Architecture Diagrams

VMware Cloud on AWS Networking Reference Architectures

VMware Cloud on AWS Networking Reference Architectures: Architecture Diagrams

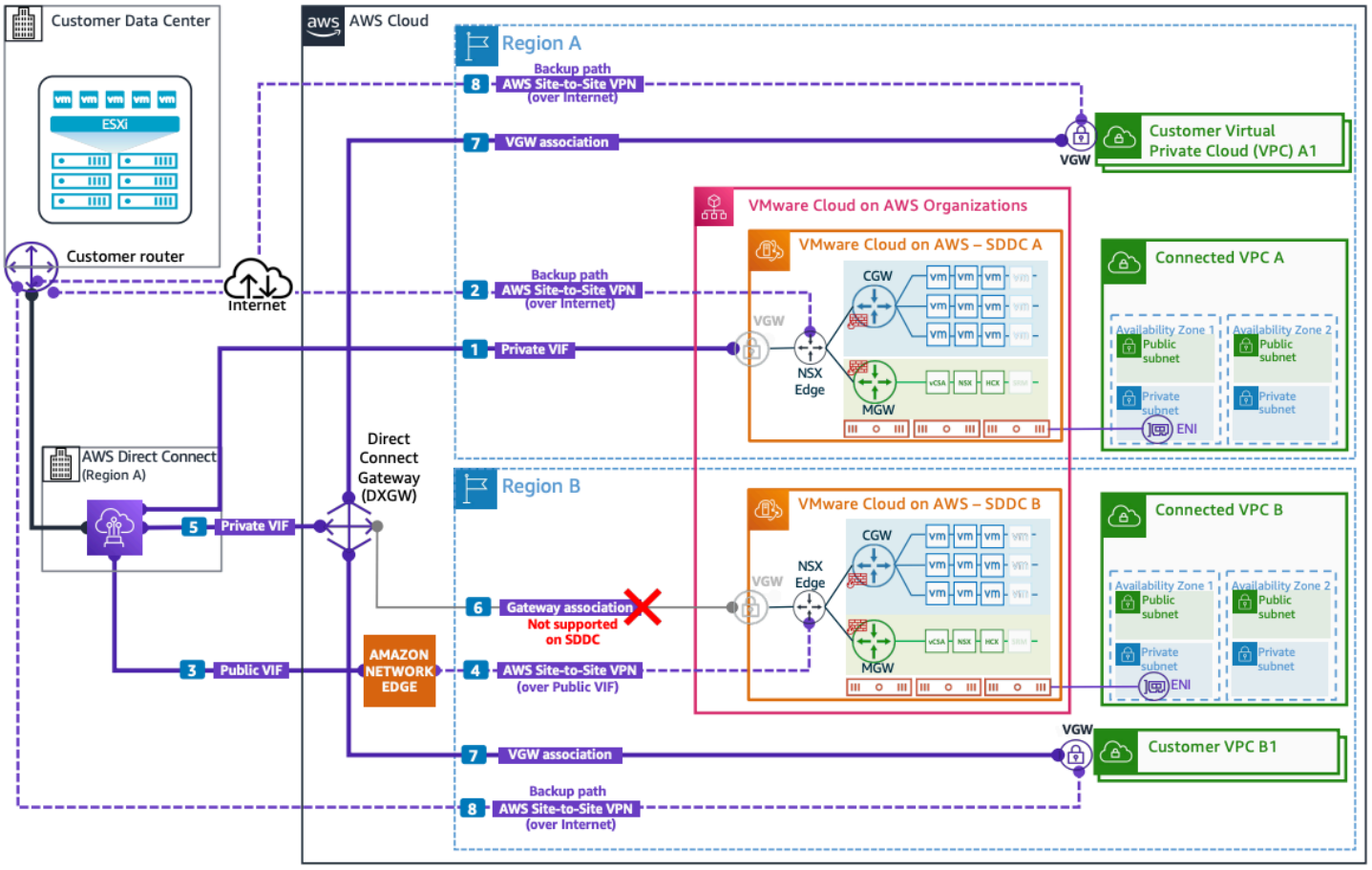
Table of Contents

On-Premises Connectivity Using AWS Direct Connect to a Virtual Private Gateway and VPN

Publication date: **March 10, 2022 (Diagram history)**

This architecture shows on-premises connectivity to VMware Cloud on AWS Software-defined Data Centers (SDDCs) using AWS Direct Connect to a virtual private gateway (VGW) and AWS Site-to-Site VPN for backup connectivity.

