An Introduction to VMware Transit Gateway for VMware Cloud on AWS

VMware Integrations

Table of contents

An Introduction to VMware Transit Gateway for VMware Cloud on AWS

Introduction

VMware Transit Connect is a VMware managed connectivity solution between the VMware Cloud on AWS SDDCs. Under the hood, VMware Transit Connect uses the AWS Transit Gateway (TGW) construct. It provides high bandwidth and low latency connectivity between SDDCs in SDDC Group within a single AWS Region. It also enables connectivity between SDDC Group and multiple AWS native Virtual Private Clouds (VPCs), as well as customer's on-premises environments connected via an AWS Direct Connect Gateway.

VMware Managed Transit Gateway (vTGW) enables connectivity across environments and adds networks with automatic set up of all the necessary routing policy configuration, transparent to the user. Since it is a VMware offering, it reduces overhead of self-deploying and managing complex configurations to establish a connectivity fabric across VMware Cloud on AWS SDDCs, AWS VPCs and on-premises environments.

Scope of the Document

This document introduces VMware Managed Transit Gateway (vTGW), its architecture, and the supported deployment scenarios as of SDDC Release 1.12. Recent features such as transit Virtual Private Cloud (VPCs) and inter-region vTGW are out of scope and will be covered in separate documents.

Connectivity Across Domains

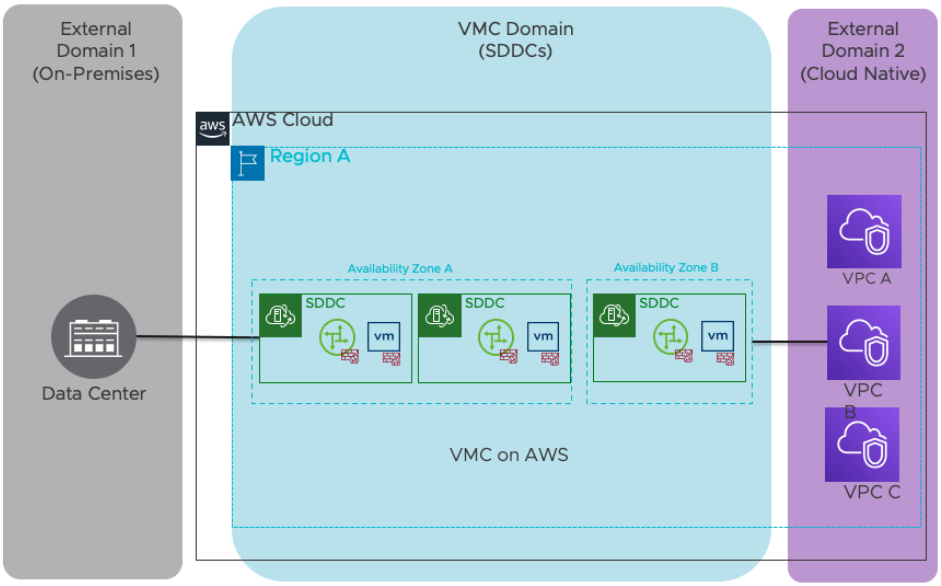

Figure 1 - Cross-domain Connectivity

As shown in Fig. 1 above, the key challenge is to provide connectivity across all the three domains and support future connections as well. vTGW is a perfect solution which groups SDDC in VMware Cloud on AWS enabling Inter-SDDC connectivity along with on-premises and AWS services.

Design Considerations and Caveats for vTGW

Keep the following considerations and caveats in mind before vTGW deployment:

- Hybrid Linked Mode over a VPN connection is incompatible with SDDC Groups. If you add an SDDC that you have configured to use Hybrid Linked Mode over a VPN connection, the connection will fail, and you won't be able to use Hybrid Linked Mode with that SDDC. Hybrid Linked Mode over a Direct Connect is unaffected when an SDDC is added to a group.
- For on-premises to VMware Cloud on AWS SDDC traffic path, routes advertised over a route-based VPN are preferred over routes advertised by vTGW or Direct Connect Gateway.
- Using a route-based VPN as backup for Direct Connect is unsupported when using vTGW and must be disabled.
- MTU is capped to 8500 bytes for vTGW.
  Note: vTGW does not support Path MTU Discovery
- vSphere replication traffic is supported through vTGW (communication between ESXi hosts of different SDDCs of a SDDC Group can happen over vTGW e.g., vSphere Replication traffic).
- For any modification of prefix-list configuration under Direct Connect Gateway, AWS console must be used for this purpose and not VMware Cloud Service Platform (CSP).
- When a connected VPC is added as a transit gateway attachment to the vTGW, and if this connected VPC has secondary CIDR specified, it may result in asymmetric routing for traffic between VMs on SDDC and EC2 instances on AWS

