A Brief Primer on VMware Transit Gateway Deployments

Table of contents

A Brief Primer on VMware Transit Gateway Deployments 3
Introduction 3
Summary and Considerations 4
Planning and Implementation 5
SDDC → SDDC Connectivity 5
Configuration 5
Verification 5
Detailed Steps 5
SDDC → VPC Connectivity 10
Configuration 11
Verification 11
Detailed Steps 11
SDDC → On-premises Connectivity 15
Configuration 16
Verification 16
Detailed Steps 17
Author and Contributors 20

A Brief Primer on VMware Transit Gateway Deployments

Introduction

As discussed in the introduction article about VMware Managed Transit Gateway (vTGW), there are three possible deployment scenarios:

- SDDC → SDDC Connectivity
- SDDC → VPC Connectivity
- SDDC → On-premises connectivity

This document provides information about these three types of deployments for vTGW. There are two possible options for each deployment.

1**. You can create a new SDDC group with member SDDCs** - vTGW will provide connectivity across these SDDCs, advertise and learn the routes for the SDDCs and connected VPCs.

2. **You can add a member SDDC to an existing SDDC group** - This will make use of already existing vTGW that will learn the routes of newly added SDDC and advertise the routes to this SDDC.

Summary and Considerations

Use Cases	VMware HCX
Pre-requisites	
General Considerations/Recommendations	
Cost Implications	here
Performance Considerations	On-premises to VMC on AWS SDDC connectivity for a SDDC group over Direct Connect will have better performance as compared to Internet connectivity (due to latency).
Documentation reference	VMware Transit Connect
Last Updated	July 2021

Planning and Implementation

Read the pre-requisites section in the Summary and Considerations table and ensure that all the pre-requisites are met before you begin implementation of the deployment use cases.

Following are the implementation steps for the three deployment patterns for VMware Transit Connect.

SDDC → SDDC Connectivity

Following are the high-level steps to establish SDDC→ SDDC Connectivity. Please note that the SDDC grouping is common for all the three deployment scenarios.

Configuration

1. Create a SDDC group with at least two member SDDCs.
2. Deploy the VM in each SDDC with its compute network backing.
3. Enable Compute Gateway Firewall rules to allow traffic between the VMs in each SDDC.

Verification

1. Created SDDC groups should show status as connected.
2. Connected VPCs and compute networks should be advertised for both the SDDCs.
3. Traffic should be allowed between the VMs of both the SDDCs.

Detailed Steps

Create a SDDC group consisting of two SDDCs as shown below in figure 1, 2 and 3

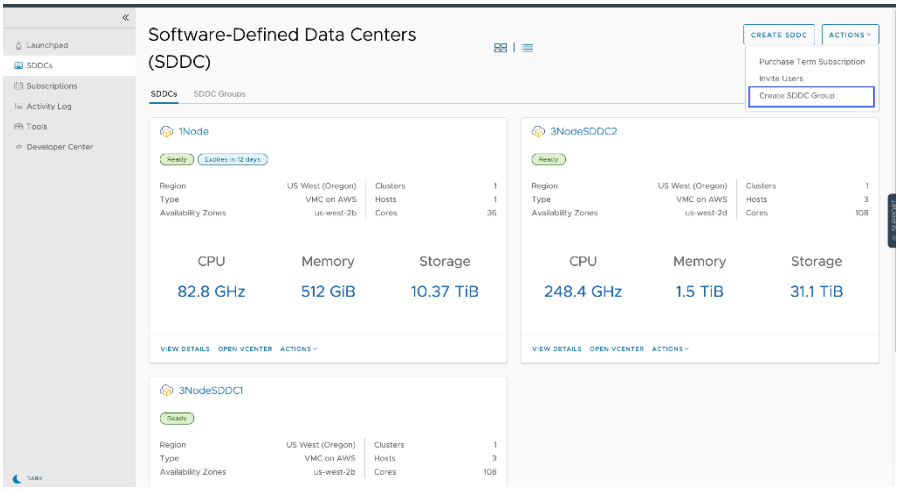


Figure 1 - Create SDDC Group

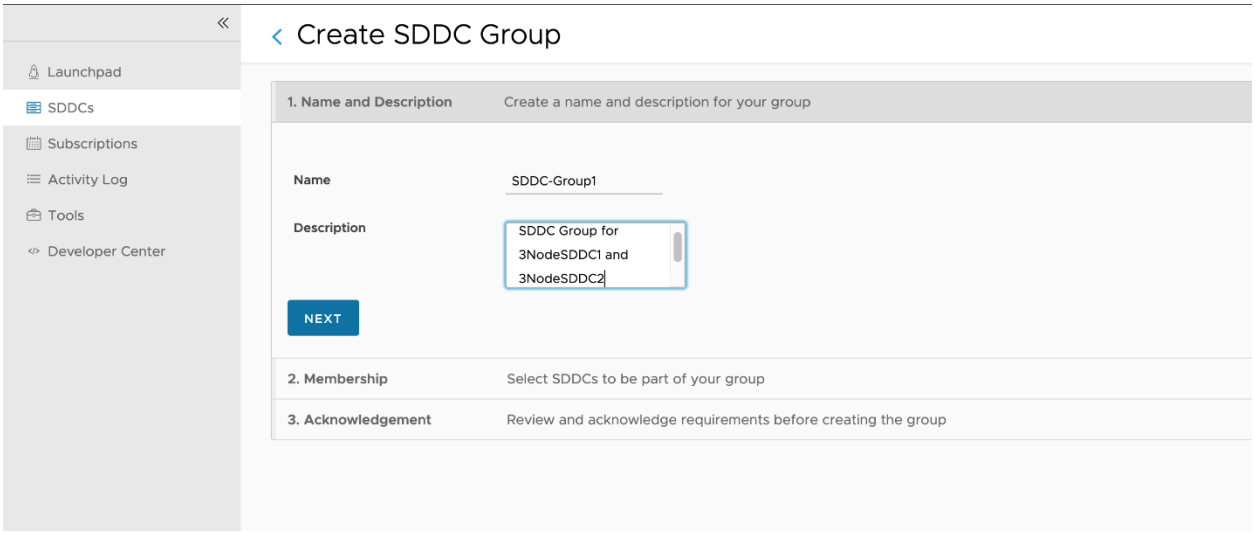


Figure 2 - Add SDDC

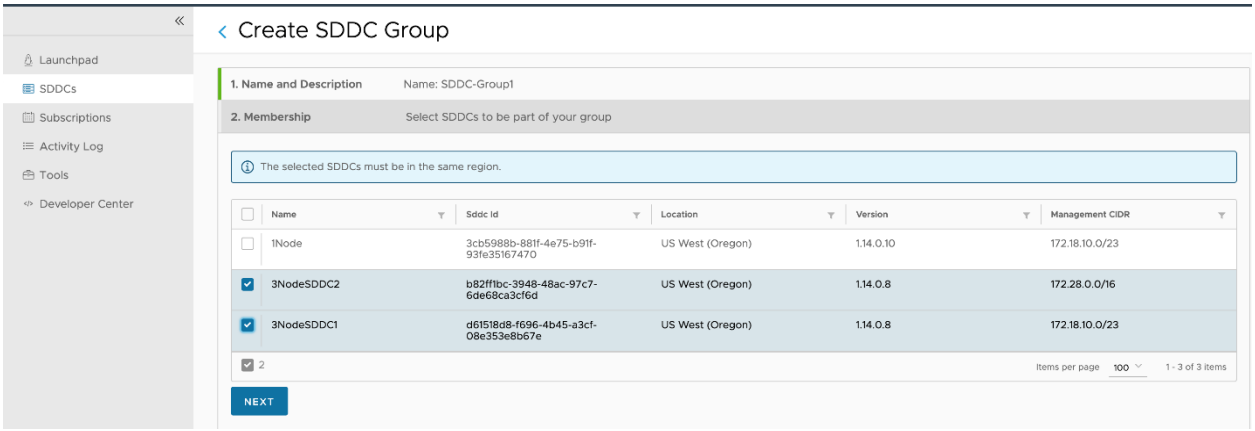


Figure 3 - Name the SDDC Group

Verify the status of SDDC Group to be in connected state as shown in Figures 4 and 5.

