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 Cloud WAN Connect attachments

3. SD-WAN Connectivity with AWS Cloud WAN Tunnel-less connect attachments

4. SD-WAN connectivity with AWS Site-to-Site VPN to AWS Transit Gateway

5. SD-WAN connectivity with AWS Site-to-Site VPN to AWS Cloud WAN

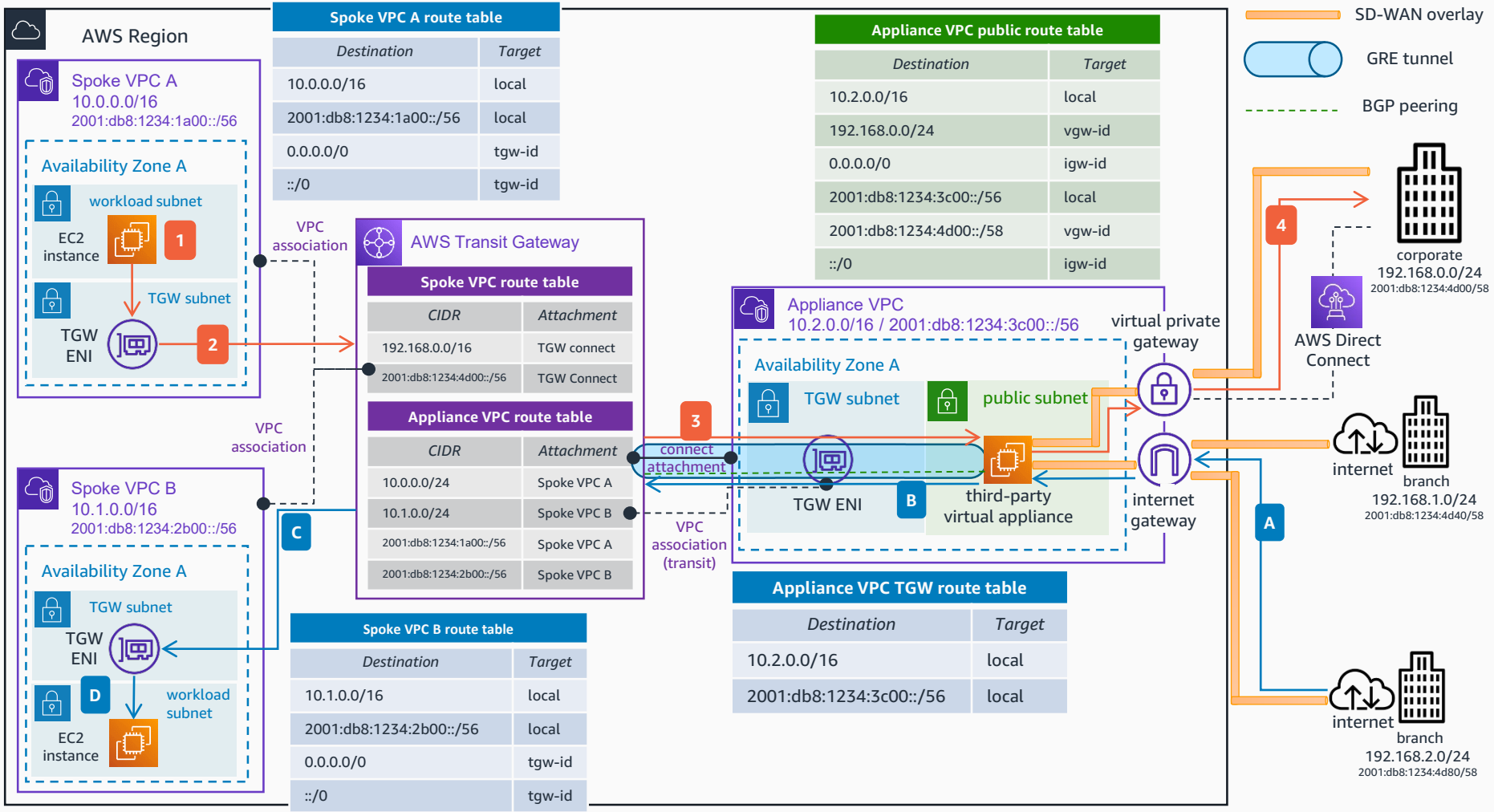
6. SD-WAN devices integration with AWS Transit Gateway and AWS Direct Connect

7. SD-WAN devices integration with AWS Cloud WAN and AWS Direct Connect

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.



