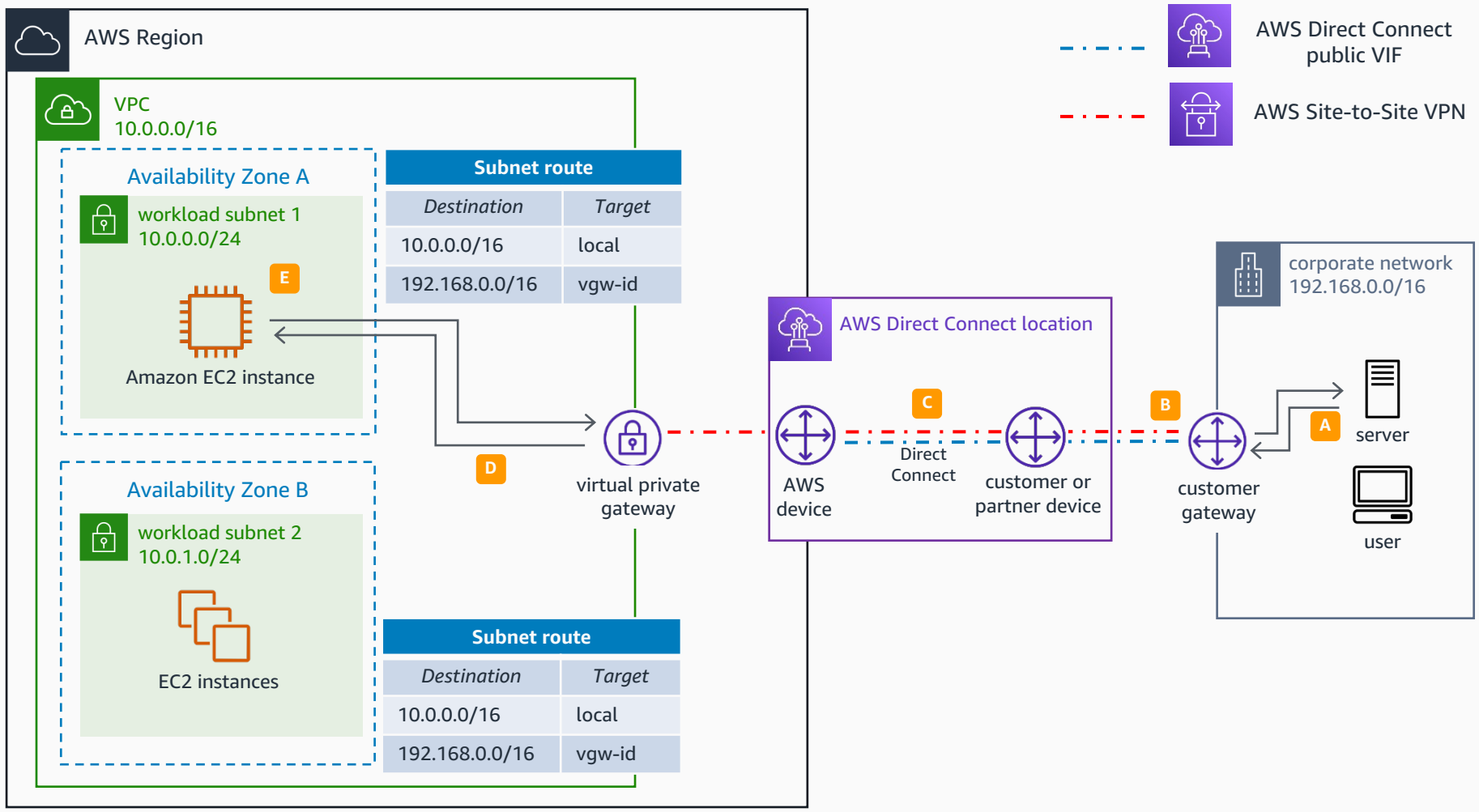
Traffic Encryption Options in AWS Direct Connect

1. *AWS Site-to-Site VPN to an Amazon VPC*
2. *AWS Site-to-Site VPN to a Transit Gateway (Public VIF)*
3. *AWS Site-to-Site VPN Private IP VPN to AWS Transit Gateway*
4. *MACsec Security in AWS Direct Connect*

Reviewed for technical accuracy March 3, 2025
© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Site-to-Site VPN to an Amazon VPC

This method achieves traffic encryption by combining the benefits of the end-to-end secure IPSec connection, with low latency and consistent network experience of AWS Direct Connect when reaching resources in your Amazon VPC.



