

# Multi-Region Transit Routing from AWS to OCI

**Author:** Shadab Mohammad, Master Principal Cloud Architect

---

## Executive Summary

This whitepaper presents a scalable, high-performance solution for establishing multi-region transit routing between AWS and OCI using Transit Gateway (TGW) and Dynamic Routing Gateway (DRG). The architecture enables secure and optimized connectivity across multiple AWS and OCI regions via IPsec VPN. The solution is designed to facilitate seamless communication across AWS VPCs and OCI VCNs using a single transit region in both clouds, with the capability to extend into additional regions as needed.

*Important Note : The setup documented in this Whitepaper can also be used to create a Transit Routing network topology for DB@AWS. The only requirement is to ensure the ODB Network Peering route is added to the Route tables for the VPC and then extended to connect to other VPCs in one or more regions using Transit Gateway and Transit Gateway peering on AWS.*

## Introduction

Organizations increasingly operate in multi-cloud environments to leverage the unique capabilities of various cloud providers. This solution integrates AWS Transit Gateway (TGW) and OCI Dynamic Routing Gateway (DRG) to create a highly available, secure, and scalable transit routing framework, facilitating cross-region and cross-cloud connectivity.

### Key Objectives:

- Establish a multi-region transit architecture between AWS and OCI.
- Utilize AWS Transit Gateway and OCI DRG to enable secure connectivity.
- Ensure seamless routing and high availability across multiple cloud regions.
- Implement a scalable, extendable mesh network architecture.

## Architecture Overview

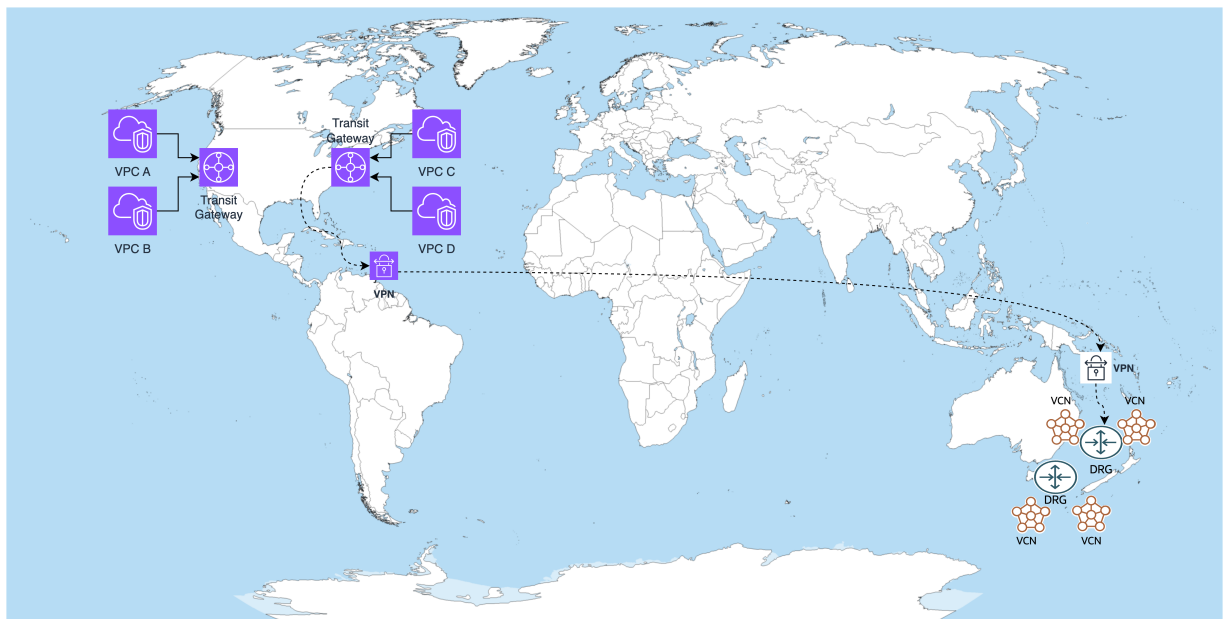
The architecture consists of the following key components:

### AWS Components:

- **AWS Transit Gateway (TGW):** Centralized hub for routing between AWS VPCs and OCI.
- **AWS Customer Gateway:** Used to establish an IPsec VPN connection.
- **AWS Site-to-Site VPN:** Provides secure communication with OCI.
- **AWS VPC Route Tables:** Configured to facilitate cross-region connectivity.

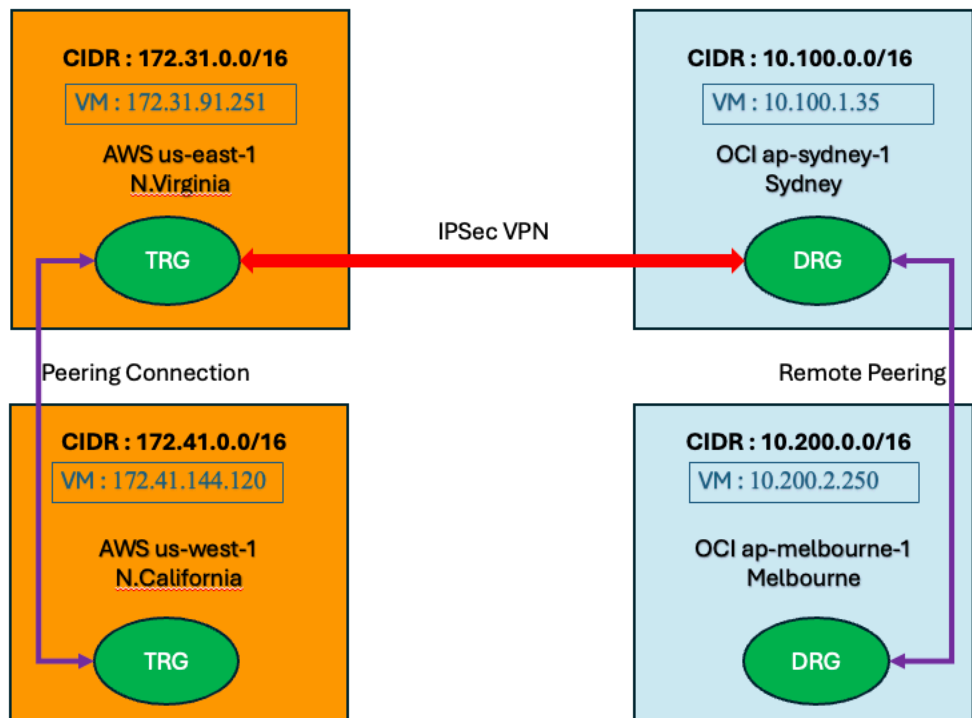
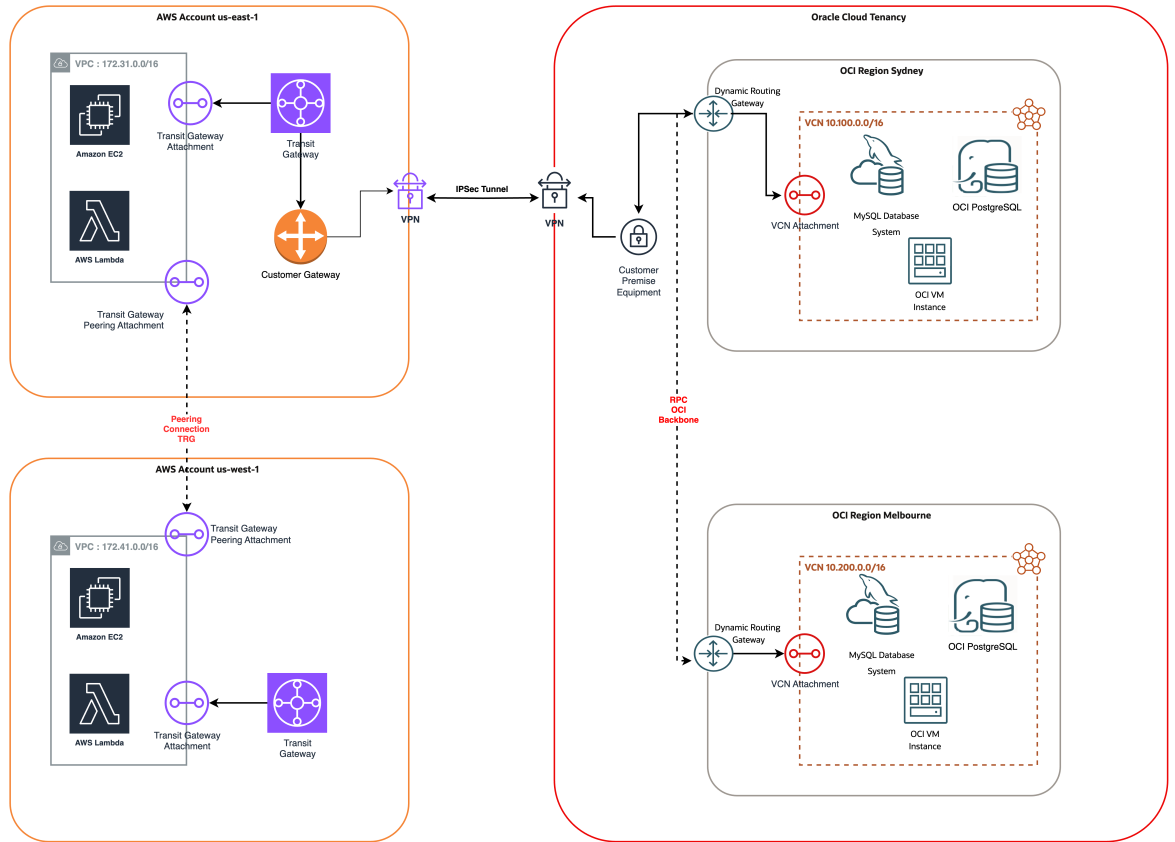
## OCI Components:

- **Dynamic Routing Gateway (DRG):** Acts as a central routing hub for OCI VCNs.
- **Customer Premises Equipment (CPE):** Represents AWS as a remote VPN peer.
- **OCI Site-to-Site VPN:** Enables connectivity between OCI and AWS.
- **Remote Peering Connection (RPC):** Extends connectivity across multiple OCI regions.





## Architecture



### Site-to-Site VPN OCI ap-sydney-1 BGP Routes received:

#### BGP routes received

IP route prefix	Route age	Is best path	AS path length	AS path
172.31.0.0/16	29337 Seconds	No	2	65515... <a href="#">Show all (2)</a>
172.41.0.0/16	8306 Seconds	No	2	65515... <a href="#">Show all (2)</a>
Showing 2 items < Page 1 >				

### Site-to-Site VPN OCI ap-sydney-1 BGP Routes advertised:

#### BGP routes advertised

IP route prefix	Route age	Is best path	AS path length	AS path
10.100.1.0/24	899721 Seconds	No	0	-
10.100.2.0/24	899721 Seconds	No	0	-
10.200.1.0/24	807321 Seconds	No	0	-
10.200.2.0/24	807321 Seconds	No	0	-
Showing 4 items < Page 1 >				

### AWS Route Tables for Transit Routing Gateway us-east-1 :

Routes (6) <a href="#">info</a>								<a href="#">Actions</a>	<a href="#">Create static route</a>
<input type="text" value="Find route by attribute or tag"/>							< 1 >		
<input type="checkbox"/>	CIDR	Attachment ID	Resource ID	Resource type	Route type	Route state			
<input type="checkbox"/>	10.100.1.0/24	<a href="#">tgw-attach-0826fb2097ce1c62e</a>	<a href="#">vpn-0b732e51d8e13201c3...</a>	VPN	Propagated				
<input type="checkbox"/>	10.100.2.0/24	<a href="#">tgw-attach-0826fb2097ce1c62e</a>	<a href="#">vpn-0b732e51d8e13201c3...</a>	VPN	Propagated				
<input type="checkbox"/>	10.200.1.0/24	<a href="#">tgw-attach-0826fb2097ce1c62e</a>	<a href="#">vpn-0b732e51d8e13201c3...</a>	VPN	Propagated				
<input type="checkbox"/>	10.200.2.0/24	<a href="#">tgw-attach-0826fb2097ce1c62e</a>	<a href="#">vpn-0b732e51d8e13201c3...</a>	VPN	Propagated				
<input type="checkbox"/>	172.31.0.0/16	<a href="#">tgw-attach-0ea473f30c8380a66</a>	<a href="#">vpc-0b6de2f65f971840b</a>	VPC	Propagated				
<input type="checkbox"/>	172.41.0.0/16	<a href="#">tgw-attach-0fbb0083169ca71a4</a>	<a href="#">tgw-08c5eb41bf661444e</a>	Peering	Static				

### AWS Route Tables for Transit Routing Gateway us-west-1 :

Routes (4) <a href="#">info</a>								<a href="#">Actions</a>	<a href="#">Create static route</a>
<input type="text" value="Find route by attribute or tag"/>							< 1 >		
<input type="checkbox"/>	CIDR	Attachment ID	Resource ID	Resource type	Route type	Route state			
<input type="checkbox"/>	10.100.0.0/16	<a href="#">tgw-attach-0fbb0083169ca71a4</a>	<a href="#">tgw-09fcad83501f16313</a>	Peering	Static				
<input type="checkbox"/>	10.200.0.0/16	<a href="#">tgw-attach-0fbb0083169ca71a4</a>	<a href="#">tgw-09fcad83501f16313</a>	Peering	Static				
<input type="checkbox"/>	172.31.0.0/16	<a href="#">tgw-attach-0fbb0083169ca71a4</a>	<a href="#">tgw-09fcad83501f16313</a>	Peering	Static				
<input type="checkbox"/>	172.41.0.0/16	<a href="#">tgw-attach-0064f0317ded73e16</a>	<a href="#">vpc-00d41f2f634572ffa</a>	VPC	Propagated				

Sydney DRG:

Route rules for Autogenerated Drg Route Table for VCN attachments

Last checked: Mon, Mar 24, 2025, 13:39:26 UTC

Download route rules		Refresh table		Search by CIDR block	
Type	Destination CIDR block	Next hop attachment type	Next hop attachment name	Route status	
DYNAMIC	10.100.1.0/24	Virtual Cloud Network	<a href="#">drgattachment20250313061949</a>	Active	
DYNAMIC	10.100.2.0/24	Virtual Cloud Network	<a href="#">drgattachment20250313061949</a>	Active	
DYNAMIC	10.200.1.0/24	Remote Peering Connection	<a href="#">DRG Attachment for RPC: SYD-RPC-CONNECTION</a>	Active	
DYNAMIC	10.200.2.0/24	Remote Peering Connection	<a href="#">DRG Attachment for RPC: SYD-RPC-CONNECTION</a>	Active	
DYNAMIC	172.31.0.0/16	IPSec Tunnel	<a href="#">DRG Attachment for IPSec Tunnel: ipsectunnel20250314034733-1</a>	Active	
DYNAMIC	172.41.0.0/16	IPSec Tunnel	<a href="#">DRG Attachment for IPSec Tunnel: ipsectunnel20250314034733-1</a>	Active	

Route distribution statements

Import route distribution statements describe the advertisement of routes to attachments from their assigned route table, [Learn more](#).

Add route distribution statements

Edit

Remove

<input type="checkbox"/>	Priority	Match type	Match criteria	Action
<input type="checkbox"/>	1	Attachment type	Virtual Cloud Network	ACCEPT ⋮
<input type="checkbox"/>	10	Attachment	<a href="#">DRG Attachment for IPSec Tunnel: ipsectunnel20250314034733-1</a>	ACCEPT ⋮
<input type="checkbox"/>	20	Attachment	<a href="#">DRG Attachment for RPC: SYD-RPC-CONNECTION</a>	ACCEPT ⋮

Melbourne DRG:

Route rules for Autogenerated Drg Route Table for VCN attachments

Last checked: Mon, Mar 24, 2025, 13:43:42 UTC

Download route rules		Refresh table		Search by CIDR block	
Type	Destination CIDR block	Next hop attachment type	Next hop attachment name	Route status	
DYNAMIC	10.100.1.0/24	Remote Peering Connection	<a href="#">DRG Attachment for RPC: RPC-CONN-MELB</a>	Active	
DYNAMIC	10.100.2.0/24	Remote Peering Connection	<a href="#">DRG Attachment for RPC: RPC-CONN-MELB</a>	Active	
DYNAMIC	10.200.1.0/24	Virtual Cloud Network	<a href="#">drgattachment20250315044021</a>	Active	
DYNAMIC	10.200.2.0/24	Virtual Cloud Network	<a href="#">drgattachment20250315044021</a>	Active	
DYNAMIC	172.31.0.0/16	Remote Peering Connection	<a href="#">DRG Attachment for RPC: RPC-CONN-MELB</a>	Active	
DYNAMIC	172.41.0.0/16	Remote Peering Connection	<a href="#">DRG Attachment for RPC: RPC-CONN-MELB</a>	Active	

## High-Level Implementation Steps

### 1. Configure AWS Transit Gateway

1. **Create AWS Transit Gateway**
  - Navigate to AWS Console > VPC > Transit Gateway > Create Transit Gateway.
  - Attach AWS VPCs to TGW.
2. **Create AWS Customer Gateway**
  - Use a temporary mock IP initially.
  - Assign Oracle's BGP ASN (31898 for most regions).
3. **Establish AWS Site-to-Site VPN**
  - Navigate to AWS Console > VPC > Virtual Private Network > Site-to-Site VPN > Create VPN Connection.
  - Configure Tunnel 1 only.
  - Download the VPN configuration.
4. **Modify AWS Route Tables**
  - Add OCI VCN CIDR (e.g., 10.100.0.0/16) to AWS VPC Subnet Route Table.

### 2. Configure OCI Dynamic Routing Gateway

1. **Create and Attach DRG to OCI VCN**
  - Attach the AWS VPC CIDR (172.31.0.0/16) to the DRG.
2. **Create Customer Premises Equipment (CPE) in OCI**
  - Use AWS VPN Tunnel 1 Public IP.
3. **Create Site-to-Site VPN in OCI**
  - Match AWS VPN settings and shared secret key.
  - Configure ISAKMP settings for Tunnel 1.

### 3. Establish Cross-Region Peering in OCI

1. **Create OCI VCN in Secondary Region (e.g., Melbourne)**
2. **Deploy a DRG in Melbourne and Attach VCN**
3. **Create Remote Peering Connection (RPC) Between Regions**
  - Establish an RPC in Sydney DRG and Melbourne DRG.
  - Exchange OCIDs and verify connectivity.

### 4. Extend AWS Transit Gateway Across Regions

1. **Deploy Another AWS Transit Gateway in a Different Region (e.g., us-west-1).**
2. **Create Peering Connection Between AWS TGWs**
  - Accept the peering request in the target region.
  - Update route tables for cross-region connectivity.

### 5. Verify Connectivity

- Ensure AWS VPC Route Tables include OCI VCN routes.
- Check BGP Route Propagation in OCI.

## Implementation Steps

### 1. Create AWS Transit Gateway and Attach to VPC

Go to AWS Console

VPC > Transit Gateway > Create Transit Gateway

The screenshot shows the AWS Management Console interface for creating a transit gateway. The breadcrumb navigation at the top reads 'VPC > Transit gateways > Create transit gateway'. The main heading is 'Create transit gateway' with an 'Info' link. Below this is a descriptive sentence: 'A transit gateway (TGW) is a network transit hub that interconnects attachments (VPCs and VPNs) within the same AWS account or across AWS accounts.'

The 'Details - optional' section is expanded, showing two fields:

- Name tag:** A text input field containing 'Transit-Gateway-01'. A tooltip explains: 'Creates a tag with the key set to Name and the value set to the specified string.'
- Description:** A text input field containing 'Transit Gateway for AWS - OCI Connectivity'. A tooltip explains: 'Set the description of your transit gateway to help you identify it in the future.'

Below this is the 'Configure the transit gateway' section, which includes:

- Amazon side Autonomous System Number (ASN):** A text input field containing 'ASN'. A tooltip is available.
- Options:** Three checkboxes are shown: 'DNS support' (checked), 'Security Group Referencing support' (unchecked), and 'VPN ECMP support' (checked). Each has an 'Info' link.
- Default route table association:** A checkbox that is currently unchecked.

On the right side of the console, there is a sidebar with the heading 'Amazon side Autonomous System Number(ASN)' and a brief explanation of ASNs. Below this is a 'Learn more' link and a 'Creating a transit gateway' link.

This screenshot shows the lower portion of the 'Create transit gateway' page. The breadcrumb navigation remains 'VPC > Transit gateways > Create transit gateway'.

The 'Configure cross-account sharing options' section contains a single checkbox: 'Auto accept shared attachments' (unchecked), with an 'Info' link.

