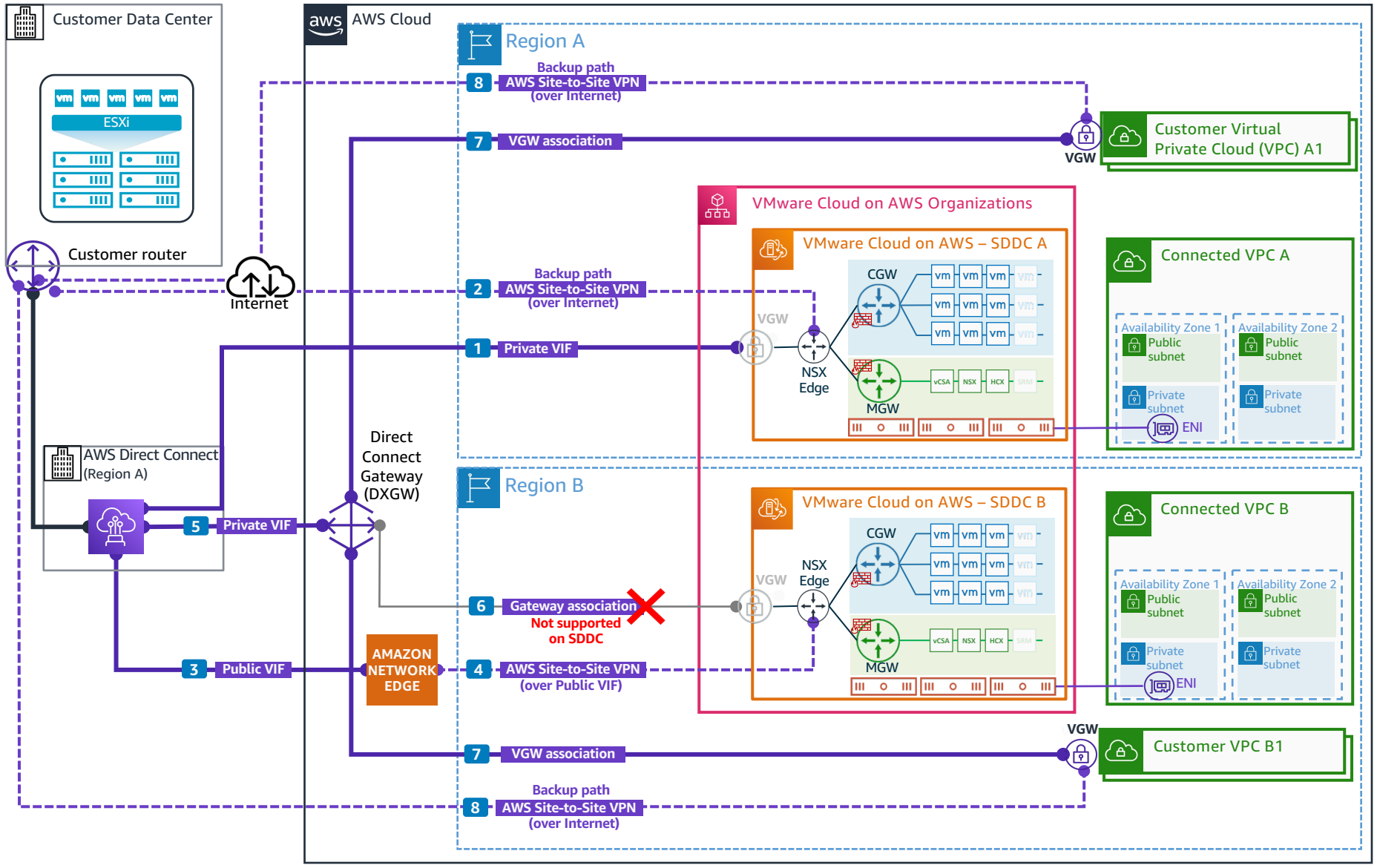
# VMware Cloud on AWS – Networking Reference Architecture – 1

On-premises connectivity using AWS Direct Connect to a virtual private gateway and AWS Site-to-Site Virtual Private Network (VPNs).




1. A private virtual interface (VIF) establishes connectivity to the VMware Software-defined Data Center (SDDC) A in AWS Region A.

2. The **AWS Site-to-Site VPN** (over internet) provides backup connectivity to the private VIF to provide resilient connectivity to the VMware SDDC A.

