aws

Architecture Diagrams

Reference Architectures for Implementing SD-WAN Solutions on AWS

Reference Architectures for Implementing SD-WAN Solutions on AWS: Architecture Diagrams

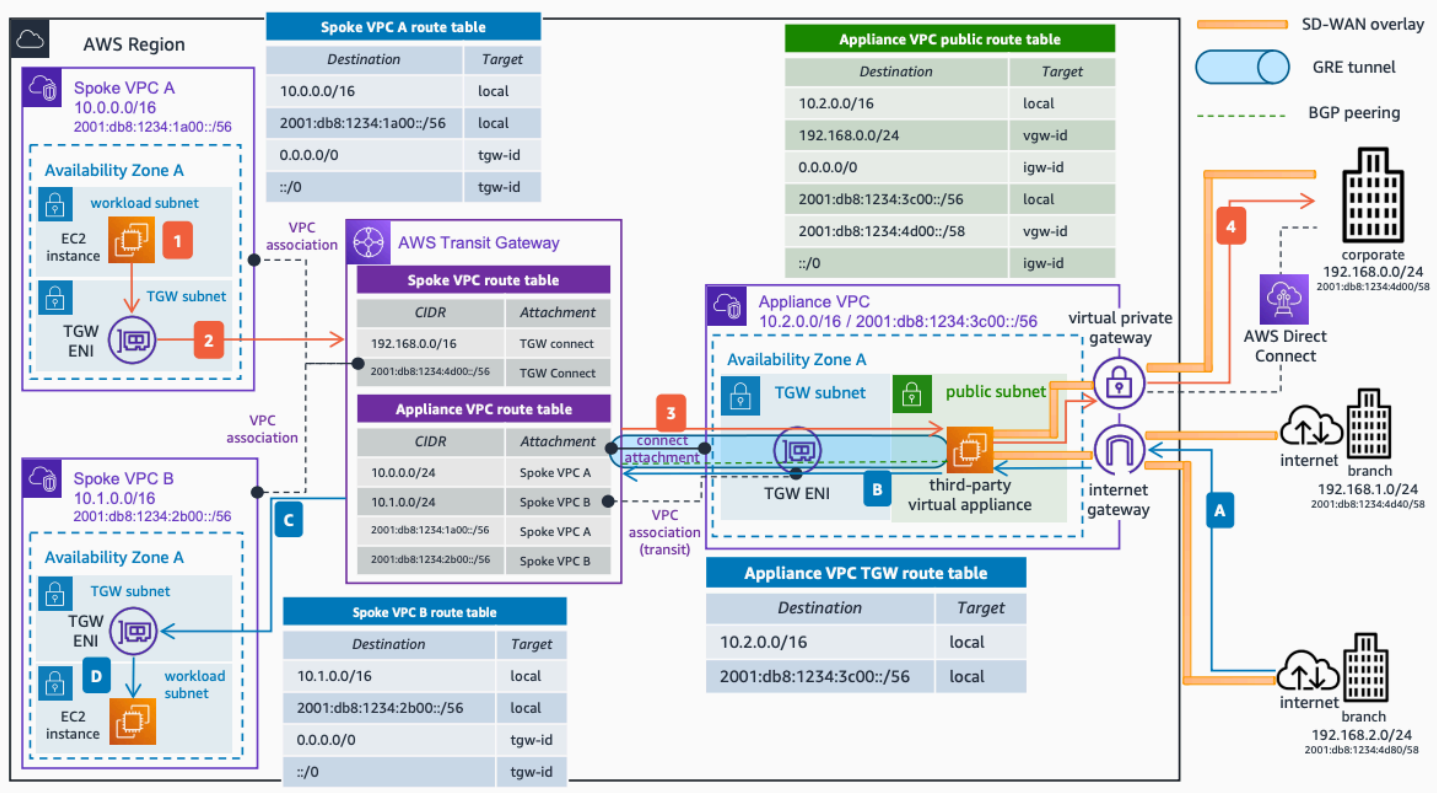
Table of Contents

SD-WAN Connectivity with AWS Transit Gateway Connect Attachments

Publication date: **December 28, 2024 (Diagram history)**

This architecture shows how to 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 can scale horizontally the bandwidth of your connection up to 20 Gbps.

SD-WAN connectivity with AWS Transit Gateway Connect architecture



The following steps describe the AWS to on-premises traffic flow:

1. Traffic initiated from an Amazon Elastic Compute Cloud instance in the Spoke Amazon 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 VPC** through the Transit Gateway Connect attachment.
3. The Transit Gateway Connect attachment uses the Amazon 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.

The following steps describe the on-premises to AWS traffic flow:

Na. Traffic from branches outside AWS destined to the Spoke Amazon VPC B reaches the internet gateway of the **appliance VPC** through the SD-WAN overlay - on top of the internet.

Na. The third-party virtual appliance in the **Connect VPC** forwards the traffic to the Transit Gateway through the Connect attachment.