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.

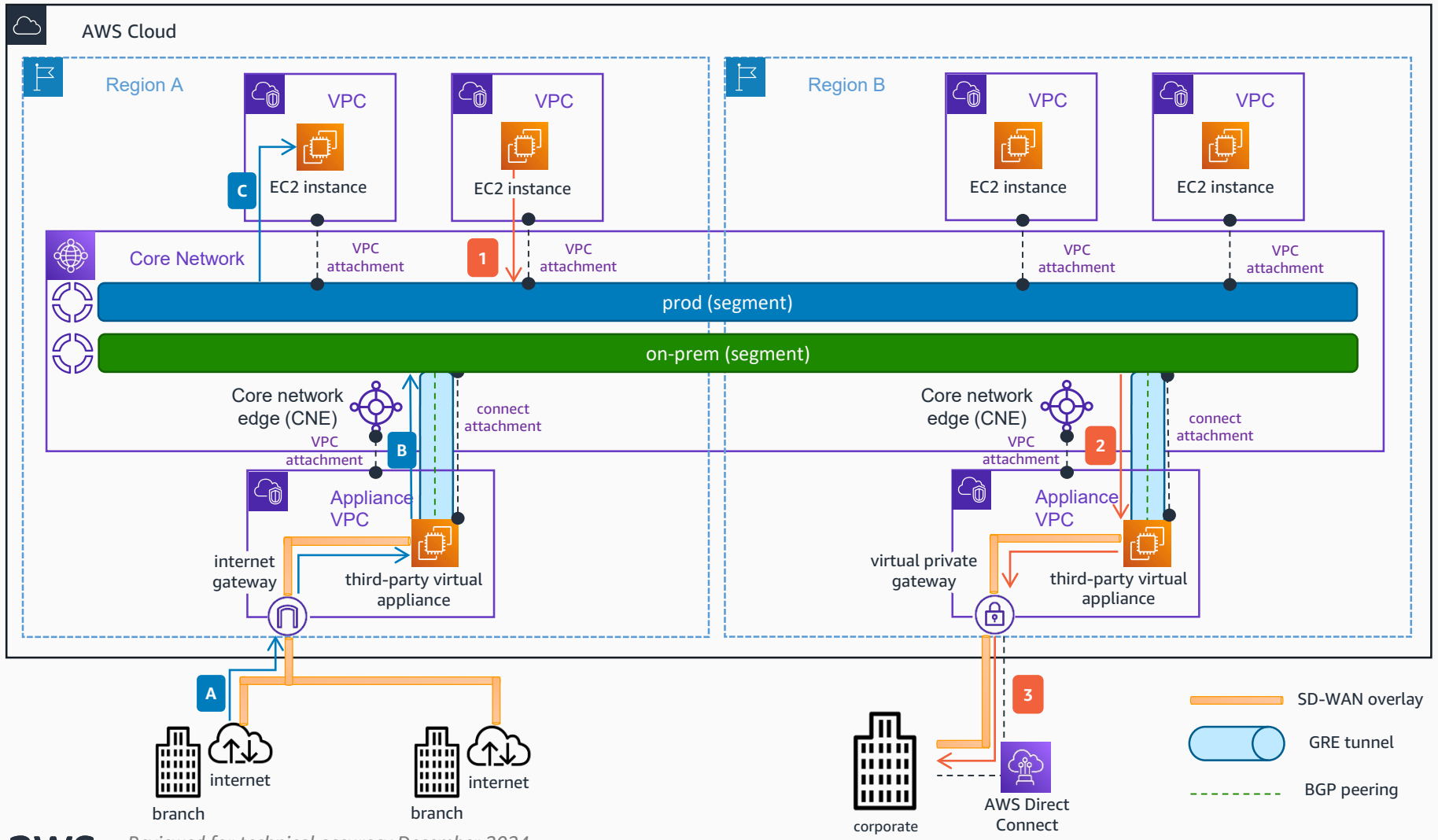
For more information about AWS Transit Gateway Connect attachments and SD-WAN connectivity, refer to: Simplify SD-WAN connectivity with AWS Transit Gateway Connect.

