table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	tgw-id

Spoke VPC B route table

Destination	Target
10.1.0.0/16	local
0.0.0.0/0	tgw-id

Spoke VPC route table

CIDR	Attachment
0.0.0.0/0	TGW connect

Appliance VPC route table

CIDR	Attachment
10.0.0.0/24	Spoke VPC A
10.1.0.0/24	Spoke VPC B

Appliance VPC Public route table

Destination	Target
10.2.0.0/16	local
192.168.0.0/24	vgw-id
0.0.0.0/0	igw-id

Appliance VPC TGW route table

Destination	Target
10.2.0.0/16	local

1 Traffic initiated from an **Amazon Elastic Compute Cloud (Amazon EC2)** instance in the Spoke VPC A and destined for the corporate data center is routed to the transit gateway elastic network interface (TGW ENI) as per the spoke VPC A route table.

2 Traffic is forwarded to **AWS Transit Gateway**. As per the spoke VPC route table, the traffic is routed to the appliance virtual private cloud (VPC) via the **Transit Gateway** connect attachment.

3 The **Transit Gateway** connect attachment uses the VPC attachment as transport, and connects **Transit Gateway** to the third-party appliance in the appliance VPC using GRE tunneling and BGP.

4 The third-party virtual appliance encapsulates the traffic, which uses the SD-WAN overlay – on top of the **AWS Direct Connect** link – to reach the corporate data center.

A Traffic from branches outside AWS destined to the spoke VPC B reaches the internet gateway of the appliance VPC via the SD-WAN overlay - on top of the internet.

B The third-party virtual appliance in the Connect VPC forwards the traffic to the **Transit Gateway** via the connect attachment.

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

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

For more information about AWS Transit Gateway Connect attachments and SD-WAN connectivity, refer to: Simplify SD-WAN connectivity with AWS Transit Gateway Connect.

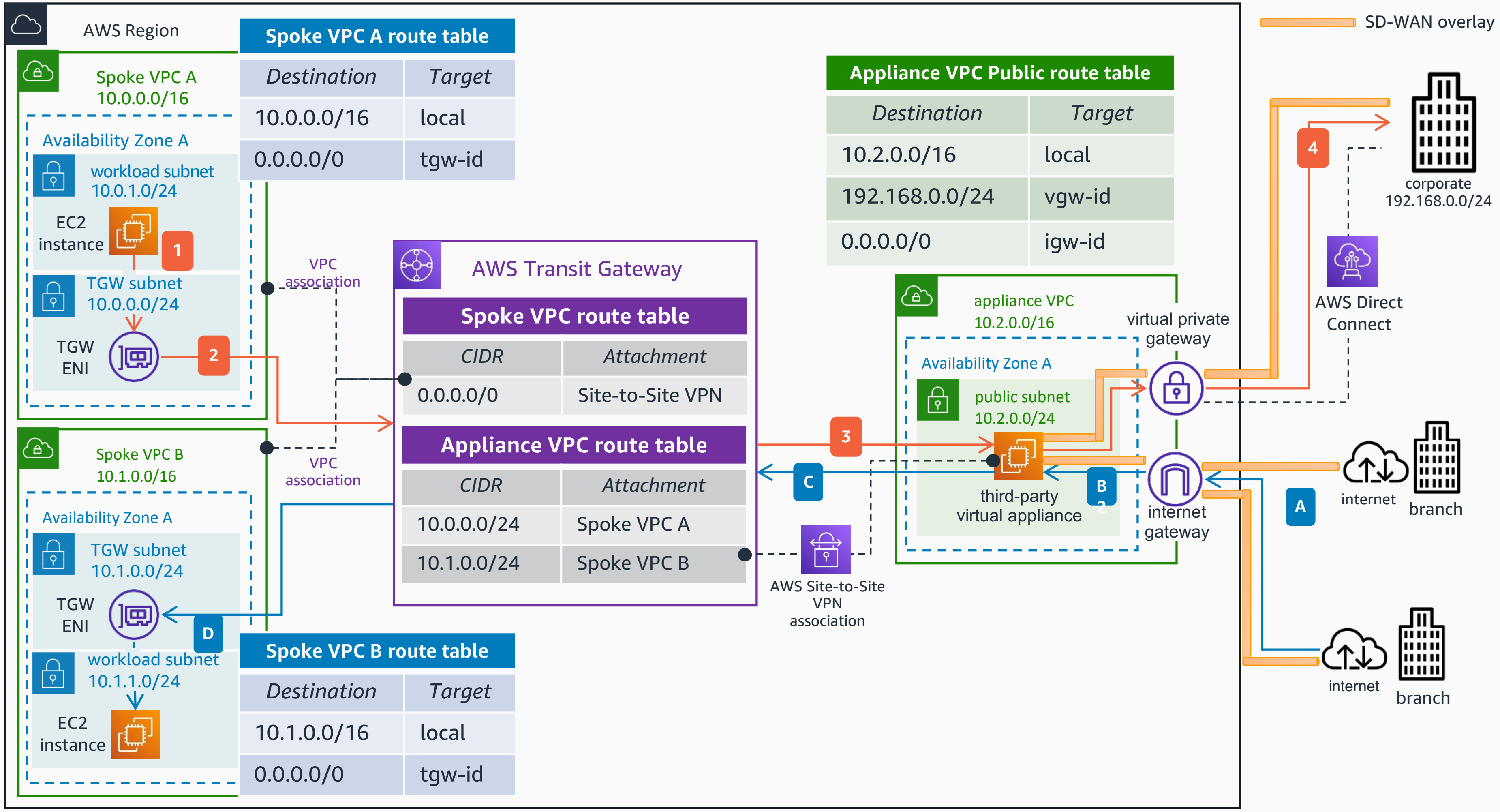
To check an example of this architecture in Terraform, check AWS Hub and Spoke with Transit Gateway Connect VPC.