Na. As per the Transit Gateway Appliance Amazon VPC Route Table, the traffic is forwarded to the **Spoke VPC B** attachment.

Na. 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, see Simplify SD-WAN connectivity with AWS Transit Gateway Connect.

Further reading

For additional information, see the following resources:

- AWS Architecture Icons
- AWS Well-Architected

Diagram history

To be notified about updates to this reference architecture diagram, subscribe to the RSS feed.

Change	Description	Date
Initial publication	Reference architecture diagram first published.	December 28, 2024
Initial publication	Reference architecture diagram first published.	December 28, 2024
Initial publication	Reference architecture diagram first published.	December 28, 2024
Initial publication	Reference architecture diagram first published.	December 28, 2024
Initial publication	Reference architecture diagram first published.	December 28, 2024
Initial publication	Reference architecture diagram first published.	December 28, 2024
Initial publication	Reference architecture diagram first published.	December 28, 2024

Note

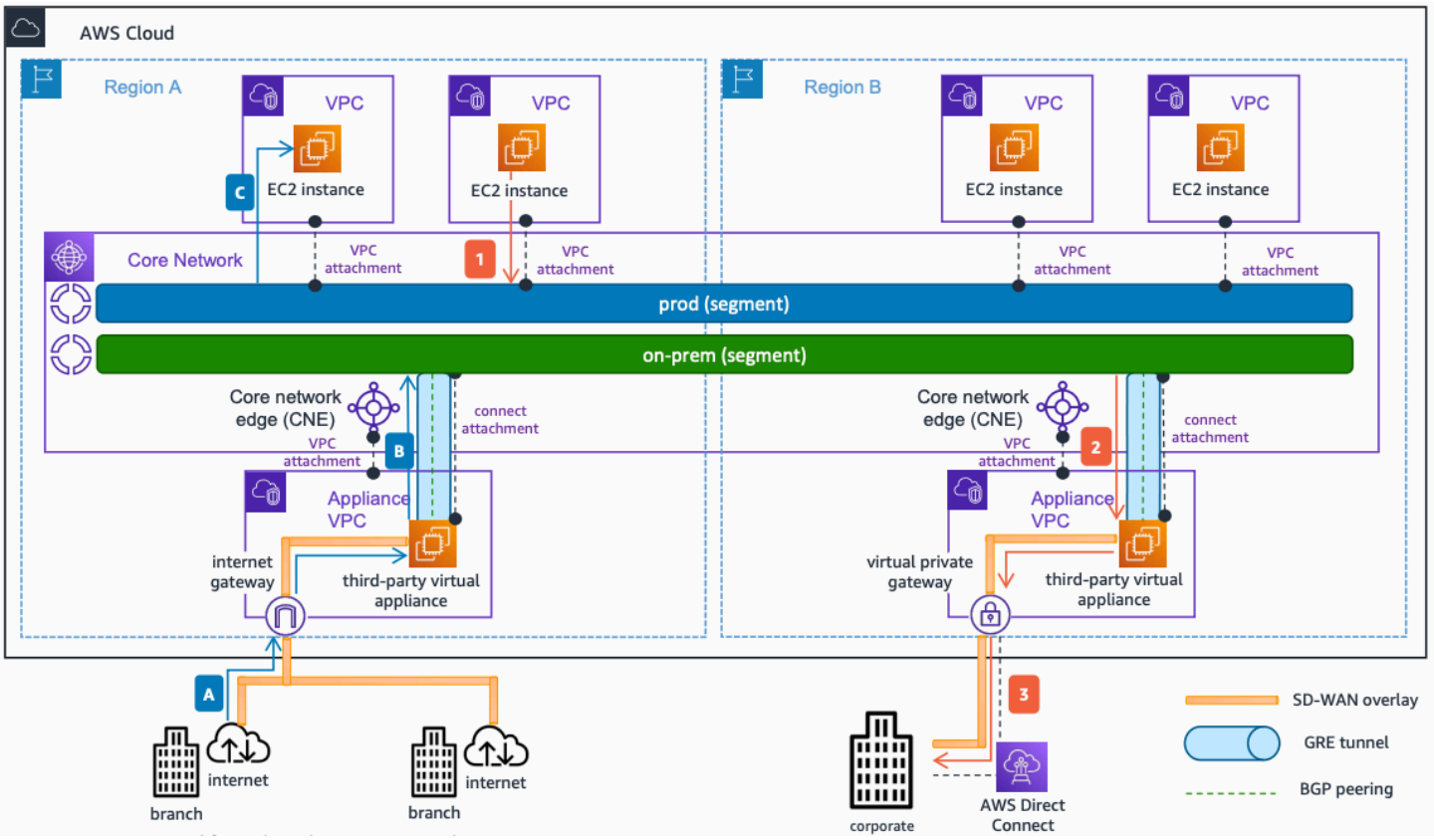
To subscribe to RSS updates, you must have an RSS plugin enabled for the browser you are using.