Reviewed for technical accuracy December 2024

AWS Reference Architecture

SD-WAN Connectivity with AWS Cloud WAN Connect attachments

Use Connect attachments to connect your software defined-wide area network (SD-WAN) to AWS Cloud WAN, and simplify your route management across hybrid cloud environments. The SD-WAN headend peers with Cloud WAN's Core Network Edges (CNEs) 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.



1 Traffic initiated from an **Amazon Elastic Compute Cloud (Amazon EC2)** instance in a VPC in Region A and destined for the corporate data center is forwarded to the Core Network. VPC's attachment is associated to the *prod* segment.

2 As per the Core Network policy, traffic arriving to the *prod* segment destined to the corporate data center should be forwarded to the Connect attachment in Region B. The connect attachment uses the VPC attachment as transport, and connects the Core Network to the third-party appliance in the appliance VPC using GRE tunneling and BGP.

3 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 a VPC in Region A 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 Core Network via the connect attachment. The connect attachment is associated to the *on-prem* segment.

C As per the Core Network policy, the traffic is forwarded to the corresponding VPC, forwarding the traffic to the destination.

For more information about AWS Cloud WAN Connect attachments and SD-WAN connectivity, refer to the **documentation**.

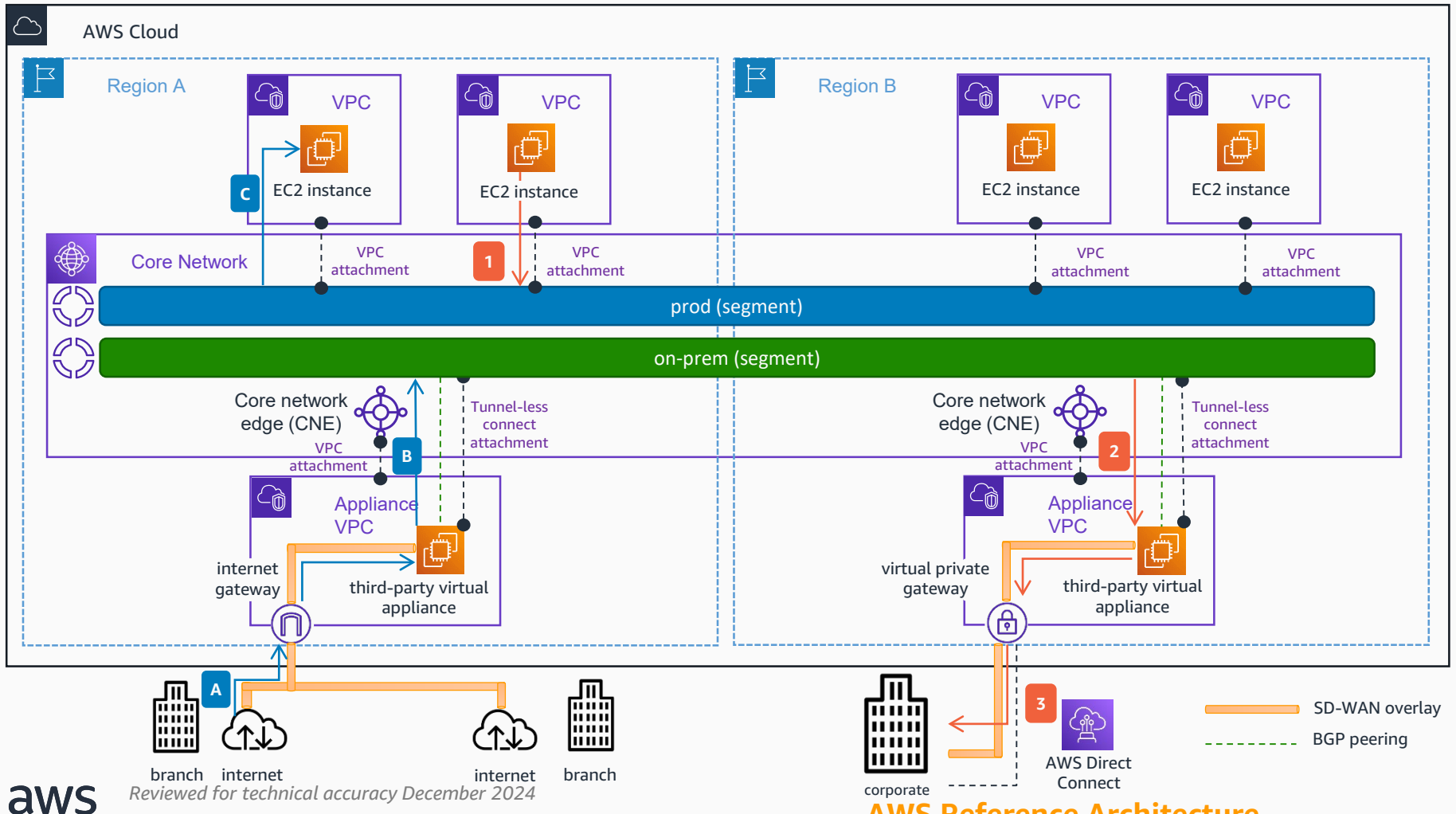
All the VPC routing configuration follows the same pattern as the previous use case – *SD-WAN connectivity with AWS Transit Gateway Connect*.