VMware Cloud on AWS networking with Direct Connect to VGW architecture



The following numbered items describe the key components in this architecture:

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

2. An 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 public IP addresses.
4. The lack of an AWS 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 uses the public VIF from the Direct Connect connection in Region A. Site-to-Site VPNs over a public VIF can be used to establish a more consistent network experience compared to internet-based VPNs.
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.

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.	March 10, 2022
Initial publication	Reference architecture diagram first published.	March 10, 2022

Initial publication	Reference architecture diagram first published.	March 10, 2022
Initial publication	Reference architecture diagram first published.	March 10, 2022

Note

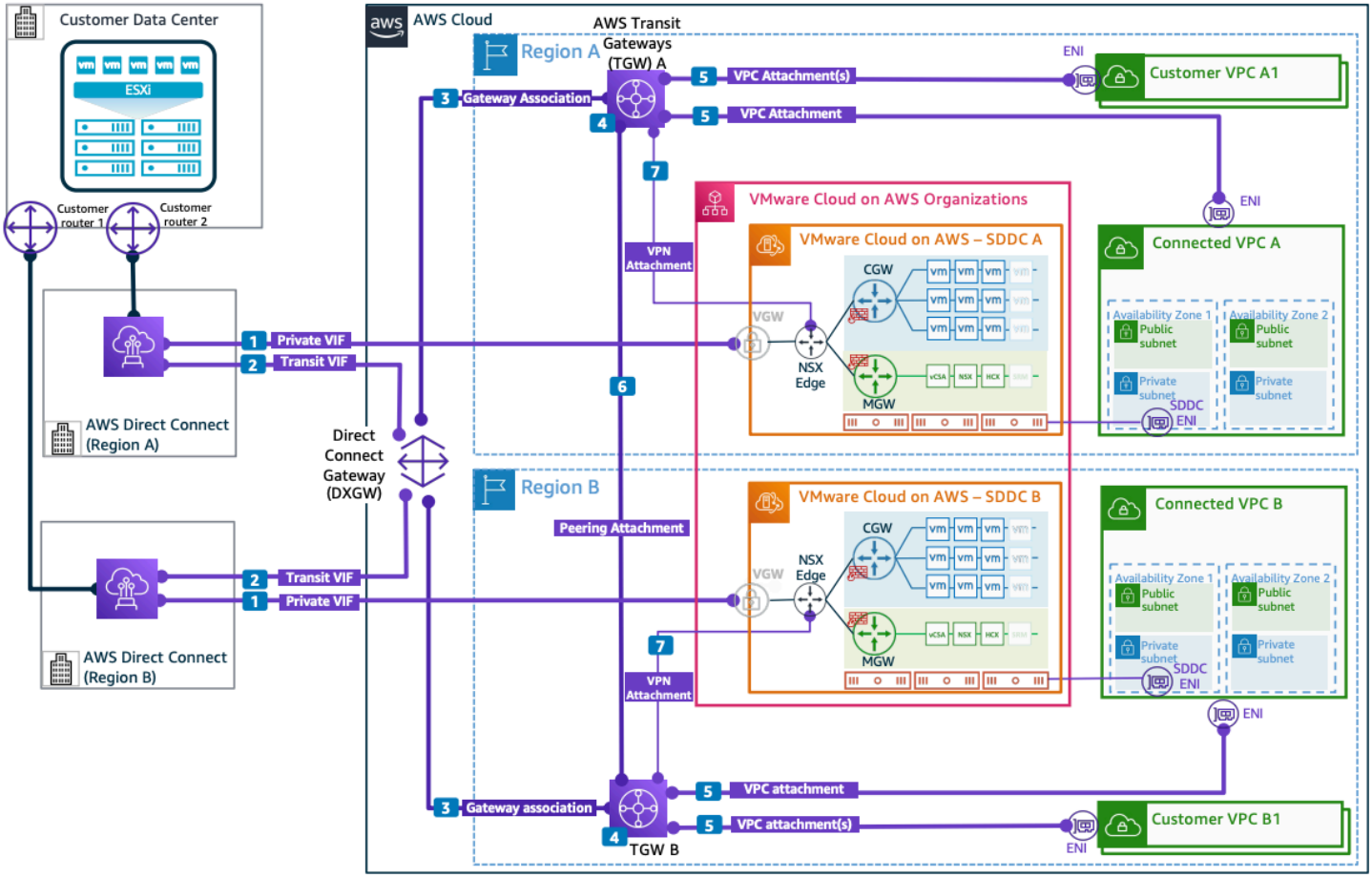
To subscribe to RSS updates, you must have an RSS plugin enabled for the browser you are using.