SD-WAN Connectivity with AWS Cloud WAN Connect Attachments

Publication date: **December 28, 2024 (Diagram history)**

This architecture shows how to use Connect attachments to connect your 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 GRE tunnel, allowing this design to take advantage of the higher BGP prefix limit of AWS Transit Gateway. Additionally, with a single Transit Gateway Connect attachment, you can scale horizontally the bandwidth of your connection up to 20 Gbps.

SD-WAN connectivity with AWS Cloud WAN Connect architecture



The following steps describe the AWS to on-premises traffic flow:

1. Traffic initiated from an Amazon Elastic Compute Cloud instance in a Amazon VPC in Region A and destined for the corporate data center is forwarded to the Core Network. The Amazon VPC 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 Amazon VPC attachment as transport, and connects the Core Network to the third-party appliance in the appliance Amazon 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.

The following steps describe the on-premises to AWS traffic flow:

Na. Traffic from branches outside AWS destined to a Amazon VPC in Region A reaches the internet gateway of the appliance Amazon VPC through the SD-WAN overlay - on top of the internet.

Na. The third-party virtual appliance in the Connect Amazon VPC forwards the traffic to the Core Network through the Connect attachment. The Connect attachment is associated to the on-prem segment.

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

Further reading

For additional information, see the following resources:

- AWS Architecture Icons
- AWS Well-Architected

Diagram history

To be notified about updates to this reference architecture diagram, subscribe to the RSS feed.

Change	Description	Date
Initial publication	Reference architecture diagram first published.	December 28, 2024

Initial publication	Reference architecture diagram first published.	December 28, 2024
Initial publication	Reference architecture diagram first published.	December 28, 2024
Initial publication	Reference architecture diagram first published.	December 28, 2024
Initial publication	Reference architecture diagram first published.	December 28, 2024
Initial publication	Reference architecture diagram first published.	December 28, 2024
Initial publication	Reference architecture diagram first published.	December 28, 2024

Note

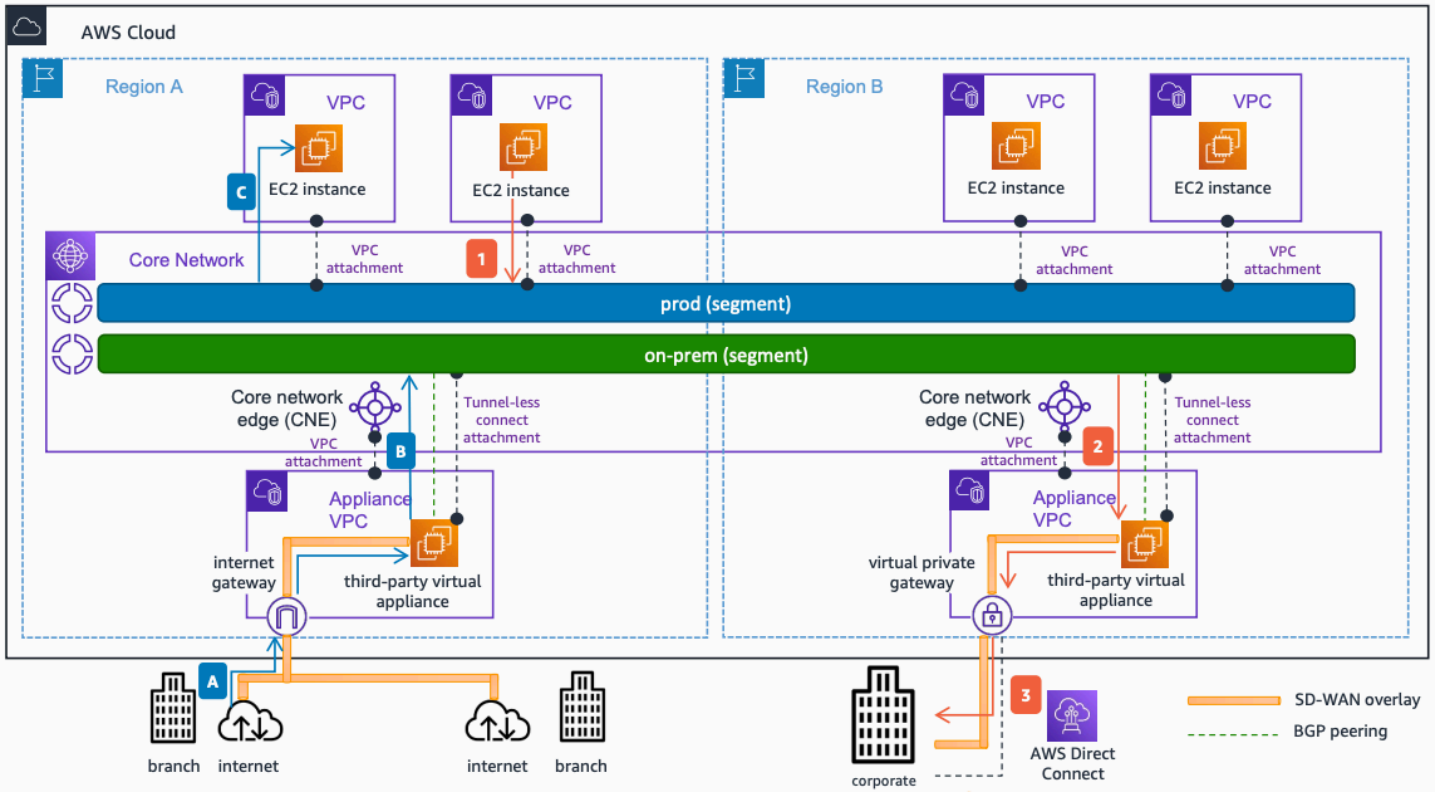
To subscribe to RSS updates, you must have an RSS plugin enabled for the browser you are using.