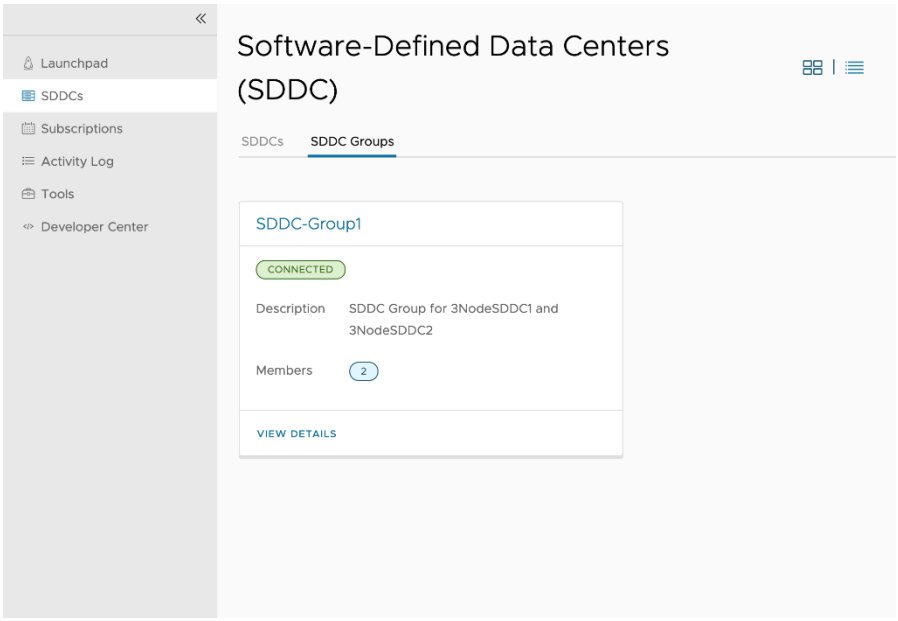


Figure 4 - SDDC Group Status

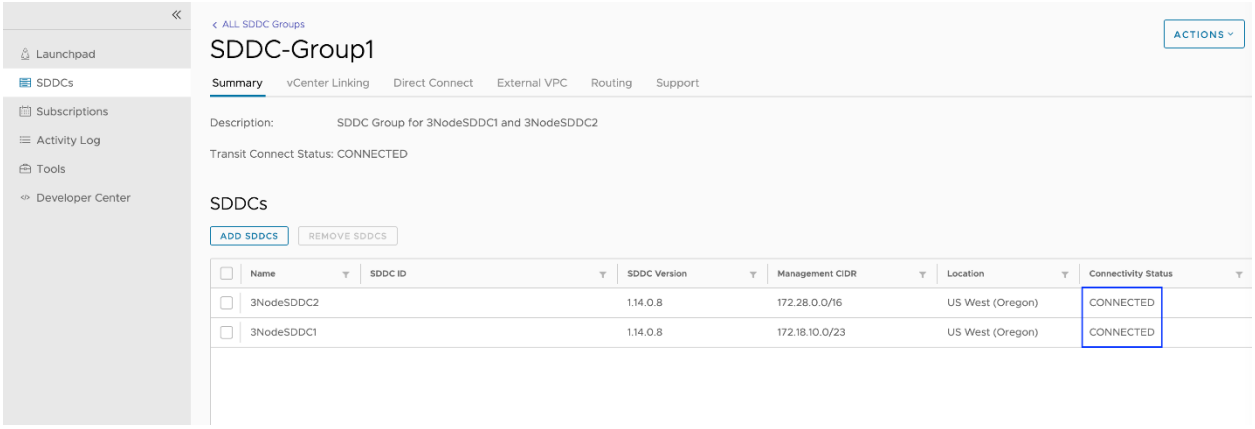


Figure 5 - SDDC Group Status Connected

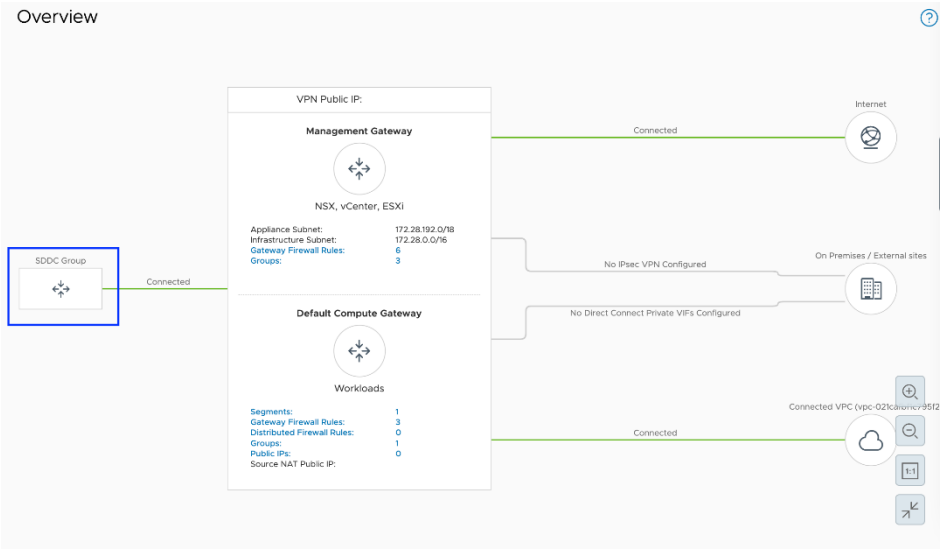


Figure 6 - SDDC Group in the overview page

Verify the route status on both the SDDCs advertising it is connected compute and management segments as shown in Figure 7.

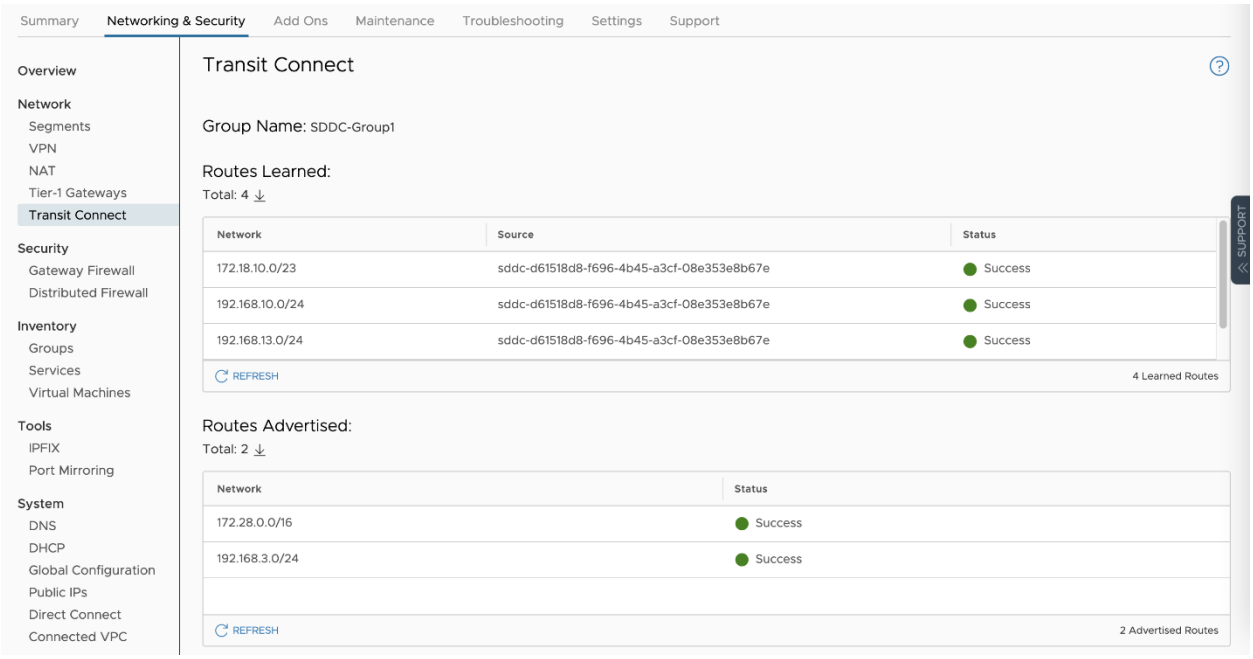


Fig 7 Route advertisement on one of the SDDCs

Note that the overlapping compute segments would not be advertised and are excluded from the vTGW route table as shown in Figure 8.