On-Premises Connectivity Using AWS Direct Connect with Direct Connect Gateway and AWS Transit Gateway

Publication date: **March 10, 2022 (Diagram history)**

This architecture shows on-premises connectivity to VMware Cloud on AWS using AWS Direct Connect with a Direct Connect gateway (DXGW) associated to AWS Transit Gateway instances in multiple Regions for scalable transitive routing.

VMware Cloud on AWS networking with Direct Connect gateway and Transit Gateway architecture



The following numbered items describe the key components in this architecture:

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 the 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 VPC attachments, VPN attachments, DXGW attachments, and 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 VMware 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 that are used with a private VIF.

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.	March 10, 2022

Initial publication	Reference architecture diagram first published.	March 10, 2022
Initial publication	Reference architecture diagram first published.	March 10, 2022
Initial publication	Reference architecture diagram first published.	March 10, 2022

Note

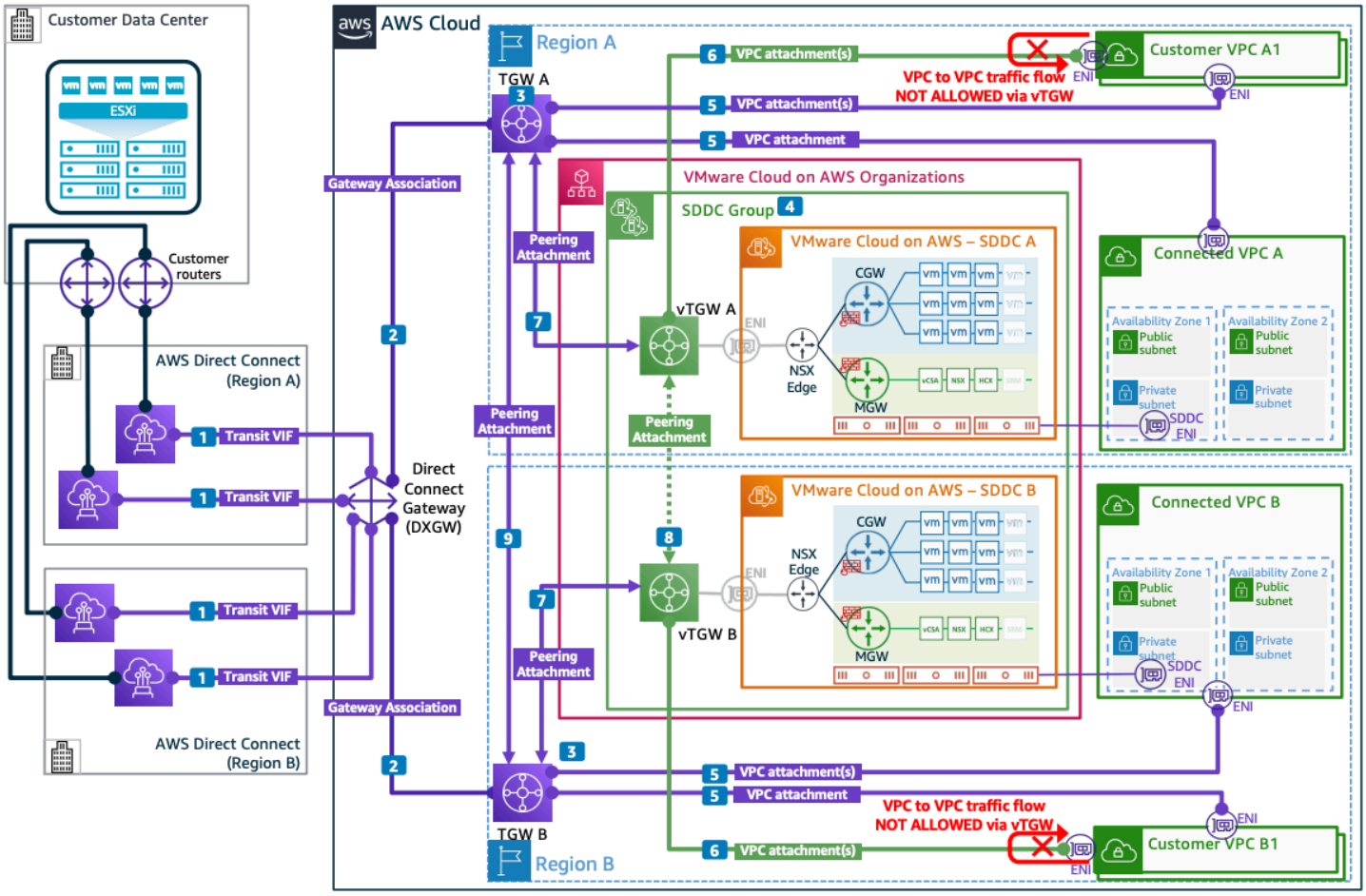
To subscribe to RSS updates, you must have an RSS plugin enabled for the browser you are using.