The 'Transit gateway CIDR blocks' section is expanded, showing a 'CIDR - optional' field with a text input containing '10.0.0.0/24'.

The 'Tags - optional' section is also expanded, showing a list of tags. It includes a 'Key' field with 'Name' and a 'Value - optional' field with 'Transit-Gateway-01'. There is a 'Remove' button next to the value field and an 'Add new tag' button below. A note states: 'You can add up to 49 more tags.'

At the bottom right of the form, there are two buttons: 'Cancel' and 'Create transit gateway'.

The right sidebar is identical to the one in the previous screenshot, showing information about the Amazon side Autonomous System Number (ASN).

Transit gateways (2) [info](#)

Find transit gateway by attribute or tag

<input type="checkbox"/>	Name	Transit gateway ID	State
<input type="checkbox"/>	Transit-Gateway-01	<a href="#">tgw-09fcad83501f16313</a>	Available

Select a transit gateway

## Attach Your existing AWS VPC to the Transit Gateway

VPC > Transit gateway attachments > Create transit gateway attachment

### Create transit gateway attachment [info](#)

A transit gateway (TGW) is a network transit hub that interconnects attachments (VPCs and VPNs) within the same AWS account or across AWS accounts.

**Details**

**Name tag - optional**  
Creates a tag with the key set to Name and the value set to the specified string.

**Transit gateway ID** [info](#)  
[tgw-09fcad83501f16313](#)

**Attachment type** [info](#)  
VPC

**VPC attachment**  
Select and configure your VPC attachment.

☒ DNS support [info](#)

☒ Security Group Referencing support [info](#)

☐ IPv6 support [info](#)

VPC ID  
Select the VPC to attach to the transit gateway.  
[vpc-0b6de2f65f971840b](#)

**Subnet IDs** [info](#)  
Select the subnets in which to create the transit gateway VPC attachment.

<input checked="" type="checkbox"/> us-east-1a	<a href="#">subnet-0e870da404fb31ebe</a>
<input checked="" type="checkbox"/> us-east-1b	<a href="#">subnet-04607c1b7e3d78ff6</a>
<input checked="" type="checkbox"/> us-east-1c	<a href="#">subnet-03adc46dcc608fd82</a>
<input checked="" type="checkbox"/> us-east-1d	<a href="#">subnet-03d2752670df2f612</a>
<input checked="" type="checkbox"/> us-east-1e	<a href="#">subnet-08c256c1828816718</a>
<input checked="" type="checkbox"/> us-east-1f	<a href="#">subnet-043f23a07c3fcd099</a>

[subnet-0e870da404fb31ebe](#)
[subnet-04607c1b7e3d78ff6](#)
[subnet-03adc46dcc608fd82](#)
[subnet-03d2752670df2f612](#)
[subnet-08c256c1828816718](#)
[subnet-043f23a07c3fcd099](#)

**Tags - optional**

Subnets: subnet-03d2752670df2f612, subnet-08c256c1828816718, subnet-043f23a07c3fcd099

**Tags - optional**  
 A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key: Name Value: transit-gateway-attachement-01

Buttons: Add new tag, Cancel, Create transit gateway attachment

Transit gateway attachments (1)

Name	Transit gateway attachment ID	Transit gateway ID	State	Resource type	Resource ID
transit-gateway-atta...	tgw-attach-Oea473f30c8380a66	tgw-09fcad83501f16313	Available	VPC	vpc-0b6de2f65f971840b

Buttons: Actions, Create transit gateway attachment

## 2. Create AWS Customer Gateway

Create a temporary AWS customer gateway with a mock ip 1.1.1.1, this will eventually be replaced with a permanent CustomerGateway once we know the Public IP of OCI VPN Tunnel

**BGP ASN:** Enter the OCI BGP ASN. Oracle's BGP ASN for the commercial cloud is 31898, except the Serbia Central (Jovanovac) region which is 14544.

**Create customer gateway** [Info](#)

A customer gateway is a resource that you create in AWS that represents the customer gateway device in your on-premises network.

**Details**

**Name tag - optional**  
Creates a tag with a key of 'Name' and a value that you specify.  
customer-gateway-for-oci  
Value must be 256 characters or less in length.

**BGP ASN** [Info](#)  
The ASN of your customer gateway device.  
31898  
Value must be in 1 - 4294967294 range.

**IP address** [Info](#)  
Specify the IP address for your customer gateway device's external interface.  
1.1.1.1

**Certificate ARN - optional**  
The ARN of a private certificate provisioned in AWS Certificate Manager (ACM).  
Select certificate ARN

**Device - optional**  
Enter a name for the customer gateway device.

**VPC dashboard** [EC2 Global View](#)

Filter by VPC

- Virtual private cloud
  - Your VPCs
  - Subnets
  - Route tables
  - Internet gateways
  - Egress-only Internet gateways
  - Carrier gateways
  - DHCP option sets
  - Elastic IPs
  - Managed prefix lists
  - NAT gateways
  - Peering connections
- Security

**Customer gateways (2)** [Info](#)

Find resource by attribute or tag

Name	Customer gateway ID	State	BGP ASN	IP address	Type
customer-gateway-f...	cgw-0353d3768e3ee26fe	Available	31898	1.1.1.1	Ipsec.1

Select a customer gateway

### 3. Create Site-to-Site VPN from AWS Console

*AWS Console > VPC > Virtual Private Network > Site-to-Site VPN > Create VPN Connection*

**Create VPN connection** [Info](#)

Select the resources and additional configuration options that you want to use for the site-to-site VPN connection.

**Details**

**Name tag - optional**  
Creates a tag with a key of 'Name' and a value that you specify.  
VPN-TO-OCI-VIA-TGW  
Value must be 256 characters or less in length.

**Target gateway type** [Info](#)  
☐ Virtual private gateway  
☒ Transit gateway  
☐ Not associated

**Transit gateway**  
tgw-09fcad83501f16313

**Customer gateway** [Info](#)  
☒ Existing  
☐ New

**Customer gateway ID**  
cgw-0353d3768e3ee26fe



aws [Search] [Option+S] United States (N. Virginia) Cybrysis Admin

VPC > VPN connections > Create VPN connection

**▼ Tunnel 1 options – optional** [Info](#)  
Customize tunnel inside CIDR and pre-shared keys for your VPN tunnels. Unspecified tunnel options will be randomly generated by Amazon.

**Inside IPv4 CIDR for tunnel 1**  
169.254.40.0/30  
A size /30 IPv4 CIDR block from the 169.254.0.0/16 range.

**Pre-shared key for tunnel 1**  
The pre-shared key (PSK) to establish initial authentication between the virtual private gateway and customer gateway.  
Generated by Amazon  
The pre-shared key must have 8-64 characters. Valid characters: A-Z, a-z, 0-9, \_ and . The key cannot begin with a zero.

**Advanced options for tunnel 1**  
☐ Use default options  
☒ Edit tunnel 1 options

**Phase 1 encryption algorithms**  
The permitted encryption algorithms for the VPN tunnel for phase 1 IKE negotiations.  
Select encryption algorithms  
AES256 X

**Phase 2 encryption algorithms**  
The permitted encryption algorithms for the VPN tunnel for phase 2 IKE negotiations.  
Select encryption algorithms

*Use the Options in the Screenshot and remove the other ones as per below*

aws [Search] [Option+S] United States (N. Virginia) Cybrysis Admin

VPC > VPN connections > Create VPN connection

**Phase 2 encryption algorithms**  
The permitted encryption algorithms for the VPN tunnel for phase 2 IKE negotiations.  
Select encryption algorithms  
AES256 X

**Phase 1 integrity algorithms**  
The permitted integrity algorithms for the VPN tunnel for phase 1 IKE negotiations.  
Select integrity algorithms  
SHA2-256 X

**Phase 2 integrity algorithms**  
The permitted integrity algorithms for the VPN tunnel for phase 2 IKE negotiations.  
Select integrity algorithms  
SHA2-256 X

**Phase 1 DH group numbers**  
The permitted Diffie-Hellman group numbers for the VPN tunnel for phase 1 IKE negotiations.  
Select DH group numbers  
14 X

**Phase 2 DH group numbers**  
The permitted Diffie-Hellman group numbers for the VPN tunnel for phase 2 IKE negotiations.  
Select DH group numbers

aws [Search] [Option+S] United States (N. Virginia) Cybrysis Admin

VPC > VPN connections > Create VPN connection

**Phase 2 DH group numbers**  
The permitted Diffie-Hellman group numbers for the VPN tunnel for phase 2 IKE negotiations.  
Select DH group numbers  
14 X

**IKE Version**  
The internet key exchange (IKE) version permitted for the VPN tunnel.  
Select IKE Version  
ikev2 X

**Phase 1 lifetime (seconds)**  
The lifetime for phase 1 of the IKE negotiation, in seconds.  
28,800  
Supported values between: 900 and 28,800.

**Phase 2 lifetime (seconds)**  
The lifetime for phase 2 of the IKE negotiation, in seconds.  
3,600  
Supported values between: 900 and 3,600, has to be less than phase 1 lifetime.

**Rekey margin time (seconds)**  
The period of time before phase 1 and 2 lifetimes expire, during which AWS initiates an IKE rekey.  
270  
Supported values between: 60 and half of phase 2 lifetime.

**Rekey margin time (seconds)**  
The period of time before phase 1 and 2 lifetimes expires, during which AWS initiates an IKE rekey.  
270  
Supported values between: 60 and half of phase 2 lifetime.

**Rekey fuzz (percentage)**  
The percentage of the rekey window during which the rekey time is randomly selected.  
100  
Supported values between: 0 and 100.

**Replay window size (packets)**  
The number of packets in an IKE replay window.  
1024  
Supported values between: 64 and 2048.

**DPD timeout (seconds)**  
The number of seconds after which a DPD timeout occurs.  
30  
Supported values must be 30 or higher.

**DPD timeout action** | Info  
☒ Clear  
☐ Restart  
☐ None

**Startup action** | Info

*Leave out Tunnel 2, as we will be only doing this for one tunnel*

☐ Enable

**Tunnel maintenance**  
**Tunnel endpoint lifecycle control** | Info  
Tunnel endpoint lifecycle control provides control over the schedule of endpoint replacements.  
☐ Turn on

**Tunnel 2 options - optional** | Info  
Customize tunnel inside CIDR and pre-shared keys for your VPN tunnels. Unspecified tunnel options will be randomly generated by Amazon.

**Tags**  
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs. Name tag helps you track your resources more easily. We recommend adding Name tag.

**Key**  
Q Name X

**Value - optional**  
Q VPN-TO-OCI-VIA-TGW X Remove

Add new tag  
You can add up to 49 more tags.

Cancel Create VPN connection

*Once the VPN connection is completed, download the profile, by selecting the VPN connection and clicking Download configuration*

**VPN connections (1/2)** | Info | Actions | Download configuration | Create VPN connection

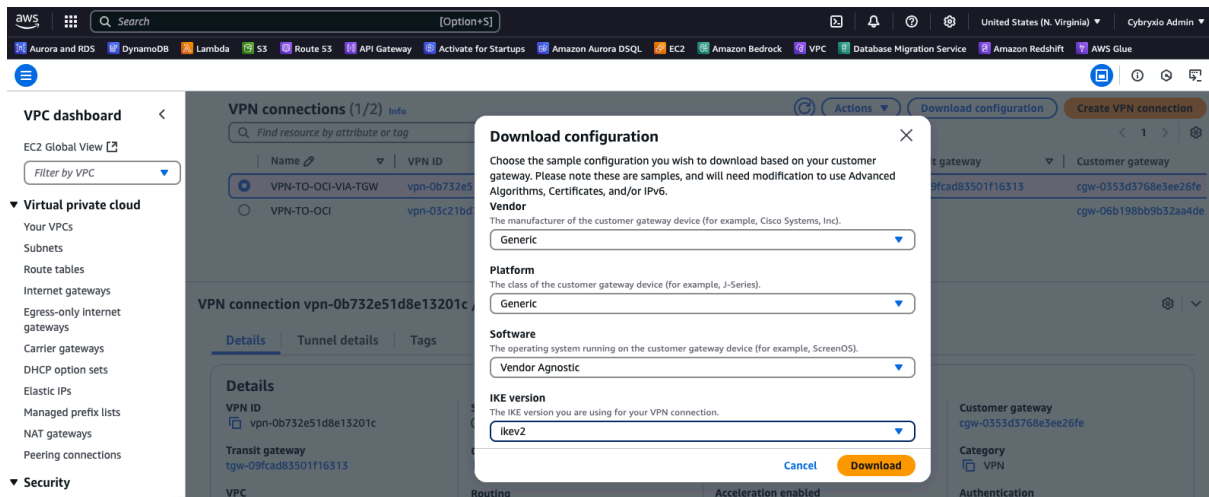
Name	VPN ID	State	Virtual private gateway	Transit gateway	Customer gateway
VPN-TO-OCI-VIA-TGW	vpn-0b732e51d8e13201c	Available	-	tgw-09fcad83501f16313	cgw-0353d3768e3ee26fe

**VPN connection vpn-0b732e51d8e13201c / VPN-TO-OCI-VIA-TGW**

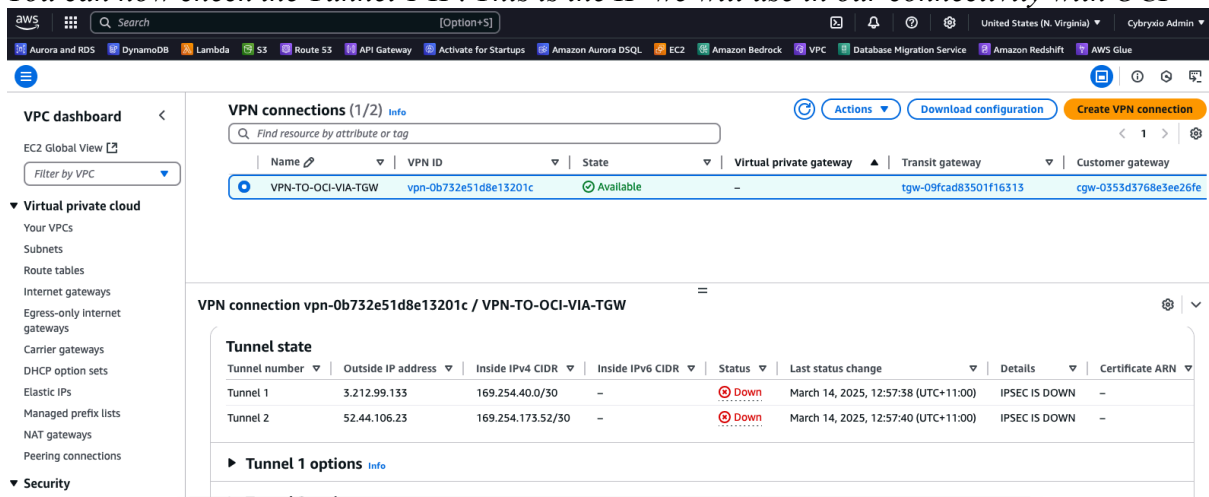
**Details** | Tunnel details | Tags

<b>VPN ID</b> vpn-0b732e51d8e13201c	<b>State</b> Available	<b>Virtual private gateway</b> -	<b>Customer gateway</b> cgw-0353d3768e3ee26fe
<b>Transit gateway</b> tgw-09fcad83501f16313	<b>Customer gateway address</b> 1.1.1.1	<b>Type</b> Ipsec.1	<b>Category</b> VPN
<b>VPC</b>	<b>Routing</b>	<b>Acceleration enabled</b>	<b>Authentication</b>

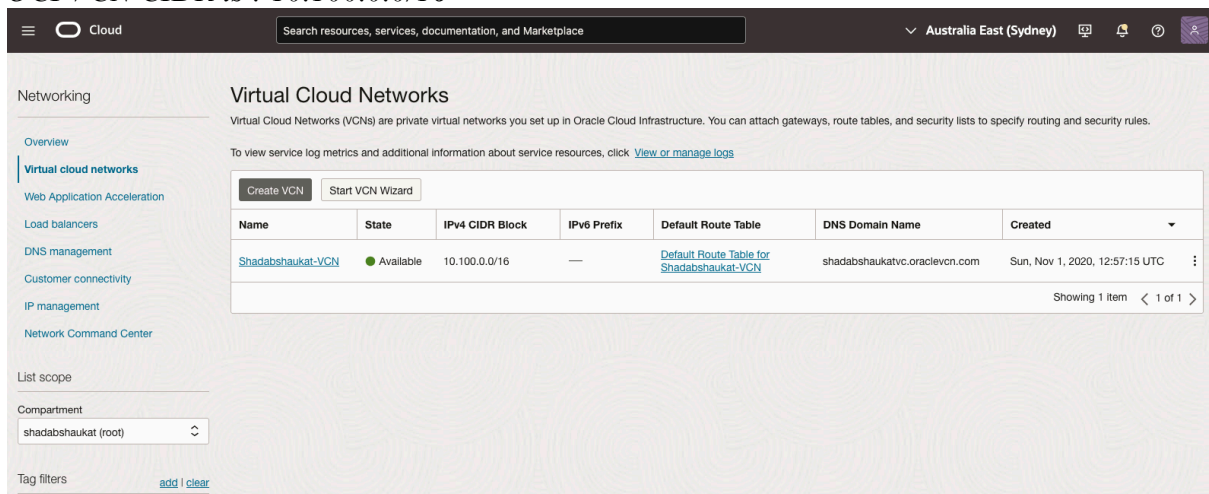
*Download Configuration*



*You can now check the Tunnel 1 IP. This is the IP we will use in our connectivity with OCI*



*4. Add your OCI VCN Routes to the Subnet in your AWS VPC*  
*OCI VCN CIDR is : 10.100.0.0/16*



*Add 10.100.0.0/16 to AWS VPC Subnet's **Route Table***

aws [Search] [Option+S] United States (N. Virginia) Cybrysis Admin

**VPC dashboard** EC2 Global View Filter by VPC

**Virtual private cloud** Your VPCs Subnets **Route tables** Internet gateways Egress-only internet gateways Carrier gateways DHCP option sets Elastic IPs Managed prefix lists NAT gateways Peering connections

**Security**

**Route tables (1)** Info Last updated about 3 hours ago Actions Create route table

Find resources by attribute or tag

Name	Route table ID	Explicit subnet associ...	Edge associations	Main	VPC
-	rtb-0041609d91503c97b	-	-	Yes	vpc-0b6de2f65f971840b

Select a route table

aws [Search] [Option+S] United States (N. Virginia) Cybrysis Admin

VPC > Route tables > rtb-0041609d91503c97b > Edit routes

**Edit routes**

Destination	Target	Status	Propagated
172.31.0.0/16	local	Active	No
10.230.0.0/16	Virtual Private Gateway	Active	No
0.0.0.0/0	Internet Gateway	Active	No
10.100.0.0/16	Transit Gateway	-	No

Add route

Cancel Preview Save changes

aws [Search] [Option+S] United States (N. Virginia) Cybrysis Admin

VPC > Route tables > rtb-0041609d91503c97b

**VPC dashboard** EC2 Global View Filter by VPC

**Virtual private cloud** Your VPCs Subnets **Route tables** Internet gateways Egress-only internet gateways Carrier gateways DHCP option sets Elastic IPs Managed prefix lists NAT gateways Peering connections

**Security**

**rtb-0041609d91503c97b** ACTIONS

**Details** Info

Route table ID rtb-0041609d91503c97b	Main Yes	Explicit subnet associations -	Edge associations -
VPC vpc-0b6de2f65f971840b	Owner ID 241526791455		

**Routes** Subnet associations Edge associations Route propagation Tags

**Routes (4)** Both Edit routes

Filter routes

Destination	Target	Status	Propagated
0.0.0.0/0	lgw-0f9fc5ac8461e59ca	Active	No
10.100.0.0/16	tgw-09fcad83501f16313	Active	No
10.230.0.0/16	vgw-0ce14a175ddc623c0	Active	No
172.31.0.0/16	local	Active	No

5. Add a DRG on OCI and Attach your VCN to it

Cloud

Search resources, services, documentation, and Marketplace

Australia East (Sydney)

Networking > Customer connectivity > Dynamic routing gateways

### Customer connectivity

- Overview
- Site-to-Site VPN
- FastConnect
- Dynamic routing gateway**
- Customer-premises equipment

List scope

Compartment: shadabshaukat (root)

Tag filters: [add](#) | [clear](#)

no tag filters applied

## Dynamic routing gateways

Dynamic routing gateways (DRGs) are optional virtual routers that you can add to your VCN. They provide a path for private network traffic between your VCN and on-premises network.