Reviewed for technical accuracy April 27, 2022

AWS Reference Architecture

SD-WAN connectivity with AWS Site-to-Site VPN

If your third-party virtual appliance does not support GRE, you can still integrate your SD-WAN network to AWS Transit Gateway by creating an AWS Site-to-Site VPN connection, peering the SD-WAN headend with the Transit Gateway using IPSec tunnels. The SD-WAN headend can use BGP to peer with the Transit Gateway to exchange route prefixes. If you want to increase the bandwidth to more than the 1.25 Gbps limit of one single Site-to-Site VPN connection, additional IPSec VPN connections can be used with Transit Gateway's support for Equal-Cost Multi-Path (ECMP).



Spoke VPC A route table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	tgw-id

Appliance VPC Public route table

Destination	Target
10.2.0.0/16	local
192.168.0.0/24	vgw-id
0.0.0.0/0	igw-id

Spoke VPC route table

CIDR	Attachment
0.0.0.0/0	Site-to-Site VPN

Appliance VPC route table

CIDR	Attachment
10.0.0.0/24	Spoke VPC A
10.1.0.0/24	Spoke VPC B

Spoke VPC B route table

Destination	Target
10.1.0.0/16	local
0.0.0.0/0	tgw-id

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 appliance VPC via the **Site-to-Site VPN** attachment.

3 The traffic is routed between the **Transit Gateway** and the third-party virtual appliance between a **Site-to-Site VPN** connection.

4 The third-party virtual appliance encapsulates the traffic, which uses the SD-WAN overlay – on top of the **AWS Direct Connect** link – to reach the corporate data center.

A Traffic from branches outside AWS destined to the spoke VPC B reaches the Internet gateway of the appliance VPC via the SD-WAN overlay - on top of the internet.

B The third-party virtual appliance in the appliance VPC forwards the traffic to the **Transit Gateway** via the Site-to-Site VPN connection.