Highly Resilient On-Premises Connectivity with AWS Transit Gateway and VMware Transit Connect

Publication date: **March 10, 2022 (Diagram history)**

This architecture shows highly resilient on-premises connectivity to VMware Cloud on AWS using AWS Direct Connect, Direct Connect gateway, AWS Transit Gateway, and VMware Transit Connect (vTGW) for high-bandwidth, low-latency connectivity between SDDCs in an SDDC group.

Highly resilient connectivity with VMware Transit Connect architecture



The following numbered items describe the key components in this architecture:

1. Transit virtual interfaces (VIFs) 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, and SDDCs and on-premises through the DXGW.
5. Amazon VPC attachments enable VPCs to establish communication with other VPCs and networks connected to the Transit Gateway. Alternatively, VPC attachments to VMware Transit Connect (vTGW) enable VPCs to establish communication with only SDDC networks connected to the same vTGW.
6. External TGW peering attachments enable communication between the SDDC networks and networks connected to the TGW.
7. The cross-Region VMware Transit Connect peering enables communication only between SDDC networks connected to vTGW A and vTGW B.
8. The cross-Region AWS Transit Gateway peering attachment enables communication between networks connected to TGW A and TGW B.

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.	March 10, 2022
Initial publication	Reference architecture diagram first published.	March 10, 2022
Initial publication	Reference architecture diagram first published.	March 10, 2022
Initial publication	Reference architecture diagram first published.	March 10, 2022