Architecture

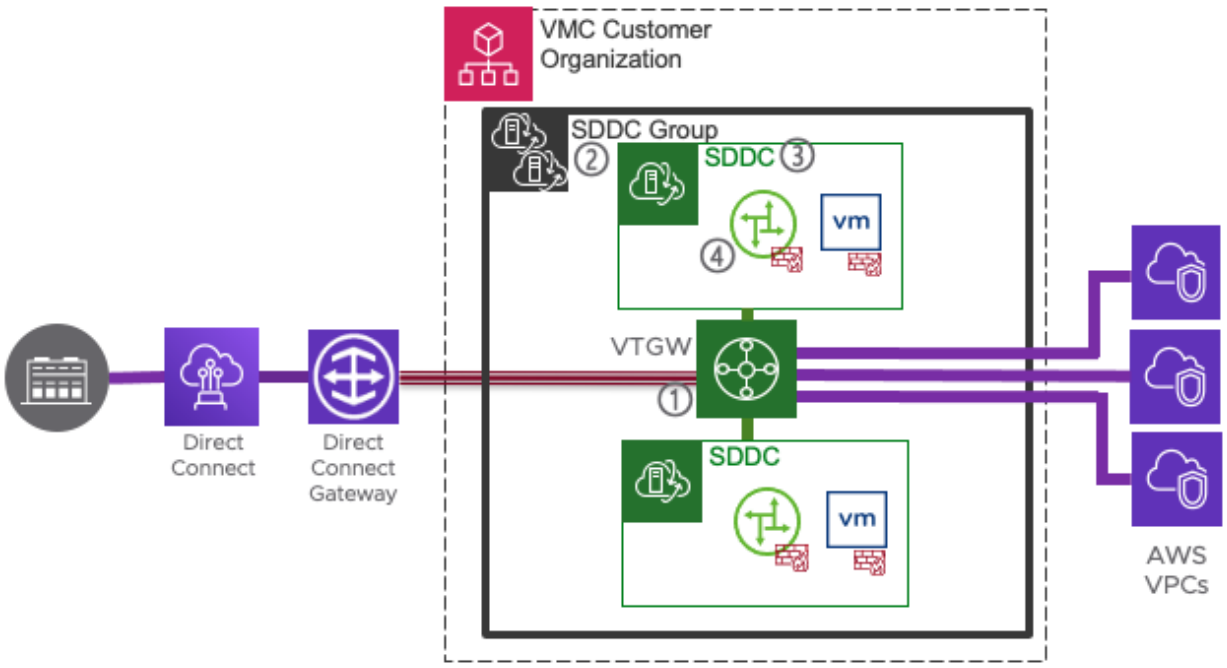

Figure 2 - vTGW Architecture

As shown in Fig 2, VMware Managed Transit Gateway (vTGW) acts like a hub that has ability to connect to multiple endpoints such as Direct Connect gateway and multiple VPC attachments from both native AWS VPCs and Connected VPCs from a VMware Cloud on AWS SDDC. Fig 2 also shows the high-level architecture of vTGW connecting two SDDCs.

The major components of a vTGW (highlighted in the figure 2) are listed below:

1. vTGW : VMware Managed Transit Gateway which is an AWS construct but owned and managed by VMware that can connect more than one VMware Cloud on AWS SDDCs within a region.
2. SDDC Group: SDDC Group logically organizes a set of SDDCs to simplify management at scale. It also lays the foundational infrastructure capability such as vCenter linking. It provides interconnectivity between the SDDCs within the group. When a SDDC Group is created that prompts the user to select the VMC on AWS SDDCs, the VMware CSP deploys vTGW that learns routes within the SDDCs and advertises the network of customer VPCs (native AWS VPCs).
3. SDDC: These are owned and managed by VMware and are referred to as VMC on AWS SDDC. Each of the SDDCs have their Connected VPCs which are different than customer VPCs (native AWS VPCs).
4. SDDC Edge: The SDDC edge is a Tier0 router provided by NSX-T within the VMC on AWS SDDC that provides East-West connectivity (within the SDDC) and North-South (outside the SDDC).