Reviewed for technical accuracy December 2024

AWS Reference Architecture

SD-WAN Connectivity with AWS Cloud WAN Tunnel-less connect attachments

Use Tunnel-less Connect attachments to connect your software defined-wide area network (SD-WAN) to AWS Cloud WAN in a simpler and higher performance way using the AWS Global Network as a middle-mile transport network. The SD-WAN headend natively peers with Cloud WAN's Core Network Edges (CNEs) over a border gateway protocol (BGP) without using specialized tunneling protocols such as GRE, removing tunneling overhead and improving throughput performance, leveraging the full VPC attachment bandwidth (up to 100GBps per AZ).



Reviewed for technical accuracy December 2024

AWS Reference Architecture

1 Traffic initiated from an **Amazon Elastic Compute Cloud (Amazon EC2)** instance in a VPC in Region A and destined for the corporate data center is forwarded to the Core Network. VPC's attachment is associated to the *prod* segment.

2 As per the Core Network policy, traffic arriving to the *prod* segment destined to the corporate data center should be forwarded to the Tunnel-less Connect attachment in Region B. The tunnel-less **c**onnect attachment uses the VPC attachment as transport, and connects the Core Network to the third-party appliance in the appliance VPC using native BGP.

3 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 a VPC in Region A 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 core network via the tunnel-less connect attachment. The tunnel-less connect attachment is associated to the *on-prem* segment.

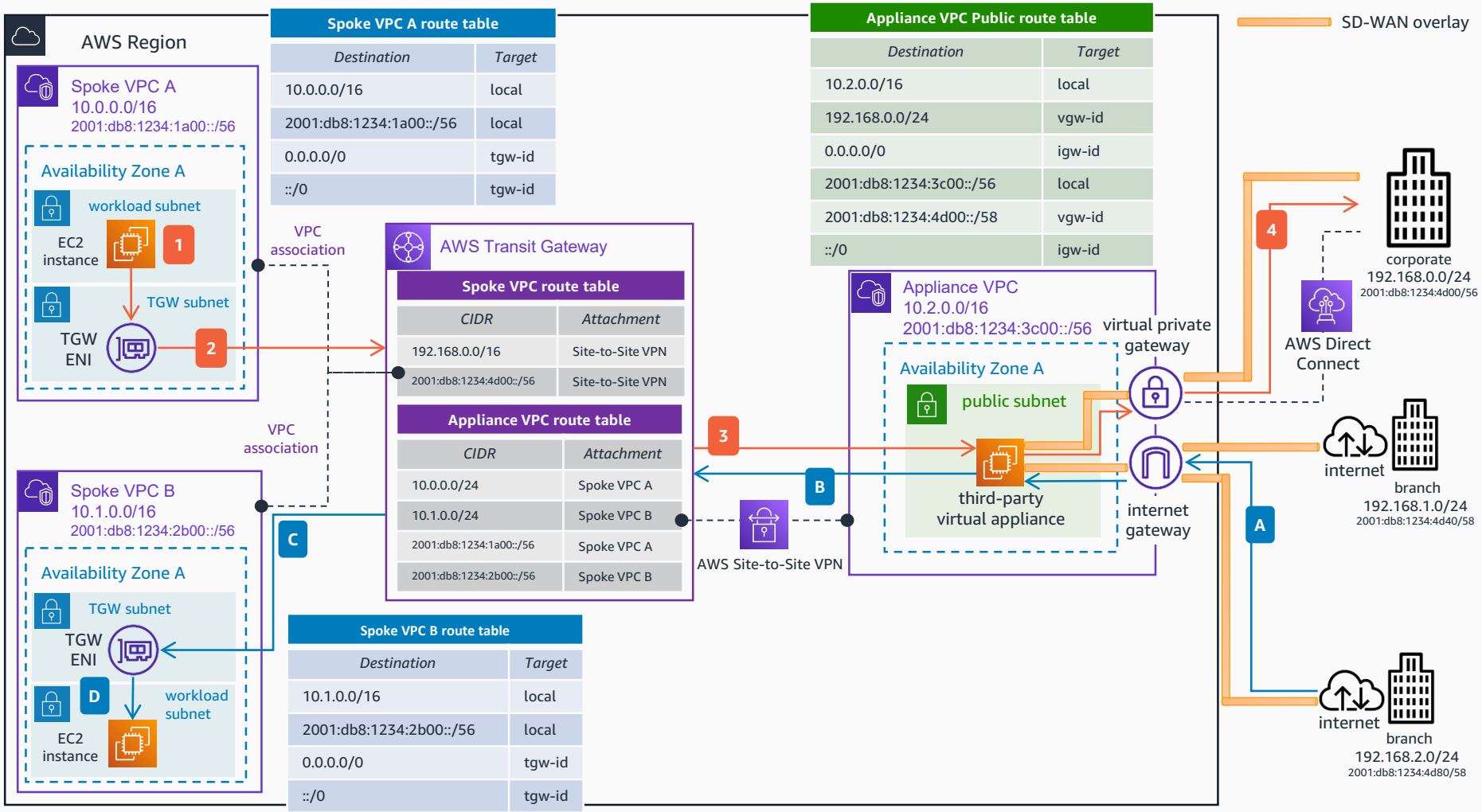
C As per the Core Network policy, the traffic is forwarded to the corresponding VPC, forwarding the traffic to the destination.