SD-WAN Connectivity with AWS Cloud WAN Tunnel-less Connect Attachments

Publication date: **December 28, 2024 (Diagram history)**

This architecture shows how to use Tunnel-less Connect attachments to connect your 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 BGP without using specialized tunneling protocols such as GRE, removing tunneling overhead and improving throughput performance, which uses the full Amazon VPC attachment bandwidth (up to 100 Gbps per Availability Zone).

SD-WAN connectivity with AWS Cloud WAN Tunnel-less Connect architecture



The following steps describe the AWS to on-premises traffic flow:

1. Traffic initiated from an Amazon Elastic Compute Cloud instance in a Amazon VPC in Region A and destined for the corporate data center is forwarded to the Core Network. The Amazon VPC 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 Connect attachment uses the Amazon VPC attachment as transport, and connects the Core Network to the third-party appliance in the appliance Amazon 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.

The following steps describe the on-premises to AWS traffic flow:

Na. Traffic from branches outside AWS destined to a Amazon VPC in Region A reaches the internet gateway of the appliance Amazon VPC through the SD-WAN overlay - on top of the internet.

Na. The third-party virtual appliance in the Connect Amazon VPC forwards the traffic to the Core Network through the Tunnel-less Connect attachment. The Tunnel-less Connect attachment is associated to the on-prem segment.

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

Further reading

For additional information, see the following resources:

- AWS Architecture Icons
- AWS Well-Architected

Diagram history

To be notified about updates to this reference architecture diagram, subscribe to the RSS feed.

Change	Description	Date
Initial publication	Reference architecture diagram first published.	December 28, 2024

Initial publication	Reference architecture diagram first published.	December 28, 2024
Initial publication	Reference architecture diagram first published.	December 28, 2024
Initial publication	Reference architecture diagram first published.	December 28, 2024
Initial publication	Reference architecture diagram first published.	December 28, 2024
Initial publication	Reference architecture diagram first published.	December 28, 2024
Initial publication	Reference architecture diagram first published.	December 28, 2024

Note

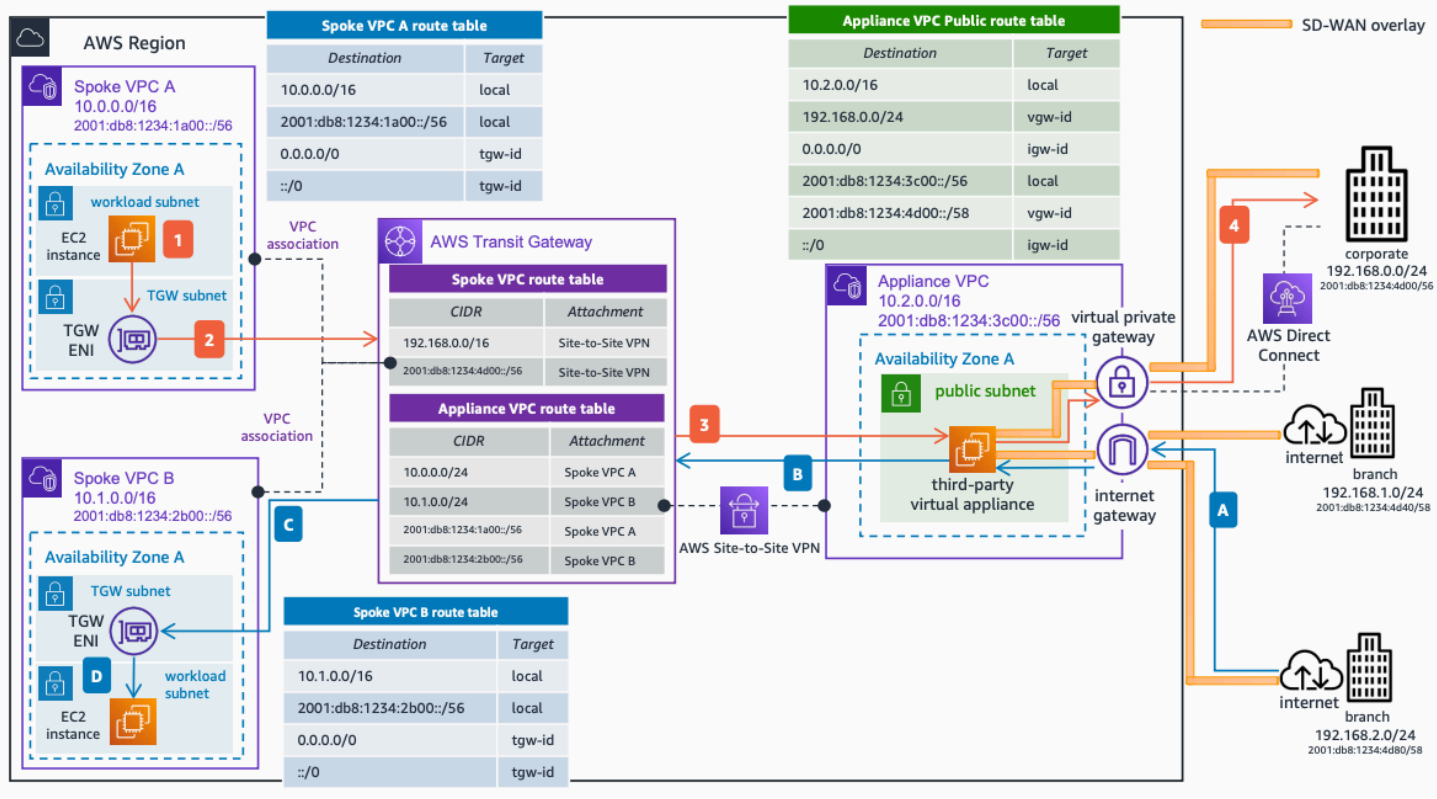
To subscribe to RSS updates, you must have an RSS plugin enabled for the browser you are using.