Prerequisites and Best Practices

Note the following requirements to set up vTGW:

- SDDCs must be at v1.11 or higher to connect to a vTGW.
- SDDCs and VPCs connected to the same vTGW must be in the same region.
- Management CIDRs must be non-overlapping.
- Workload CIDRs should not overlap;if they do, remote overlapping networks are rejected.
- An SDDC must be owned by the organization that owns the group.
- An SDDC cannot be a member of another SDDC Group.
- vTGW is a cost per usage feature:
    - Cost per attachment per hour.
    - Cost per GB of traffic as documented by AWS.
- vTGW will be shared under Resource Access Manager in AWS console.
    - You should accept the shared resource.
    - When the VPC(s) attachments are created on the AWS console, they need acceptance on VMC CSP.
- One end of every flow must be a SDDC.
- Any other combinations of flows are not supported, for instance:
    - VPC to on-premises via vTGW.
    - VPC to VPC via vTGW.

Networking

Route table for vTGW	vTGW implements two route tables:
Firewall Rules	
Scale	Configuration maximums are available on this page.

Supported Designs

There are three supported designs with vTGW– SDDC to SDDC, SDDC to VPC, and SDDC to on-prem.

SDDC to SDDC

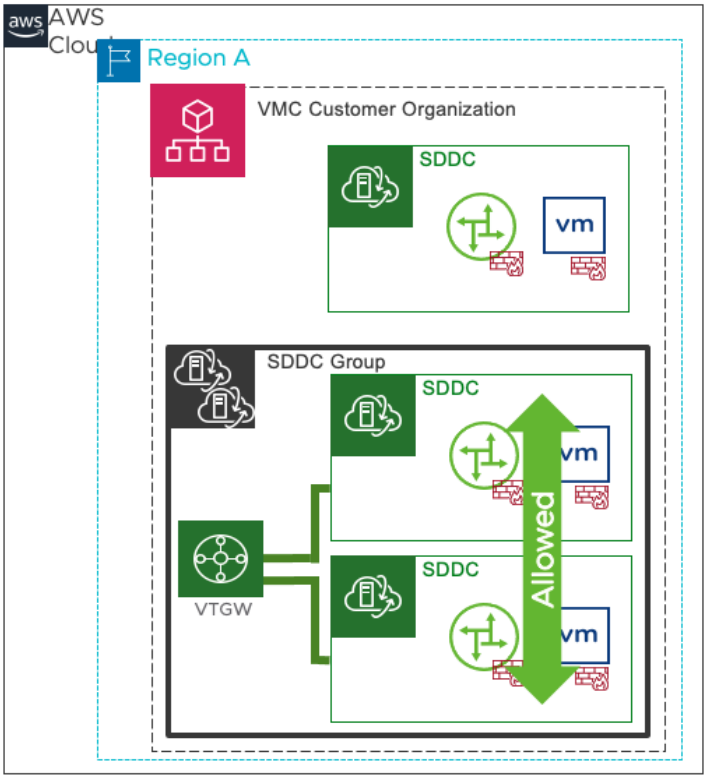

Figure 3 - SDDC to SDDC connectivity

As shown in figure 3, the SDDC-to-SDDC design will have an ability to provide connectivity across all SDDCs within the organization. As a first step, you choose which SDDCs within the org will have vTGW based connectivity.

After the SDDCs are connected to the SDDC Group, depending on the firewall rules set on the MGW and CGW:

- All logical networks across all SDDCs should have connectivity.
- All management appliances in one SDDC should have connectivity to management appliances in other SDDCs.
- Warn about the overlapping IPs across connected SDDCs.