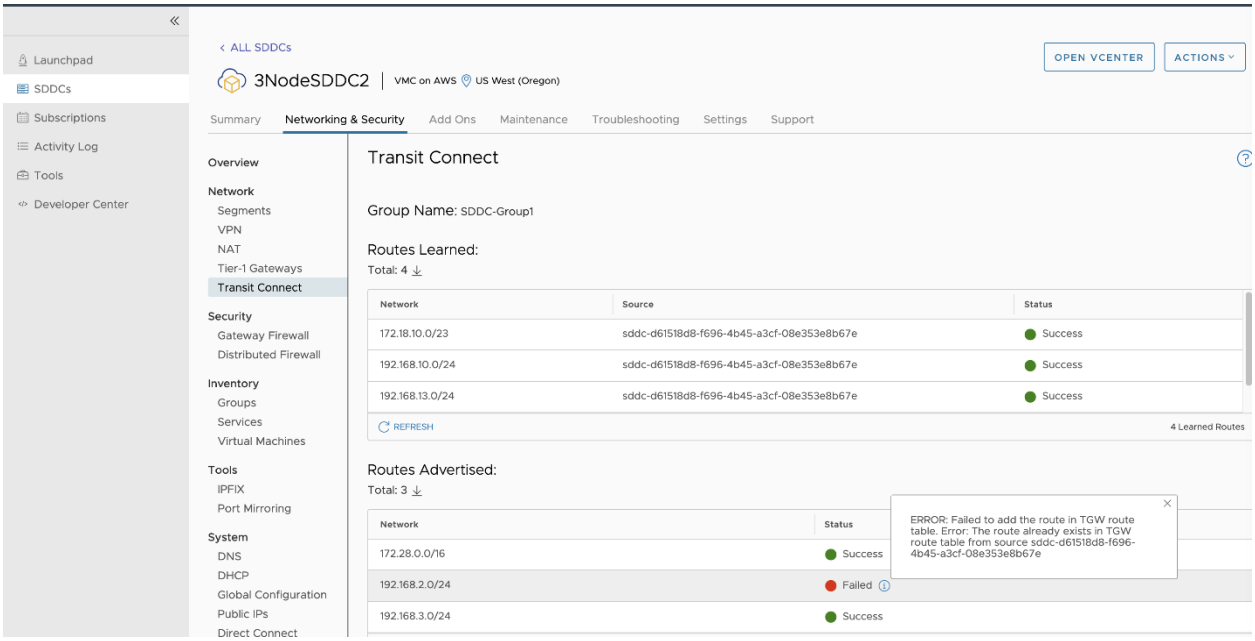
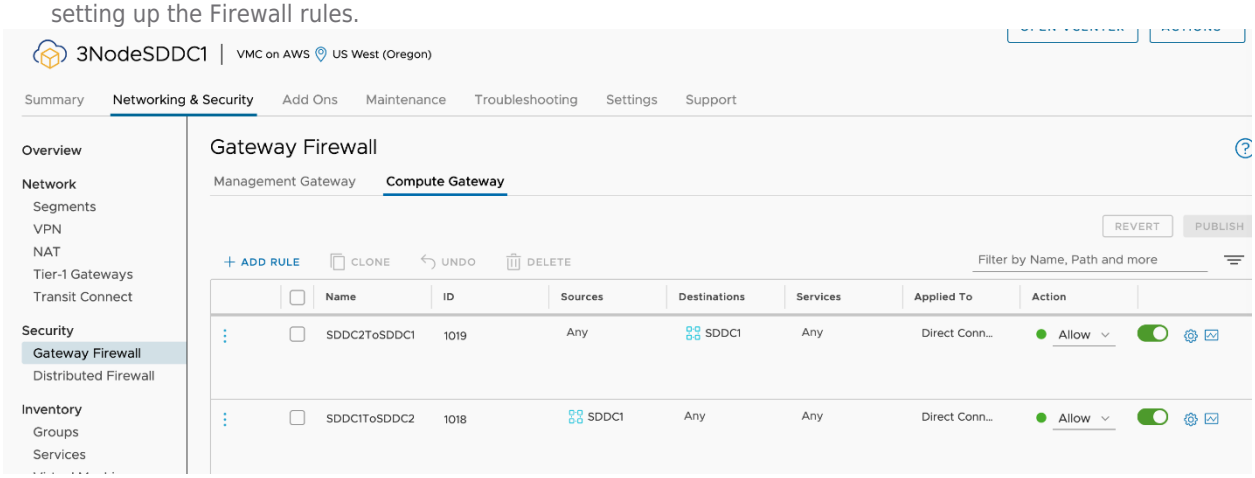


Fig 8 Overlapping Routes are unadvertised

1. Setup Compute Gateway Firewall rules to allow traffic between the workloads of both the SDDCs (select the appropriate upstream interface i.e. Direct Connect or Internet) as shown in Figure 9. The capture below shows 'Any' as source/destination as it is meant for demonstration only.
2. It is recommended to have appropriate groups configured for source/destination VMs. Pre-configured groups can simplify setting up the Firewall rules.



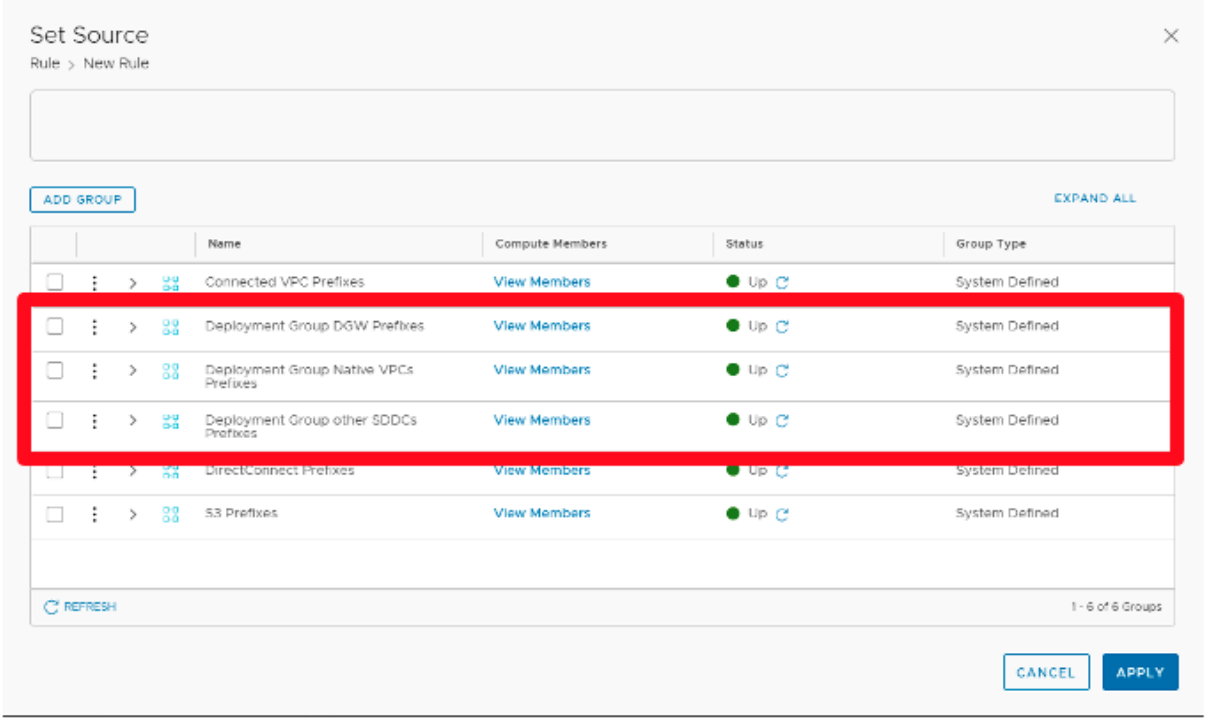


Figure 9 Compute Gateway Firewall rule to allow traffic between the workloads and pre-defined groups

Figure 10 shows the lab setup to allow traffic between workloads SDDC-VM1 and SDDC2-VM1 of both the SDDCs.