For more information about AWS Cloud WAN tunnel-less Connect attachments and SD-WAN connectivity, refer to the **documentation**.

All the VPC routing configuration follows the same pattern as the previous use case – *SD-WAN connectivity with AWS Transit Gateway Connect*.

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).



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 using the **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.

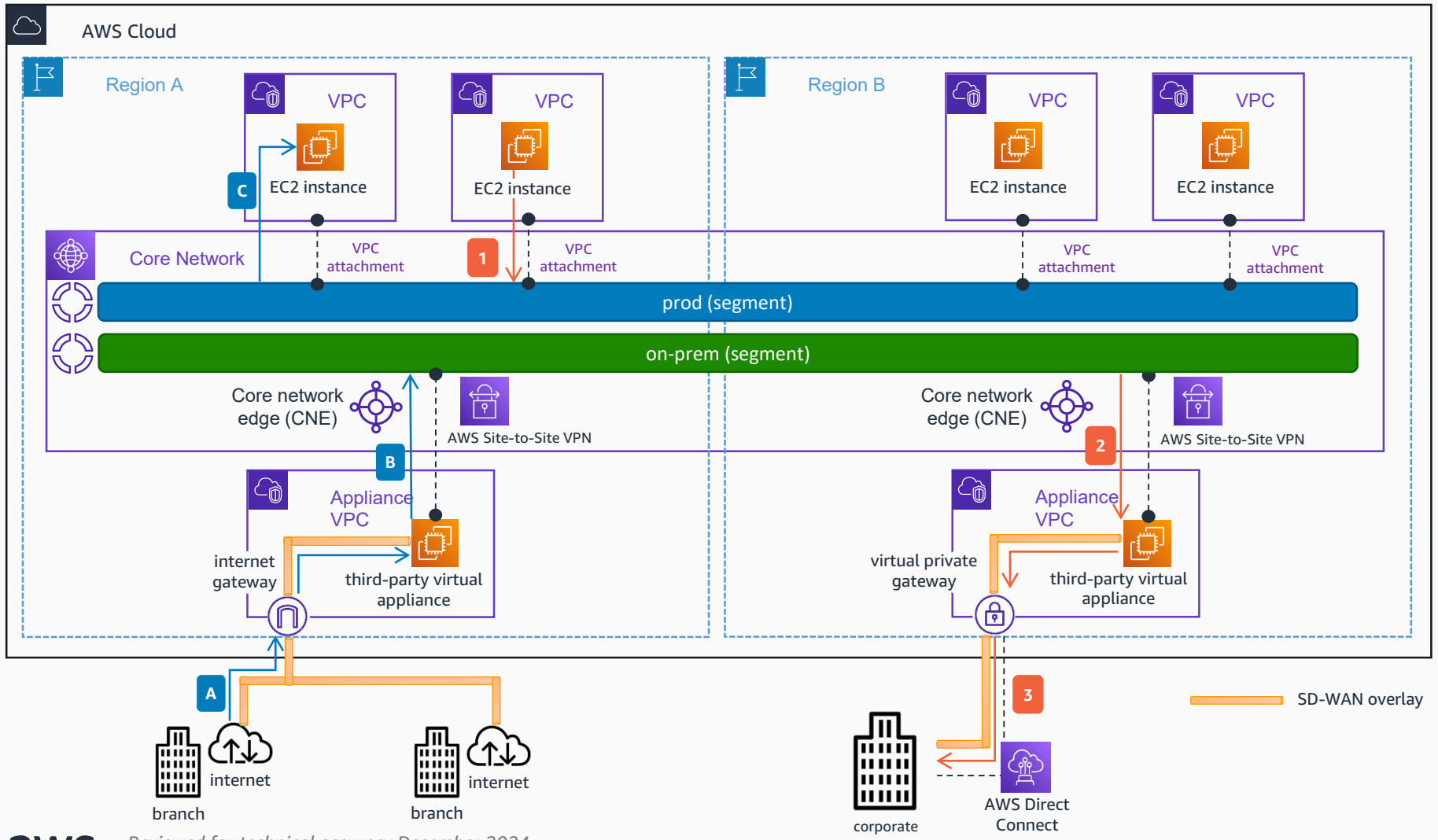
- **A** Traffic from branches outside AWS destined to the Spoke VPC B reaches the Internet gateway of the appliance VPC via the SD-WAN overlay - on top of the internet.
- **B** The third-party virtual appliance in the appliance VPC forwards the traffic to the **Transit Gateway** via the Site-to-Site 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 December 2024