SD-WAN Connectivity with AWS Site-to-Site VPN to AWS Transit Gateway

Publication date: **December 28, 2024 (Diagram history)**

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).

SD-WAN connectivity with AWS Site-to-Site VPN to AWS Transit Gateway architecture



The following steps describe the AWS to on-premises traffic flow:

1. Traffic initiated from an instance in the Spoke Amazon 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** through 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.

The following steps describe the on-premises to AWS traffic flow:

Na. Traffic from branches outside AWS destined to the Spoke Amazon VPC B reaches the internet gateway of the **appliance VPC** through the SD-WAN overlay - on top of the internet.

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

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

Na. The TGW ENI of the **Spoke VPC B** forwards the traffic to the destination.

Further reading

For additional information, see the following resources:

- AWS Architecture Icons
- AWS Well-Architected

Diagram history

To be notified about updates to this reference architecture diagram, subscribe to the RSS feed.

Change	Description	Date
Initial publication	Reference architecture diagram first published.	December 28, 2024

Initial publication	Reference architecture diagram first published.	December 28, 2024
Initial publication	Reference architecture diagram first published.	December 28, 2024
Initial publication	Reference architecture diagram first published.	December 28, 2024
Initial publication	Reference architecture diagram first published.	December 28, 2024
Initial publication	Reference architecture diagram first published.	December 28, 2024
Initial publication	Reference architecture diagram first published.	December 28, 2024