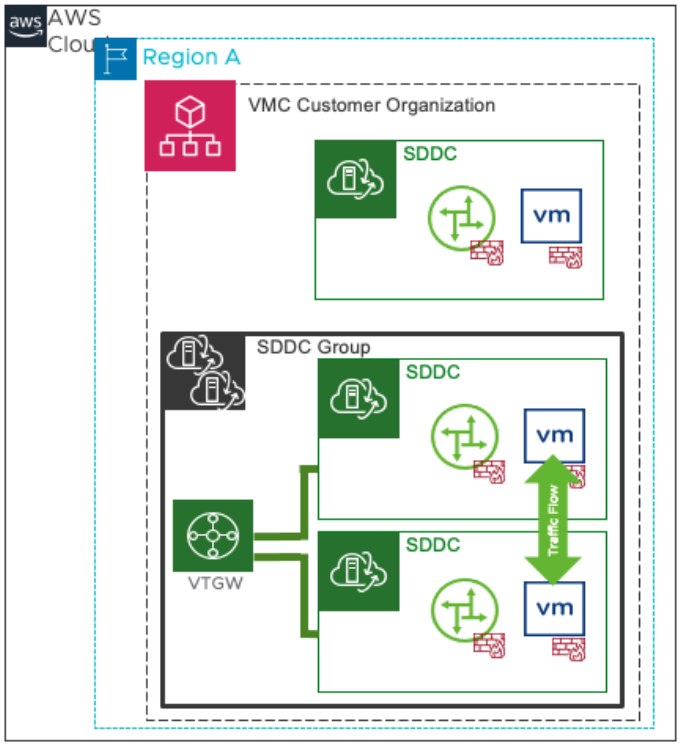


Figure 10 - SDDC - > SDDC Lab Setup

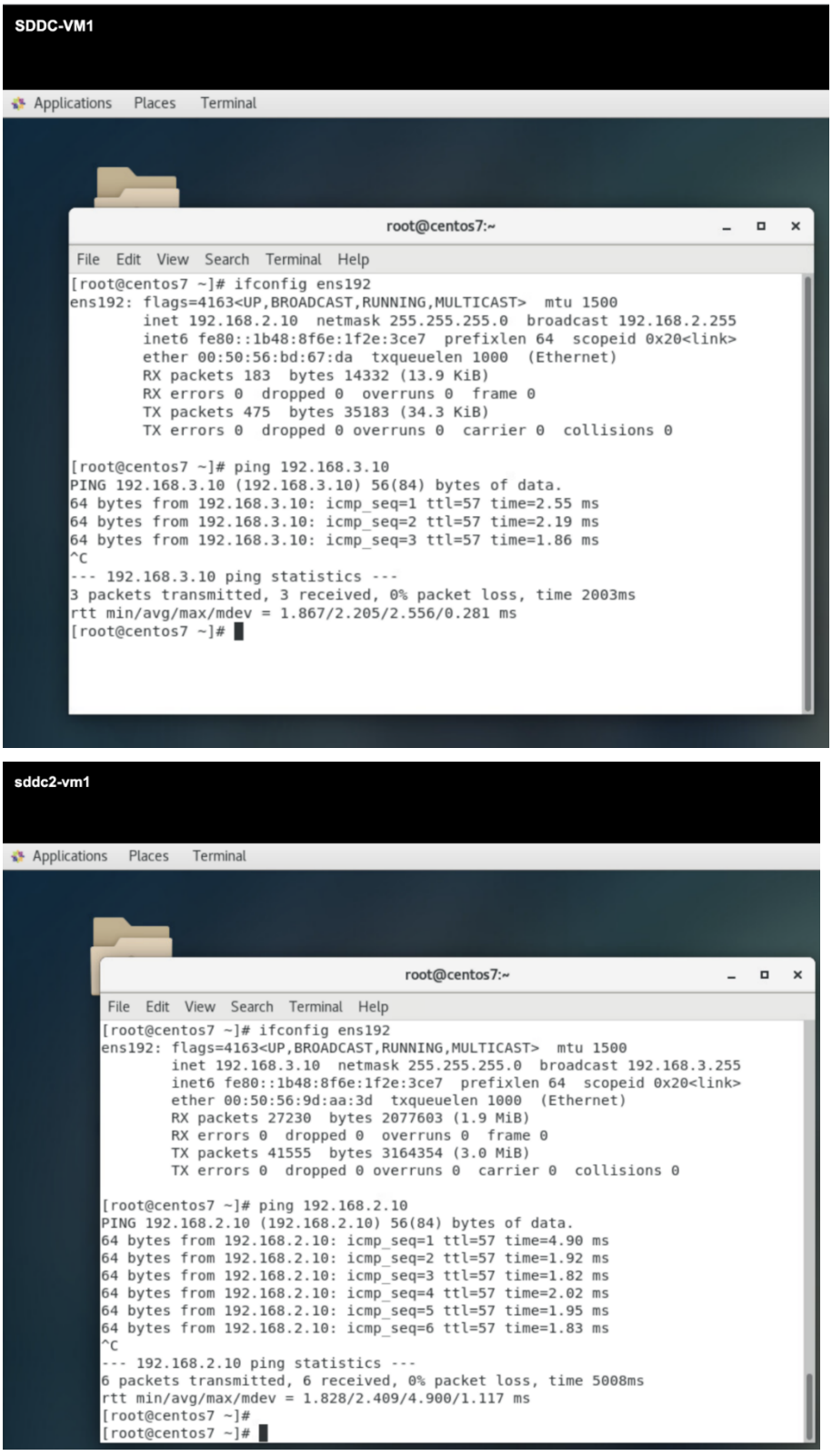


Figure 11 - Traffic flow from VM in SDDC1 to VM in SDDC2

SDDC → VPC Connectivity

Before you configure SDDC to VPC Connectivity, ensure that the SDDC grouping configuration is completed as mentioned under SDDC-to-SDDC connectivity.

Configuration

1. Set up the Customer AWS account in VMC CSP by providing the account number.
2. Accept the resource share on AWS console through Resource Access Manager. Access to AWS console is required for this purpose.
3. Ensure that Transit Gateway gets created in AWS console.
4. Create Transit Gateway attachment with native AWS VPC on the Transit Gateway.
5. Accept the VPC attachment(s) in both AWS console as well as VMC CSP.
6. Modify the AWS VPC route table to allow the Compute networks of the SDDC with target as Transit Gateway.
7. Deploy an EC2 instance in AWS console with the native AWS VPC (same VPC that is attached to Transit Gateway).
8. Keep the VMs with their compute network deployed in both the SDDCs.
9. Add the required Compute Gateway Firewall rules to allow traffic between EC2 and VMs on both the SDDCs.

Verification

1. Associate the customer AWS account to create a resource share in AWS.
2. Accept the resource share in AWS, then the console's Resource Access Manager should show a Transit Gateway deployed as a shared resource.
3. Create a Transit Gateway attachment for the VPC . You will see a "pending acceptance" request for the VPC both in AWS and VMC CSP.
   After accepting the request in VMware Cloud CSP, the status should become available in both the portals.
4. The native AWS VPC network should be advertised to both the SDDCs.
5. After modifying the route table of VPC using AWS console and adding the Compute Gateway Firewall rule, EC2 instance in native AWS VPC and the VMs in SDDCs should be able to communicate with each other.

Detailed Steps

Add the Customer AWS account details for the SDDC Group as shown in Figure 12 and 13.

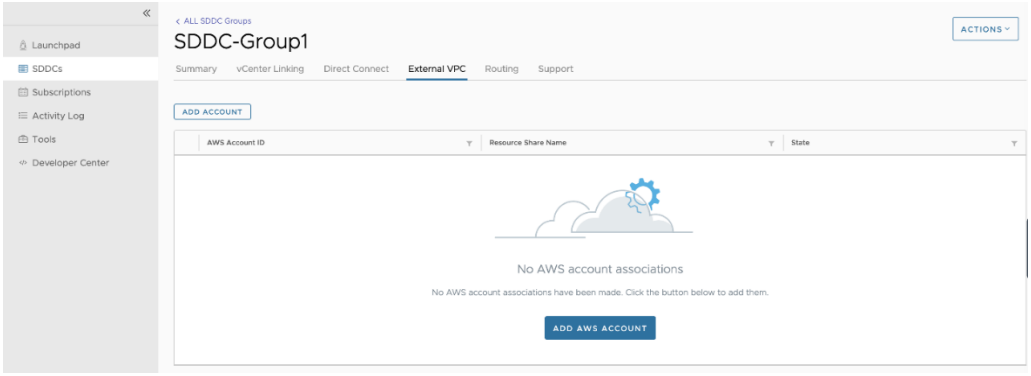


Figure 12 - Add customer AWS account

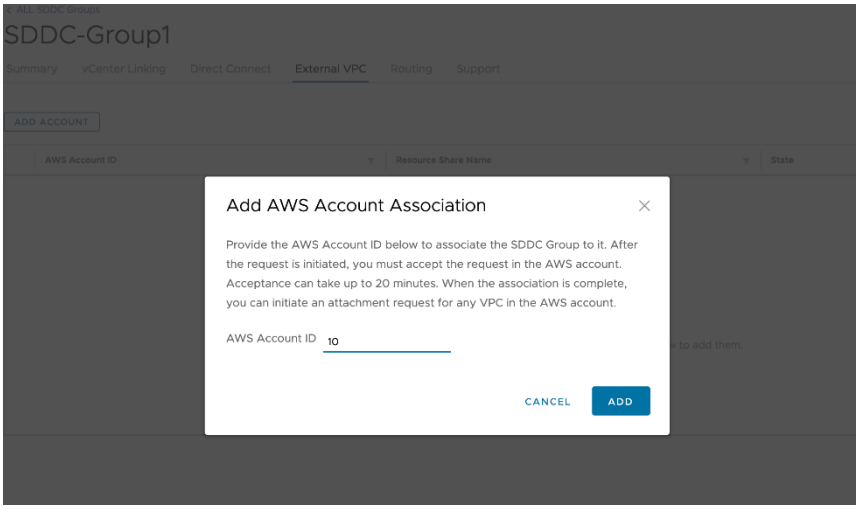


Fig 13 Add AWS account ID

Accept the shared resources from AWS Console as shown in Figure 14 and Figure 15.