Create dynamic routing gateway

Name	Lifecycle state	Oracle redundancy status	Created
<a href="#">Shadab-DRG</a>	Available	—	Thu, Mar 13, 2025, 06:18:37 UTC

Showing 1 item < 1 of 1 >

Cloud

Search resources, services, documentation, and Marketplace

Australia East (Sydney)

Networking > Customer connectivity > Dynamic routing gateways > Shadab-DRG

## Shadab-DRG

DRG

AVAILABLE

Dynamic routing gateway information

Compartment: shadabshaukat (root)

Oracle redundancy status: —

VCN attachments in shadabshaukat (root) *Compartment*

VCNs are connected to a DRG by an attachment with the VCN type. You can configure all VCNs to use the same route table. [Learn more](#).

Create virtual cloud network attachment

Attachment name:

Virtual cloud network in shadabshaukat (root) [\(Change compartment\)](#)

Shadabshaukat-VCN

[Show Advanced options](#)

Create VCN attachment Cancel

Cloud

Search resources, services, documentation, and Marketplace

Australia East (Sydney)

Networking > Customer connectivity > Dynamic routing gateways > Shadab-DRG

## Shadab-DRG

DRG

AVAILABLE

Dynamic routing gateway information

Compartment: shadabshaukat (root)

Oracle redundancy status: —

OCID: ...nkp2bppqoa [Show](#) [Copy](#)

Created: Thu, Mar 13, 2025, 06:18:37 UTC

VCN attachments in shadabshaukat (root) *Compartment*

VCNs are connected to a DRG by an attachment with the VCN type. You can configure all VCNs to use the same route table. [Learn more](#).

Create virtual cloud network attachment

Attachment name	Lifecycle state	Virtual cloud network	DRG route table	VCN route type	Created
<a href="#">drgattachment20250313061949</a>	Attached	Shadabshaukat-VCN	<a href="#">Autogenerated Drg Route Table for VCN attachments</a>	Subnet CIDR blocks	Thu, Mar 13, 2025, 06:19:49 UTC

6. Add your AWS VPC CIDR to Route tables on OCI

AWS VPC CIDR is 172.31.0.0/16

**Virtual private cloud**

**Your VPCs**

Name	VPC ID	State	Block Public...	IPv4 CIDR	IPv6 CIDR
-	vpc-0b6de2f65f971840b	Available	Off	172.31.0.0/16	-

**vpc-0b6de2f65f971840b**

**Details**

VPC ID	State	Block Public Access	DNS hostnames
vpc-0b6de2f65f971840b	Available	Off	Enabled

## Add Route Table Rule on OCI VCN Subnet

**Add Route Rules**

**Important:**  
For a route rule that targets a Private IP, you must first enable "Skip Source/Destination Check" on the VNIC that the Private IP is assigned to.

**Route Rule**

Target Type: Dynamic Routing Gateway

Destination Type: CIDR Block

Destination CIDR Block: 172.31.0.0/16

Target Dynamic Routing Gateway in shadabshaukat (root): Shadab-DRG

**Add Route Rules** **Cancel**

## 7. Create Customer Premise Equipment on OCI

**Customer-premises equipment in shadabshaukat (root) Compartment**

Configure your on-premises device (the customer-premises equipment, or CPE) at your end of the Site-to-Site VPN so traffic can flow between your on-premises network and virtual cloud network (VCN).

**Create CPE**

Name	IP address	Created
No items found.		

Showing 0 items < 1 of 1 >

Use the Public IP address of your Tunnel 1 which we provisioned earlier 3.212.99.133



**Create CPE**

Name: CPE-AWS-TGW

Create in compartment: shadabshaukat (root)

☐ Allow IPsec over FastConnect

Public IP address: 3.212.99.133

CPE vendor information: Other

Buttons: Create CPE, Save as stack, Cancel

## 8. Create Site-to-Site VPN on OCI

**Site-to-Site VPN in shadabshaukat (root) Compartment**

Site-to-Site VPN securely connects your on-premises corporate network to Oracle Cloud Infrastructure, using your existing internet connection.

If your users have client devices that need offsite access to Oracle Cloud resources, you can also create an OpenVPN access server. See their [marketplace solution](#).

Buttons: Create IPsec connection, Start VPN wizard

Name	Lifecycle state	Customer-premises equipment	Dynamic routing gateway	Created
No items found.				

Showing 0 items < 1 of 1 >

**Create IPsec connection**

Name: VPN-TO-AWS-TGW

Create in compartment: shadabshaukat (root)

Customer-premises equipment in shadabshaukat (root) (Change compartment): CPE-AWS-TGW (3.212.99.133)

☐ This CPE is behind a NAT device

Dynamic routing gateway compartment in shadabshaukat (root) (Change compartment): Shadab-DRG

Note: This will create an attachment to the DRG for each IPsec tunnel. The attachment has the type IPSEC\_TUNNEL, and uses the default route table for that attachment type.

Buttons: Create IPsec connection, Cancel

*AWS BGP ASN is 64512.*

**Create IPsec connection**

Device with static routes to the VCN's subnets.

BGP ASN  
64512

IPv4 inside tunnel interface - CPE  
169.254.40.1/30  
Provide IPv4 CIDR block. Example: 10.0.0.0/30

IPv4 inside tunnel interface - Oracle  
169.254.40.2/30  
Provide IPv4 CIDR block. Example: 10.0.0.0/31

☐ IPv6 addressing

[Hide advanced options](#)

Oracle IKE initiation  
Initiator or responder

[Create IPsec connection](#) [Cancel](#)

Show advanced option

Go-to 'Phase one (ISAKMP) configuration'

**Create IPsec connection**

Oracle IKE initiation  
Initiator or responder

NAT-T enabled  
Auto

Enable dead peer detection timeout  
Initiate and respond

Dead peer detection timeout in seconds  
20

**Phase one (ISAKMP) configuration**

Internet security association and key management protocol (ISAKMP) is a protocol for establishing security associations and cryptographic keys. [Learn more](#)

☒ Set custom configurations

[Create IPsec connection](#) [Cancel](#)

**Create IPsec connection**

**Phase two (IPsec) configuration**

Internet protocol security (IPsec) authenticates and encrypts data packets to provide secure encrypted communication. [Learn more](#)

☒ Set custom configurations

Custom encryption algorithm  
AES\_256\_CBC

Custom authentication algorithm  
HMAC\_SHA2\_256\_128

IPsec session key lifetime in seconds  
3600

☒ Enable perfect forward secrecy

Perfect forward secrecy Diffie-Hellman group  
GROUP14

[Create IPsec connection](#) [Cancel](#)



Do the same for Tunnel 2 - Phase one and two (ISAKMP) configuration.

**Important Note: We're only going to configure this for Tunnel 1 on AWS to Tunnel 2 on OCI. For redundancy you need to create a second Site to Site VPN on AWS and map to Tunnel 2 on OCI.**

The screenshot shows the 'Create IPSec connection' page in the OCI console for 'Tunnel 2'. The left sidebar shows the navigation menu with 'Site-to-Site VPN' selected. The main content area has a 'Name' field and a 'Lifecycle state' dropdown. Below these are three options for 'Routing type': 'BGP dynamic routing' (selected with a checkmark), 'Static routing', and 'Policy based routing'. Each option has a brief description. At the bottom, there is a 'BGP ASN' field and 'Create IPSec connection' and 'Cancel' buttons.

This screenshot shows the 'Create IPSec connection' page for 'Tunnel 2' with the 'BGP dynamic routing' option selected. The 'BGP ASN' field is populated with '64512'. Below it are fields for 'IPv4 inside tunnel interface - CPE' (169.254.69.1/30) and 'IPv4 inside tunnel interface - Oracle' (169.254.69.2/30). There are also fields for 'Provide IPv4 CIDR block' with example values. A 'Hide advanced options' link is visible. At the bottom are 'Create IPSec connection' and 'Cancel' buttons.

This screenshot shows the 'Create IPSec connection' page for 'Tunnel 2' with the 'Hide advanced options' link expanded. It reveals additional configuration fields: 'Oracle IKE initiation' (set to 'Initiator or responder'), 'NAT-T enabled' (set to 'Auto'), 'Enable dead peer detection timeout' (set to 'Initiate and respond'), and 'Dead peer detection timeout in seconds' (set to '20'). At the bottom are 'Create IPSec connection' and 'Cancel' buttons.

Cloud

Search resources, services, documentation, and Marketplace

Australia East (Sydney)

Networking > Customer connectivity > Site-to-Site VPN

Customer connectivity

Overview

Site-to-Site VPN

FastConnect

Dynamic routing gateway

Customer-premises equipment

List scope

Compartment

Filters

Dynamic routing gateway in shadabshaukat (root)

Site-to-Site VPN in shadabshaukat (root)

Site-to-Site VPN securely connects your on-premises network to a virtual private cloud (VPC) in Oracle Cloud. If your users have client devices that need to connect to the VPC, you can use Site-to-Site VPN to create a secure connection.

Create IPsec connection

Start

Name

Lifecycle state

Create IPsec connection

Cancel

Create IPsec connection

Phase one (ISAKMP) configuration

Internet security association and key management protocol (ISAKMP) is a protocol for establishing security associations and cryptographic keys. [Learn more](#)

Set custom configurations

Custom encryption algorithm

AES\_256\_CBC

Custom authentication algorithm

SHA2\_256

Custom Diffie-Hellman group

GROUP14

IKE session key lifetime in seconds

28800

Cloud

Search resources, services, documentation, and Marketplace

Australia East (Sydney)

Networking > Customer connectivity > Site-to-Site VPN

Customer connectivity

Overview

Site-to-Site VPN

FastConnect

Dynamic routing gateway

Customer-premises equipment

List scope

Compartment

Filters

Dynamic routing gateway in shadabshaukat (root)

Site-to-Site VPN in shadabshaukat (root)

Site-to-Site VPN securely connects your on-premises network to a virtual private cloud (VPC) in Oracle Cloud. If your users have client devices that need to connect to the VPC, you can use Site-to-Site VPN to create a secure connection.

Create IPsec connection

Start

Name

Lifecycle state

Create IPsec connection

Cancel

Create IPsec connection

Phase two (IPsec) configuration

Internet protocol security (IPsec) authenticates and encrypts data packets to provide secure encrypted communication. [Learn more](#)

Set custom configurations

Custom encryption algorithm

AES\_256\_CBC

Custom authentication algorithm

HMAC\_SHA2\_256\_128

IPsec session key lifetime in seconds

3600

Enable perfect forward secrecy

Perfect forward secrecy Diffie-Hellman group

GROUP14

Go to Tunnel 1 and copy the Shared Secret

Cloud

Search resources, services, documentation, and Marketplace

Australia East (Sydney)

Networking > Customer connectivity > Site-to-Site VPN > VPN-TO-AWS-TGW

VPN-TO-AWS-TGW

Edit

Choose new compartment

Add tags

Open CPE configuration helper

Terminate

IPsec connection information

CPE & tunnels information

Tags

Static route CIDR block: -1

Created: Fri, Mar 14, 2025, 03:47:33 UTC

Site-to-Site VPN version: v2 1

OCID: ...2y46pa Show Copy

DRG: Shadab-DRG

CPE: CPE-AWS-TGW

Tunnels in shadabshaukat (root) Compartment

Name	Lifecycle state 1	IPsec status 1	Oracle VPN IP address	IPv4 BGP status 1	IPv6 BGP status 1	Routing type
ipsectunnel20250314034733-2	Available	Down	152.67.117.68	Down	Down	BGP dynamic routing
ipsectunnel20250314034733-1	Available	Down	152.67.119.165	Down	Down	BGP dynamic routing

Cloud Search resources, services, documentation, and Marketplace Australia East (Sydney)

[View documentation](#)

## ipsectunnel20250314034733-1

AVAILABLE Edit Open CPE configuration helper

**Tunnel information** Phase details

**IPSec status:** Down

**IPv4 BGP status:** Down

**IPv6 BGP status:** Down

**IKE version:** IKEv2

**Created:** Fri, Mar 14, 2025, 03:47:33 UTC

**OCID:** ...qonmaq Show Copy

**Routing type:** BGP dynamic routing

**Oracle BGP ASN:** 31898

**Customer BGP ASN:** 64512

**IPv4 inside tunnel interface - CPE:** 169.254.40.1/30

**IPv4 inside tunnel interface - Oracle:** 169.254.40.2/30

**IPv6 inside tunnel interface - CPE:** -

**IPv6 inside tunnel interface - Oracle:** -

**Shared secret:** \*\*\*\*\* Show Edit

**Oracle can initiate:** INITIATOR\_OR\_RESPONDER

**NAT-T enabled:** AUTO

**Dead peer detection mode:** INITIATE\_AND\_RESPOND

**DPD timeout in seconds:** 20

Cloud Search resources, services, documentation, and Marketplace Australia East (Sydney)

[Networking](#) > [Customer connectivity](#) > [Site-to-Site VPN](#) > [VPN-TO-AWS-TGW](#) > ipsectunnel20250314034733-1

**Tunnel down**

**Error:** IKE SA not established; IPsec SA not established

**Tunnel down since:** Fri, Mar 14, 2025, 04:25:26 UTC

**Issue/Action:** The DRG has not received any IKE packets from the CPE. Please check the CPE configuration.

[View documentation](#)

**ipsectunnel20250314034733-1**

AVAILABLE Edit Open CPE configuration helper

**Tunnel information** Phase details

**IPSec status:** Down

**IPv4 BGP status:** Down

**IPv6 BGP status:** Down

**Oracle BGP ASN:** 31898

**Customer BGP ASN:** 64512

**IPv4 inside tunnel interface - CPE:** 169.254.40.1/30

**IPv4 inside tunnel interface - Oracle:** 169.254.40.2/30

**IPv6 inside tunnel interface - CPE:** -

**IPv6 inside tunnel interface - Oracle:** -

### View shared secret

Shared secret Read-only

ZEQ8onuquzcDmLPkdopBNcghBg58k9hxnPQhaNPH3cX3qYS3axPd3j

Close Cancel

## 9. Go back to AWS Console and Create new Customer Gateway with Public IP of OCI Tunnel 1 152.67.119.165 and Oracle ASN 31898

aws Search [Option+5] United States (N. Virginia) Cyberata Admin

[VPC](#) > [Customer gateways](#) > Create customer gateway

### Create customer gateway Info

A customer gateway is a resource that you create in AWS that represents the customer gateway device in your on-premises network.

**Details**

**Name tag - optional**  
Creates a tag with a key of 'Name' and a value that you specify.

Value must be 256 characters or less in length.

**BGP ASN** Info  
The ASN of your customer gateway device.

Value must be in 1 - 4294967294 range.

**IP address** Info  
Specify the IP address for your customer gateway device's external interface.

**Certificate ARN - optional**  
The ARN of a private certificate provisioned in AWS Certificate Manager (ACM).

Select certificate ARN

**Device - optional**  
Enter a name for the customer gateway device.

## Create Customer Gateway

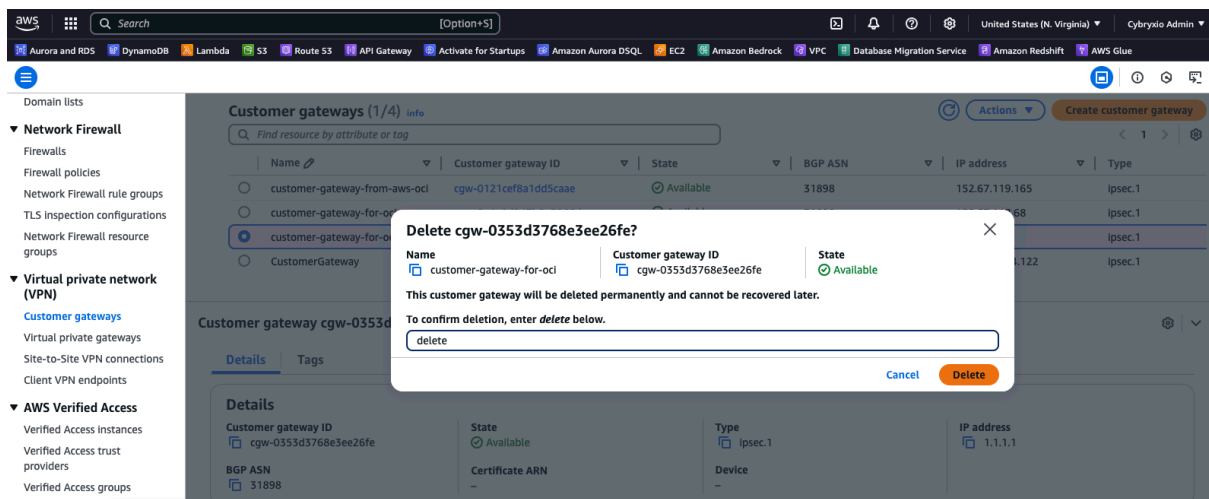
## Modify the VPN connection and add the new customer gateway

The screenshot shows the AWS Management Console interface for a VPN connection. The left sidebar contains navigation links for Rule groups, Domain lists, Network Firewall, Virtual private network (VPN), and AWS Verified Access. The main content area displays the details of the VPN connection **vpn-0b732e51d8e13201c / VPN-TO-OCI-VIA-TGW**. The details are organized into sections: **Details** (VPN ID, State, Transit gateway, VPC, Local IPv4 network CIDR, Remote IPv4 network CIDR, Core network ARN), **Virtual private gateway** (Type, Acceleration enabled, Local IPv6 network CIDR, Gateway association state), and **Customer gateway** (cgw-0e4e1d847b9e3266d). The **Actions** menu is open, showing options like **Modify VPN connection**, **Modify VPN tunnel certificate**, **Modify VPN connection options**, **Modify VPN tunnel options**, **Replace VPN tunnel**, **Manage tags**, and **Delete VPN connection**.

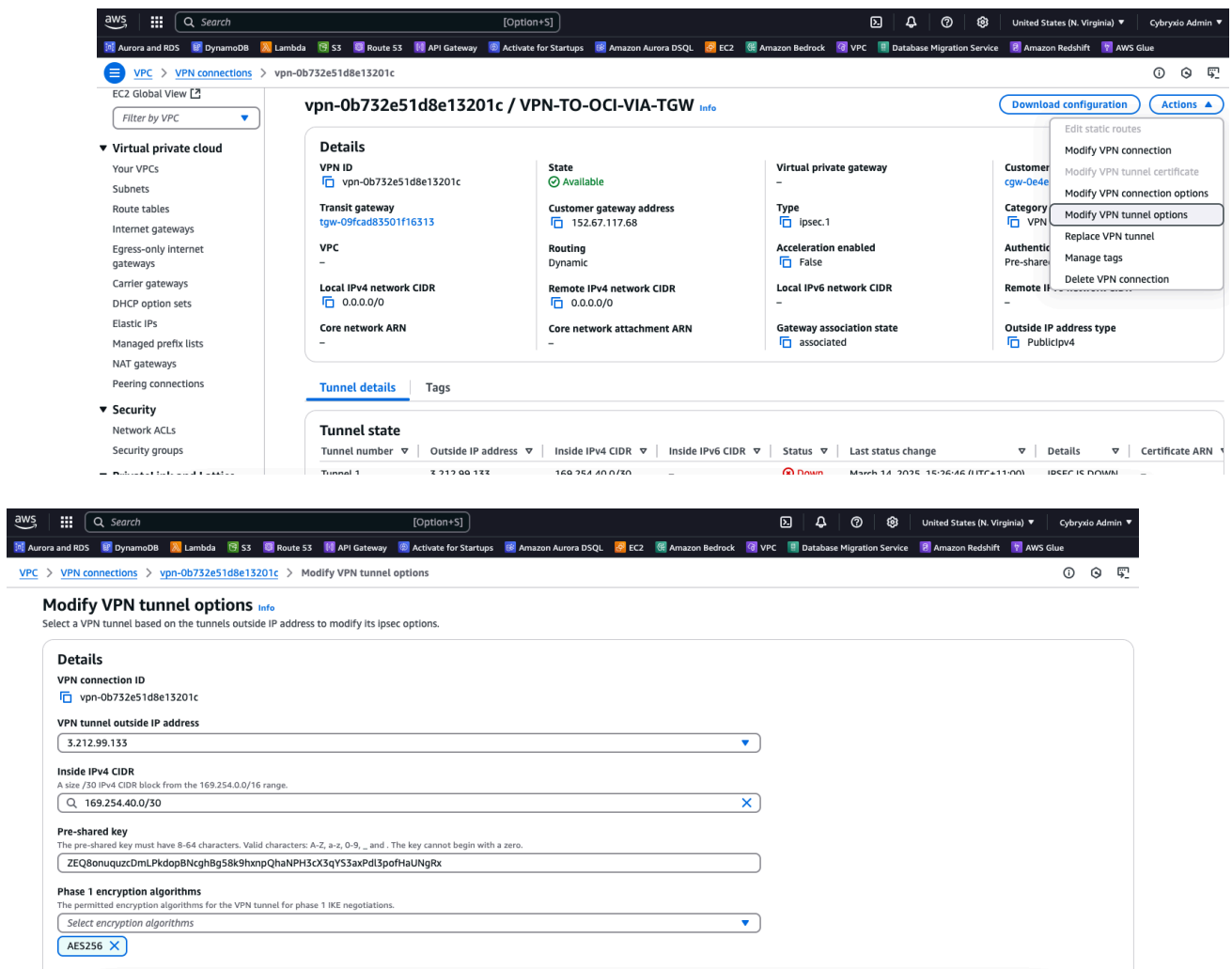
The screenshot shows the **Modify VPN connection** page in the AWS Management Console. The page displays the details of the VPN connection and the **Change target** section. The **Change target** section has two dropdown menus: **Target type** (set to **Customer gateway**) and **Target customer gateway** (set to **cgw-0121cef8a1dd5cae**). The **Save changes** button is highlighted in orange.