Note

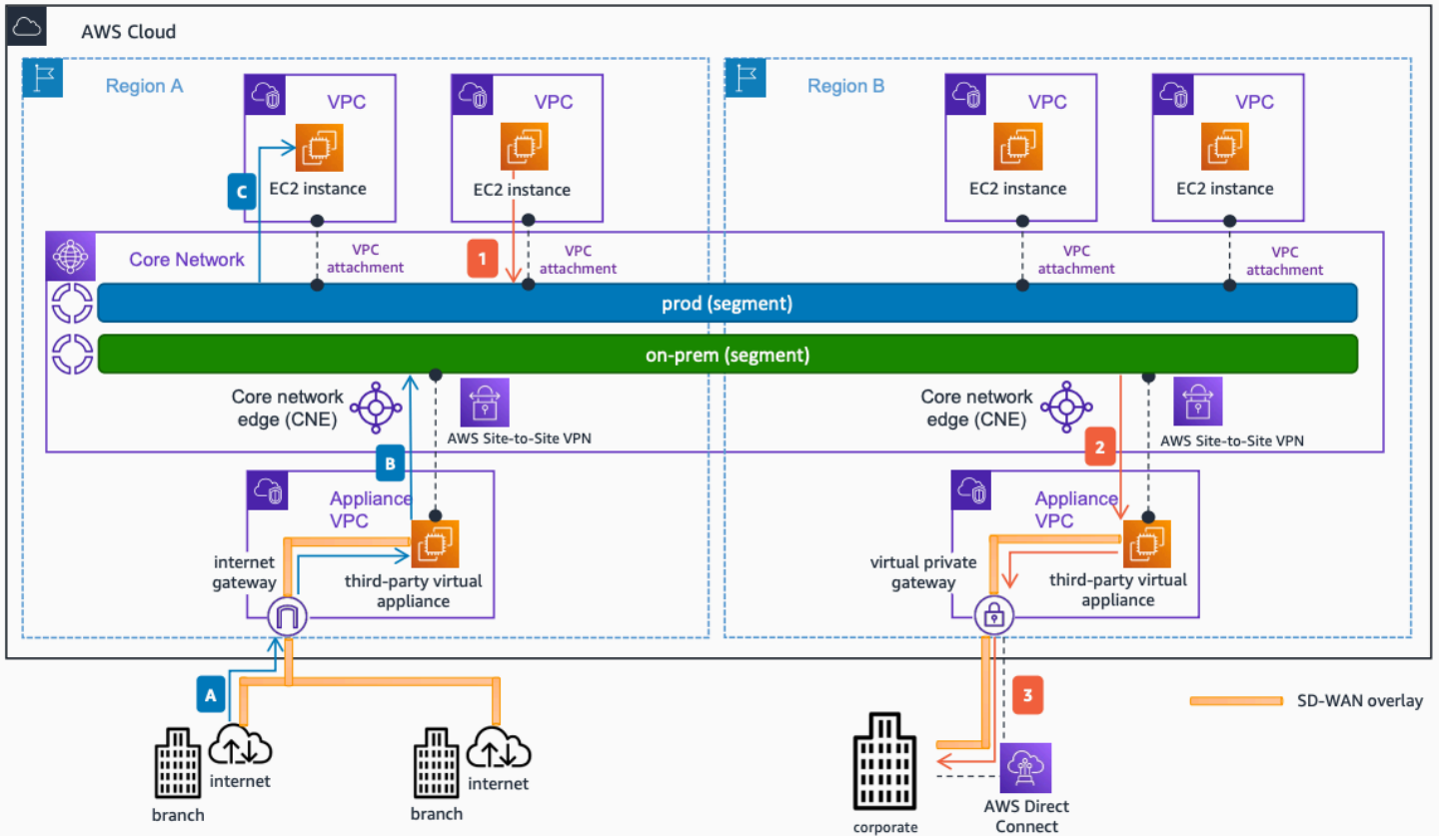
To subscribe to RSS updates, you must have an RSS plugin enabled for the browser you are using.

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

Publication date: **December 28, 2024 (Diagram history)**

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).

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



The following steps describe the AWS to on-premises traffic flow:

1. Traffic initiated from an Amazon Elastic Compute Cloud instance in a Amazon VPC in Region A and destined for the corporate data center is forwarded to the Core Network. The Amazon VPC 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.

The following steps describe the on-premises to AWS traffic flow:

Na. Traffic from branches outside AWS destined to a Amazon VPC in Region A reaches the internet gateway of the **appliance VPC** in that Region through the SD-WAN overlay - on top of the internet.

Na. The third-party virtual appliance in the **appliance VPC** forwards the traffic to the Core Network through the Site-to-Site VPN connection.

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

Further reading

For additional information, see the following resources:

- AWS Architecture Icons
- AWS Well-Architected

Diagram history

To be notified about updates to this reference architecture diagram, subscribe to the RSS feed.

Change	Description	Date
Initial publication	Reference architecture diagram first published.	December 28, 2024

Initial publication	Reference architecture diagram first published.	December 28, 2024
Initial publication	Reference architecture diagram first published.	December 28, 2024
Initial publication	Reference architecture diagram first published.	December 28, 2024
Initial publication	Reference architecture diagram first published.	December 28, 2024
Initial publication	Reference architecture diagram first published.	December 28, 2024
Initial publication	Reference architecture diagram first published.	December 28, 2024