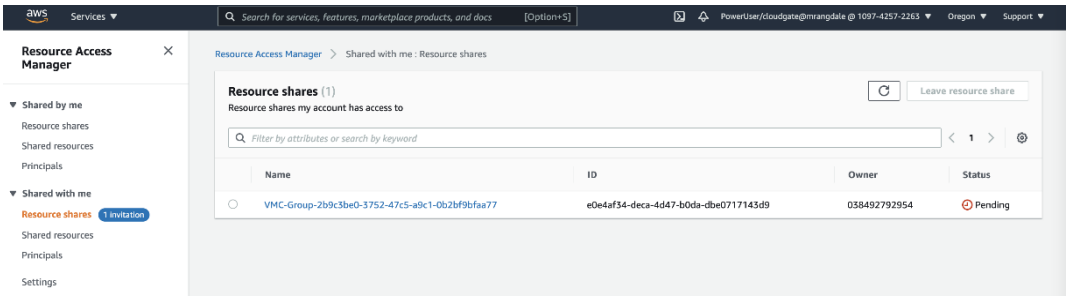


Fig 14 Resource Access Manager - Available resource share

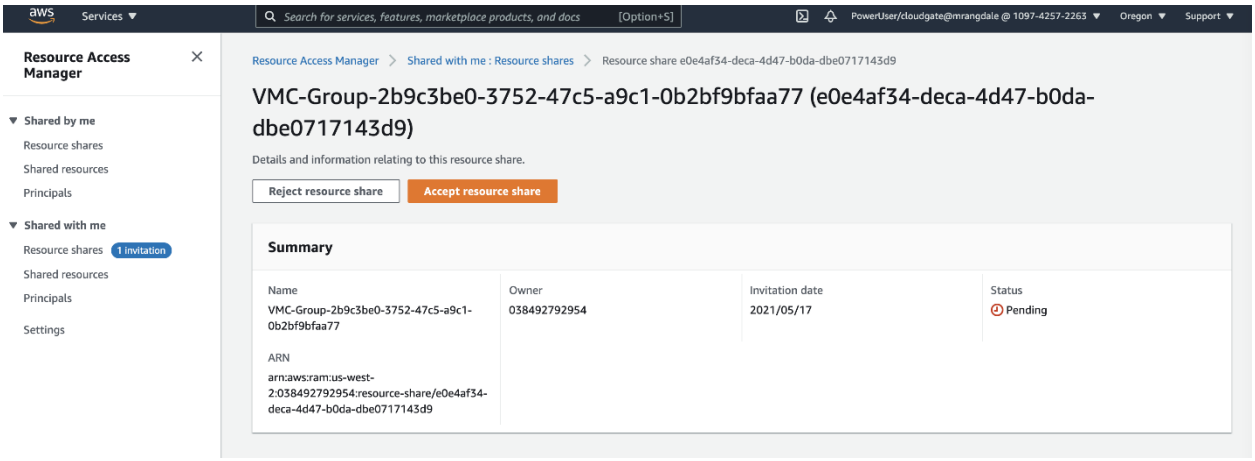


Figure 14 Accept Resource Share

The transit gateway should be available in the AWS Console now as shown in Figure 16.

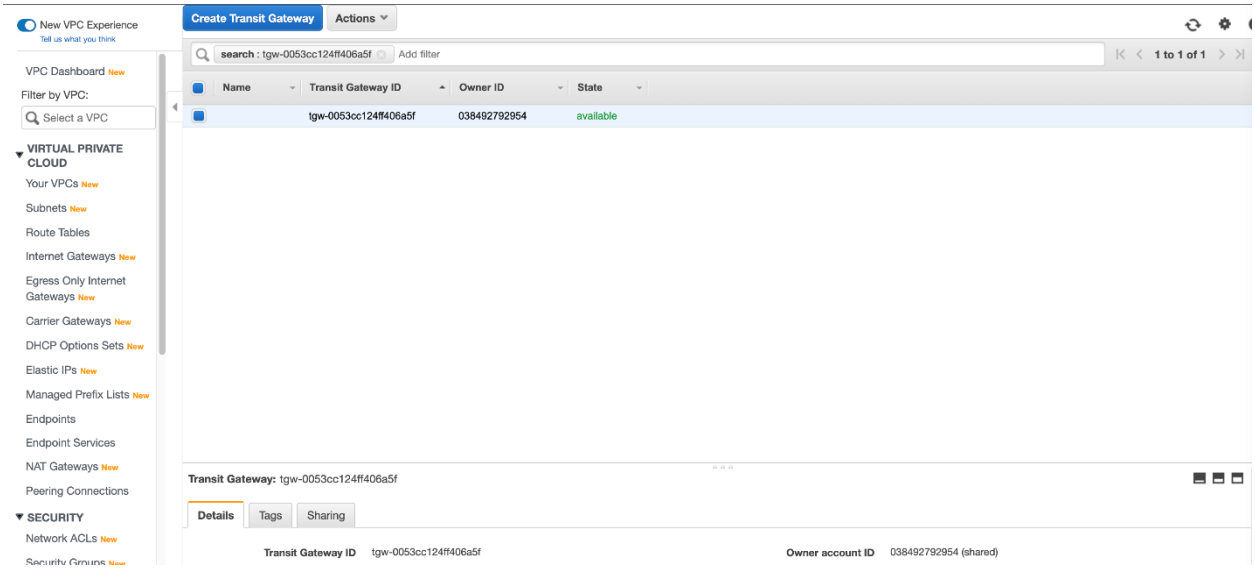


Figure 16 - Available Transit Gateway - AWS Console

Create the VPC attachment from AWS Console. This is needed so that workloads under SDDC1 and SDDC2 can talk to EC2 instances that are connected to native AWS VPC attachment using vTGW as shown in Figure 17a.

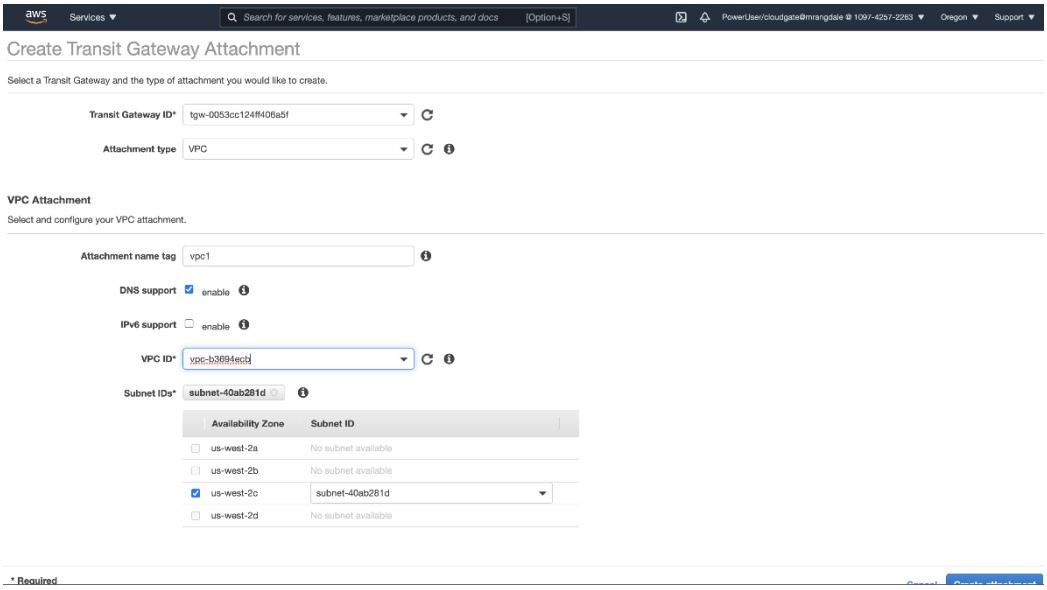


Figure 17a VPC Attachment on vTGW

The VPC attachment shows pending acceptance in AWS Console as shown in Figure 17b. Accept the VPC attachment from the VMC CSP as shown in Figure 18. After accepting the attachment, the status will change from Pending Acceptance to Available after a while in VMC CSP.