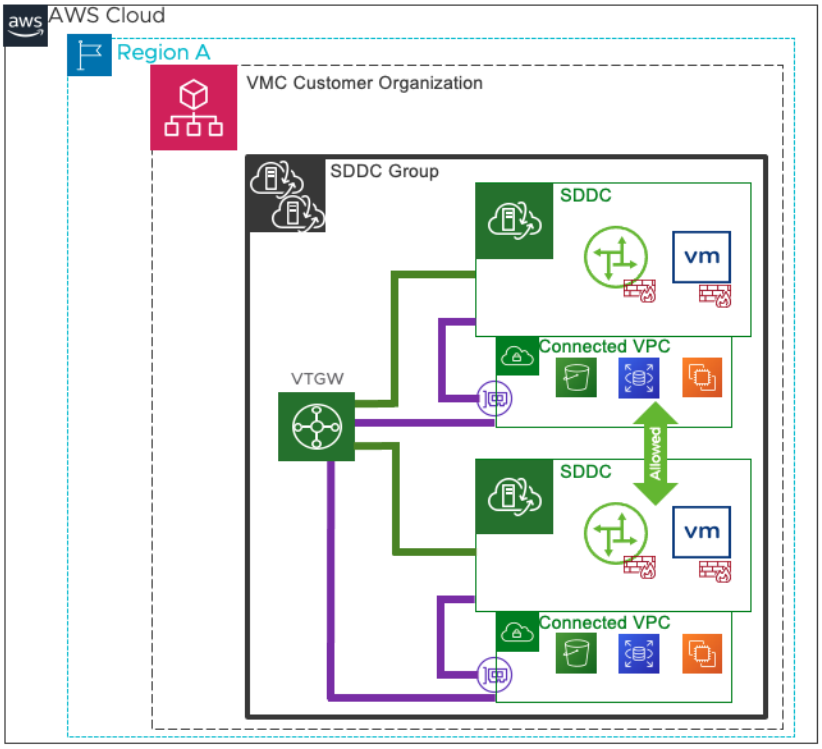

Figure 4 - SDDC to SDDC connectivity with Connected VPCs

The following rules apply to Connected VPC at their respective SDDCs:

- The Connected VPC already will have an ENI attachment to the SDDC it is assigned to.
- You may attach Connected VPC to the vTGW.
- Enables SDDC Group members access to endpoints in Connected VPCs.
- vTGW traffic rules apply; traffic between SDDCs and Connected VPC to SDDC is allowed.
- Traffic between the Connected VPCs is not permitted.

SDDC to VPC

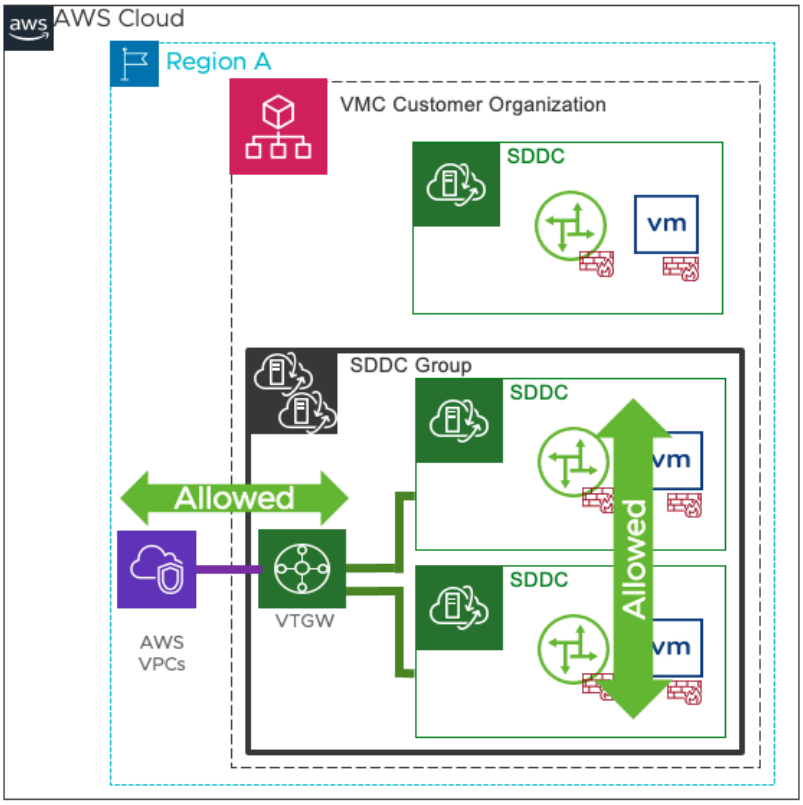

Figure 5 - SDDC to VPC connectivity

Figure 5 shows the SDDC Group that consists of VMware Cloud on AWS SDDC. Native AWS VPCs have attachment with vTGW as well. The vTGW facilitates connectivity between native AWS VPCs and VMware Cloud on AWS SDDCs.

Following are some of the characteristics for SDDC to VPC Connectivity:

- Native AWS VPC must be in the same region as that of SDDC.
- It may be in different Availability Zone.
- VPC belongs to Customer AWS account.
- Traffic from native AWS VPC to any SDDC is allowed. The earlier restriction for traffic between Connected VPCs still applies.