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

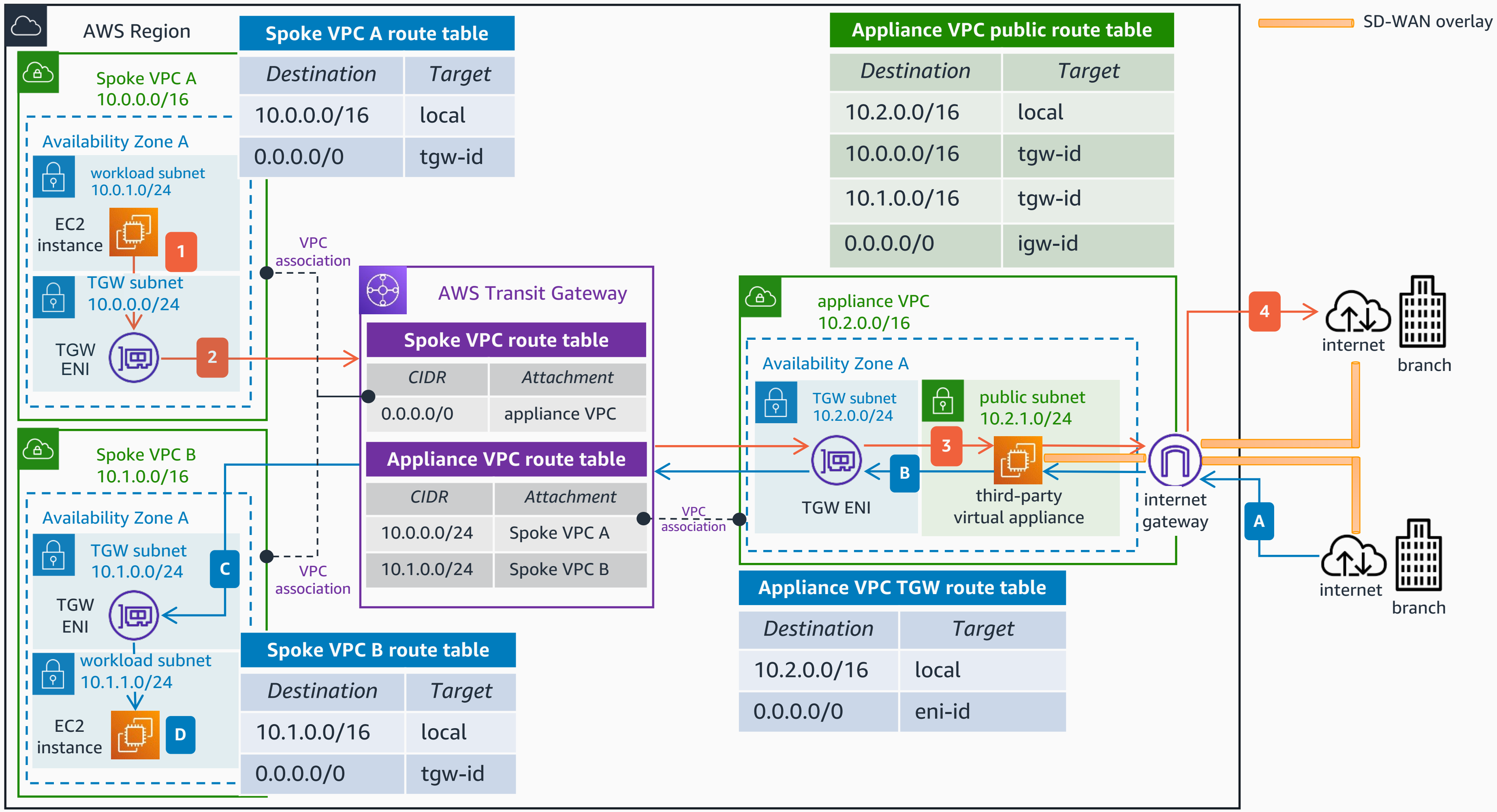
D The TGW ENI of the spoke VPC B forwards the traffic to the destination.

Reviewed for technical accuracy April 27, 2022

AWS Reference Architecture

SD-WAN connectivity with VPC attachments

If your third-party virtual appliance does not support GRE and you don't want to manage IPsec VPN connections, you can integrate your SD-WAN network to AWS Transit Gateway with a VPC attachment. This option will require a more complex setup with VPC and Transit Gateway route tables, as the SD-WAN headend and the Transit Gateway are not peered.



Spoke VPC A route table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	tgw-id

Spoke VPC route table

CIDR	Attachment
0.0.0.0/0	appliance VPC

Appliance VPC route table

CIDR	Attachment
10.0.0.0/24	Spoke VPC A
10.1.0.0/24	Spoke VPC B

Spoke VPC B route table

Destination	Target
10.1.0.0/16	local
0.0.0.0/0	tgw-id

Appliance VPC public route table

Destination	Target
10.2.0.0/16	local
10.0.0.0/16	tgw-id
10.1.0.0/16	tgw-id
0.0.0.0/0	igw-id

Appliance VPC TGW route table

Destination	Target
10.2.0.0/16	local
0.0.0.0/0	eni-id

1 Traffic initiated from an instance in the Spoke VPC A and destined to the branches outside AWS 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 appliance VPC via the appliance VPC attachment.

3 The traffic is sent to the appliance VPC by the **Transit Gateway**. As per the appliance VPC TGW route table, traffic is redirected to the third-party virtual appliance.

4 The third-party virtual appliance encapsulates the traffic, which uses the SD-WAN overlay – on top of the internet – to reach the corporate data center.

A Traffic from branches outside AWS destined to the spoke VPC B reaches the internet gateway of the appliance VPC via the SD-WAN overlay - on top of the internet.

B The third-party virtual appliance in the appliance VPC forwards the traffic to the TGW ENI as per the appliance VPC public route table. Traffic is sent to the **Transit Gateway**.