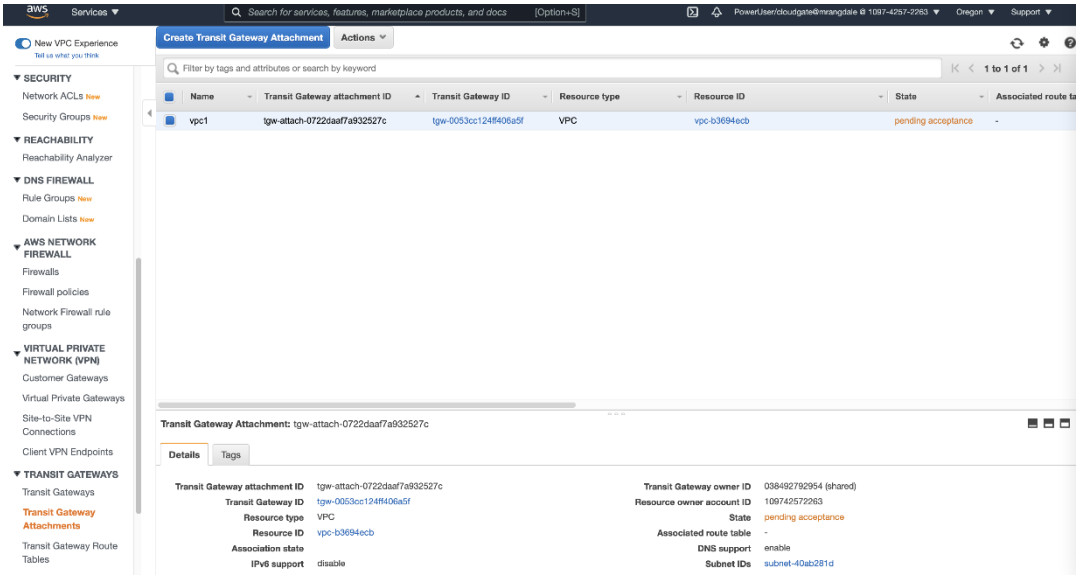


Figure 17b - VPC Attachment Status in AWS Console

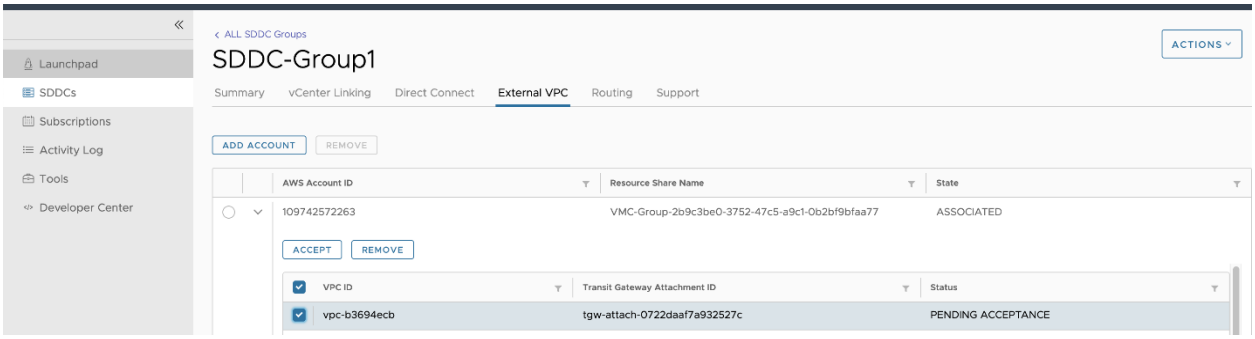


Figure 18 - VPC attachment pending acceptance VMC CSP

Verify that the native AWS VPC route is learnt in SDDC's route table as shown in Figure 19.

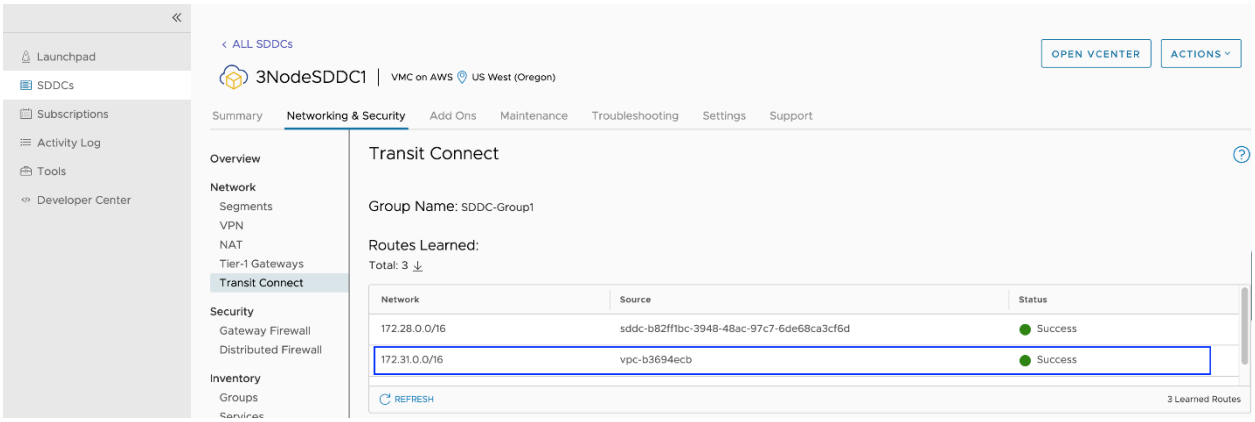


Figure 19 - vTGW Route Table showing learnt native AWS VPC route

Modify the Target for SDDC Compute networks with target as vTGW in AWS route table as shown in Figure 20.

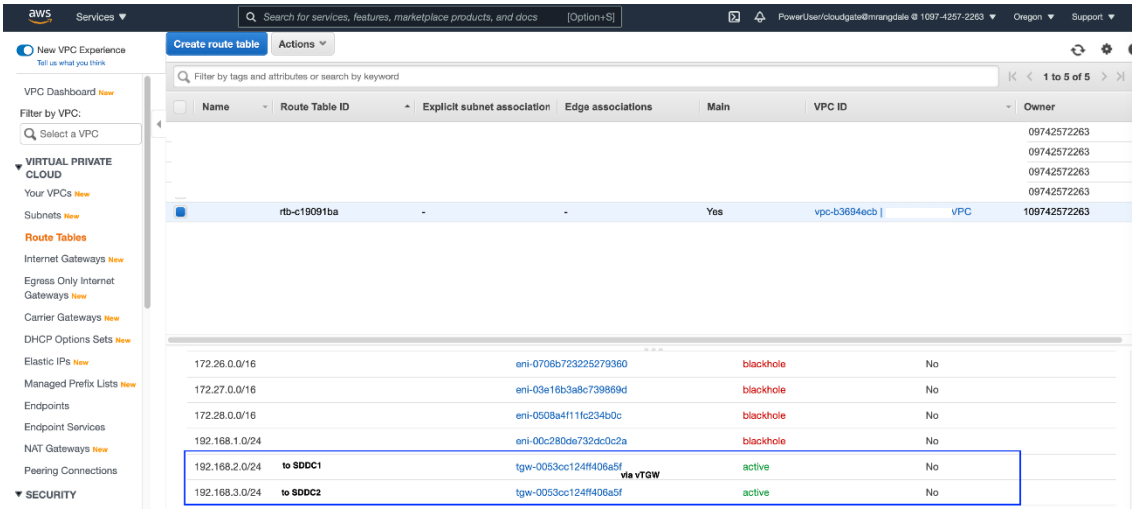


Figure 20 - AWS Route Table

1. Add the required Compute Gateway firewall rules (like SDDC→ SDDC Connectivity section).
2. Deploy an EC2 instance from AWS Console with same AWS VPC as what we have used to create the Transit Gateway attachment in above steps.
3. Verify the reachability from EC2 instance to VMs on SDDC1 and SDDC2 as shown in Fig 21 (note the IP addresses of SDDC VMs

from SDDC→ SDDC Connectivity section).