Note

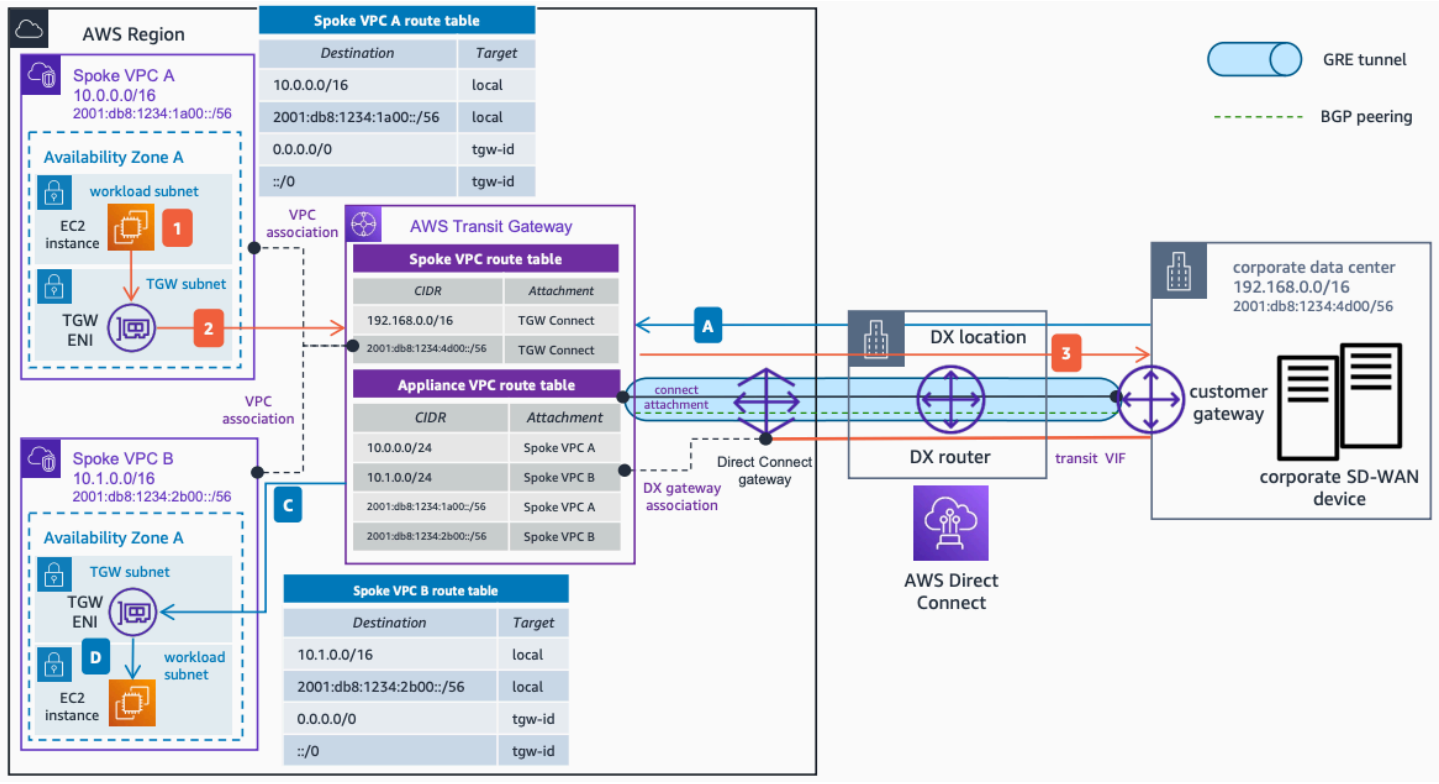
To subscribe to RSS updates, you must have an RSS plugin enabled for the browser you are using.

SD-WAN Devices Integration with AWS Transit Gateway and AWS Direct Connect

Publication date: **December 28, 2024 (Diagram history)**

This architecture shows how to 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.

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



The following steps describe the AWS to on-premises traffic flow:

1. Traffic initiated from an instance in the Spoke Amazon VPC A and destined to the corporate data center SD-WAN device is routed to the TGW ENI as per the Spoke Amazon 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 through 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.

The following steps describe the on-premises to AWS traffic flow:

Na. Traffic from the corporate data center SD-WAN device destined to the **Spoke VPC B** is forwarded to the Transit Gateway through the GRE tunnel of the Transit Gateway attachment, over the Direct Connect link.

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

Na. 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, see Integrate SD-WAN devices with AWS Transit Gateway and AWS Direct Connect.

Further reading

For additional information, see the following resources:

- AWS Architecture Icons
- AWS Well-Architected

Diagram history

To be notified about updates to this reference architecture diagram, subscribe to the RSS feed.

Change	Description	Date
Initial publication	Reference architecture diagram first published.	December 28, 2024
Initial publication	Reference architecture diagram first published.	December 28, 2024

Initial publication	Reference architecture diagram first published.	December 28, 2024
Initial publication	Reference architecture diagram first published.	December 28, 2024
Initial publication	Reference architecture diagram first published.	December 28, 2024
Initial publication	Reference architecture diagram first published.	December 28, 2024
Initial publication	Reference architecture diagram first published.	December 28, 2024