3. A public VIF enables access to all AWS public services and endpoints using the public IP addresses.

4. The lack of a **Direct Connect** connection in Region B creates a design constraint; therefore, a site-to-site VPN is established to the VMware SDDC B. This VPN leverages the public VIF from the **Direct Connect** connection in Region A. Also, Site-to-Site VPNs over a public VIF can be used to establish a more consistent network experience compared to internet-based VPNs. Alternatively, redundant Site-to-Site VPNs (not shown) can be established for resiliency.

5. A private VIF to the **AWS Direct Connect** gateway (DXGW) enables the DXGW to establish on-premises communication to Amazon VPCs in different Regions by associating the DXGW to the virtual private gateways (VGW).

6. The private VIF to DXGW cannot be used for gateway associations to a VMware SDDC. This feature is not supported on VMware Cloud on AWS.

7. Gateway associations are established between the DXGW and the VGW to enable on-premises communication with Amazon VPCs in multiple Regions.

8. Site-to-Site VPNs are configured as a backup to the DXGW-VGW associations for more resilient connectivity to Amazon VPCs.

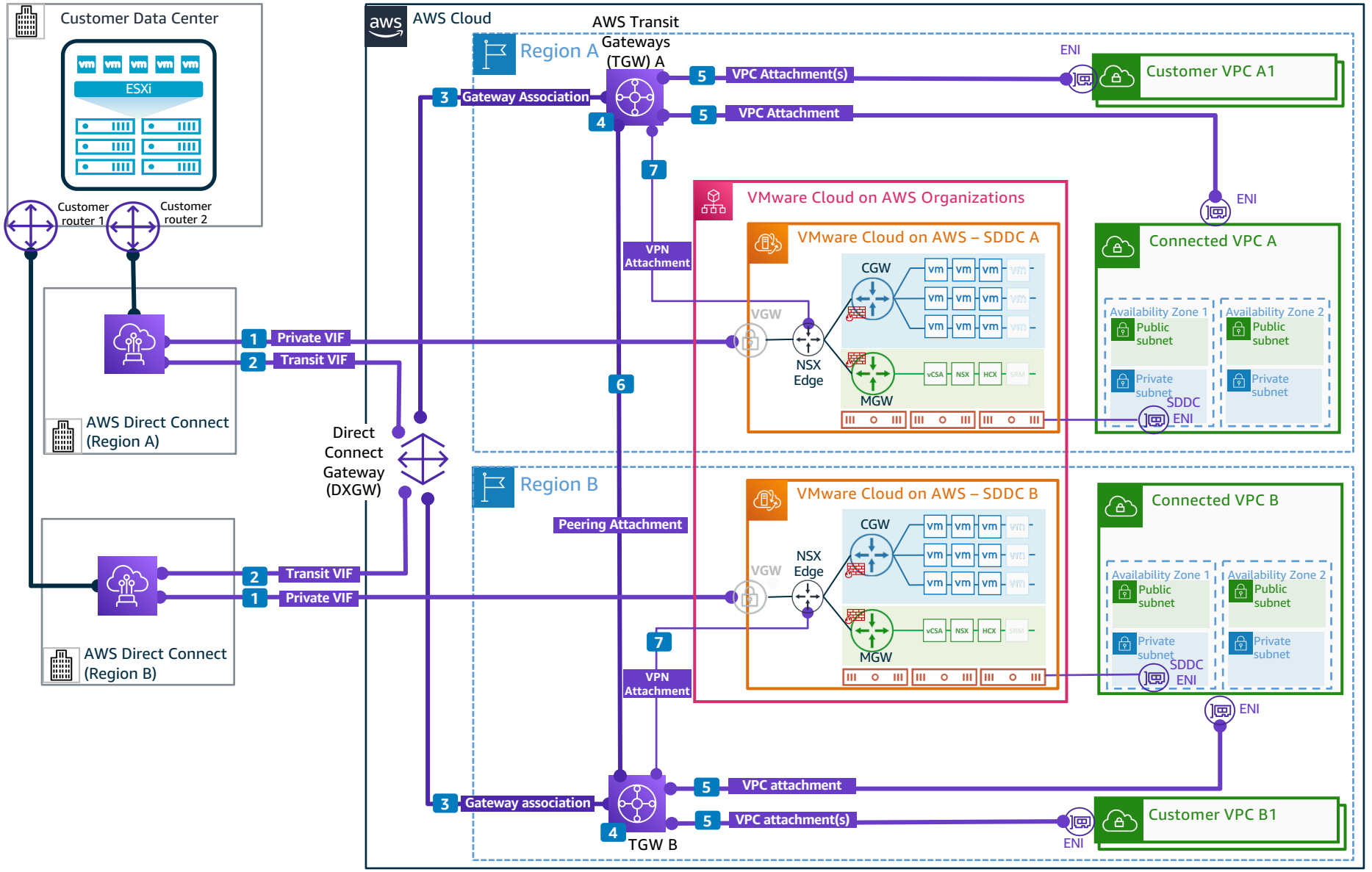
*Reviewed for technical accuracy March 10, 2022*