SDDC to On-Premises

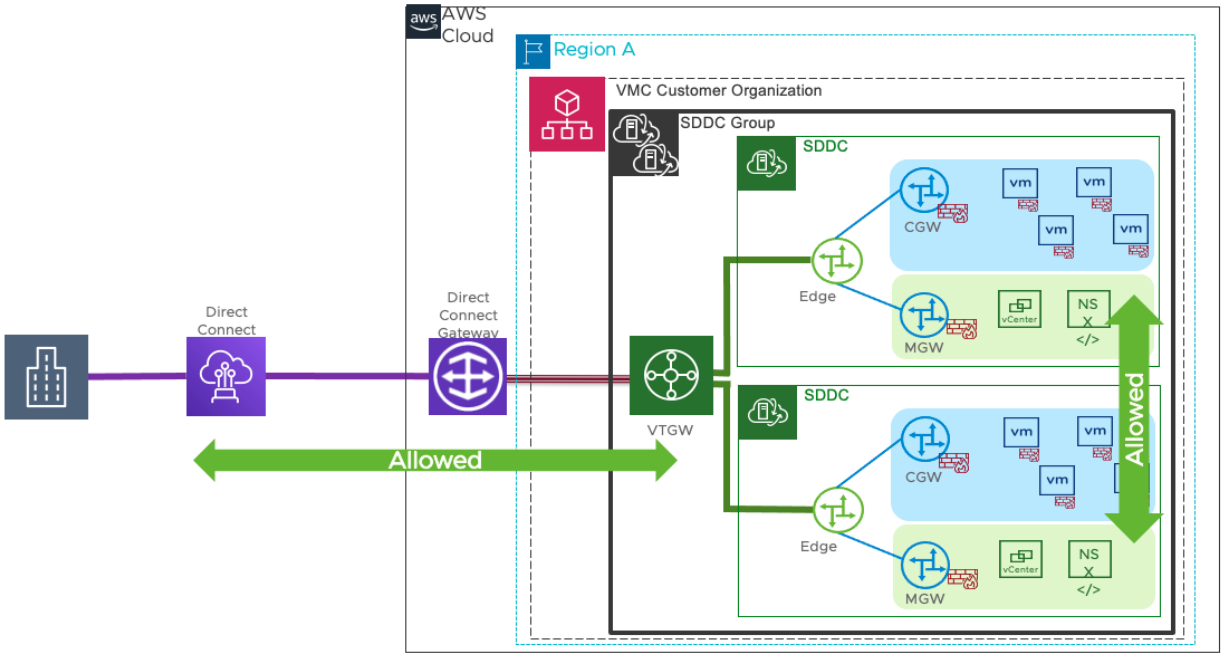

Figure 6- SDDC to On-Premises connectivity with vTGW

As shown in Figure 6, here the vTGW facilitates the connection between VMware Cloud on AWS SDDCs and on-premises with Direct Connect (private VIFs). Additionally, the vTGW may also have a native AWS VPC connection that was shown earlier in Figure 5. Following are allowed traffic flows from on-premises to VMC on AWS SDDC:

- Traffic between SDDCs is allowed as in earlier scenarios (between Connected VPC and SDDC).
- Traffic between on-premises to SDDCs within the SDDC Group is allowed.