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

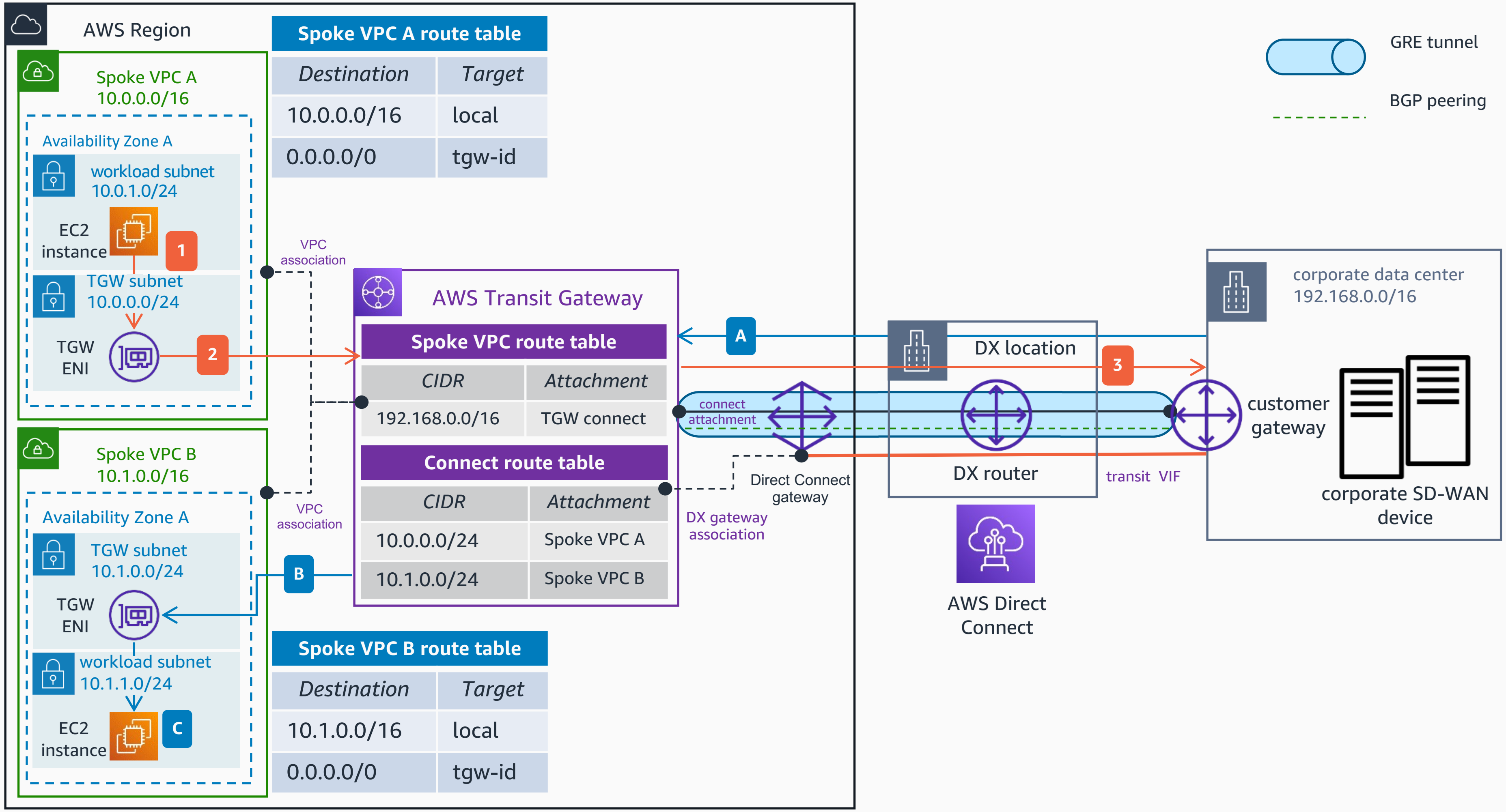
D The TGW ENI of the spoke VPC B forwards the traffic to the destination.

Reviewed for technical accuracy April 27, 2022

AWS Reference Architecture

SD-WAN device integration with AWS Transit Gateway and AWS Direct Connect

Use AWS Transit Gateway Connect attachments and AWS Direct Connect to extend and segment your SD-WAN traffic to AWS without adding extra infrastructure. Each Transit Gateway Connect Peer can have its own Transit Gateway Route Table and BGP peer to extend an on-premises VRF if required.



Spoke VPC A route table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	tgw-id

Spoke VPC route table

CIDR	Attachment
192.168.0.0/16	TGW connect

Connect route table

CIDR	Attachment
10.0.0.0/24	Spoke VPC A
10.1.0.0/24	Spoke VPC B

Spoke VPC B route table

Destination	Target
10.1.0.0/16	local
0.0.0.0/0	tgw-id

1 Traffic initiated from an instance in the spoke VPC A and destined to the corporate data center SD-WAN device 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 SD-WAN device using GRE tunneling and BGP

A Traffic from the corporate data center SD-WAN device destined to the spoke VPC B is forwarded to the **Transit Gateway** via the GRE tunnel of the **Transit Gateway** 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.

For more information about how to integrate your on-premises SD-WAN devices using AWS Transit Gateway and AWS Direct Connect, refer to: Integrate SD-WAN devices with AWS Transit Gateway and AWS Direct Connect

Reviewed for technical accuracy April 27, 2022

AWS Reference Architecture