Configuration steps

1. Create an **AWS Direct Connect** connection. For dedicated connections, set up a cross-connect between the AWS device and your device (or partner device) at the location. For hosted connections, you must accept the hosted connection before you can use it.
2. Once the connection is established, create an **AWS Direct Connect** public virtual interface (VIF) over the existing connection. Configure your customer gateway to bring up the VIF.
3. Once the border gateway protocol (BGP) peer on the VIF is established, AWS advertises its public IP range to the customer gateway device over the public VIF.
4. Create an **AWS Site-to-Site VPN** to the virtual private gateway associated to the virtual private cloud (VPC). AWS provides two **AWS VPN** endpoints attached to the virtual private gateway, which have public IP addresses that are reachable over the public VIF.
5. Configure your customer gateway with the VPN parameters to bring up the **AWS Site-to-Site VPN** connection.

Sample traffic flow

A A client located in the corporate network needs to reach the IP address of an **Amazon EC2** instance in the VPC, so the traffic is routed through the customer gateway (CGW).

B The customer gateway determines that the best route to the VPC is through the **AWS Site-to-Site VPN** tunnel. The traffic is then encrypted based on cryptographic parameters for the IPSec tunnel, with the destination of the encrypted packet being the **Site-to-Site VPN** endpoint public IP address.

C The customer gateway determines that the best route to the **AWS VPN** endpoint public IP address is through the **Direct Connect** public VIF.

D The **AWS VPN** endpoint receives the encrypted IPSec traffic and decrypts it. Because the original IP destination address is the **Amazon EC2** instance in the VPC, the traffic is routed through the VPC fabric to the **EC2** instance.

E Return traffic from the **EC2** instance to the client located in the corporate network follows a reverse but identical path.