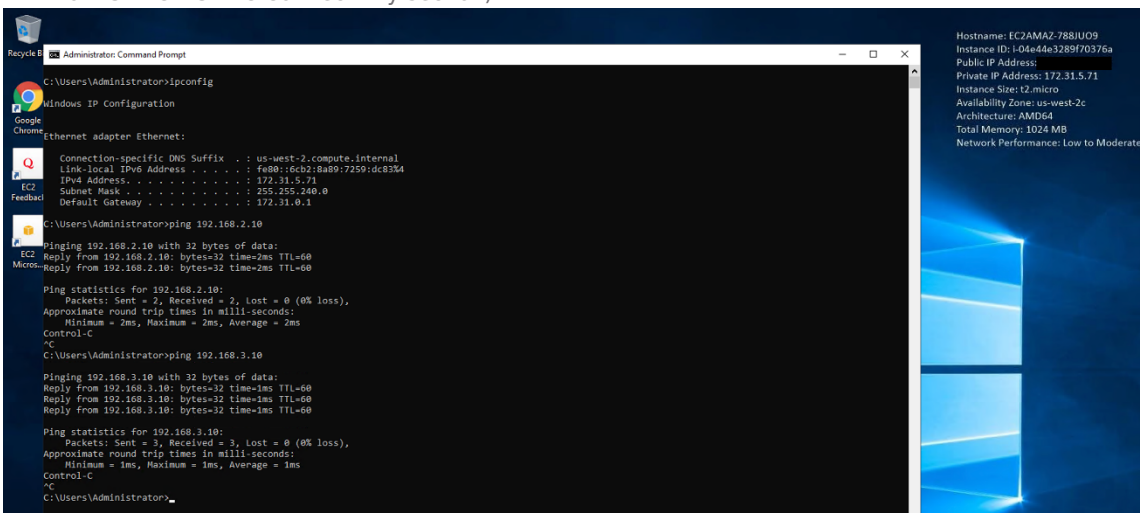


Figure 21 - Communication from EC2 instance to VMs on SDDC

4. The traffic flow is shown in Fig 22 for this topology.

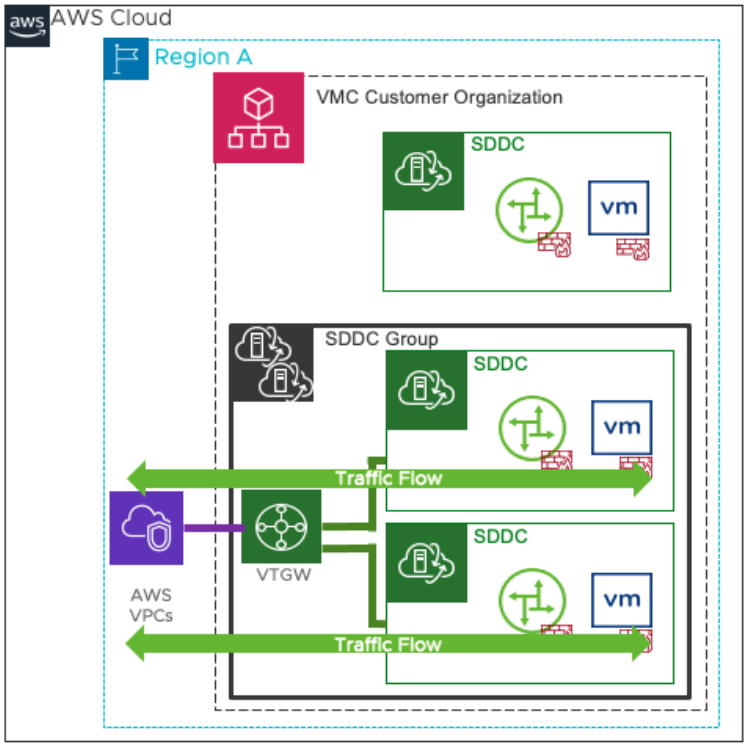


Figure 22 – Traffic Flow from EC2 on Native AWS VPCs to SDDC Compute VMs

Note: If there is another EC2 instance running on another native AWS VPC and that VPC is also attached to the vTGW, these two EC2 instances cannot talk to each other as per vTGW design.

SDDC → On-premises Connectivity

Before you configure SDDC to On-premises Connectivity, ensure that the SDDC grouping configuration is completed as mentioned under SDDC-to-SDDC connectivity.

Configuration

1. Deploy workloads in the on-premises datacenter with its network backing.
2. Deploy workloads on VMC on AWS SDDCs.
3. Deploy few EC2 instance in native AWS VPCs.
4. Establish connectivity between on-premises to VMC on AWS using Direct Connect. The vTGW should have one of its connections with on-premises using the Direct Connect Gateway.
5. Setup appropriate Compute Gateway firewall rules to allow communication between on-premises to VMC on AWS SDDC VMs using Direct Connect Interface.
6. Additionally, setup Management Gateway firewall rules to allow vMotion traffic and SSH connections between both the sites.
7. Use HCX between on-premises and VMC on AWS that will help in migrating workloads from on-premises to VMC on AWS. Alternatively, Cross-vCenter xvMotion can also be used (if vCenters are linked), but it offers lesser benefits than HCX when it comes to extending networks or creating a migration or DR plan.
8. Trigger migration of few workloads from on-premises to any one of the SDDCs by mapping the destination network of the VMC on AWS SDDC.

Verification

1. After a successful pairing of sites using HCX, ensure that workload migration is successfully done using HCX.
2. Other workloads from on-premises should be able to communicate with the VMs on VMC on AWS SDDCs.
3. Verify that EC2 instances of AWS native VPCs cannot communicate with workloads on on-premises Datacenter.
4. Verify that EC2 instances of AWS native VPCs cannot communicate with each other when attached through vTGW.

Allowed and Denied Traffic Flows

Figures 23 and 24 show the allowed and denied traffic flow from SDDC to on-premises. As seen here, traffic between SDDCs of a SDDC group and on-premises is allowed. Traffic between on-premises and native AWS VPCs and between the native AWS VPCs that have attachment with vTGW is not allowed. Traffic between the VMC on AWS SDDCs is allowed as demonstrated in the section of SDDC→ SDDC Connectivity.

The configuration and deployment for this scenario is similar to setting up vTGW and configuring native AWS VPC attachment as demonstrated in earlier sections.

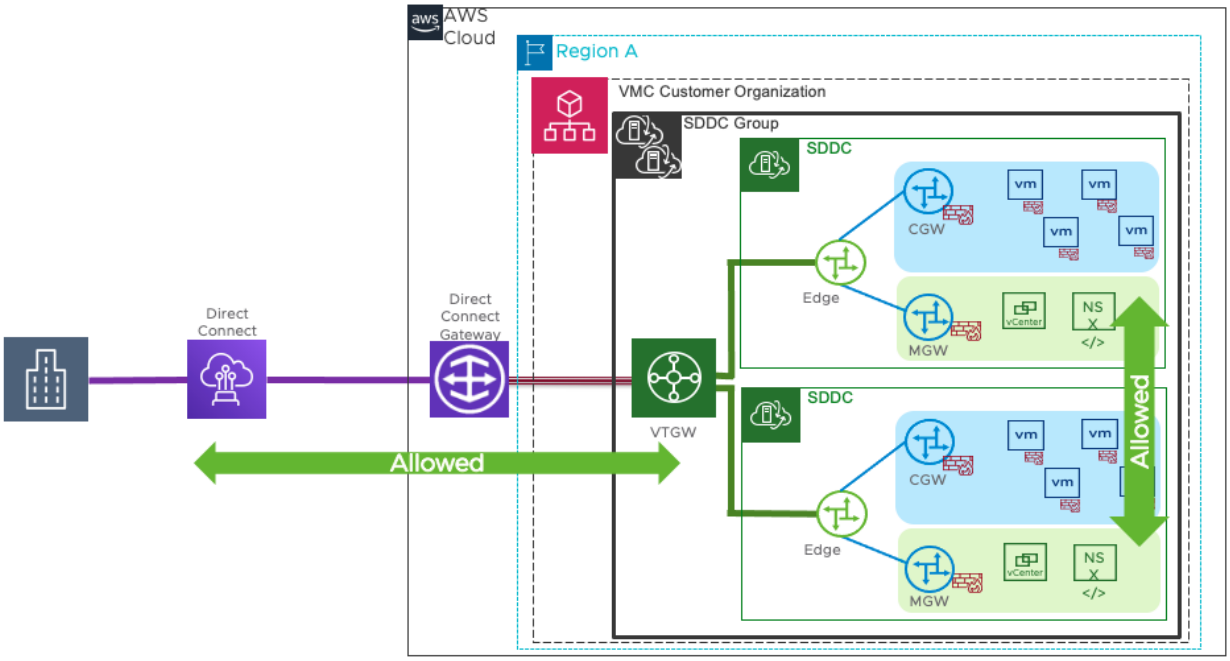


Figure 23 SDDC → On-prem with Direct Connect through vTGW - Allowed flow

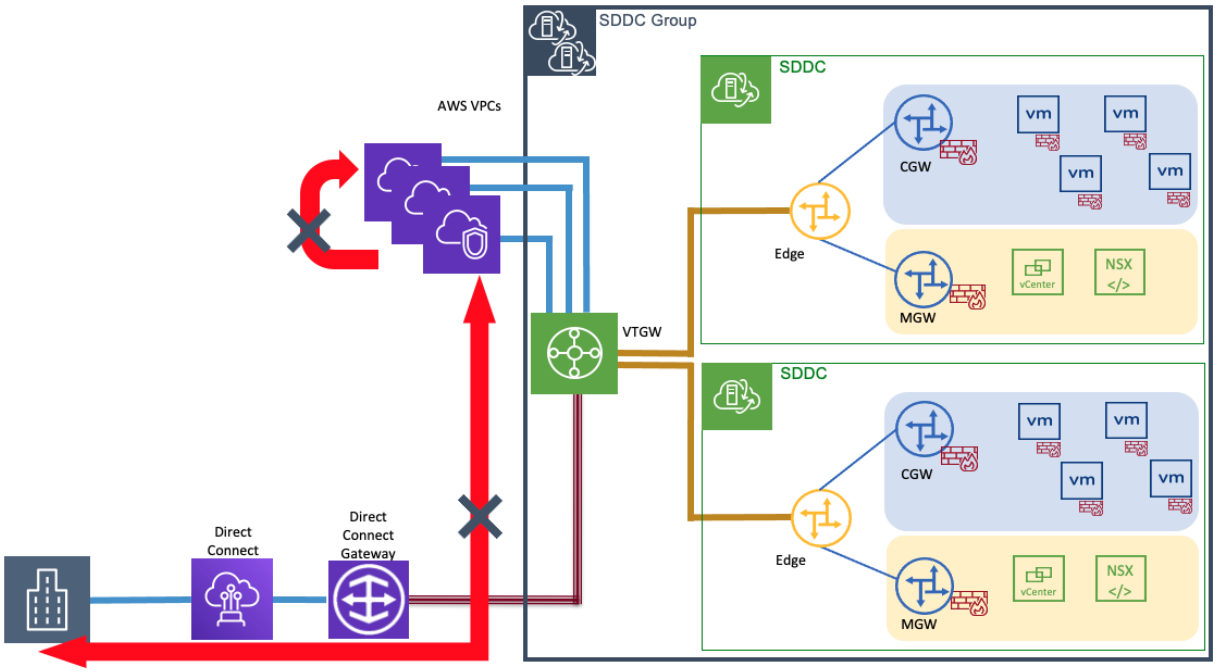


Fig 24 SDDC → On-prem with Direct Connect through vTGW - Denied Flow

Detailed Steps

To configure Direct Connect Gateway in Transit Connect, click on the Direct Connect Gateway tab in the VMC Console and click on Add Account as shown in Fig 25.