AWS Reference Architecture

SD-WAN Connectivity with AWS Site-to-Site VPN to AWS Cloud WAN

If your third-party virtual appliance does not support GRE, you can still integrate your SD-WAN network to AWS Cloud WAN 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 Cloud WAN's support for Equal-Cost Multi-Path (ECMP).



1 Traffic initiated from an **Amazon Elastic Compute Cloud (Amazon EC2)** instance in a VPC in Region A and destined for the corporate data center is forwarded to the Core Network. VPC's attachment is associated to the *prod* segment.

2 As per the Core Network policy, traffic arriving to the *prod* segment destined to the corporate data center should be forwarded to the **Site-to-Site VPN** attachment in Region B. The traffic is routed between the Core Network and the third-party virtual appliance using the **Site-to-Site VPN** connection.

3 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 a VPC in Region A reaches the Internet gateway of the appliance VPC in that Region 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 Core Network via the Site-to-Site VPN connection.

C As per the Core Network policy, the traffic is forwarded to the corresponding VPC, forwarding the traffic to the destination.

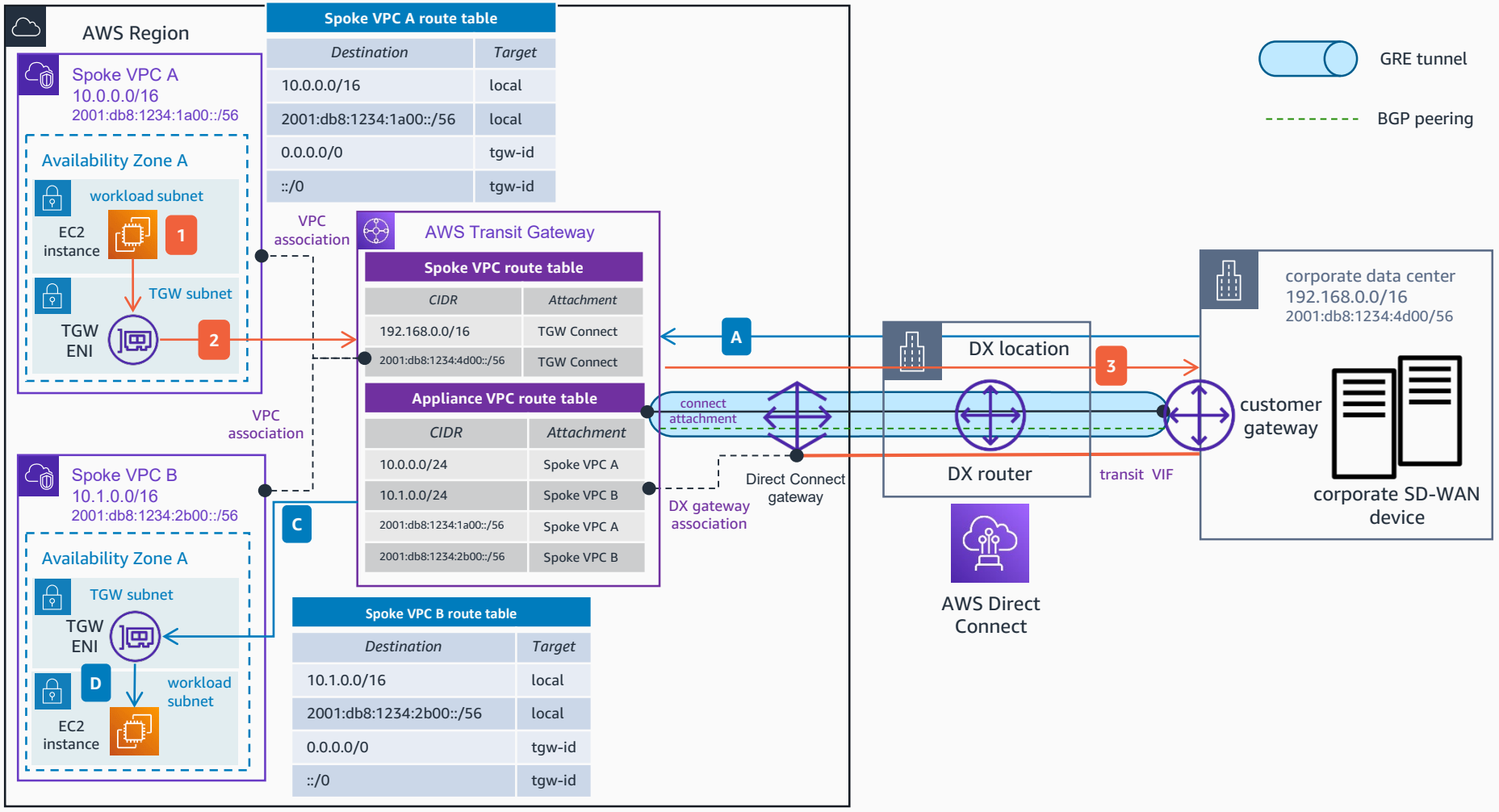
All the VPC routing configuration follows the same pattern as the previous use case – *SD-WAN connectivity with AWS Site-to-Site VPN*.

Reviewed for technical accuracy December 2024

AWS Reference Architecture

SD-WAN devices 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.



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.