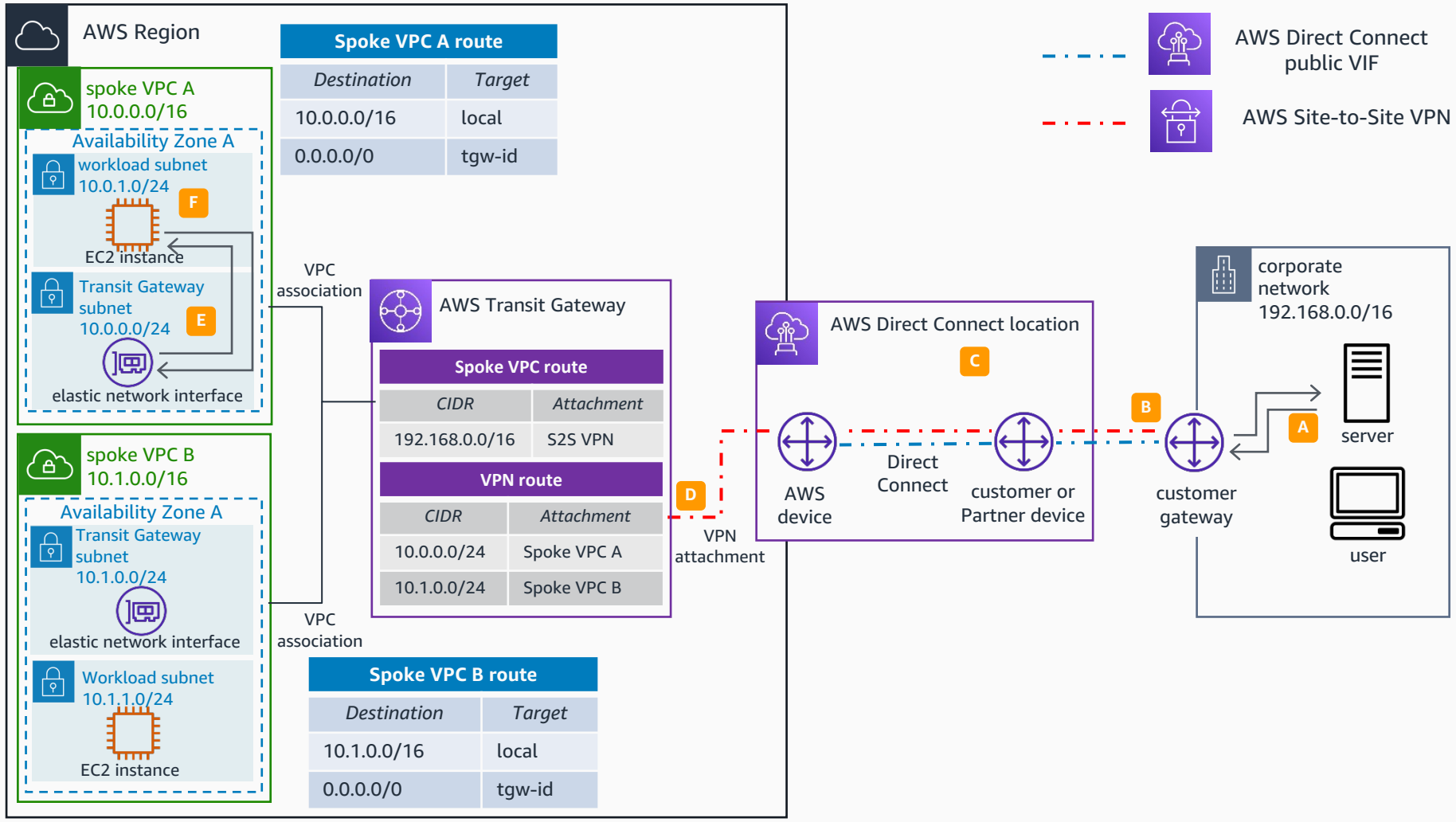
Reviewed for technical accuracy March 3, 2025

© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Reference Architecture

AWS Site-to-Site VPN to AWS Transit Gateway (Public VIF)

This method achieves traffic encryption by combining the benefits of the end-to-end secure IPSec connection, with the low latency and consistent network experience of AWS Direct Connect when reaching resources in your Amazon VPCs through AWS Transit Gateway. This approach is suitable for customers that need to reach multiple VPCs in their AWS environment.



Configuration steps

1. Create an **AWS Direct Connect** connection. For dedicated connections, proceed to set up a cross-connect between the AWS device and your device (or partner device) at the location. For hosted connections, you must accept the connection before you can use it.
2. Once the connection is established, create an **AWS Direct Connect** public virtual interface. Configure your customer gateway to bring up the VIF.
3. Once the BGP peer on the VIF is established, AWS advertises its public IP range to the customer gateway device over the public VIF.
4. Create an **AWS Site-to-Site VPN** and choose your **AWS Transit Gateway** instance as the VPN concentrator for the AWS side.
5. Configure the customer gateway with the VPN parameters to bring up the **AWS VPN** connection and route traffic destined to the **Transit Gateway** through the **AWS VPN** connection.

Sample traffic flow

A A client located in the corporate network needs to route network traffic to the IP address of an **Amazon EC2** instance in the spoke VPC A, and routes the traffic through the customer gateway.

B The customer gateway determines that the best route to the VPC is through the **AWS Site-to-Site VPN** tunnel. The traffic is then encrypted based on cryptographic parameters for the IPSec tunnel, with the destination of the encrypted packet being the **AWS VPN** endpoint public IP address.

C The customer gateway determines that the best route to the **AWS VPN** endpoint public IP address is through the **Direct Connect** public VIF.

D The **AWS VPN** endpoint attached to the **Transit Gateway** receives the encrypted IPSec traffic and forwards it to the **Transit Gateway**.

E The traffic is decrypted, forwarded to the spoke VPC A, and routed to the **Amazon EC2** instance.

F Return traffic from the **EC2** instance to the corporate network follows a reverse but identical path.