Note

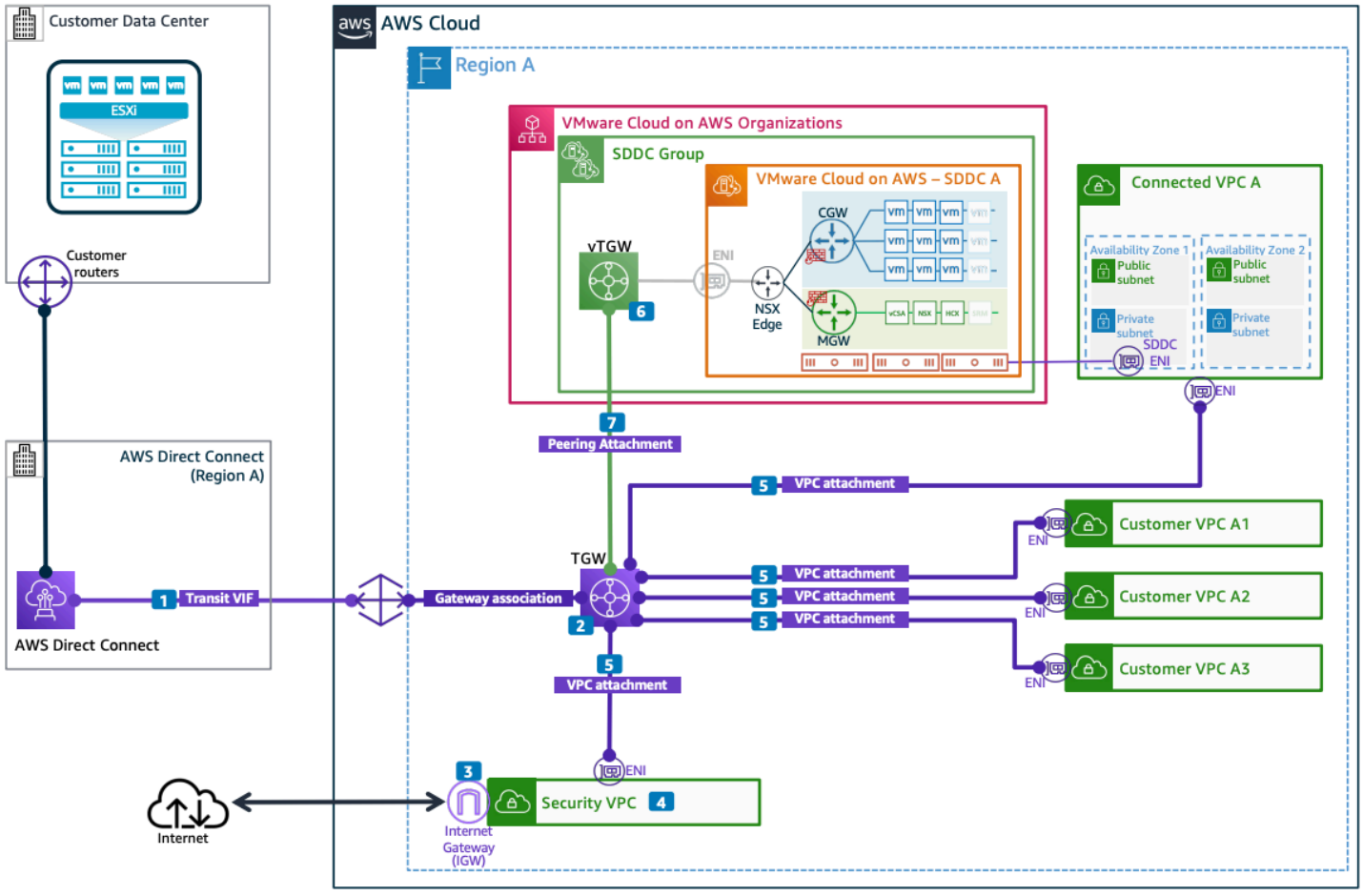
To subscribe to RSS updates, you must have an RSS plugin enabled for the browser you are using.

Using a Security VPC for Inspecting SDDC Traffic

Publication date: **March 10, 2022 (Diagram history)**

This architecture shows how to use a security Amazon VPC for inspecting north-south internet-to-SDDC traffic, VPC-to-SDDC traffic, and on-premises-to-SDDC traffic in VMware Cloud on AWS. The security VPC can be configured with AWS Network Firewall or third-party firewalls for SDDC egress and ingress traffic inspection and perimeter security.

Security VPC inspection for VMware Cloud on AWS traffic architecture



The following numbered items describe the key components in this architecture:

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 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 AWS Network Firewall or third-party firewalls for SDDC egress and ingress traffic inspection and 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, and SDDCs and on-premises through the DXGW.
7. The external TGW peering attachment ensures that all SDDC ingress and egress traffic traverses through the **security VPC**. This includes AWS VPC traffic, on-premises traffic, and internet traffic.

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.	March 10, 2022

Initial publication	Reference architecture diagram first published.	March 10, 2022
Initial publication	Reference architecture diagram first published.	March 10, 2022
Initial publication	Reference architecture diagram first published.	March 10, 2022

Note

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