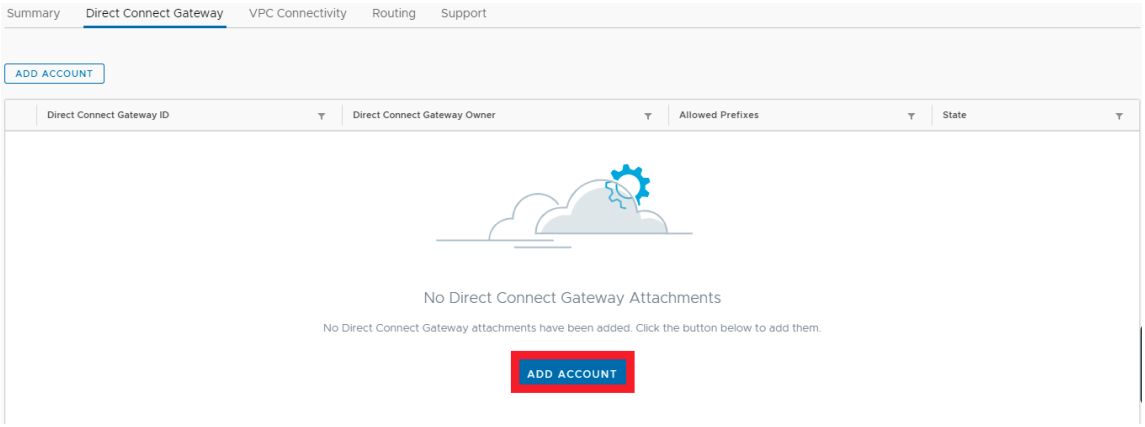


Figure 25 – Adding an account for Direct Connect Gateway

Populate the fields required with a special focus on the Allowed Prefixes as shown in Fig 26. Note that AWS supports 20 prefixes being advertised to the on-premises networks, so consider summarization of the networks.

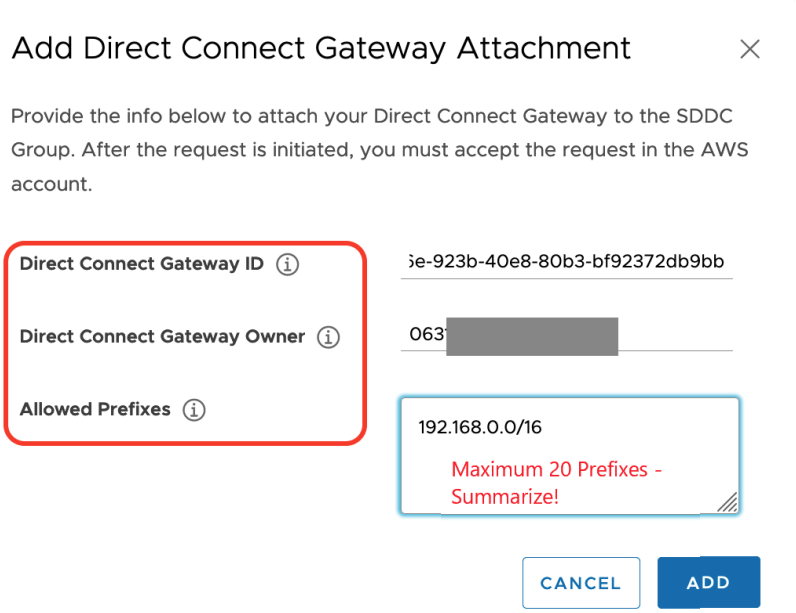


Figure 26 – DXGW attachment and adding Prefixes under the DXGW

The vTGW will request an association with the Direct Connect Gateway owner. This will show as "Requested" in the VMware CSP as illustrated below in Fig 27.

Figure 27 – DXGW request in VMware CSP

1. In the AWS Console, accept the proposed TGW association as shown in Fig 28.

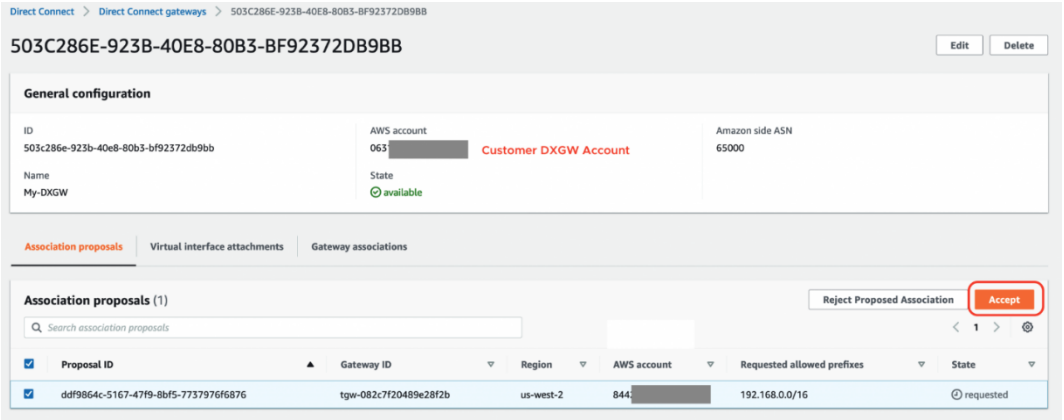


Figure 28 – Accepting the TGW proposed association.

After accepting the association, the opportunity to accept the BGP proposal is presented as shown in Fig 29 below.

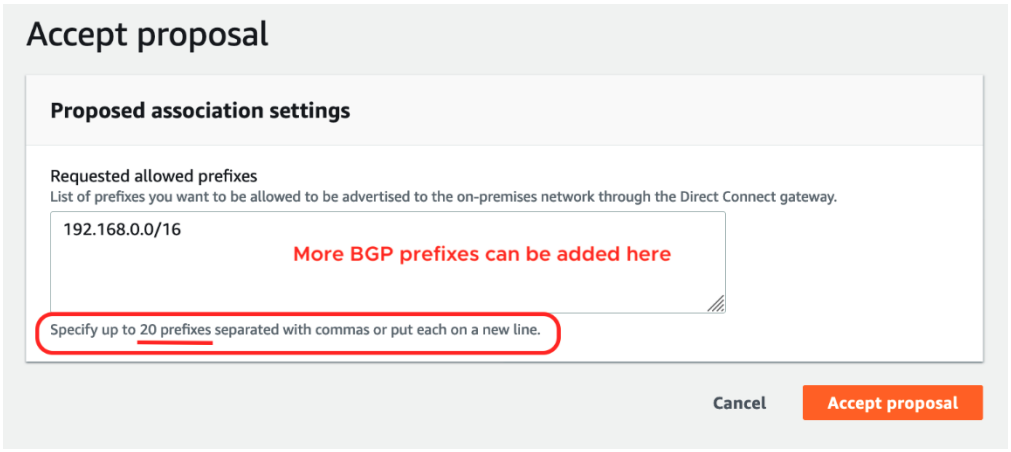


Figure 29 – Accepting the BGP proposed settings.

Click Accept proposal and the systems will process the requests. Please note that this may take up to 20 minutes.

Verify the state in VMware CSP to reflect as “Connected” as shown in Fig 30.

Figure 30 – DXGW Status in VMware CSP

As with the SDDC to SDDC and the SDDC to VPC communication models, when a Direct Connect Gateway connection is established, security policy must be updated to complete the connection. One notable difference is that with an on-premises environment there may be physical firewalls that could need updated with routing and/or security policy to communicate with the Transit Connect resources.

Author and Contributors

Mithil Rangdale

Ron Fuller