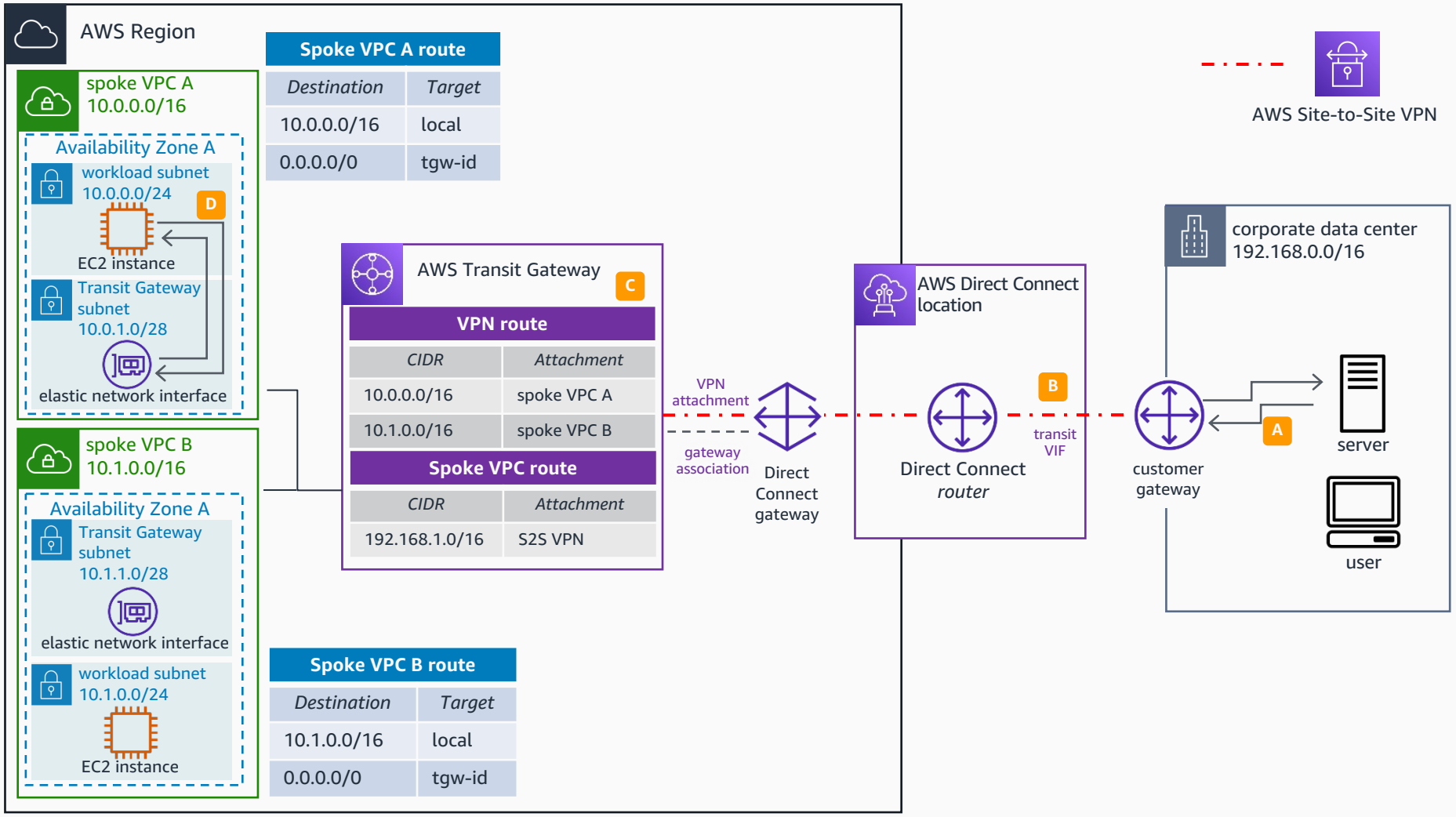
Reviewed for technical accuracy March 3, 2025

© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Reference Architecture

AWS Site-to-Site VPN Private IP VPN to AWS Transit Gateway

AWS Site-to-Site VPN Private IP VPN connections are created over Direct Connect using private IP addresses, enabling enhanced security and network privacy at the same time. Private IP VPNs are deployed on top of Transit VIFs and Direct Connect gateways as underlying transport.