Save changes.

Make sure to delete the previous temporary customer gateway one after successfully adding new one.



10. Modify VPN Tunnel Options and Select Tunnel 1; Add the OCI VPN Tunnel 1 secret key and save changes



Wait for the 'modifying' to complete and VPN connection to be 'available' on AWS.

Now check the Tunnel Status on OCI and AWS. If everything was setup correctly, the Tunnel 1 on AWS will be connected to IPSEC VPN connection Tunnel on OCI.



Cloud Australia East (Sydney)

Networking > Customer connectivity > Site-to-Site VPN > VPN-TO-AWS-TGW

## VPN-TO-AWS-TGW

**IPC** AVAILABLE

Edit Choose new compartment Add tags Open CPE configuration helper Terminate

**IPSec connection information** CPE & tunnels information Tags

Static route CIDR block: - ⓘ OCID: ...2y46pa Show Copy  
 Created: Fri, Mar 14, 2025, 03:47:33 UTC DRG: Shadab-DRG  
 Site-to-Site VPN version: v2 ⓘ CPE: CPE-AWS-TGW

Resources

**Tunnels** (2)

Dynamic routing gateway attachments (2)

Logs

### Tunnels in shadabshaukat (root) Compartment

Name	Lifecycle state ⓘ	IPSec status ⓘ	Oracle VPN IP address	IPv4 BGP status ⓘ	IPv6 BGP status ⓘ	Routing type
ipsectunnel20250314034733-2	Available	Down	152.67.117.68	Down	Down	BGP dynamic routing
ipsectunnel20250314034733-1	Available	Down	152.67.119.165	Up	Down	BGP dynamic routing

Showing 2 items

aws Search [Option+] United States (N. Virginia) Cybriso Admin

Aurora and RDS DynamoDB Lambda S3 Route 53 API Gateway Activate for Startups Amazon Aurora D5QL EC2 Amazon Bedrock VPC Database Migration Service Amazon Redshift AWS Glue

VPC > VPN connections > vpn-0b732e51d8e13201c

### VPN dashboard

EC2 Global View [Filter by VPC](#)

Virtual private cloud

- Your VPCs
- Subnets
- Route tables
- Internet gateways
- Egress-only internet gateways
- Carrier gateways
- DHCP option sets
- Elastic IPs
- Managed prefix lists
- NAT gateways
- Peering connections

Security

**Transit gateway**  
tgw-09fcd83501f16313

**VPC**  
-

**Local IPv4 network CIDR**  
0.0.0.0/0

**Core network ARN**  
-

**Customer gateway address**  
152.67.119.165

**Routing**  
Dynamic

**Remote IPv4 network CIDR**  
0.0.0.0/0

**Core network attachment ARN**  
-

**Type**  
Ipsec.1

**Acceleration enabled**  
False

**Local IPv6 network CIDR**  
-

**Gateway association state**  
associated

**Category**  
VPN

**Authentication**  
Pre-shared key

**Remote IPv6 network CIDR**  
-

**Outside IP address type**  
PublicIpv4

### Tunnel details

Tags

**Tunnel state**

Tunnel number	Outside IP address	Inside IPv4 CIDR	Inside IPv6 CIDR	Status	Last status change	Details	Certificate ARN
Tunnel 1	3.212.99.133	169.254.40.0/30	-	Up	March 14, 2025, 15:45:36 (UTC+11:00)	2 BGP ROUTES	-
Tunnel 2	52.44.106.23	169.254.173.52/30	-	Down	March 14, 2025, 15:43:18 (UTC+11:00)	IPSEC IS DOWN	-

► Tunnel 1 options

► Tunnel 2 options

11. Now we will Create the Cross-Region RPC from OCI Region Sydney to Melbourne

Create OCI VCN in Melbourne with CIDR 10.200.0.0/16

Cloud Australia Southeast (Melbourne)

Networking

Virtual Cloud Networks

Virtual Cloud Networks (VCNs) are private virtual networks you set up in Oracle Cloud Infrastructure. You can attach gateways, route tables, and security lists to specify routing and security rules.

To view service log metrics and additional information about service resources, click [View or manage logs](#).

Create VCN Start VCN Wizard

Name	State	IPv4 CIDR Block	IPv6 Prefix	Default Route Table	DNS Domain Name	Created
No items found.						

Showing 0 items < 1 of 1 >

List scope

Compartment  
shadabshaukat (root)

Tag filters  
add | clear

no tag filters applied

Filters

Cloud

Search resources, services, documentation, and Marketplace

Australia Southeast (Melbourne)

Networking

Overview

Virtual cloud networks

Web Application Acceleration

Load balancers

DNS management

Customer connectivity

IP management

Network Command Center

List scope

Compartment

shadabshaukat (root)

Tag filters

add | clear

no tag filters applied

Filters

Virtual Cloud Net

Virtual Cloud Networks (VCNs) are rules.

To view service log metrics and ad

Create VCN

Start VCN Wizard

Name	State

Start VCN Wizard

Cancel

Start VCN Wizard

Cancel

Cloud

Search resources, services, documentation, and Marketplace

Australia Southeast (Melbourne)

Create a VCN with internet connectivity

Help

1 Configuration

2 Review and create

Resource availability checked successfully.

Close

Basic information

VCN name

VCN-MELB

Compartment

shadabshaukat (root)

Configure VCN

VCN IPv4 CIDR block

10.200.0.0/16

IPv6 prefixes

Optional

☐ Enable IPv6 in this VCN

DNS resolution

☐ Use DNS resolution for this VCN

Includes:

- Virtual cloud network (VCN)
- Public subnet
- Private subnet
- Internet gateway (IG)
- NAT gateway (NAT)
- Service gateway (SG)

Next

Cancel

Cloud

Search resources, services, documentation, and Marketplace

Australia Southeast (Melbourne)

Create a VCN with internet connectivity

Help

1 Configuration

2 Review and create

Required for instance hostname assignment if you plan to use VCN DNS or a third-party DNS. This choice cannot be changed after the VCN is created. [Learn more.](#)

Configure public subnet

IP address type

IPv4 CIDR block

10.200.1.0/24

×

Example: 172.16.0.0/16.

(Maximum number of items added)

+ Another IP address type

Configure private subnet

IP address type

IPv4 CIDR block

10.200.2.0/24

×

Example: 172.16.0.0/16.

(Maximum number of items added)

+ Another IP address type

Next

Cancel

Cloud Search resources, services, documentation, and Marketplace Australia Southeast (Melbourne)

### Create a VCN with internet connectivity

Help

1 Configuration  
2 Review and create

#### Creating resources

VCN creation complete

▶ Create VCN (1 resolved)	Done	✓
▶ Create subnets (2 resolved)	Done	✓
▶ Create internet gateway (1 resolved)	Done	✓
▶ Create NAT gateway (1 resolved)	Done	✓
▶ Create service gateway (1 resolved)	Done	✓
▶ Create route table for private subnet (1 resolved)	Done	✓
▶ Create security list for private subnet (1 resolved)	Done	✓
▶ Update route tables (2 resolved)	Done	✓
▶ Update private subnet (1 resolved)	Done	✓

View VCN

*Add DRG in Melbourne region and Attach VCN*

Cloud Search resources, services, documentation, and Marketplace Australia Southeast (Melbourne)

Networking > Customer connectivity > Dynamic routing gateways

### Create dynamic routing gateway

Help

Customer connectivity

Overview  
Site-to-Site VPN  
FastConnect  
**Dynamic routing gateway**  
Customer-premises equipment

List scope

Compartment  
shadabshaukat (root)

Tag filters  
add | clear  
no tag filters applied

#### Dynamic routing

Dynamic routing gateways (DRGs)

Create dynamic routing gateway

Name

MEL-DRG

Create in compartment

shadabshaukat (root)

Show Advanced options

Create dynamic routing gateway Cancel



Cloud

Search resources, services, documentation, and Marketplace

Australia Southeast (Melbourne)

Networking > Customer connectivity > Dynamic routing gateways > MEL-DRG

DRG

AVAILABLE

Edit

Add tags

Move resource

Terminate

Dynamic routing gateway information

Tags

Compartment: shadabshaukat (root)

OCID: ...ff7ogt4lba Show Copy

Oracle redundancy status: —

Created: Sat, Mar 15, 2025, 04:39:24 UTC

Resources

VCN attachments (0)

Virtual circuit attachments (0)

IPSec tunnel attachments (0)

Remote peering connection attachments (0)

Loopback attachments (0)

Cross-tenancy attachments (0)

VCN attachments in shadabshaukat (root) Compartment

VCNs are connected to a DRG by an attachment with the VCN type. You can configure all VCNs to use the same route table. Learn more.

Create virtual cloud network attachment

Attachment name	Lifecycle state	Virtual cloud network	DRG route table	VCN route type	Created
No items found.					

Showing 0 items < 1 of 1 >

Cloud

Search resources, services, documentation, and Marketplace

Australia Southeast (Melbourne)

Networking > Customer connectivity > Dynamic routing gateways > MEL-DRG

DRG

AVAILABLE

Edit

Add tags

Move resource

Dynamic routing gateway

Tags

Compartment: shadabshaukat (root)

Oracle redundancy status: —

Resources

VCN attachments (0)

Virtual circuit attachments (0)

IPSec tunnel attachments (0)

Remote peering connection attachments (0)

Loopback attachments (0)

Cross-tenancy attachments (0)

Create VCN attachment

Attachment name *Optional*

Virtual cloud network in shadabshaukat (root) (Change compartment)

VCN-MELB

Show Advanced options

Create VCN attachment

Cancel

Cloud

Search resources, services, documentation, and Marketplace

Australia Southeast (Melbourne)

Networking > Customer connectivity > Dynamic routing gateways > MEL-DRG

DRG

AVAILABLE

Edit

Add tags

Move resource

Terminate

Dynamic routing gateway information

Tags

Compartment: shadabshaukat (root)

OCID: ...ff7ogt4lba Show Copy

Oracle redundancy status: —

Created: Sat, Mar 15, 2025, 04:39:24 UTC

Resources

VCN attachments (1)

Virtual circuit attachments (0)

IPSec tunnel attachments (0)

Remote peering connection attachments (0)

Loopback attachments (0)

Cross-tenancy attachments (0)

VCN attachments in shadabshaukat (root) Compartment

VCNs are connected to a DRG by an attachment with the VCN type. You can configure all VCNs to use the same route table. Learn more.

Create virtual cloud network attachment

Attachment name	Lifecycle state	Virtual cloud network	DRG route table	VCN route type	Created
<a>drgattachment20250315044021</a>	Attached	<a>VCN-MELB</a>	<a>Autogenerated Drg Route Table for VCN attachments</a>	Subnet CIDR blocks	Sat, Mar 15, 2025, 04:40:22 UTC

Showing 1 item < 1 of 1 >

Create Remote Peering Connection (RPC) in DRG in Melbourne

Cloud

Search resources, services, documentation, and Marketplace

Australia Southeast (Melbourne)

DRG

AVAILABLE

Resources

- VCN attachments (1)
- Virtual circuit attachments (0)
- IPSec tunnel attachments (0)
- Remote peering connection attachments (0)
- Loopback attachments (0)
- Cross-tenancy attachments (0)
- DRG route tables (2)

MEL-DRG

EditAdd tagsMove resourceTerminate

Dynamic routing gateway information

Tags

Compartment: shadabshaukat (root)

OCID: ...ff7ogt4lba Show Copy

Oracle redundancy status: —

Created: Sat, Mar 15, 2025, 04:39:24 UTC

Remote peering connection attachments in shadabshaukat (root) Compartment

Remote peering connection (RPC) attachments are automatically created when an RPC is created. You can't directly create additional attachments for an RPC.

Create remote peering connection

Attachment name	Lifecycle state	DRG route table	Remote peering connection	Peering status	Created
No items found.					

Showing 0 items < 1 of 1 >

Cloud

Search resources, services, documentation, and Marketplace

Australia Southeast (Melbourne)

DRG

AVAILABLE

Resources

- VCN attachments (1)
- Virtual circuit attachments (0)
- IPSec tunnel attachments (0)
- Remote peering connection attachments (0)
- Loopback attachments (0)
- Cross-tenancy attachments (0)
- DRG route tables (2)

MEL-DRG

EditAdd tagsMove resource

Dynamic routing gateway

Compartment: shadabshaukat (root)

Oracle redundancy status: —

Remote peering c

Remote peering connection (RPC)

Create remote peering connection

Attachment name

L

Create remote peering connection

Name

RPC-CONN-MELB

Create in compartment

shadabshaukat (root)

This creates an attachment to the selected DRG. The attachment uses a route table based on the type of resource using the attachment.

Show Advanced options

Create remote peering connection

Cancel

Cloud

Search resources, services, documentation, and Marketplace

Australia Southeast (Melbourne)

DRG

AVAILABLE

Resources

- VCN attachments (1)
- Virtual circuit attachments (0)
- IPSec tunnel attachments (0)
- Remote peering connection attachments (1)
- Loopback attachments (0)
- Cross-tenancy attachments (0)
- DRG route tables (2)

MEL-DRG

EditAdd tagsMove resourceTerminate

Dynamic routing gateway information

Tags

Compartment: shadabshaukat (root)

OCID: ...ff7ogt4lba Show Copy

Oracle redundancy status: —

Created: Sat, Mar 15, 2025, 04:39:24 UTC

Remote peering connection attachments in shadabshaukat (root) Compartment

Remote peering connection (RPC) attachments are automatically created when an RPC is created. You can't directly create additional attachments for an RPC.

Create remote peering connection

Attachment name	Lifecycle state	DRG route table	Remote peering connection	Peering status	Created
DRG Attachment for RPC: RPC-CONN-MELB	Attached	Autogenerated Drg Route Table for RPC, VCN, and IPSec attachments	RPC-CONN-MELB	New (not peered)	Sat, Mar 15, 2025, 04:47:30 UTC

Showing 1 item < 1 of 1 >

Create Remote Peering Connection (RPC) in DRG in Sydney

Go to Sydney DRG

Cloud

Search resources, services, documentation, and Marketplace

Australia East (Sydney)

Networking > Customer connectivity > Dynamic routing gateways

Customer connectivity

Overview

Site-to-Site VPN

FastConnect

Dynamic routing gateway

Customer-premises equipment

List scope

Compartment

shadabshaukat (root)

Tag filters

add | clear

no tag filters applied

Warning: Your connection to Oracle is at risk because of a redundancy issue related to a DRG below. Click the DRG and view its details for more information.

Dynamic routing gateways

Dynamic routing gateways (DRGs) are optional virtual routers that you can add to your VCN. They provide a path for private network traffic between your VCN and on-premises network.

Create dynamic routing gateway

Name	Lifecycle state	Oracle redundancy status	Created
Shadab-DRG	Available	Not redundant	Thu, Mar 13, 2025, 06:18:37 UTC

Showing 1 item < 1 of 1 >

Cloud

Search resources, services, documentation, and Marketplace

Australia East (Sydney)

Networking > Customer connectivity > Dynamic routing gateways > Shadab-DRG > Remote peering connection attachments

DRG

AVAILABLE

Edit

Add tags

Move resource

Terminate

Dynamic routing gateway information

Tags

Compartment: shadabshaukat (root)

OCID: ...nkp2bppqoa

Oracle redundancy status: Not redundant

Created: Thu, Mar 13, 2025, 06:18:37 UTC

Resources

VCN attachments (1)

Virtual circuit attachments (0)

IPSec tunnel attachments (2)

Remote peering connection attachments (0)

Warning: This IPSec connection has only a single active tunnel. Oracle recommends having redundant connections for high availability. Learn how to fix the problem

Shadab-DRG

Remote peering connection attachments in shadabshaukat (root) Compartment

Remote peering connection (RPC) attachments are automatically created when an RPC is created. You can't directly create additional attachments for an RPC.

Create remote peering connection

Attachment name	Lifecycle state	DRG route table	Remote peering connection	Peering status	Created
No items found.					

Showing 0 items < 1 of 1 >

Confidential- Oracle Internal

Cloud Australia East (Sydney)

Networking > Customer connectivity > Dynamic routing gateways > Shadab-DRG

### Create remote peering connection

Name: SYD-RPC-CONNECTION

Create in compartment: shadabshaukat (root)

This creates an attachment to the selected DRG. The attachment uses a route table based on the type of resource using the attachment.

Show Advanced options

Create remote peering connection Cancel

**DRG** AVAILABLE

Warning: This IPSec connection is not redundant.

Shadab-DRG

Edit Add tags Move resource

Dynamic routing gateway

Compartment: shadabshaukat

Oracle redundancy status: Not redundant

Resources

- VCN attachments (1)
- Virtual circuit attachments (0)
- IPSec tunnel attachments (2)
- Remote peering connection attachments (0)

Dynamic routing gateway information

Compartment: shadabshaukat (root) OCID: ...nkp2bppqoa Show Copy

Oracle redundancy status: Not redundant Created: Thu, Mar 13, 2025, 06:18:37 UTC

Remote peering connection attachments in shadabshaukat (root) Compartment

Remote peering connection (RPC) attachments are automatically created when an RPC is created. You can't directly create additional attachments for an RPC.