**AWS Reference Architecture**

# VMware Cloud on AWS – Networking Reference Architecture – 2

On-premises connectivity using AWS Direct Connect with Direct Connect Gateway and AWS Transit Gateway.




1. The **AWS Direct Connect Private VIF in Region A** establishes connectivity from the on-premises network to the SDDC in Region A. Similarly, the **AWS Direct Connect Private VIF from Region B** establishes connectivity from on-premises network to the SDDC in Region B.

2. Dual Transit VIFs establish redundant, resilient connectivity from on-premises to the **Direct Connect** gateway (DXGW).

3. The DXGW is associated with **AWS Transit Gateway** in both Regions to provide on-premises connectivity to Amazon VPCs.

4. The **Transit Gateway** is a regional virtual router that is capable of transitive routing between networks connected to it using the following attachments:
   - VPC attachments
   - VPN attachments
   - DXGW attachments
   - Peering attachments

5. VPC attachments enable VPCs to establish communication with other VPCs and networks connected to the **Transit Gateway**.

6. The **Transit Gateway** peering attachment enables cross-Region communication between networks connected to Transit Gateway A and Transit Gateway B.

7. **Transit Gateway** VPN attachments enable communication between the SDDC and networks connected to the Transit Gateway in the respective Regions. However, the VMkernel traffic (including ESXi Management, vMotion, and vSphere Replication traffic) is prioritized over the Private VIF, making the VPN attachments unusable for this traffic. Ensure the VPN does not learn the on-premises routes which are used along with a Private VIF.

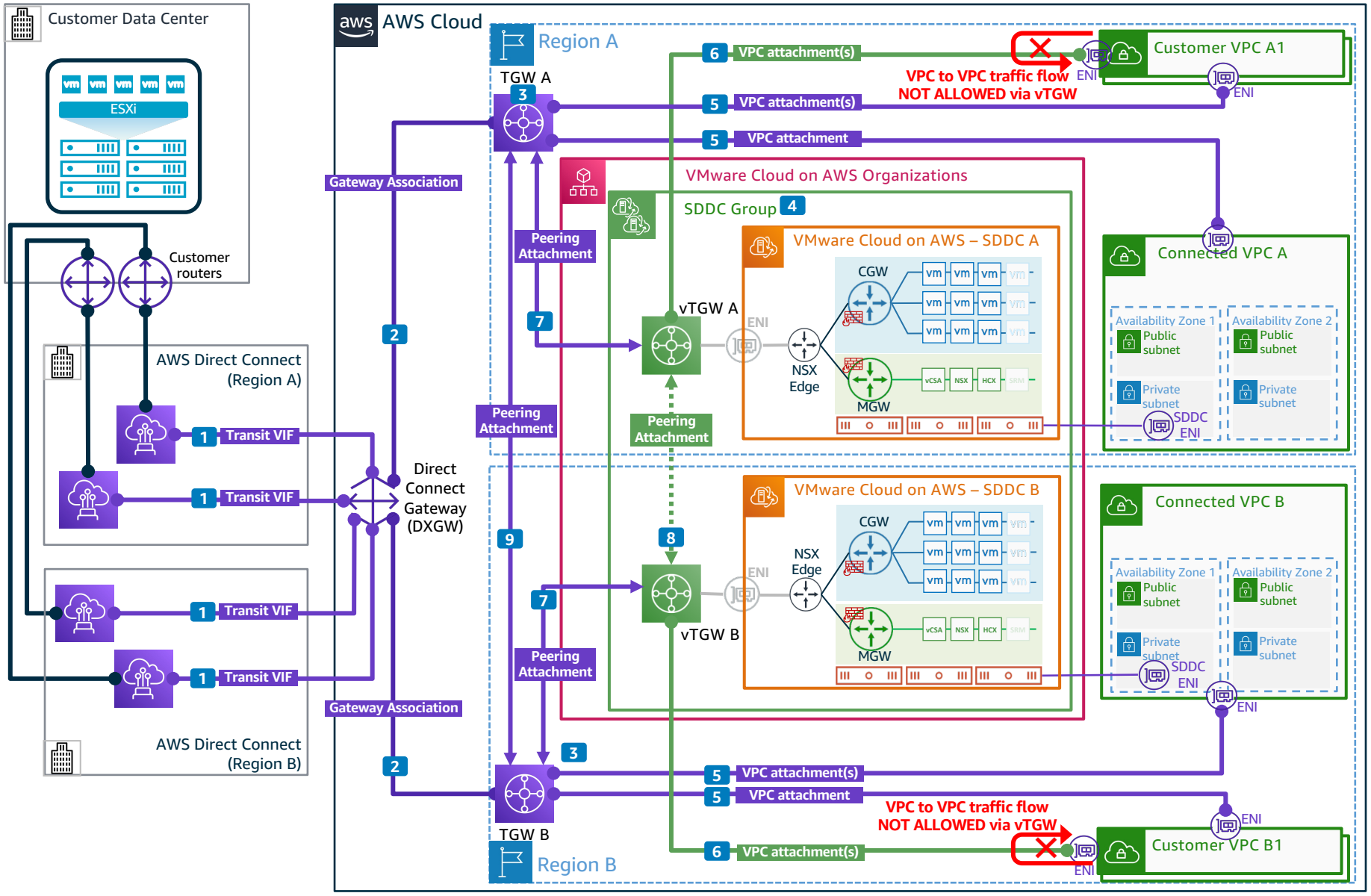
*Reviewed for technical accuracy March 10, 2022*