Configuration steps

1. Create an **AWS Direct Connect** connection. For dedicated connections, proceed to set up the cross-connect between the AWS device and your device (or partner device) at the location. For hosted connections, you must accept the hosted connection before you can use it.
2. Once the connection is established, create a **Direct Connect** transit virtual interface (VIF) and **Direct Connect gateway**. Configure your customer gateway to bring up the VIF.
3. Associate your **AWS Transit Gateway** to the Direct Connect gateway, specifying the Transit Gateway CIDR block as the allowed prefix on this attachment - make sure this CIDR block does not overlap with any VPC CIDR block or on-premises CIDR range.
4. Create the **AWS Site-to-Site VPN** using the Direct Connect gateway and Transit VIF as underlying transport.
5. Bring up the **AWS Site-to-Site VPN** tunnels and route traffic destined to the **Transit Gateway** via the **AWS Site-to-Site VPN** connection.

Sample traffic flow

A A client located in the corporate network needs to route network traffic to the IP address of an **Amazon EC2** instance in the spoke VPC A, and routes the traffic through the customer gateway.

B The customer gateway determines that the best route to the VPC is via the **AWS Site-to-Site VPN** connection. The traffic flows through the IPSec tunnels with the selected encryption method, using the Transit VIF and **Direct Connect** gateway as underlying transport network.

C The traffic arrives to the **Transit Gateway**. As per the **Transit Gateway** VPN route table, the traffic is forwarded to the spoke VPC A, and then routed to the **EC2** instance.

D The return traffic from the **EC2** instance to the client located in the corporate network follows a reverse but identical path as described in steps A-C.

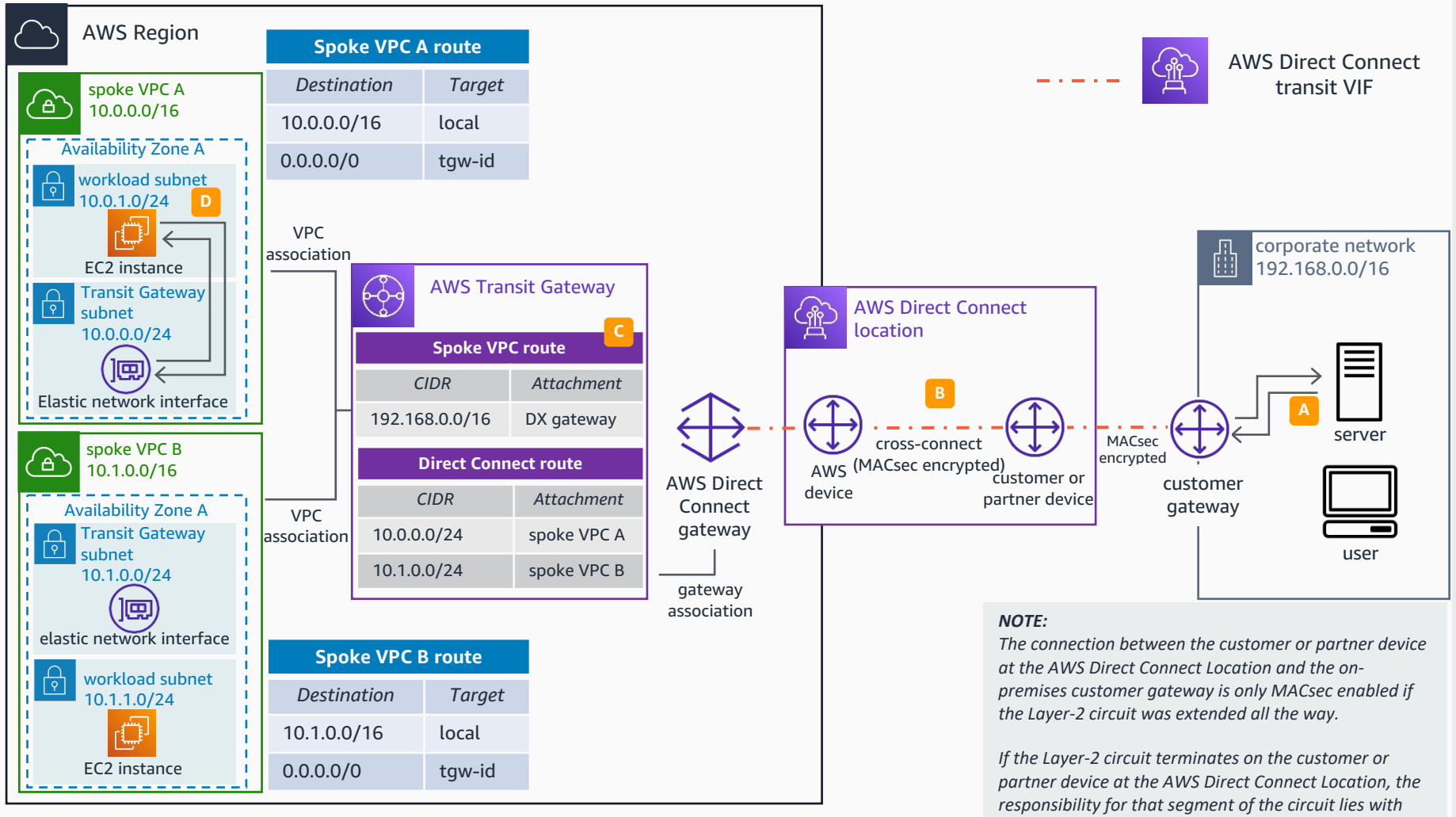
For more information about Private IP VPNs, see Introducing AWS Site-to-Site Private IP VPNs.