Create remote peering connection

Attachment name	Lifecycle state	DRG route table	Remote peering connection	Peering status	Created
DRG Attachment for RPC: SYD-RPC-CONNECTION	Attached	Autogenerated Drg Route Table for RPC, VCN, and IPSec attachments	SYD-RPC-CONNECTION	New (not peered)	Sat, Mar 15, 2025, 04:53:00 UTC

Showing 1 item 1 of 1

*Now click on the Sydney remote peering connection and establish connection with Melbourne RPC*

*First get OCID of the Melbourne RPC connection peer*

Networking > Customer connectivity > Dynamic routing gateways > MEL-DRG > Remote peering connections > RPC-CONN-MELB



AVAILABLE

## RPC-CONN-MELB

Establish connection Edit Terminate

### Remote peering connection Information

Compartment: shadabshaukat (root)

DRG OCID: ...ff7ogt4lba Show Copy

Peer status: ● New (not peered)

Peer region: —

Peer connection OCID: —

OCID: [ocid1.remotepeeringconnection.oc1.ap-melbourne-1.aaaaaaaiosamaw2xsr3dzg2t43wymrsaukdjsulgia44gim27nv5muosoq](#) Hide Copy

Created: Sat, Mar 15, 2025, 04:47:20 UTC

Cross-tenancy: No

Peer tenancy OCID: —

### Remote peering connection attachments

Attachment name	Lifecycle state	Dynamic routing gateways	DRG route table	Created
<a href="#">DRG Attachment for RPC: RPC-CONN-MELB</a>	● Attached	<a href="#">MEL-DRG</a>	<a href="#">Autogenerated Drg Route Table for RPC, VC, and IPSec attachments</a>	Sat, Mar 15, 2025, 04:47:30 UTC


Showing 1 item < 1 of 1

*ocid1.remotepeeringconnection.oc1.ap-melbourne-1.aaaaaaaiosamaw2xsr3dzg2t43wymrsaukdjsulgia44gim27nv5muosoq*

*Now go to Sydney RPC*

Cloud Search resources, services, documentation, and Marketplace Australia East (Sydney)

Networking > Customer connectivity > Dynamic routing gateways > Shadab-DRG > Remote peering connections > SYD-RPC-CONNECTION



AVAILABLE

## SYD-RPC-CONNECTION

Establish connection Edit Terminate

### Remote peering connection Information

Compartment: shadabshaukat (root)

DRG OCID: ...nkp2bppqoa Show Copy

Peer status: ● New (not peered)

Peer region: —

Peer connection OCID: —

OCID: ...dc6hz6fp3q Show Copy

Created: Sat, Mar 15, 2025, 04:52:57 UTC

Cross-tenancy: No

Peer tenancy OCID: —

### Remote peering connection attachments

Attachment name	Lifecycle state	Dynamic routing gateways	DRG route table	Created
<a href="#">DRG Attachment for RPC: SYD-RPC-CONNECTION</a>	● Attached	<a href="#">Shadab-DRG</a>	<a href="#">Autogenerated Drg Route Table for RPC, VC, and IPSec attachments</a>	Sat, Mar 15, 2025, 04:53:00 UTC

Showing 1 item < 1 of 1

*Click on Establish Connection and Add the Peer OCID :*



Cloud

Search resources, services, documentation, and Marketplace

Australia East (Sydney)

Networking > Customer connectivity > Dynamic routing gateways > Shadab-DRG > Remote peering connections > SYD-RPC-CONNECTION

## SYD-RPC-CONNECTION

Establish connection Edit Terminate

**RPC**

AVAILABLE

**Remote peering connection Information**

Compartment: shadabshaukat (root) OCID: ...dc6hz6fp3q Show Copy

DRG OCID: ...nkp2bppqoa Show Copy Created: Sat, Mar 15, 2025, 04:52:57 UTC

Peer status: ● New (not peered) Cross-tenancy: No

Peer region: — Peer tenancy OCID: ...3nv3quzhpq Show Copy

Peer connection OCID: —

**Remote peering connection attachments**

Attachment name	Lifecycle state	Dynamic routing gateways
<a href="#">DRG Attachment for RPC: SYD-RPC-CONNECTION</a>	● Attached	<a href="#">Shadab-DRG</a>

Establish connection Cancel

*If everything was setup properly the peer status will be green and 'Peered'*

Cloud

Search resources, services, documentation, and Marketplace

Australia East (Sydney)

Networking > Customer connectivity > Dynamic routing gateways > Shadab-DRG > Remote peering connections > SYD-RPC-CONNECTION

## SYD-RPC-CONNECTION

Establish connection Edit Terminate

**RPC**

AVAILABLE

**Remote peering connection Information**

Compartment: shadabshaukat (root) OCID: ...dc6hz6fp3q Show Copy

DRG OCID: ...nkp2bppqoa Show Copy Created: Sat, Mar 15, 2025, 04:52:57 UTC

Peer status: ● Peered Cross-tenancy: No

Peer region: ap-melbourne-1 Peer tenancy OCID: ...3nv3quzhpq Show Copy

Peer connection OCID: ...7nv5muosoq Show Copy

**Remote peering connection attachments**

Attachment name	Lifecycle state	Dynamic routing gateways	DRG route table	Created
<a href="#">DRG Attachment for RPC: SYD-RPC-CONNECTION</a>	● Attached	<a href="#">Shadab-DRG</a>	<a href="#">Autogenerated Drg Route Table for RPC, VC, and IPsec attachments</a>	Sat, Mar 15, 2025, 04:53:00 UTC

Showing 1 item < 1 of 1


*Your Routes for both Sydney and Melbourne VCN should be automatically published. You can go to VCN attachment in both regions DRG and check VCN Attachment's DRG Route Table*

Cloud

Search resources, services, documentation, and Marketplace

Australia Southeast (Melbourne)

Networking > Customer connectivity > Dynamic routing gateways > MEL-DRG > DRG route table details



AVAILABLE

Autogenerated Drg Route Table for VCN attachments

Edit

Get all route rules

Add tags

Delete

DRG route table information

Tags

Compartment: shadabshaukat (root)

OCID: ...tnf6o4us3q Show Copy

DRG: MEL-DRG

Import route distribution: Autogenerated Import Route Distribution for ALL routes

ECMP: Disabled

Created: Sat, Mar 15, 2025, 04:39:30 UTC

Resources

Static route rules (0)

Add static route rules

Edit

Remove

<input type="checkbox"/>	Destination CIDR block	Next hop attachment type	Next hop attachment name	Route status
No items found.				

0 selected

Showing 0 items < 1 of 1 >

Terms of Use and Privacy

Cookie Preferences

Copyright © 2025, Oracle and/or its affiliates. All rights reserved.

What's this? | Redwood preview

Cloud

Search resources, services, documentation, and Marketplace

Australia Southeast (Melbourne)

Get all route rules

Help

Filters

Route rules type

All

Next hop attachment type

All

Route status

All

Route rules for Autogenerated Drg Route Table for VCN attachments

Last checked: Sat, Mar 15, 2025, 05:09:23 UTC

Download route rules

Refresh table

Search by CIDR block

Type	Destination CIDR block	Next hop attachment type	Next hop attachment name	Route status
DYNAMIC	10.100.1.0/24	Remote Peering Connection	<a>DRG Attachment for RPC: RPC-CONN-MELB</a>	Active
DYNAMIC	10.100.2.0/24	Remote Peering Connection	<a>DRG Attachment for RPC: RPC-CONN-MELB</a>	Active
DYNAMIC	10.200.1.0/24	Virtual Cloud Network	<a>drgattachment20250315044021</a>	Active
DYNAMIC	10.200.2.0/24	Virtual Cloud Network	<a>drgattachment20250315044021</a>	Active

Showing 4 items < 1 of 1 >

Close

Terms of Use and Privacy

Cookie Preferences

Copyright © 2025, Oracle and/or its affiliates. All rights reserved.

What's this? | Redwood preview

*Configure DRG in OCI Sydney for Transit connectivity*

*Setup the DRG in Sydney for transit routing.*

*Since by default IPsec VPN and RPC are using the same DRG route, we will just modify the route. In real world production setup, you should have a separate route.*

Confidential- Oracle Internal

Cloud

Search resources, services, documentation, and Marketplace

Australia East (Sydney)

AVAILABLE

Dynamic routing gateway information

Tags

Compartment: shadabshaukat (root)OCID: ...nkp2bppqoa Show Copy

Oracle redundancy status: Not redundantCreated: Thu, Mar 13, 2025, 06:18:37 UTC

Resources

VCN attachments (1)

Virtual circuit attachments (0)

IPSec tunnel attachments (2)

Remote peering connection attachments (1)

Loopback attachments (0)

Cross-tenancy attachments (0)

DRG route tables (2)

Import route distributions (2)

Export route distributions (1)

Tag filters

add | clear

DRG route tables

A DRG route table manages routing within the DRG. Two route tables are automatically created for a new DRG, and you can create more route tables as needed. You can configure all resources of a certain type to use the same route table.

Create DRG route tableEdit default assignment

Name	Lifecycle state	Default for attachment types	Import route distribution	Created
Autogenerated Drg Route Table for RPC, VC, and IPSec attachments	Available	IPSec Tunnel, Virtual Circuit, Remote Peering Connection	Autogenerated Import Route Distribution for VCN Routes	Thu, Mar 13, 2025, 06:18:49 UTC
Autogenerated Drg Route Table for VCN attachments	Available	Virtual Cloud Network	Autogenerated Import Route Distribution for ALL routes	Thu, Mar 13, 2025, 06:18:49 UTC

Showing 2 items < 1 of 1 >

Terms of Use and Privacy

Cookie Preferences

Copyright © 2025, Oracle and/or its affiliates. All rights reserved.

What's this? | Redwood preview

Go to DRG in Sydney > DRG Route Table > 'Import Route Distribution' for 'RPC, VC and IPSec attachments'

Add 2 New Route Distribution Statements

Cloud

Search resources, services, documentation, and Marketplace

Australia East (Sydney)

RD

AVAILABLE

Autogenerated In

EditAdd tagsTerminate

Route distribution information

Compartment: shadabshaukatOCID: ...goeu6zphlq Show C

Resources

Route distribution statements (1)

Add route distribution statements

Priority

1

0 selected

Add route distribution statements

Cancel

Terms of Use and Privacy

Cookie Preferences

Copyright © 2025, Oracle and/or its affiliates. All rights reserved.

What's this? | Redwood preview

Add route distribution statements

Help

You can add up to 15 route distribution statements at a time.

Priority	Match type	Attachment type filter	DRG attachment in shadabshaukat (root) (Change compartment)	Action
10	Attachment	IPSec Tunnel	DRG Attachment for...	ACCEPT
20	Attachment	Remote Peering Co...	DRG Attachment for...	ACCEPT

+ Another statement



Cloud Australia East (Sydney)

Networking > Customer connectivity > Dynamic routing gateways > Dynamic routing gateways details > Import route distributions > Route distributions details

## Autogenerated Import Route Distribution for VCN Routes

**RD**  
AVAILABLE

Edit Add tags Terminate

Route distribution information Tags

Compartment: shadabshaukat (root)  
OCID: ...goeufzphlq Show Copy

Distribution type: IMPORT  
DRG: Shadab-DRG

### Route distribution statements

Import route distribution statements describe the advertisement of routes to attachments from their assigned route table. Learn more.

Add route distribution statements Edit Remove

Priority	Match type	Match criteria	Action
1	Attachment type	Virtual Cloud Network	ACCEPT
10	Attachment	<a>DRG Attachment for IPSec Tunnel: ipsectunnel20250314034733-1</a>	ACCEPT
20	Attachment	<a>DRG Attachment for RPC: SYD-RPC-CONNECTION</a>	ACCEPT

Terms of Use and Privacy Cookie Preferences Copyright © 2025, Oracle and/or its affiliates. All rights reserved. What's this? Redwood preview

*If you setup everything correctly in your Transit Gateway Route Tables you will see  
All routes of your 2 OCI Regions plus the AWS VPC route*

Aurora and RDS DynamoDB Lambda S3 Route 53 API Gateway Activate for Startups Amazon Aurora DSQL EC2 Amazon Bedrock VPC Database Migration Service Amazon

VPC > Transit gateway route tables > tgw-rtb-065873123199fb96c

Virtual private gateways  
Site-to-Site VPN connections  
Client VPN endpoints

▼ AWS Verified Access  
Verified Access instances  
Verified Access trust providers  
Verified Access groups  
Verified Access endpoints

▼ Transit gateways  
Transit gateways  
Transit gateway attachments  
Transit gateway policy tables  
Transit gateway route tables  
Transit gateway multicast

▼ Traffic Mirroring  
Mirror sessions  
Mirror targets  
Mirror filters

▼ Filter routes by CIDR (2)

**Exact CIDR**  
Select a valid IP4 or IPv6 CIDR.

**Longest prefix match**  
Enter a valid IP4 or IPv6 and press enter.

**Supernet of match**  
Select a valid IP4 or IPv6 CIDR.

**Subnet of match**  
Select a valid IP4 or IPv6 CIDR.

Routes (5) info

CIDR	Attachment ID	Resource ID	Resource type	Route type	R
<input type="checkbox"/> 10.100.1.0/24	<a>tgw-attach-0826fb2097ce1c62e</a>	<a>vpn-0b732e51d8e13201c3...</a>	VPN	Propagated	🟢
<input type="checkbox"/> 10.100.2.0/24	<a>tgw-attach-0826fb2097ce1c62e</a>	<a>vpn-0b732e51d8e13201c3...</a>	VPN	Propagated	🟢
<input type="checkbox"/> 10.200.1.0/24	<a>tgw-attach-0826fb2097ce1c62e</a>	<a>vpn-0b732e51d8e13201c3...</a>	VPN	Propagated	🟢
<input type="checkbox"/> 10.200.2.0/24	<a>tgw-attach-0826fb2097ce1c62e</a>	<a>vpn-0b732e51d8e13201c3...</a>	VPN	Propagated	🟢
<input type="checkbox"/> 172.31.0.0/16	<a>tgw-attach-0ea473f30c8380a66</a>	<a>vpc-0b6de2f65f971840b</a>	VPC	Propagated	🟢

*You can verify the same from Sydney DRG*

Cloud

Search resources, services, documentation, and Marketplace

Australia East (Sydney)

DRG

AVAILABLE

Resources

VCN attachments (1)

Virtual circuit attachments (0)

IPSec tunnel attachments (2)

Remote peering connection attachments (1)

Loopback attachments (0)

Cross-tenancy attachments (0)

DRG route tables (2)

Import route distributions (2)

Shadab-DRG

Edit

Add tags

Move resource

Terminate

Dynamic routing gateway information

Tags

Compartment: shadabshaukat (root)

OCID: ...nkp2bppqoa Show Copy

Oracle redundancy status: ⚠️ Not redundant

Created: Thu, Mar 13, 2025, 06:18:37 UTC

DRG route tables

A DRG route table manages routing within the DRG. Two route tables are automatically created for a new DRG, and you can create more route tables as needed. You can configure all resources of a certain type to use the same route table.

Create DRG route table

Edit default assignment

Name	Lifecycle state	Default for attachment types	Import route distribution	Created
<a href="#">Autogenerated Drg Route Table for RPC, VC, and IPSec attachments</a>	● Available	IPSec Tunnel, Virtual Circuit, Remote Peering Connection	<a href="#">Autogenerated Import Route Distribution for VCN Routes</a>	Thu, Mar 13, 2025, 06:18:49 UTC
<a href="#">Autogenerated Drg Route Table for VCN attachments</a>	● Available	Virtual Cloud Network	<a href="#">Autogenerated Import Route Distribution for ALL routes</a>	Thu, Mar 13, 2025, 06:18:49 UTC

Showing 2 items < 1 of 1 >

Terms of Use and Privacy

Cookie Preferences

Copyright © 2025, Oracle and/or its affiliates. All rights reserved.

What's this? Redwood preview

Cloud

Search resources, services, documentation, and Marketplace

Australia East (Sydney)

Get all route rules

Help

Filters

Route rules type

All

Next hop attachment type

All

Route status

All

Route rules for Autogenerated Drg Route Table for RPC, VC, and IPSec attachments

Last checked: Sat, Mar 15, 2025, 05:50:27 UTC

Download route rules

Refresh table

Search by CIDR block

Type	Destination CIDR block	Next hop attachment type	Next hop attachment name	Route status
DYNAMIC	10.100.1.0/24	Virtual Cloud Network	<a href="#">drgattachment20250313061949</a>	● Active
DYNAMIC	10.100.2.0/24	Virtual Cloud Network	<a href="#">drgattachment20250313061949</a>	● Active
DYNAMIC	10.200.1.0/24	Remote Peering Connection	<a href="#">DRG Attachment for RPC: SYD-RPC-CONNECTION</a>	● Active
DYNAMIC	10.200.2.0/24	Remote Peering Connection	<a href="#">DRG Attachment for RPC: SYD-RPC-CONNECTION</a>	● Active
DYNAMIC	172.31.0.0/16	IPSec Tunnel	<a href="#">DRG Attachment for IPSec Tunnel: ipsectunnel20250314034733-1</a>	● Active

Showing 5 items < 1 of 1 >

Close

Terms of Use and Privacy

Cookie Preferences

Copyright © 2025, Oracle and/or its affiliates. All rights reserved.

What's this? Redwood preview

Do the same from Melbourne DRG

Cloud

Search resources, services, documentation, and Marketplace

Australia Southeast (Melbourne)

Networking > Customer connectivity > Dynamic routing gateways > MEL-DRG

DRG

AVAILABLE

Edit

Add tags

Move resource

Terminate

Dynamic routing gateway information

Tags

Compartment: shadabshaukat (root)

OCID: ...ff7ogt4lba Show Copy

Oracle redundancy status: —

Created: Sat, Mar 15, 2025, 04:39:24 UTC

Resources

VCN attachments (1)

Virtual circuit attachments (0)

IPSec tunnel attachments (0)

Remote peering connection attachments (1)

Loopback attachments (0)

Cross-tenancy attachments (0)

VCN attachments in shadabshaukat (root) Compartment

VCNs are connected to a DRG by an attachment with the VCN type. You can configure all VCNs to use the same route table. [Learn more.](#)

Create virtual cloud network attachment

Attachment name	Lifecycle state	Virtual cloud network	DRG route table	VCN route type	Created
<a href="#">drgattachment20250315044021</a>	Attached	<a href="#">VCN-MELB</a>	<a href="#">Autogenerated Drg Route Table for VCN attachments</a>	Subnet CIDR blocks	Sat, Mar 15, 2025, 04:40:22 UTC

Showing 1 item < 1 of 1 >

Terms of Use and Privacy

Cookie Preferences

Copyright © 2025, Oracle and/or its affiliates. All rights reserved.

What's this? | Redwood preview

Cloud

Search resources, services, documentation, and Marketplace

Australia Southeast (Melbourne)

Networking > Customer connectivity > Dynamic routing gateways > MEL-DRG > DRG route table details

DRT

AVAILABLE

Edit

Get all route rules

Add tags

Delete

DRG route table information

Tags

Compartment: shadabshaukat (root)

OCID: ...tnf6c4us3q Show Copy

DRG: [MEL-DRG](#)

Import route distribution: [Autogenerated Import Route Distribution for ALL routes](#)

ECMP: Disabled

Created: Sat, Mar 15, 2025, 04:39:30 UTC

Resources

Static route rules (0)

Autogenerated Drg Route Table for VCN attachments

Static route rules define the priority of routes between the DRG and attached VCNs, Site-to-Site VPN IPSec tunnels, FastConnect virtual circuits, and remote peering connections to other DRGs. A DRG route table routes packets inside the DRG, while a VCN route table assigned to a subnet only routes traffic leaving that subnet. If you're having problems, use [Network Path Analyzer](#) to check your connections.

Add static route rules

Edit

Remove

Destination CIDR block	Next hop attachment type	Next hop attachment name	Route status
No items found.			

0 selected

Showing 0 items < 1 of 1 >

Terms of Use and Privacy

Cookie Preferences

Copyright © 2025, Oracle and/or its affiliates. All rights reserved.

What's this? | Redwood preview

Cloud

Search resources, services, documentation, and Marketplace

Australia Southeast (Melbourne)

Help

Get all route rules

Filters

Route rules type

All

Next hop attachment type

All

Route status

All

Route rules for Autogenerated Drg Route Table for VCN attachments

Last checked: Sat, Mar 15, 2025, 05:52:12 UTC

Download route rules

Refresh table

Search by CIDR block

Type	Destination CIDR block	Next hop attachment type	Next hop attachment name	Route status
DYNAMIC	10.100.1.0/24	Remote Peering Connection	<a href="#">DRG Attachment for RPC: RPC-CONN-MELB</a>	Active
DYNAMIC	10.100.2.0/24	Remote Peering Connection	<a href="#">DRG Attachment for RPC: RPC-CONN-MELB</a>	Active
DYNAMIC	10.200.1.0/24	Virtual Cloud Network	<a href="#">drgattachment20250315044021</a>	Active
DYNAMIC	10.200.2.0/24	Virtual Cloud Network	<a href="#">drgattachment20250315044021</a>	Active
DYNAMIC	172.31.0.0/16	Remote Peering Connection	<a href="#">DRG Attachment for RPC: RPC-CONN-MELB</a>	Active

Showing 5 items < 1 of 1 >

Close

Terms of Use and Privacy

Cookie Preferences

Copyright © 2025, Oracle and/or its affiliates. All rights reserved.

What's this?

Ref: <https://ystatit.medium.com/azure-ipsec-vpn-to-oci-plus-oci-remote-peering-0b09e62e50a2>

Ensure AWS VPC Route Table has your routes for Sydney and Melbourne VPC added

aws

Search

[Option+S]

United States (N. Virginia)

Cybrxio Admin

Aurora and RDS

DynamoDB

Lambda

S3

Route 53

API Gateway

Activate for Startups

Amazon Aurora DSQL

EC2

Amazon Bedrock

VPC

Database Migration Service

Amazon Redshift

AWS Glue

VPC > Route tables > rtb-0041609d91503c97b > Edit routes

Edit routes

Destination	Target	Status	Propagated
172.31.0.0/16	local	Active	No
	local		
10.100.0.0/16	Transit Gateway	Active	No
	tgw-09fcad83501f16313		
10.230.0.0/16	Virtual Private Gateway	Active	No
	vgw-0ce14a175ddc623c0		
0.0.0.0/0	Internet Gateway	Active	No
	igw-0f9fc5ac8461e59ca		
10.200.0.0/16	Transit Gateway	-	No
	tgw-09fcad83501f16313		

Add route

Cancel Preview Save changes

CloudShell

Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

aws

Search

[Option+S]

United States (N. Virginia)

Cybrxio Admin

Aurora and RDS

DynamoDB

Lambda

S3

Route 53

API Gateway

Activate for Startups

Amazon Aurora DSQL

EC2

Amazon Bedrock

VPC

Database Migration Service

Amazon Redshift

AWS Glue

VPC > Route tables > rtb-0041609d91503c97b

VPC dashboard

EC2 Global View

Filter by VPC

Virtual private cloud

Your VPCs

Subnets

Route tables

Internet gateways

Egress-only internet gateways

Carrier gateways

DHCP option sets

Elastic IPs

Managed prefix lists

NAT gateways

Peering connections

Security

Network ACLs

Security groups

PrivateLink and Lattice

CloudShell

Feedback

rtb-0041609d91503c97b

Details info

Route table ID

rtb-0041609d91503c97b

VPC

vpc-0b6de2f65f971840b

Main

Yes

Owner ID

241526791455

Explicit subnet associations

-

Edge associations

-

Routes

Subnet associations

Edge associations

Route propagation

Tags

Routes (5)

Filter routes

Both

Edit routes

Destination	Target	Status	Propagated
0.0.0.0/0	igw-0f9fc5ac8461e59ca	Active	No
10.100.0.0/16	tgw-09fcad83501f16313	Active	No
10.200.0.0/16	tgw-09fcad83501f16313	Active	No
10.230.0.0/16	vgw-0ce14a175ddc623c0	Active	No
172.31.0.0/16	local	Active	No

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Ensure your Sydney VCN Route tables have routes for Melbourne VCN and AWS VPC via DRG

Cloud

Search resources, services, documentation, and Marketplace

Australia East (Sydney)

RT

AVAILABLE

Move resource

Add tags

Terminate

Details

Tags

Route Table Information

OCID: ...emz3mlq Show Copy

Created: Sun, Nov 1, 2020, 12:57:15 UTC

Compartment: shadabshaukat (root)

Resources

Route Rules (2)

Route Rules

Traffic within the VCN is handled by the VCN's local routing by default. Intra-VCN routing allows you more control over routing between subnets. Learn more. If you're having problems, use Network Path Analyzer to check your connections.