**AWS Reference Architecture**

# VMware Cloud on AWS – Networking Reference Architecture – 3

Highly resilient on-premises connectivity using AWS Direct Connect, Direct Connect Gateway, AWS Transit Gateway, and VMware Transit Connect.




1. Transit Virtual Interfaces (VIF)s from two separate **AWS Direct Connect** instances in different Regions are used to establish resilient and fault-tolerant connectivity to AWS Regions A and B.
2. The **DXGW** is associated with **AWS Transit Gateway (TGW)** instances in each Region to provide on-premises connectivity.
3. The **AWS Transit Gateway** is a Regional virtual router that is capable of transitive routing between networks connected to VPC, VPN, peering attachments, and **DXGW** associations.
4. The SDDC group uses a VMware Transit Connect (vTGW) to provide high-bandwidth, low-latency connectivity between:
   - SDDCs in an SDDC Group
   - SDDCs and attached VPCs
   - SDDCs and on-premises via DXGW
5. VPC attachments enable VPCs to establish communication with other VPCs and networks connected to the **Transit Gateway**.
6. Alternatively, VPC attachments to **VMware Transit Connect (vTGW)** enable VPCs to establish communication with ONLY SDDC networks connected to the same vTGW.
7. External TGW peering attachments enable communication between the SDDC networks and networks connected to the TGW.
8. The cross-Region **VMware Transit Connect** peering enables communication ONLY between SDDC networks connected to vTGW A and vTGW B.
9. The cross-Region **AWS Transit Gateway** peering attachment enables communication between networks connected to TGW A and TGW B.