Reviewed for technical accuracy March 3, 2025
© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Reference Architecture

MACsec Security in AWS Direct Connect

This method achieves encryption of traffic using MACsec security (IEEE 802.1AE), delivering a native, near line-rate, and point-to-point encryption for 10 Gbps and 100 Gbps links.



NOTE:

The connection between the customer or partner device at the AWS Direct Connect Location and the on-premises customer gateway is only MACsec enabled if the Layer-2 circuit was extended all the way.

If the Layer-2 circuit terminates on the customer or partner device at the AWS Direct Connect Location, the responsibility for that segment of the circuit lies with the customer or partner.

Configuration steps

1. To configure MACsec in an **AWS Direct Connect** dedicated connection, ensure that the device at your end supports MACsec. Additionally, the **Direct Connect** location also must support MACsec.
2. Create a 10G/100G **AWS Direct Connect** dedicated connection, choosing the option for a MACsec enabled port.
3. Create a Connection Key Name (CKN)/ Connectivity Association Key (CAK) pair for the MACsec secret key, making sure that the key-pair is compatible with your device (or Partner device).
4. Associate the CKN/CAK pair with the connection via the **AWS Console**, AWS Command Line Interface (CLI), or API.
5. Set up the cross-connect and complete the physical connection to your device (or Partner device). Update the device at your end with the CKN/CAK pair.
6. Create a transit VIF to a **Direct Connect** gateway on the new MACsec-enabled connection, associated with your **AWS Transit Gateway**.

Sample traffic flow

A A client located in the corporate network needs to route network traffic to the IP address of an **EC2** instance in the spoke VPC A, and routes the traffic to the customer gateway.

B The customer gateway determines that the best route to the VPC is via the transit VIF, indicating the traffic should be sent over the **Direct Connect** connection.

C As per the **Transit Gateway Direct Connect** route table, the traffic is forwarded to the spoke VPC A, and then routed to the **EC2** instance.

D Return traffic from the **EC2** instance to the client located in the corporate network follows a reverse but identical path, as described in steps A-D.

For more information about MACsec in **AWS Direct Connect**, see Adding MACsec security to AWS Direct Connect connections.

Reviewed for technical accuracy March 3, 2025

© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Reference Architecture