Add Route Rules Edit Remove

Destination	Target Type	Target	Route Type	Description
10.200.0.0/16	Dynamic Routing Gateways	Shadab-DRG	Static	
172.31.0.0/16	Dynamic Routing Gateways	Shadab-DRG	Static	

0 selected

Showing 2 items < 1 of 1 >

Terms of Use and Privacy Cookie Preferences

Copyright © 2025, Oracle and/or its affiliates. All rights reserved.

What's this? Redwood preview

Cloud

Search resources, services, documentation, and Marketplace

Australia East (Sydney)

RT

AVAILABLE

Move resource

Add tags

Terminate

Details

Tags

Route Table Information

OCID: ...vnmiffiq

Show

Copy

Created: Sun, Nov 1, 2020, 12:57:15 UTC

Compartment: shadabshaukat (root)

Resources

Route Rules (3)

Route Rules

Traffic within the VCN is handled by the VCN's local routing by default. Intra-VCN routing allows you more control over routing between subnets. [Learn more](#). If you're having problems, use [Network Path Analyzer](#) to check your connections.

Add Route Rules

Edit

Remove

<input type="checkbox"/>	Destination	Target Type	Target	Route Type	Description
<input type="checkbox"/>	0.0.0.0/0	Internet Gateway	<a href="#">Internet Gateway-Shadabshaukat-VCN</a>	Static	
<input type="checkbox"/>	10.200.0.0/16	Dynamic Routing Gateways	<a href="#">Shadab-DRG</a>	Static	
<input type="checkbox"/>	172.31.0.0/16	Dynamic Routing Gateways	<a href="#">Shadab-DRG</a>	Static	

0 selected

Showing 3 items < 1 of 1 >

Terms of Use and Privacy

Cookie Preferences

Copyright © 2025, Oracle and/or its affiliates. All rights reserved.

What's this? | Redwood preview

*Add ingress rule for ports in Route Table security list in SYDNEY for AWS VPC CIDR 172.31.0.0/16*

Cloud

Search resources, services, documentation, and Marketplace

Australia East (Sydney)

Resources

Ingress Rules (5)

Egress Rules (1)

Ingress Rules

Add Ingress Rules

Edit

Remove

<input type="checkbox"/>	Stateless	Source	IP Protocol	Source Port Range	Destination Port Range	Type and Code	Allows	Description
<input type="checkbox"/>	No	10.100.0.0/16	TCP	All	22		TCP traffic for ports: 22 SSH Remote Login Protocol	
<input type="checkbox"/>	No	0.0.0.0/0	ICMP			3, 4	ICMP traffic for: 3, 4 Destination Unreachable: Fragmentation Needed and Don't Fragment was Set	
<input type="checkbox"/>	No	10.100.0.0/16	ICMP			3	ICMP traffic for: 3 Destination Unreachable	
<input type="checkbox"/>	No	0.0.0.0/0	TCP	All	3306		TCP traffic for ports: 3306	
<input type="checkbox"/>	No	172.31.0.0/16	TCP	All	22		TCP traffic for ports: 22 SSH Remote Login Protocol	

0 selected

Showing 5 items < 1 of 1 >

*And do the same in Melbourne VCN Route Tables*



Cloud

Search resources, services, documentation, and Marketplace

Australia Southeast (Melbourne)

Move resourceAdd tagsTerminate

RT

AVAILABLE

DetailsTags

Route Table Information

OCID: ...tzlydxja Show Copy

Created: Sat, Mar 15, 2025, 04:38:10 UTC

Compartment: shadabshaukat (root)

Resources

Route Rules (4)

Route Rules

Traffic within the VCN is handled by the VCN's local routing by default. Intra-VCN routing allows you more control over routing between subnets. [Learn more](#). If you're having problems, use [Network Path Analyzer](#) to check your connections.

Add Route RulesEditRemove

<input type="checkbox"/>	Destination	Target Type	Target	Route Type	Description
<input type="checkbox"/>	0.0.0.0/0	NAT Gateway	<a href="#">NAT gateway-VCN-MELB</a>	Static	
<input type="checkbox"/>	10.100.0.0/16	Dynamic Routing Gateways	<a href="#">MEL-DRG</a>	Static	
<input type="checkbox"/>	172.31.0.0/16	Dynamic Routing Gateways	<a href="#">MEL-DRG</a>	Static	
<input type="checkbox"/>	All MEL Services In Oracle Services Network	Service Gateway	<a href="#">Service gateway-VCN-MELB</a>	Static	

0 selected

Showing 4 items1 of 1

Terms of Use and PrivacyCookie Preferences

Copyright © 2025, Oracle and/or its affiliates. All rights reserved.

What's this?Redwood preview

Cloud

Search resources, services, documentation, and Marketplace

Australia Southeast (Melbourne)

Move resourceAdd tagsTerminate

RT

AVAILABLE

DetailsTags

Route Table Information

OCID: ...a5cw2qza Show Copy

Created: Sat, Mar 15, 2025, 04:38:09 UTC

Compartment: shadabshaukat (root)

Resources

Route Rules (3)

Route Rules

Traffic within the VCN is handled by the VCN's local routing by default. Intra-VCN routing allows you more control over routing between subnets. [Learn more](#). If you're having problems, use [Network Path Analyzer](#) to check your connections.

Add Route RulesEditRemove

<input type="checkbox"/>	Destination	Target Type	Target	Route Type	Description
<input type="checkbox"/>	0.0.0.0/0	Internet Gateway	<a href="#">Internet gateway-VCN-MELB</a>	Static	
<input type="checkbox"/>	10.100.0.0/16	Dynamic Routing Gateways	<a href="#">MEL-DRG</a>	Static	
<input type="checkbox"/>	172.31.0.0/16	Dynamic Routing Gateways	<a href="#">MEL-DRG</a>	Static	

0 selected

Showing 3 items1 of 1

Terms of Use and PrivacyCookie Preferences

Copyright © 2025, Oracle and/or its affiliates. All rights reserved.

What's this?Redwood preview

Add ingress rule for ports in Route Table security list in Melbourne for AWS VPC CIDR 172.31.0.0/16

Resources		Ingress Rules							
Ingress Rules (4)		<div> Add Ingress Rules Edit Remove </div>							
<input type="checkbox"/>	Stateless	Source	IP Protocol	Source Port Range	Destination Port Range	Type and Code	Allows	Description	
<input type="checkbox"/>	No	10.200.0.0/16	TCP	All	22		TCP traffic for ports: 22 SSH Remote Login Protocol	⋮	
<input type="checkbox"/>	No	0.0.0.0/0	ICMP			3, 4	ICMP traffic for: 3, 4 Destination Unreachable: Fragmentation Needed and Don't Fragment was Set	⋮	
<input type="checkbox"/>	No	10.200.0.0/16	ICMP			3	ICMP traffic for: 3 Destination Unreachable	⋮	
<input type="checkbox"/>	No	172.31.0.0/16	TCP	All	22		TCP traffic for ports: 22 SSH Remote Login Protocol	⋮	
0 selected								Showing 4 items < 1 of 1 >	

Create an EC2 instance in the AWS VPC and connect to 2 VMs in OCI one in Sydney and Melbourne respectively

AWS Instance IP : 172.31.91.251

OCI Sydney VM : 10.100.1.35

OCI Melbourne VM : 10.200.2.250

AWS → OCI Sydney SSH Connection

```

ec2-user@ip-172-31-91-251:~
ec2-user@ip-172-31-91-251:~ (ssh)  ⌘1  ec2-
[ec2-user@ip-172-31-91-251 ~]$ telnet 10.100.1.35 22
Trying 10.100.1.35...
Connected to 10.100.1.35.
Escape character is '^]'.

```

AWS → OCI Melbourne SSH Connection

```

ec2-user@ip-172-31-91-251:~
[ec2-user@ip-172-31-91-251 ~]$ telnet 10.200.2.250 22
Trying 10.200.2.250...
Connected to 10.200.2.250.
Escape character is '^]'.
SSH-2.0-OpenSSH_8.0

```

*We can further extend this solution by Creating another Transit Gateway in another AWS Region, attach your VPCs to them, and then create a Transit Gateway peering attachment between the two Transit Gateways, ensuring proper route table updates.*

We now have another VPC in us-west-1 (N. California) region.

The screenshot shows the AWS VPC console for the 'California-VPC-vpc' (VPC ID: vpc-00d41f2f634572ffa) in the us-west-1 region. The left sidebar shows the 'VPC dashboard' with options like 'Virtual private cloud', 'Subnets', 'Route tables', etc. The main panel displays the 'Details' tab for the VPC, showing various configurations:

- VPC ID:** vpc-00d41f2f634572ffa
- State:** Available
- Block Public Access:** Off
- DNS hostnames:** Enabled
- DNS resolution:** Enabled
- Tenancy:** default
- DHCP option set:** dopt-08a1dcf3ac04dcd8
- Main network ACL:** acl-09de00bde385731c
- Default VPC:** No
- IPv4 CIDR:** 172.41.0.0/16
- Main route table:** rtb-046e76c767f83a885
- IPv6 CIDR:** -
- Network Address Usage metrics:** Disabled
- Route 53 Resolver DNS Firewall rule groups:** -
- IPv6 pool:** -
- Owner ID:** 241526791455

Below the details, there are tabs for 'Resource map', 'CIDRs', 'Flow logs', 'Tags', and 'Integrations'.

First let us create another Transit Routing Gateway in us-west-1 and attach the VPC to it.

The screenshot shows the AWS VPC console 'Transit gateways' page. The left sidebar shows the 'VPN' section with options like 'Customer gateways', 'Virtual private gateways', etc. The main panel shows a list of transit gateways, but it is empty with the message: 'No transit gateways. You do not have any transit gateways in this region.' There is a 'Create transit gateway' button. Below the list, there is a 'Select a transit gateway' section.

The screenshot shows the 'Create transit gateway' wizard in the AWS VPC console. The page title is 'Create transit gateway' and it includes a brief description: 'A transit gateway (TGW) is a network transit hub that interconnects attachments (VPCs and VPNs) within the same AWS account or across AWS accounts.'

The wizard has two main sections:

- Details - optional:** This section allows you to set optional details for the transit gateway.
  - Name tag:** A text input field with the value 'transit-gateway-california'.
  - Description:** A text input field with the value 'description'.
- Configure the transit gateway:** This section allows you to configure the transit gateway.
  - Amazon side Autonomous System Number (ASN):** A text input field with the value '12345'.
  - DNS support:** A checkbox that is checked.
  - Security Group Referencing support:** A checkbox that is unchecked.
  - VPN ECMP support:** A checkbox that is checked.

aws

Search

[Option+S]

United States (N. California)

Cybrxio Admin

Aurora and RDS

DynamoDB

Lambda

S3

Route 53

API Gateway

Activate for Startups

Aurora DSQL

EC2

Amazon Bedrock

VPC

Database Migration Service

Amazon Redshift

AWS Glue

VPC

Transit gateways

Create transit gateway

Configure cross-account sharing options

☐ Auto accept shared attachments

Transit gateway CIDR blocks

CIDR - optional

10.0.0.0/24

Tags - optional

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key

Name

Value - optional

transit-gateway-california

Remove

Add new tag

You can add up to 49 more tags.

Cancel

Create transit gateway

aws

Search

[Option+S]

United States (N. California)

Cybrxio Admin

Aurora and RDS

DynamoDB

Lambda

S3

Route 53

API Gateway

Activate for Startups

Aurora DSQL

EC2

Amazon Bedrock

VPC

Database Migration Service

Amazon Redshift

AWS Glue

Virtual private network (VPN)

Customer gateways

Virtual private gateways

Site-to-Site VPN connections

Client VPN endpoints

AWS Verified Access

Verified Access instances

Verified Access trust providers

Verified Access groups

Verified Access endpoints

Transit gateways

Transit gateway attachments

Transit gateway policy tables

Transit gateway route tables

Transit gateway multicast

Traffic Mirroring

Transit gateways (1)

Find transit gateway by attribute or tag

transit-gateway-calif...

tgw-08c5eb41bf661444e

Available

Select a transit gateway

## Create Transit Gateway attachment

aws

Search

[Option+S]

United States (N. California)

Cybrxio Admin

Aurora and RDS

DynamoDB

Lambda

S3

Route 53

API Gateway

Activate for Startups

Aurora DSQL

EC2

Amazon Bedrock

VPC

Database Migration Service

Amazon Redshift

AWS Glue

VPC

Transit gateway attachments

Create transit gateway attachment

Create transit gateway attachment

A transit gateway (TGW) is a network transit hub that interconnects attachments (VPCs and VPNs) within the same AWS account or across AWS accounts.

Details

Name tag - optional

transit-gw-attachment-n-california-01

Transit gateway ID

tgw-08c5eb41bf661444e

Attachment type

VPC

VPC attachment

Select and configure your VPC attachment.

☒ DNS support

☒ Security Group Referencing support

☐ IPv6 support

**VPC ID**  
Select the VPC to attach to the transit gateway.  
vpc-00d41f2f634572ffa

**Subnet IDs**  
Select the subnets in which to create the transit gateway VPC attachment.  
☒ us-west-1a subnet-00556ca964971b697  
☒ us-west-1b subnet-046d573fdd4ee2935

**Tags - optional**  
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - optional
Name	transit-gw-attachment-n-california-01

[Add new tag](#)  
You can add up to 49 more tags.

## Create Transit Gateway Attachment

**Transit gateway attachments (1/1)**

Name	Transit gateway attachment ID	Transit gateway ID	State	Resource t...	Resource ID
transit-gw-attachme...	tgw-attach-0064f0317ded73e16	tgw-08c5eb41bf661444e	Available	VPC	vpc-00d41f2f634572ffa

**Transit gateway attachment: tgw-attach-0064f0317ded73e16 / transit-gw-attachment-n-california-01**

State: Available	Resource owner ID: 241526791455	DNS support: Enable	Subnet IDs: 2 Subnets
Resource type: VPC	Resource ID: vpc-00d41f2f634572ffa	Security Group Referencing support: Enable	Association state: Associated
Association route table ID: tgw-rtb-07fe4321458b1f939	IPv6 support: Disable		

We now need to connect the Transit Routing Gateways in us-east-1 and us-west-1 via Peering connection.

Ref : <https://docs.aws.amazon.com/vpc/latest/tgw/tgw-peering.html>

Before you begin, ensure that you have the ID of the transit gateway that you want to attach. If the transit gateway is in another AWS account, ensure that you have the AWS account ID of the owner of the transit gateway.

My Transit Gateway ID in us-east-1 is tgw-09fcad83501f16313

Go back to Transit Gateway Attachments and Create Transit Gateway Attachment in us-west-1

Ref : <https://docs.aws.amazon.com/vpc/latest/tgw/tgw-peering-create.html>

**Create transit gateway attachment** [Info](#)

A transit gateway (TGW) is a network transit hub that interconnects attachments (VPCs and VPNs) within the same AWS account or across AWS accounts.

**Details**

**Name tag - optional**  
Creates a tag with the key set to Name and the value set to the specified string.

transit-gw-attachment-rpc-n-california

**Transit gateway ID** [Info](#)  
tgw-08c5eb41bf661444e

**Attachment type** [Info](#)  
Peering Connection

**Peering connection attachment**  
Select and configure your peering connection attachment.

**Account** [Info](#)  
☒ My account  
☐ Other account

**Region** [Info](#)

Make sure there are no empty spaces in the string when you paste the Transit Gateway ID

Create the peering connection attachment and wait for it to become 'Pending Acceptance'. Go to us-east-1 TRG Attachments and accept the request

**VPC dashboard**

EC2 Global View [Filter by VPC](#)

▼ **Virtual private cloud**

- Your VPCs
- Subnets
- Route tables
- Internet gateways
- Egress-only Internet gateways
- Carrier gateways
- DHCP option sets
- Elastic IPs
- Managed prefix lists
- NAT gateways
- Peering connections

▼ **Security**

**Transit gateway attachments (1/3)** [Info](#)

[Find transit gateway attachment by attribute or tag](#)

	Name	Transit gateway attachment ID	Transit gateway ID	State
<input checked="" type="checkbox"/>		tgw-attach-0fbb0083169ca71a4	tgw-09fcad83501f16313	Pending
<input type="checkbox"/>	transit-gateway-atta...	tgw-attach-0ea473f30c8380a66	tgw-09fcad83501f16313	Available

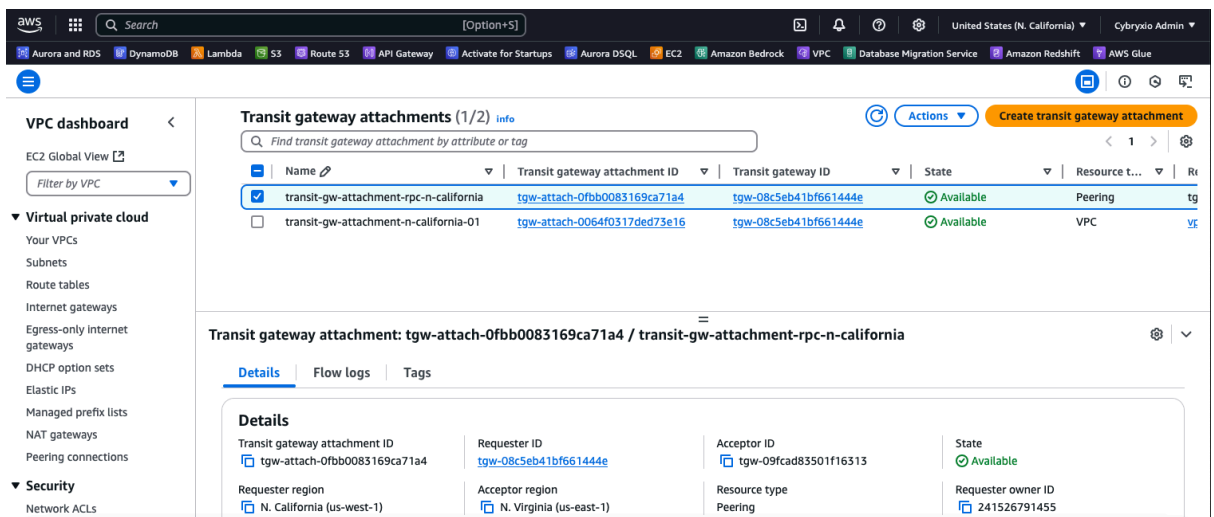
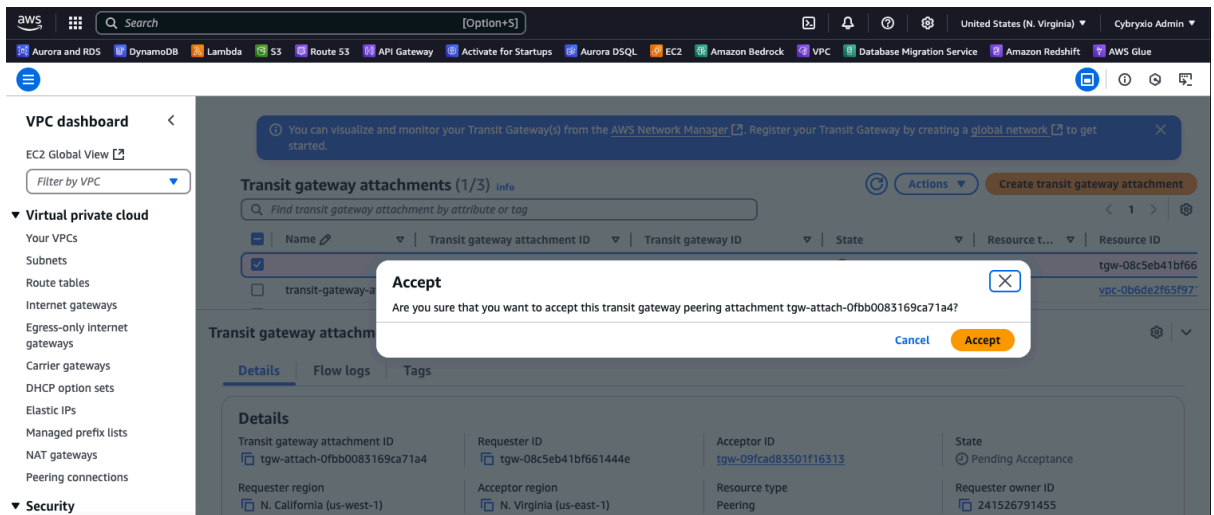
**Transit gateway attachment: tgw-attach-0fbb0083169ca71a4**