Note

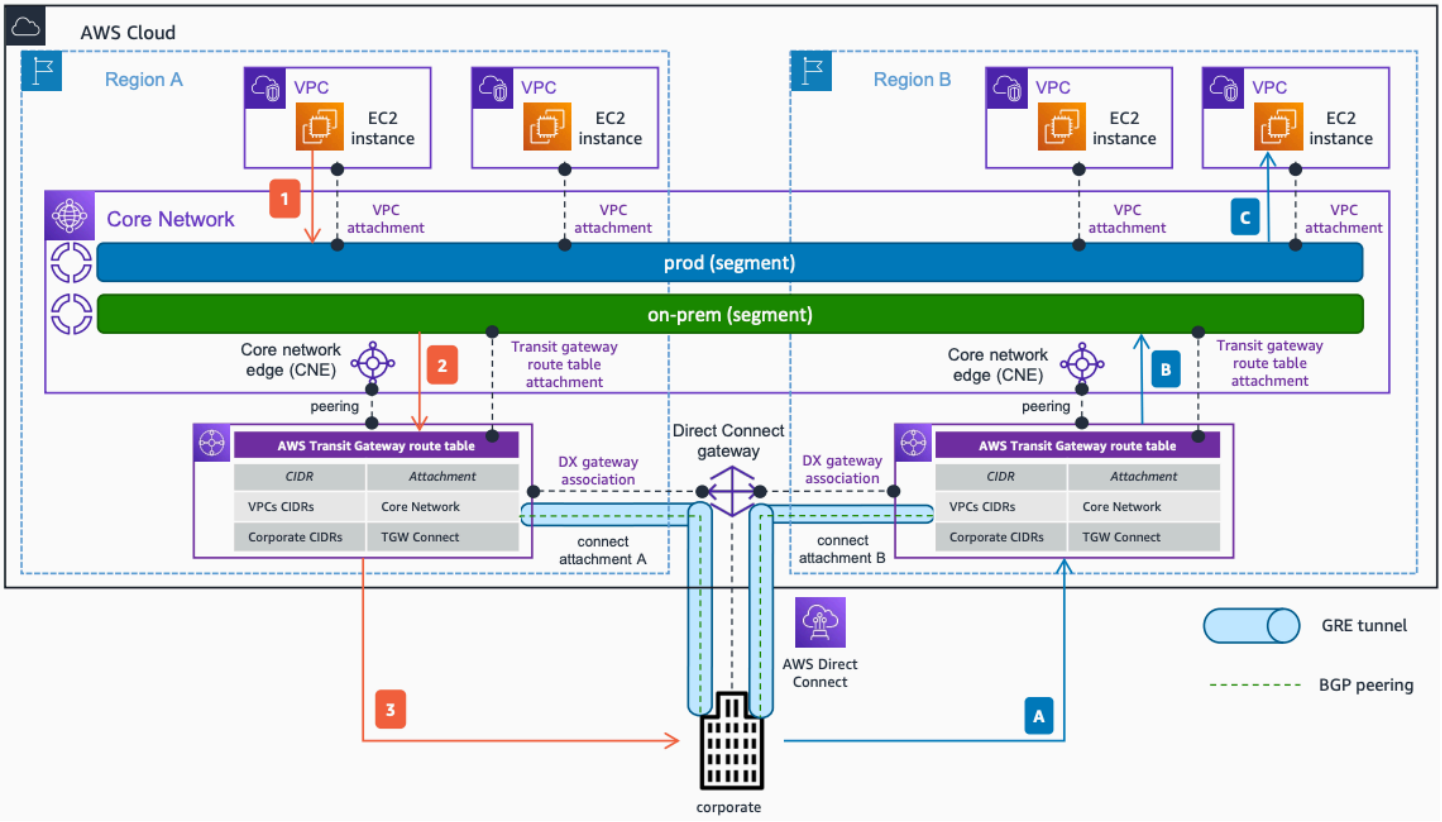
To subscribe to RSS updates, you must have an RSS plugin enabled for the browser you are using.

SD-WAN Devices Integration with AWS Cloud WAN and AWS Direct Connect through AWS Transit Gateway

Publication date: **December 28, 2024 (Diagram history)**

When extending your SD-WAN traffic to AWS through 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.

SD-WAN devices integration with AWS Cloud WAN and AWS Direct Connect architecture



The following steps describe the AWS to on-premises traffic flow:

1. Traffic initiated from an instance in a Amazon VPC in Region A and destined to the corporate data center SD-WAN device is forwarded to the Core Network. The Amazon VPC 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 through 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.

The following steps describe the on-premises to AWS traffic flow:

Na. Traffic from the corporate data center SD-WAN device destined to a Amazon VPC in Region B is forwarded to the Transit Gateway in Region B through the Transit Gateway Connect attachment B, over the Direct Connect link.

Na. 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.

Na. The Core Network forwards the traffic to the corresponding Amazon VPC.

Further reading

For additional information, see the following resources:

- AWS Architecture Icons
- AWS Well-Architected

Diagram history

To be notified about updates to this reference architecture diagram, subscribe to the RSS feed.

Change	Description	Date
Initial publication	Reference architecture diagram first published.	December 28, 2024

Initial publication	Reference architecture diagram first published.	December 28, 2024
Initial publication	Reference architecture diagram first published.	December 28, 2024
Initial publication	Reference architecture diagram first published.	December 28, 2024
Initial publication	Reference architecture diagram first published.	December 28, 2024
Initial publication	Reference architecture diagram first published.	December 28, 2024
Initial publication	Reference architecture diagram first published.	December 28, 2024

Note

To subscribe to RSS updates, you must have an RSS plugin enabled for the browser you are using.