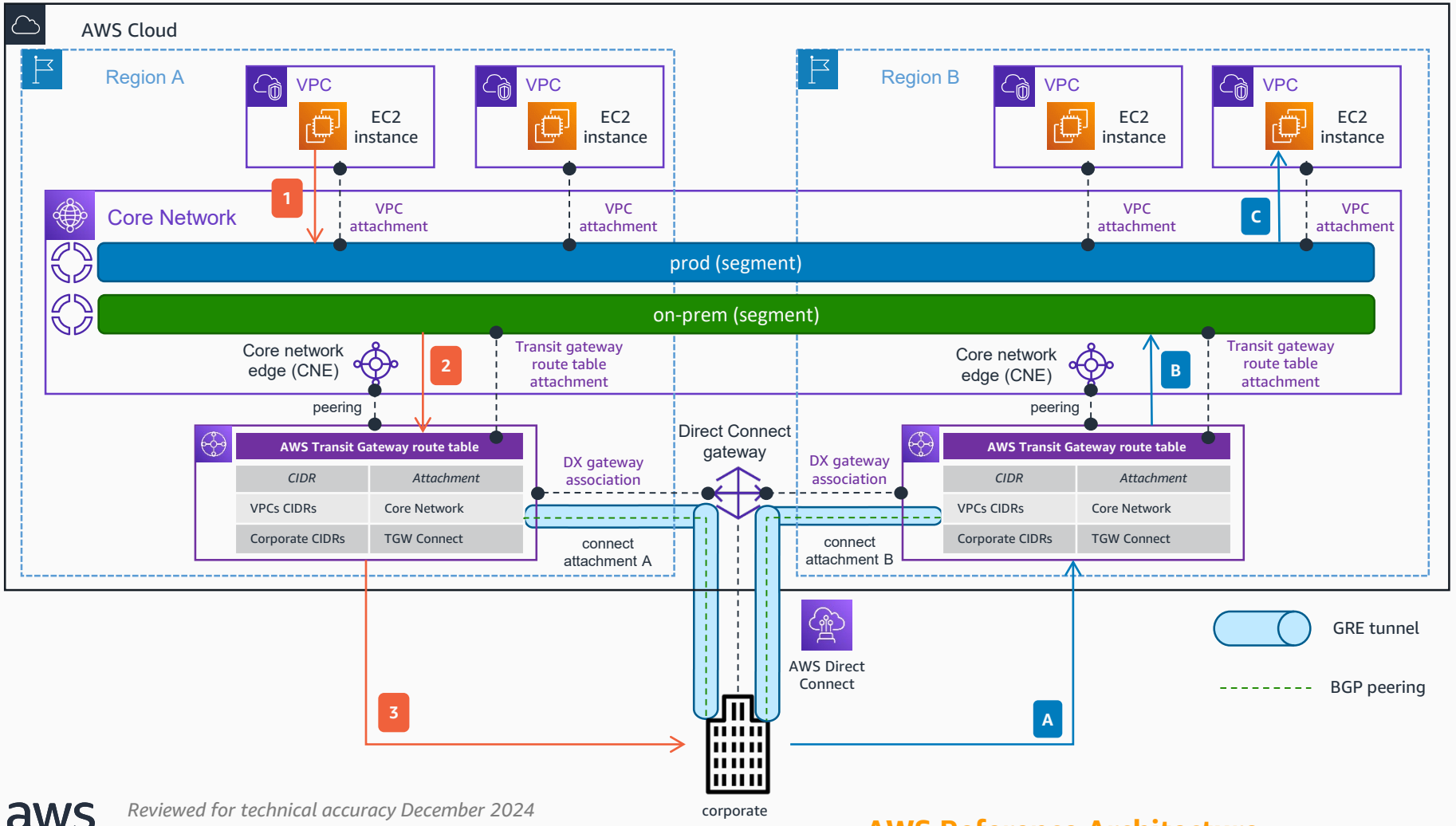
For more information about how to integrate your on-premises SD-WAN devices using AWS Transit Gateway and AWS Direct Connect, refer to: [Integrate SD-WAN devices with AWS Transit Gateway and AWS Direct Connect]

Reviewed for technical accuracy December 2024

AWS Reference Architecture

SD-WAN devices integration with AWS Cloud WAN and AWS Direct Connect via AWS Transit Gateway

When extending your SD-WAN traffic to AWS via AWS Direct Connect to AWS Cloud WAN, you can make use of AWS Transit Gateway Connect attachments and a peering between Cloud WAN and Transit Gateway to achieve end-to-end dynamic routing. You can extend each VRF in your on-premises environment by using a different Transit Gateway Connect peer and route table, and Cloud WAN route table attachment and segment.



1. Traffic initiated from an instance in a VPC in Region A and destined to the corporate data center SD-WAN device is forwarded to the Core Network. VPC's attachment is associated to the *prod* segment.

2. As per the Core Network policy, traffic arriving to the *prod* segment destined to the corporate data center should be forwarded to the Transit Gateway route table attachment – the local attachment will be preferred. Traffic will be forwarded to the **AWS Transit Gateway** in Region A.

3. As per the **Transit Gateway** route table, traffic will be forwarded via the Transit Gateway Connect attachment A. This 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 a VPC in Region B is forwarded to the **Transit Gateway in Region B** via the **Transit Gateway connect** attachment B – over the **Direct Connect** link.

B. As per the **Transit Gateway** route table, the traffic is forwarded to the Core Network. The Transit Gateway route table attachment is associated to the *on-prem* segment.

C. The Core Network forwards the traffic to the corresponding VPC.

Reviewed for technical accuracy December 2024

AWS Reference Architecture