[Details](#) [Flow logs](#) [Tags](#)

**Details**

Transit gateway attachment ID <a href="#">tgw-attach-0fbb0083169ca71a4</a>	Requester ID <a href="#">tgw-08c5eb41bf661444e</a>	Acceptor ID <a href="#">tgw-09fcad83501f16313</a>	State Pending Acceptance
Requester region N. California (us-west-1)	Acceptor region N. Virginia (us-east-1)	Resource type Peering	Requester owner ID <a href="#">241526791455</a>





Once it is completed, add the routes of both VPC's to the respective Route tables in each regions

In California VPC Route tables add 172.31.0.0/16 (CIDR for us-east-1) to the private route tables for which you created the TRG attachments

**VPC dashboard** < EC2 Global View [Filter by VPC](#)

▼ **Virtual private cloud**

- Your VPCs
- Subnets
- Route tables**
- Internet gateways
- Egress-only Internet gateways
- DHCP option sets
- Elastic IPs
- Managed prefix lists
- NAT gateways
- Peering connections

▼ **Security**

- Network ACLs

**Route tables (1/5)** Info Last updated less than a minute ago [Actions](#) [Create route table](#)

[Find resources by attribute or tag](#)

<input type="checkbox"/>	Name	Route table ID	Explicit subnet associ...	Edge associations	Main	VPC
<input type="checkbox"/>	-	rtb-046e76c767f83a885	-	-	Yes	<a href="#">vpc-00d41f2f634572ffa   C</a>
<input type="checkbox"/>	California-VPC-rtb-public	rtb-0af4c3288519c3630	2 subnets	-	No	<a href="#">vpc-00d41f2f634572ffa   C</a>
<input checked="" type="checkbox"/>	California-VPC-rtb-private2-us-west-1b	rtb-0b8554b45e88b8831	subnet-046d573fdd4ee2...	-	No	<a href="#">vpc-00d41f2f634572ffa   C</a>
<input type="checkbox"/>	California-VPC-rtb-private1-us-west-1a	rtb-0f6a5581c14f21db3	subnet-00556ca964971b...	-	No	<a href="#">vpc-00d41f2f634572ffa   C</a>
<input type="checkbox"/>	-	rtb-05ec71da539b6fca8	-	-	Yes	<a href="#">vpc-096678f6e188a1c12</a>

**Routes (2)** [Both](#) [Edit routes](#)

[Filter routes](#)

Destination	Target	Status	Propagated
<a href="#">pl-6ba54002</a>	<a href="#">vpce-08a18b2c75046a659</a>	Active	No
172.31.0.0/16	local	Active	No

VPC > Route tables > [rtb-0b8554b45e88b8831](#) > Edit routes

**Edit routes**

Destination	Target	Status	Propagated
pl-6ba54002	vpce-08a18b2c75046a659	Active	No
172.31.0.0/16	local	Active	No
<input type="text" value="172.31.0.0/16"/>	<input type="text" value="local"/>	-	No
	<input type="text" value="Transit Gateway"/>	-	No
	<input type="text" value="tgw-08c5eb41bf661444e"/>	-	No

[Add route](#) [Remove](#)

[Cancel](#) [Preview](#) [Save changes](#)

VPC > Route tables > [rtb-0b8554b45e88b8831](#)

**VPC dashboard** < EC2 Global View [Filter by VPC](#)

▼ **Virtual private cloud**

- Your VPCs
- Subnets
- Route tables**
- Internet gateways
- Egress-only Internet gateways
- DHCP option sets
- Elastic IPs
- Managed prefix lists
- NAT gateways
- Peering connections

▼ **Security**

- Network ACLs

**Updated routes for rtb-0b8554b45e88b8831 / California-VPC-rtb-private2-us-west-1b successfully** [Details](#)

**Details** Info

Route table ID	Main	Explicit subnet associations	Edge associations
rtb-0b8554b45e88b8831	No	subnet-046d573fdd4ee2935 / California-VPC-subnet-private2-us-west-1b	-

VPC [vpc-00d41f2f634572ffa | California-VPC-vpc](#) Owner ID [241526791455](#)

**Routes** Subnet associations Edge associations Route propagation Tags

**Routes (3)** [Both](#) [Edit routes](#)

[Filter routes](#)

Destination	Target	Status	Propagated
<a href="#">pl-6ba54002</a>	<a href="#">vpce-08a18b2c75046a659</a>	Active	No
172.31.0.0/16	<a href="#">tgw-08c5eb41bf661444e</a>	Active	No
172.31.0.0/16	local	Active	No

Add it for the other private subnet as well

**Route tables (1/5) Info** Last updated 1 minute ago Actions Create route table

Find resources by attribute or tag

Name	Route table ID	Explicit subnet associ...	Edge associations	Main	VPC
-	rtb-046e76c767f83a885	-	-	Yes	<a href="#">vpc-00d41f2f634572ffa   C</a>
California-VPC-rtb-public	rtb-0af4c3288519c3630	2 subnets	-	No	<a href="#">vpc-00d41f2f634572ffa   C</a>
California-VPC-rtb-private2-us-west-1b	rtb-0b8554b45e88b8831	subnet-046d573fdd4ee2...	-	No	<a href="#">vpc-00d41f2f634572ffa   C</a>
<input checked="" type="checkbox"/> California-VPC-rtb-private1-us-west-1a	rtb-0f6a5581c14f21db3	subnet-00556ca964971b...	-	No	<a href="#">vpc-00d41f2f634572ffa   C</a>
-	rtb-05ec71da539b6fca8	-	-	Yes	<a href="#">vpc-096678f6e188a1c12</a>

**rtb-0f6a5581c14f21db3 / California-VPC-rtb-private1-us-west-1a**

[Details](#) [Routes](#) [Subnet associations](#) [Edge associations](#) [Route propagation](#) [Tags](#)

**Details**

Route table ID <a href="#">rtb-0f6a5581c14f21db3</a>	Main <input checked="" type="checkbox"/> No	Explicit subnet associations <a href="#">subnet-00556ca964971b697 / California-VPC-subnet-private1-us-west-1a</a>	Edge associations -
---	--	--	------------------------

**Edit routes**

Destination	Target	Status	Propagated
pl-6ba54002 172.41.0.0/16	vpce-08a18b2c75046a659 local	Active	No
172.31.0.0/16	Transit Gateway tgw-08c5eb41bf661444e	Active	No

[Add route](#) [Remove](#) [Cancel](#) [Preview](#) [Save changes](#)

**Updated routes for rtb-0f6a5581c14f21db3 / California-VPC-rtb-private1-us-west-1a successfully**

[Details](#)

**Details Info**

Route table ID <a href="#">rtb-0f6a5581c14f21db3</a>	Main <input checked="" type="checkbox"/> No	Explicit subnet associations <a href="#">subnet-00556ca964971b697 / California-VPC-subnet-private1-us-west-1a</a>	Edge associations -
VPC <a href="#">vpc-00d41f2f634572ffa   California-VPC-vpc</a>	Owner ID <a href="#">241526791455</a>		

[Routes](#) [Subnet associations](#) [Edge associations](#) [Route propagation](#) [Tags](#)

**Routes (3)**

Destination	Target	Status	Propagated
<a href="#">pl-6ba54002</a>	<a href="#">vpce-08a18b2c75046a659</a>	Active	No
172.31.0.0/16	<a href="#">tgw-08c5eb41bf661444e</a>	Active	No
172.41.0.0/16	local	Active	No

Now In N Virginia VPC Route tables add 172.41.0.0/16 (CIDR for us-west-1) to the private route tables for which you created the TRG attachments

aws [Search] [Option+S] United States (N. Virginia) Cybrylo Admin

Aurora and RDS DynamoDB Lambda S3 Route 53 API Gateway Activate for Startups Aurora DSQL EC2 Amazon Bedrock VPC Database Migration Service Amazon Redshift AWS Glue

VPC > Route tables > rtb-0041609d91503c97b

**VPC dashboard** < EC2 Global View [?] Filter by VPC

▼ **Virtual private cloud**  
 Your VPCs  
 Subnets  
**Route tables**  
 Internet gateways  
 Egress-only Internet gateways  
 Carrier gateways  
 DHCP option sets  
 Elastic IPs  
 Managed prefix lists  
 NAT gateways  
 Peering connections

▼ **Security**

**rtb-0041609d91503c97b** Actions

**Details** Info

<b>Route table ID</b> rtb-0041609d91503c97b	<b>Main</b> Yes	<b>Explicit subnet associations</b> -	<b>Edge associations</b> -
<b>VPC</b> vpc-0b6de2f65f971840b	<b>Owner ID</b> 241526791455		

**Routes** Subnet associations Edge associations Route propagation Tags

**Routes (5)** Both Edit routes

Destination	Target	Status	Propagated
0.0.0.0/0	igw-0f9fc5ac8461e59ca	Active	No
10.100.0.0/16	tgw-09fcad83501f16313	Active	No
10.200.0.0/16	tgw-09fcad83501f16313	Active	No
10.230.0.0/16	vgw-0ce14a175ddc623c0	Active	No

aws [Search] [Option+S] United States (N. Virginia) Cybrylo Admin

Aurora and RDS DynamoDB Lambda S3 Route 53 API Gateway Activate for Startups Aurora DSQL EC2 Amazon Bedrock VPC Database Migration Service Amazon Redshift AWS Glue

VPC > Route tables > rtb-0041609d91503c97b > Edit routes

Destination	Target	Status	Propagated
172.31.0.0/16	local	Active	No
10.100.0.0/16	Transit Gateway	Active	No
10.200.0.0/16	Transit Gateway	Active	No
10.230.0.0/16	Virtual Private Gateway	Active	No
0.0.0.0/0	Internet Gateway	Active	No
172.41.0.0/16	Transit Gateway	-	No

Add route

aws [Search] [Option+S] United States (N. Virginia) Cybrylo Admin

Aurora and RDS DynamoDB Lambda S3 Route 53 API Gateway Activate for Startups Aurora DSQL EC2 Amazon Bedrock VPC Database Migration Service Amazon Redshift AWS Glue

VPC > Route tables > rtb-0041609d91503c97b

**VPC dashboard** < EC2 Global View [?] Filter by VPC

▼ **Virtual private cloud**  
 Your VPCs  
 Subnets  
**Route tables**  
 Internet gateways  
 Egress-only Internet gateways  
 Carrier gateways  
 DHCP option sets  
 Elastic IPs  
 Managed prefix lists  
 NAT gateways  
 Peering connections

▼ **Security**

**Updated routes for rtb-0041609d91503c97b successfully** Details

**VPC** vpc-0b6de2f65f971840b **Owner ID** 241526791455

**Routes** Subnet associations Edge associations Route propagation Tags

**Routes (6)** Both Edit routes

Destination	Target	Status	Propagated
0.0.0.0/0	igw-0f9fc5ac8461e59ca	Active	No
10.100.0.0/16	tgw-09fcad83501f16313	Active	No
10.200.0.0/16	tgw-09fcad83501f16313	Active	No
10.230.0.0/16	vgw-0ce14a175ddc623c0	Active	No
172.31.0.0/16	local	Active	No
172.41.0.0/16	tgw-09fcad83501f16313	Active	No

Add a route to a transit gateway route table using Amazon VPC Transit Gateways  
 Ref : <https://docs.aws.amazon.com/vpc/latest/tgw/tgw-peering-add-route.html>

In us-east-1



Static route was created successfully.

### Transit gateway route tables (1/1) info

Find transit gateway route table by attribute or tag

<input checked="" type="checkbox"/>	Name	Transit gateway route table ID	Transit gateway ID	State	Default association route table
<input checked="" type="checkbox"/>	tgw-rtb-065873123199fb96c	tgw-rtb-065873123199fb96c	tgw-09fcad83501f16313	Available	Yes

#### Transit gateway route tables: tgw-rtb-065873123199fb96c

Find route by attribute or tag

<input type="checkbox"/>	CIDR	Attachment ID	Resource ID	Resource type	Route type	Route state
<input type="checkbox"/>	10.200.1.0/24	tgw-attach-0826fb2097ce1c62e	vpn-0b732e51d8e13201c3...	VPN	Propagated	Active
<input type="checkbox"/>	10.200.2.0/24	tgw-attach-0826fb2097ce1c62e	vpn-0b732e51d8e13201c3...	VPN	Propagated	Active
<input type="checkbox"/>	172.31.0.0/16	tgw-attach-0ea473f30c8380a66	vpc-0b6de2f65f971840b	VPC	Propagated	Active
<input type="checkbox"/>	172.41.0.0/16	tgw-attach-0fbb0083169ca71a4	tgw-08c5eb41bf661444e	Peering	Static	Active

Add a route to a transit gateway route table using Amazon VPC Transit Gateways  
 Ref : <https://docs.aws.amazon.com/vpc/latest/tgw/tgw-peering-add-route.html>

In us-west-1

### Transit gateway route tables (1) info

Find transit gateway route table by attribute or tag

<input type="checkbox"/>	Name	Transit gateway route table ID	Transit gateway ID	State	Default association route table
<input type="checkbox"/>	tgw-rtb-07fe4321458b1f939	tgw-rtb-07fe4321458b1f939	tgw-08c5eb41bf661444e	Available	Yes

#### Select a transit gateway route table



Transit gateway route tables > tgw-rtb-07fe4321458b1f939

**tgw-rtb-07fe4321458b1f939** info

**Details**

Transit gateway route table ID: [tgw-rtb-07fe4321458b1f939](#)

Transit gateway ID: [tgw-08c5eb41bf661444e](#)

State: Available

Default propagation route table: Yes

**Associations** | Propagations | Prefix list references | Routes | Tags

**Associations (2)** info

Find association by attribute or tag

Attachment ID	Resource type	Resource ID	State
<a href="#">tgw-attach-0fbb0083169ca71a4</a>	Peering	<a href="#">tgw-09fcad83501f16313</a>	<span>Associated</span>
<a href="#">tgw-attach-0064f0317ded73e16</a>	VPC	<a href="#">vpc-00d41f2f634572ffa</a>	<span>Associated</span>

Actions: Create association, Create propagation, Create prefix list reference, Create static route, Export routes, Manage tags, Delete transit gateway route table

VPC > Transit gateway route tables > [tgw-rtb-07fe4321458b1f939](#) > Create static route

**Create static route** info

Add a static route to your transit gateway route table.

**Details**

Transit gateway ID: [tgw-08c5eb41bf661444e](#)

Transit gateway route table ID: [tgw-rtb-07fe4321458b1f939](#)

CIDR:

Type: ☒ Active ☐ Blackhole

Choose attachment: [tgw-attach-0fbb0083169ca71a4](#)

Cancel Create static route

Static route was created successfully.

**Transit gateway route tables (1/1)** info

Find transit gateway route table by attribute or tag

Name	Transit gateway route table ID	Transit gateway ID	State	Default association route table
<a href="#">tgw-rtb-07fe4321458b1f939</a>	<a href="#">tgw-08c5eb41bf661444e</a>	<a href="#">tgw-09fcad83501f16313</a>	<span>Available</span>	Yes

**Transit gateway route tables: tgw-rtb-07fe4321458b1f939**

**Routes (2)** info

Find route by attribute or tag

CIDR	Attachment ID	Resource ID	Resource type	Route type	Route state
172.31.0.0/16	<a href="#">tgw-attach-0fbb0083169ca71a4</a>	<a href="#">tgw-09fcad83501f16313</a>	Peering	Static	<span>Active</span>
172.41.0.0/16	<a href="#">tgw-attach-0064f0317ded73e16</a>	<a href="#">vpc-00d41f2f634572ffa</a>	VPC	Propagated	<span>Active</span>

Create an Instance in us-west-2 and test connectivity to Instance in us-east-1

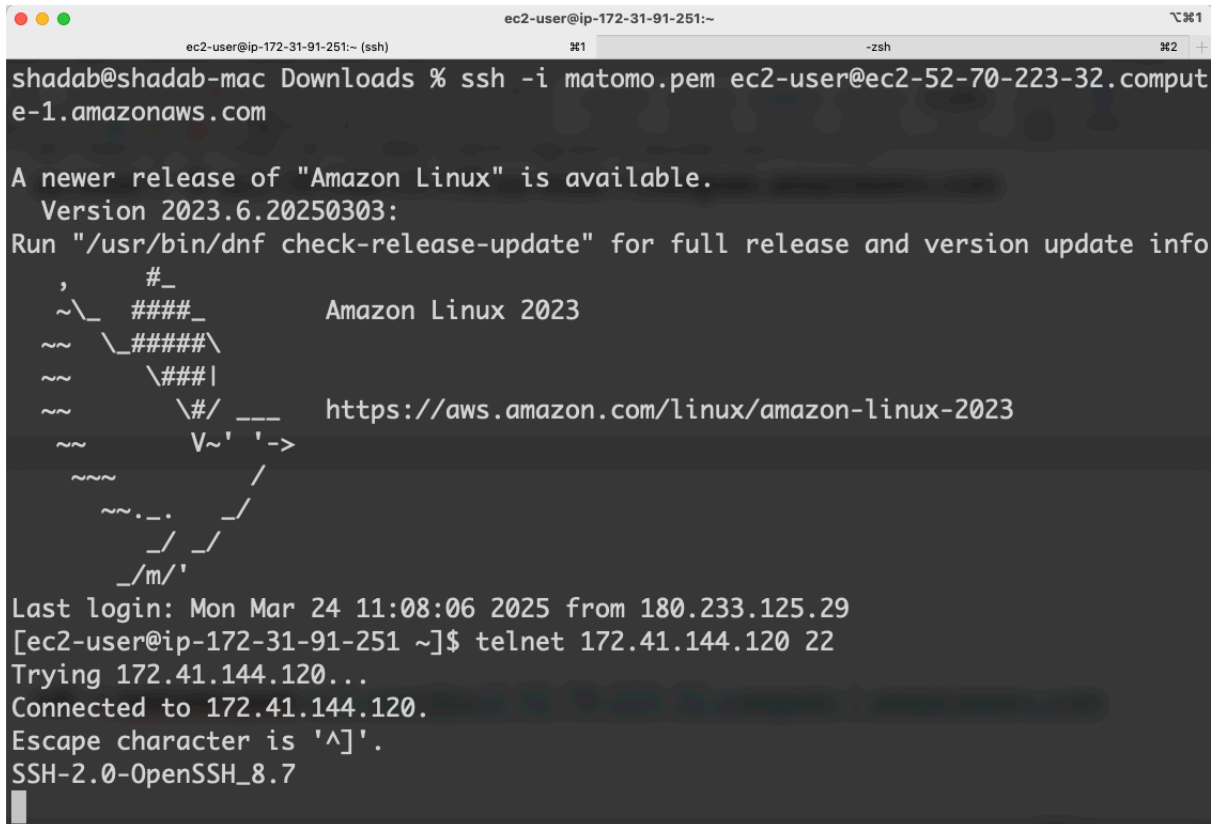
us -east-1 → ec2-52-70-223-32.compute-1.amazonaws.com

us-west-1 → ec2-18-144-13-158.us-west-1.compute.amazonaws.com

From us-east-1 Instance :

ssh -i matomo.pem [ec2-user@ec2-52-70-223-32.compute-1.amazonaws.com](mailto:ec2-user@ec2-52-70-223-32.compute-1.amazonaws.com)

telnet 172.41.144.120 22



```
ec2-user@ip-172-31-91-251:~ (ssh)
shadab@shadab-mac Downloads % ssh -i matomo.pem ec2-user@ec2-52-70-223-32.compute-1.amazonaws.com

A newer release of "Amazon Linux" is available.
Version 2023.6.20250303:
Run "/usr/bin/dnf check-release-update" for full release and version update info

      #_
     ~\ #####_      Amazon Linux 2023
    ~ ~\#####\
    ~ ~ \###|
    ~ ~  \#/  _--  https://aws.amazon.com/linux/amazon-linux-2023
    ~ ~   V~'  '->
      ~~~
      ~ ~. _ _/
      ~ ~ _/_/_/
      ~ ~ _/m/'

Last login: Mon Mar 24 11:08:06 2025 from 180.233.125.29
[ec2-user@ip-172-31-91-251 ~]$ telnet 172.41.144.120 22
Trying 172.41.144.120...
Connected to 172.41.144.120.
Escape character is '^]'.
SSH-2.0-OpenSSH_8.7
```