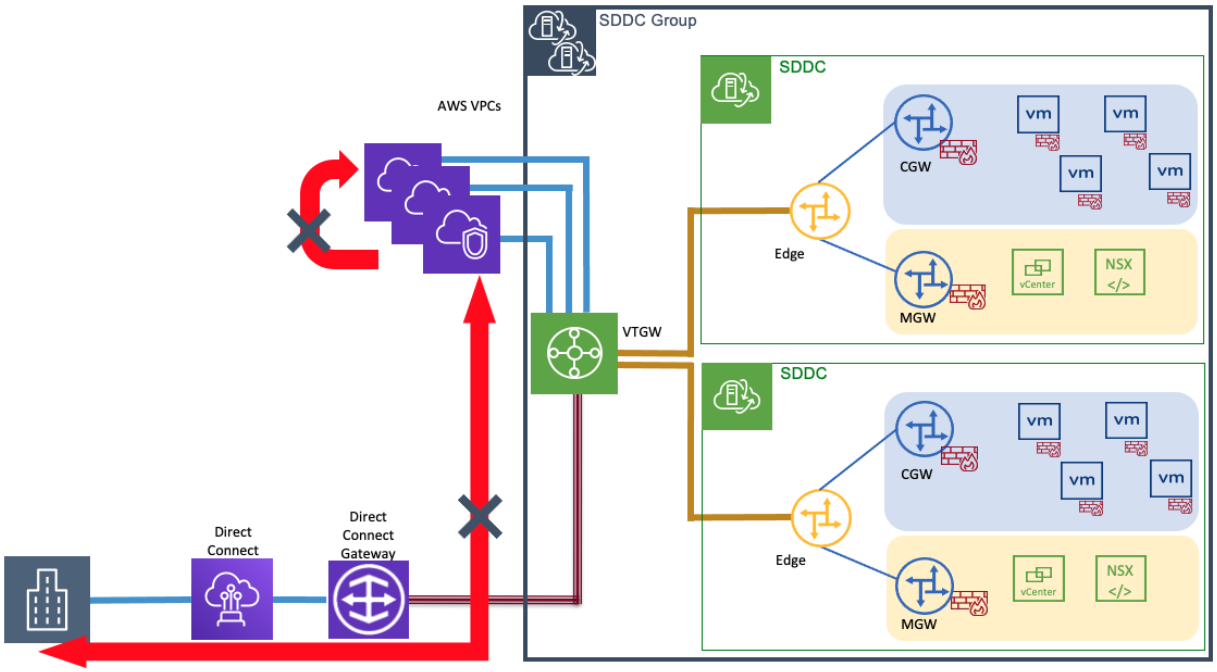

Figure 7 - On-premises to SDDC denied Traffic Flows with vTGW

Following are the denied traffic flows as indicated in Figure 7:

- Native AWS VPC to VPC via vTGW
- On-premises datacenter to Native AWS VPCs via vTGW

SDDC to On-Premises Alternate Design

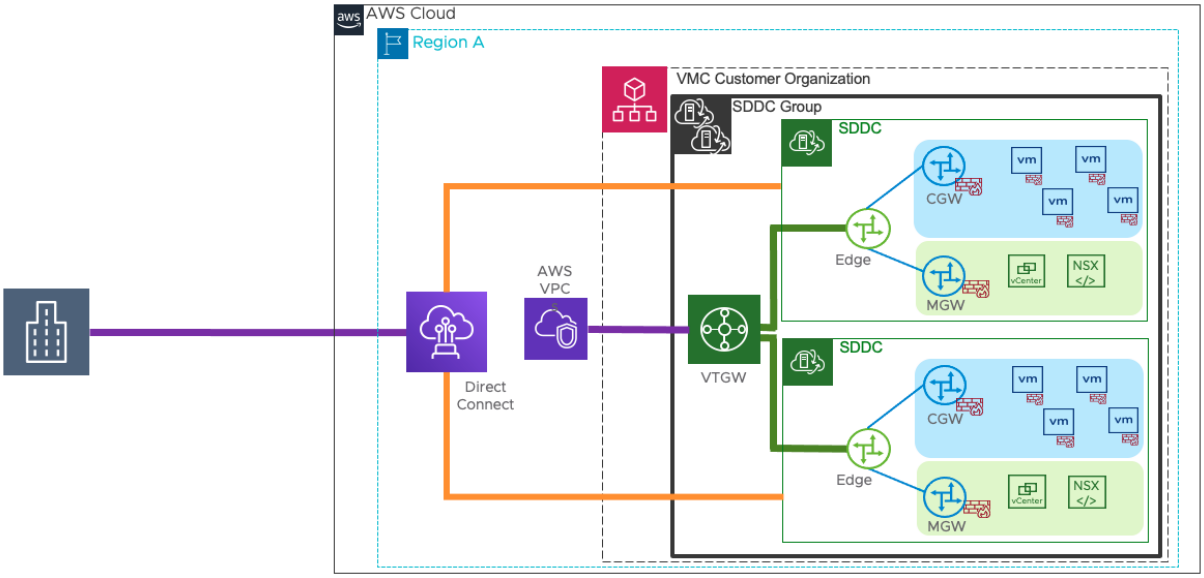

Figure 8 – Alternate design for SDDC to on-premises connectivity

Note the following highlights of this alternate design as shown in Fig 8 above:

- Direct Connect VIFs are connected to specific SDDCs.
- vTGW is used for SDDC to SDDC and SDDC to native AWS VPC communication.
- This design may be desirable when Direct Connect Gateway route table limitations are a challenge.

Author and Contributors

The following authors have contributed to this article.

Mithil Rangdale

Ron Fuller