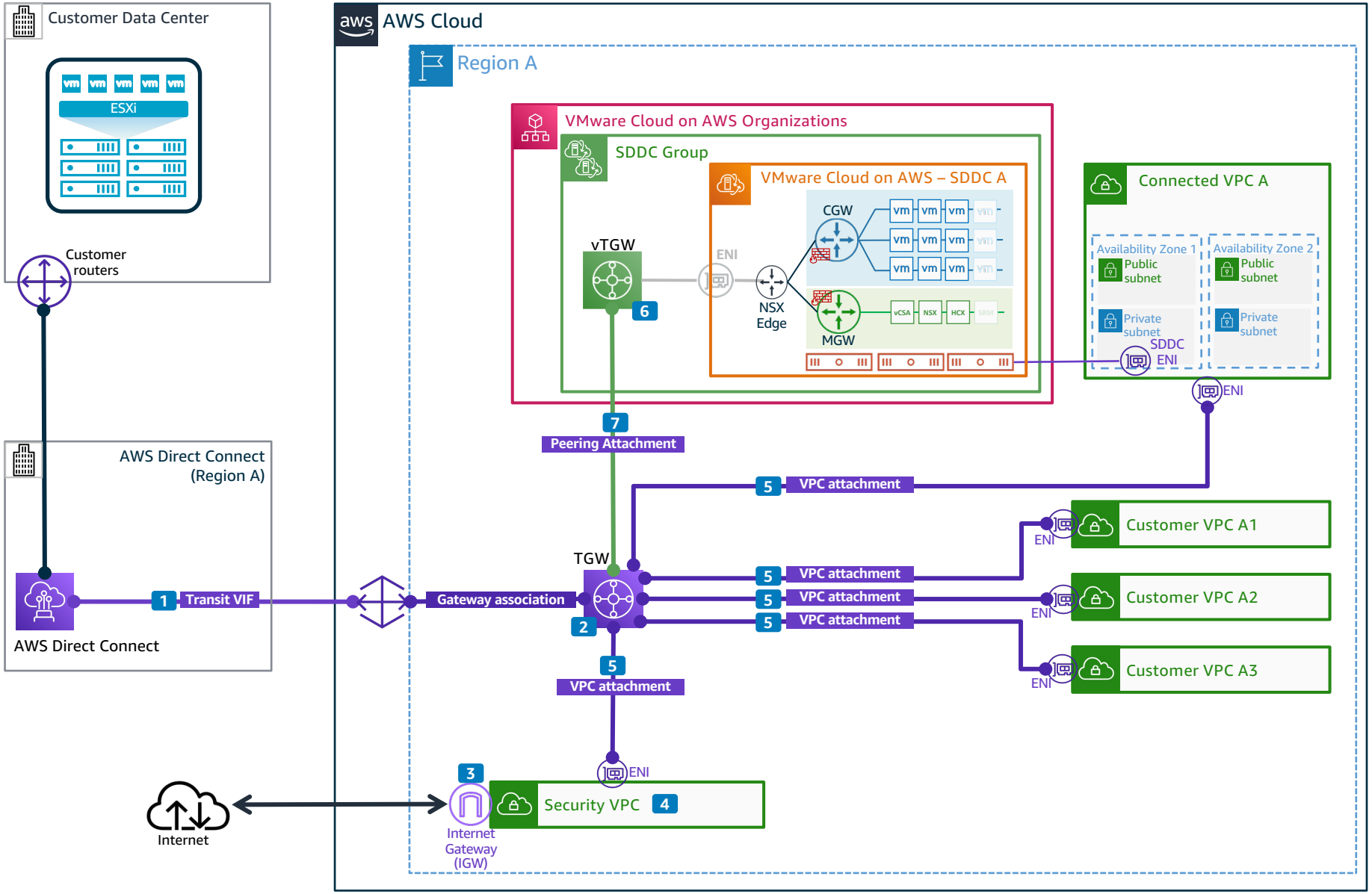
*Reviewed for technical accuracy March 10, 2022*



**AWS Reference Architecture**

# VMware Cloud on AWS – Networking Reference Architecture – 4

Using a security VPC for inspecting north-south Internet-to-SDDC traffic, VPC-to-SDDC traffic, and on-premises-to-SDDC traffic.




1. A Transit VIF over an **AWS Direct Connect** instance is used to connect to an **AWS Direct Connect Gateway** (DXGW) which is associated with **AWS Transit Gateway (TGW)** instances to complete the on-premises connectivity to the AWS Region.

2. The **Transit Gateway (TGW)** is a Regional virtual router that is capable of transitive routing between networks. The TGW is capable of redirecting all the incoming traffic from the on-premises towards the security VPC.

3. The **Internet Gateway (IGW)** is a VPC component that provides centralized internet access for the AWS workloads.

4. The security VPC can be configured with an AWS Network Firewall or third-party firewalls for:
   - SDDC egress/ingress traffic inspection
   - Perimeter security

5. VPC attachments are used to connect to one or more spoke VPCs. Traffic between the spoke VPCs and SDDCs always traverses through the security VPC.

6. The SDDC group uses a VMware Transit Connect (vTGW) to provide high-bandwidth, low-latency connectivity between:
   - SDDCs in an SDDC Group
   - SDDCs and attached VPCs
   - SDDCs and on-premises via DXGW

7. The external TGW peering attachment ensures that all SDDC ingress/egress traffic traverses through the Security VPC. This includes:
   - AWS VPCs traffic
   - On premises traffic
   - Internet traffic

*Reviewed for technical accuracy March 10, 2022*



**AWS Reference Architecture**