From us-west-1 Instance :

ssh -i cali.pem [ec2-user@172.41.144.120](mailto:ec2-user@172.41.144.120)

telnet 172.31.91.251 22



Cloud

Search resources, services, documentation, and Marketplace

Australia East (Sydney)

IPV6 BGP status: Down

IKE version: IKEv2

Created: Fri, Mar 14, 2025, 03:47:33 UTC

OCID: ...qonmaq Show Copy

Routing type: BGP dynamic routing

IPV4 inside tunnel interface - Oracle: 169.254.40.2/30

IPV6 inside tunnel interface - CPE: -

IPV6 inside tunnel interface - Oracle: -

Shared secret: \*\*\*\*\* Show Edit

Oracle can initiate: INITIATOR\_OR\_RESPONDER

NAT-T enabled: AUTO

Dead peer detection mode: INITIATE\_AND\_RESPOND

DPD timeout in seconds: 20

Resources

Metrics

Tunnel security associations

BGP routes received (2)

BGP routes advertised (4)

BGP routes received

IP route prefix	Route age	Is best path	AS path length	AS path
172.31.0.0/16	22811 Seconds	No	2	65515... <a>Show all (2)</a>
172.41.0.0/16	1780 Seconds	No	2	65515... <a>Show all (2)</a>

Showing 2 items < Page 1 >

In us-east-1. The TRG route table already has the OCI routes propagated

aws

Search

[Option+S]

Aurora and RDS DynamoDB Lambda S3 Route 53 API Gateway Activate for Startups Aurora DSQL EC2 Amazon Bedrock VPC Database Migration Service Amazon Redshift AWS Glue

VPC > Transit gateway route tables > tgw-rtb-065873123199fb96c

Customer gateways

Virtual private gateways

Site-to-Site VPN connections

Client VPN endpoints

AWS Verified Access

Verified Access instances

Verified Access trust providers

Verified Access groups

Verified Access endpoints

Transit gateways

Transit gateways

Transit gateway attachments

Transit gateway policy tables

Transit gateway route tables

Transit gateway multicast

Traffic Mirroring

Mirror sessions

Mirror targets

Mirror filters

Filter routes by CIDR (2)

Exact CIDR  
Select a valid IP4 or IPv6 CIDR.

Longest prefix match  
Enter a valid IP4 or IPv6 and press enter.

Supernet of match  
Select a valid IP4 or IPv6 CIDR.

Subnet of match  
Select a valid IP4 or IPv6 CIDR.

Routes (6) info

<input type="checkbox"/>	CIDR	Attachment ID	Resource ID	Resource type	Route type	Route state
<input type="checkbox"/>	10.100.1.0/24	tgw-attach-0826fb2097ce1c62e	vpn-0b732e51d8e13201c3...	VPN	Propagated	Active
<input type="checkbox"/>	10.100.2.0/24	tgw-attach-0826fb2097ce1c62e	vpn-0b732e51d8e13201c3...	VPN	Propagated	Active
<input type="checkbox"/>	10.200.1.0/24	tgw-attach-0826fb2097ce1c62e	vpn-0b732e51d8e13201c3...	VPN	Propagated	Active
<input type="checkbox"/>	10.200.2.0/24	tgw-attach-0826fb2097ce1c62e	vpn-0b732e51d8e13201c3...	VPN	Propagated	Active
<input type="checkbox"/>	172.31.0.0/16	tgw-attach-0ea473f30c8380a66	vpc-0b6de2f65f971840b	VPC	Propagated	Active
<input type="checkbox"/>	172.41.0.0/16	tgw-attach-0fbb0083169ca71a4	tgw-08c5eb41bf661444e	Peering	Static	Active

But we need to add the OCI routes in us-west-1 TRG Route table as static routes

aws

Search

[Option+S]

Aurora and RDS DynamoDB Lambda S3 Route 53 API Gateway Activate for Startups Aurora DSQL EC2 Amazon Bedrock VPC Database Migration Service Amazon Redshift AWS Glue

VPC > Transit gateway route tables

Verified Access trust providers

Verified Access groups

Verified Access endpoints

Transit gateways

Transit gateways

Transit gateway attachments

Transit gateway policy tables

Transit gateway route tables

Transit gateway multicast

Traffic Mirroring

Mirror sessions

Mirror targets

Mirror filters

Network Manager

Cloud WAN

VPC IP Address Manager

Transit gateway route tables (1) info

<input type="checkbox"/>	Name	Transit gateway route table ID	Transit gateway ID	State	Default association route table
<input type="checkbox"/>	tgw-rtb-07fe4321458b1f939	tgw-08c5eb41bf661444e	tgw-08c5eb41bf661444e	Available	Yes

Select a transit gateway route table

aws

Search

[Option+S]

United States (N. California)

Cybrxio Admin

Aurora and RDS

DynamoDB

Lambda

S3

Route 53

API Gateway

Activate for Startups

Aurora DSQL

EC2

Amazon Bedrock

VPC

Database Migration Service

Amazon Redshift

AWS Glue

VPC

Transit gateway route tables

tgw-rtb-07fe4321458b1f939

Verified Access trust providers

Verified Access groups

Verified Access endpoints

Transit gateways

Transit gateway attachments

Transit gateway policy tables

Transit gateway route tables

Transit gateway multicast

Traffic Mirroring

Mirror sessions

Mirror targets

Mirror filters

Network Manager

Cloud WAN

VPC IP Address Manager

tgw-rtb-07fe4321458b1f939

Info

Actions

Details

Transit gateway route table ID

tgw-rtb-07fe4321458b1f939

Transit gateway ID

tgw-08c5eb41bf661444e

State

Available

Default propagation route table

Yes

Associations

Propagations

Prefix list references

Routes

Tags

Associations (2)

Find association by attribute or tag

Attachment ID

Resource type

Resource ID

State

tgw-attach-0fbb0083169ca71a4

Peering

tgw-09fca8d83501f16313

Associated

tgw-attach-0064f0317ded73e16

VPC

vpc-00d41f2f634572ffa

Associated

Create association

Create propagation

Create prefix list reference

Create static route

Export routes

Manage tags

Delete transit gateway route table

aws

Search

[Option+S]

United States (N. California)

Cybrxio Admin

Aurora and RDS

DynamoDB

Lambda

S3

Route 53

API Gateway

Activate for Startups

Aurora DSQL

EC2

Amazon Bedrock

VPC

Database Migration Service

Amazon Redshift

AWS Glue

VPC

Transit gateway route tables

tgw-rtb-07fe4321458b1f939

Create static route

Create static route

Info

Add a static route to your transit gateway route table.

Details

Transit gateway ID

tgw-08c5eb41bf661444e

Transit gateway route table ID

tgw-rtb-07fe4321458b1f939

CIDR

10.100.0.0/16

Type

Active

Blackhole

Choose attachment

tgw-attach-0fbb0083169ca71a4

Cancel

Create static route

aws

Search

[Option+S]

United States (N. California)

Cybrxio Admin

Aurora and RDS

DynamoDB

Lambda

S3

Route 53

API Gateway

Activate for Startups

Aurora DSQL

EC2

Amazon Bedrock

VPC

Database Migration Service

Amazon Redshift

AWS Glue

VPC

Transit gateway route tables

tgw-rtb-07fe4321458b1f939

Create static route

Create static route

Info

Add a static route to your transit gateway route table.

Details

Transit gateway ID

tgw-08c5eb41bf661444e

Transit gateway route table ID

tgw-rtb-07fe4321458b1f939

CIDR

10.200.0.0/16

Type

Active

Blackhole

Choose attachment

tgw-attach-0fbb0083169ca71a4

Cancel

Create static route

aws [Search] [Option+S] United States (N. California) Cybrylio Admin

VPC > Transit gateway route tables > tgw-rtb-07fe4321458b1f939

VPC dashboard < EC2 Global View [x] Filter by VPC

Virtual private cloud Your VPCs Subnets Route tables Internet gateways Egress-only Internet gateways DHCP option sets Elastic IPs Managed prefix lists NAT gateways Peering connections Security Network ACLs

Associations | Propagations | Prefix list references | **Routes** | Tags

▼ Filter routes by CIDR (2)

Exact CIDR Select a valid IP4 or IPv6 CIDR.

Longest prefix match Enter a valid IP4 or IPv6 and press enter.

Supernet of match Select a valid IP4 or IPv6 CIDR.

Subnet of match Select a valid IP4 or IPv6 CIDR.

Routes (4) info  Actions Create static route

<input type="checkbox"/>	CIDR	Attachment ID	Resource ID	Resource type	Route type	Route state
<input type="checkbox"/>	10.100.0.0/16	<a href="#">tgw-attach-0fb0083169ca71a4</a>	tgw-09fcad83501f16313	Peering	Static	Active
<input type="checkbox"/>	10.200.0.0/16	<a href="#">tgw-attach-0fb0083169ca71a4</a>	tgw-09fcad83501f16313	Peering	Static	Active
<input type="checkbox"/>	172.31.0.0/16	<a href="#">tgw-attach-0fb0083169ca71a4</a>	tgw-09fcad83501f16313	Peering	Static	Active
<input type="checkbox"/>	172.41.0.0/16	<a href="#">tgw-attach-0064f0317ded73e16</a>	<a href="#">vpc-00d41f2f634572ffa</a>	VPC	Propagated	Active

Add 10.100.0.0/16 and 10.200.0.0/16 OCI VCN CIDR to us-west-1 VPC (172.41.0.0/16) Route Table

aws [Search] [Option+S] United States (N. California) Cybrylio Admin

VPC > Route tables > rtb-0b8554b45e88b8831

VPC dashboard < EC2 Global View [x] Filter by VPC

Virtual private cloud Your VPCs Subnets Route tables Internet gateways Egress-only Internet gateways DHCP option sets Elastic IPs Managed prefix lists NAT gateways Peering connections Security Network ACLs

rtb-0b8554b45e88b8831 / California-VPC-rtb-private2-us-west-1b Actions

Details info

Route table ID [rtb-0b8554b45e88b8831](#)

VPC [vpc-00d41f2f634572ffa](#) | California-VPC-vpc

Main ☐ No

Owner ID ☐ 241526791455

Explicit subnet associations [subnet-046d573fdd4ee2935](#) / California-VPC-subnet-private2-us-west-1b

Edge associations -

Routes Subnet associations Edge associations Route propagation Tags

Routes (3)  Both Edit routes

Destination	Target	Status	Propagated
<a href="#">pl-6ba54002</a>	<a href="#">vpce-08a18b2c75046a659</a>	Active	No
172.31.0.0/16	<a href="#">tgw-08c5eb41bf661444e</a>	Active	No
172.41.0.0/16	local	Active	No

aws [Search] [Option+S] United States (N. California) Cybrylio Admin

VPC > Route tables > [rtb-0b8554b45e88b8831](#) > Edit routes

Edit routes

Destination	Target	Status	Propagated	
pl-6ba54002	vpce-08a18b2c75046a659	Active	No	
172.41.0.0/16	local	Active	No	
<input type="text" value="172.31.0.0/16"/>	Transit Gateway	Active	No	Remove
<input type="text" value="10.100.0.0/16"/>	Transit Gateway	-	No	Remove
<input type="text" value="10.200.0.0/16"/>	Transit Gateway	-	No	Remove

Add route

Cancel Preview Save changes





Updated routes for rtb-0f6a5581c14f21db3 / California-VPC-rtb-private1-us-west-1a successfully

**VPC**  
vpc-00d41f2f634572ffa | California-VPC-vpc

**Owner ID**  
241526791455

**Subnet**  
subnet-00590e5b41bf661444e | California-VPC-subnet-private1-us-west-1a

**Routes (5)**

Destination	Target	Status	Propagated
pl-6ba54002	vpc-08a18b2c75046a659	Active	No
10.100.0.0/16	tgw-08c5eb41bf661444e	Active	No
10.200.0.0/16	tgw-08c5eb41bf661444e	Active	No
172.31.0.0/16	tgw-08c5eb41bf661444e	Active	No
172.41.0.0/16	local	Active	No

Now add the AWS VPC new CIDR 172.41.0.0/16 to both OCI regions VCN's Route tables

In OCI Sydney VCN in both Route tables

**Route Table Information**

OCID: ...emz3mlq [Show](#) [Copy](#)

Created: Sun, Nov 1, 2020, 12:57:15 UTC

Compartment: shadabshaukat (root)

**Route Rules**

Traffic within the VCN is handled by the VCN's local routing by default. Intra-VCN routing allows you more control over routing between subnets. [Learn more](#). If you're having problems, use [Network Path Analyzer](#) to check your connections.

Destination	Target Type	Target	Route Type	Description
10.200.0.0/16	Dynamic Routing Gateways	Shadab-DRG	Static	
172.31.0.0/16	Dynamic Routing Gateways	Shadab-DRG	Static	
172.41.0.0/16	Dynamic Routing Gateways	Shadab-DRG	Static	

**Route Table Information**

OCID: ...vmmiffq [Show](#) [Copy](#)

Created: Sun, Nov 1, 2020, 12:57:15 UTC

Compartment: shadabshaukat (root)

**Route Rules**

Traffic within the VCN is handled by the VCN's local routing by default. Intra-VCN routing allows you more control over routing between subnets. [Learn more](#). If you're having problems, use [Network Path Analyzer](#) to check your connections.

Destination	Target Type	Target	Route Type	Description
0.0.0.0/0	Internet Gateway	Internet Gateway-Shadabshaukat-VCN	Static	
10.200.0.0/16	Dynamic Routing Gateways	Shadab-DRG	Static	
172.31.0.0/16	Dynamic Routing Gateways	Shadab-DRG	Static	
172.41.0.0/16	Dynamic Routing Gateways	Shadab-DRG	Static	

In OCI Melbourne VCN in both Route tables

Cloud

Search resources, services, documentation, and Marketplace

Australia Southeast (Melbourne)

OCID: ...tzydxja Show Copy

Created: Sat, Mar 15, 2025, 04:36:10 UTC

Compartment: shadabshaukat (root)

AVAILABLE

Resources

Route Rules (5)

Route Rules

Traffic within the VCN is handled by the VCN's local routing by default. Intra-VCN routing allows you more control over routing between subnets. [Learn more](#). If you're having problems, use [Network Path Analyzer](#) to check your connections.

Add Route Rules Edit Remove

<input type="checkbox"/>	Destination	Target Type	Target	Route Type	Description
<input type="checkbox"/>	0.0.0.0/0	NAT Gateway	<a href="#">NAT_gateway-VCN-MELB</a>	Static	
<input type="checkbox"/>	10.100.0.0/16	Dynamic Routing Gateways	<a href="#">MEL-DRG</a>	Static	
<input type="checkbox"/>	172.31.0.0/16	Dynamic Routing Gateways	<a href="#">MEL-DRG</a>	Static	
<input type="checkbox"/>	172.41.0.0/16	Dynamic Routing Gateways	<a href="#">MEL-DRG</a>	Static	
<input type="checkbox"/>	All MEL Services In Oracle Services Network	Service Gateway	<a href="#">Service_gateway-VCN-MELB</a>	Static	

0 selected

Showing 5 items < 1 of 1 >

Cloud

Search resources, services, documentation, and Marketplace

Australia Southeast (Melbourne)

OCID: ...a5cw2qza Show Copy

Created: Sat, Mar 15, 2025, 04:36:09 UTC

Compartment: shadabshaukat (root)

AVAILABLE

Resources

Route Rules (4)

Route Rules

Traffic within the VCN is handled by the VCN's local routing by default. Intra-VCN routing allows you more control over routing between subnets. [Learn more](#). If you're having problems, use [Network Path Analyzer](#) to check your connections.

Add Route Rules Edit Remove

<input type="checkbox"/>	Destination	Target Type	Target	Route Type	Description
<input type="checkbox"/>	0.0.0.0/0	Internet Gateway	<a href="#">Internet_gateway-VCN-MELB</a>	Static	
<input type="checkbox"/>	10.100.0.0/16	Dynamic Routing Gateways	<a href="#">MEL-DRG</a>	Static	
<input type="checkbox"/>	172.31.0.0/16	Dynamic Routing Gateways	<a href="#">MEL-DRG</a>	Static	
<input type="checkbox"/>	172.41.0.0/16	Dynamic Routing Gateways	<a href="#">MEL-DRG</a>	Static	

0 selected

Showing 4 items < 1 of 1 >

Make sure your Security list on OCI VCNs in Sydney and Melbourne allows port 22 connection from both AWS VPC CIDRs

Cloud

Search resources, services, documentation, and Marketplace

Australia Southeast (Melbourne)

<input type="checkbox"/>	No	10.200.0.0/16	TCP	All	22	ports: 22 SSH Remote Login Protocol
<input type="checkbox"/>	No	0.0.0.0/0	ICMP		3, 4	ICMP traffic for: 3, 4 Destination Unreachable: Fragmentation Needed and Don't Fragment was Set
<input type="checkbox"/>	No	10.200.0.0/16	ICMP		3	ICMP traffic for: 3 Destination Unreachable
<input type="checkbox"/>	No	172.31.0.0/16	TCP	All	22	TCP traffic for ports: 22 SSH Remote Login Protocol
<input type="checkbox"/>	No	172.41.0.0/16	TCP	All	22	TCP traffic for ports: 22 SSH Remote Login Protocol
<input type="checkbox"/>	No	10.100.0.0/16	TCP	All	22	TCP traffic for ports: 22 SSH Remote Login Protocol

0 selected

Showing 6 items < 1 of 1 >

Now Lets do a connectivity test from each instance in 1 AWS region to other regions in OCI and repeat for all regions in both AWS and OCI.

*AWS us-east-1 Instance IP : 172.31.91.251*  
*AWS us-west-1 Instance IP : 172.41.144.120*  
*OCI Sydney VM : 10.100.1.35*  
*OCI Melbourne VM : 10.200.2.250*

*From AWS us-east-1 Instance IP : 172.31.91.251 to :*  
*AWS us-west-1 Instance IP : 172.41.144.120*  
*[ec2-user@ip-172-31-91-251 ~]\$ telnet 172.41.144.120 22*  
*Trying 172.41.144.120...*  
*Connected to 172.41.144.120.*  
*Escape character is '^]'.*  
*SSH-2.0-OpenSSH\_8.7*

*OCI Sydney VM : 10.100.1.35*  
*[ec2-user@ip-172-31-91-251 ~]\$ telnet 10.100.1.35 22*  
*Trying 10.100.1.35...*  
*Connected to 10.100.1.35.*  
*Escape character is '^]'.*  
*SSH-2.0-OpenSSH\_8.0*

*OCI Melbourne VM : 10.200.2.250*  
*[ec2-user@ip-172-31-91-251 ~]\$ telnet 10.200.2.250 22*  
*Trying 10.200.2.250...*  
*Connected to 10.200.2.250.*  
*Escape character is '^]'.*  
*SSH-2.0-OpenSSH\_8.0*

*From AWS us-west-1 Instance IP : 172.41.144.120 to :*  
*AWS us-east-1 Instance IP : 172.31.91.251*  
*[ec2-user@ip-172-41-144-120 ~]\$ telnet 172.31.91.251 22*  
*Trying 172.31.91.251...*  
*Connected to 172.31.91.251.*  
*Escape character is '^]'.*  
*SSH-2.0-OpenSSH\_8.7*

*OCI Sydney VM : 10.100.1.35*  
*[ec2-user@ip-172-41-144-120 ~]\$ telnet 10.100.1.35 22*  
*Trying 10.100.1.35...*  
*Connected to 10.100.1.35.*  
*Escape character is '^]'.*  
*SSH-2.0-OpenSSH\_8.0*

*OCI Melbourne VM : 10.200.2.250*  
*[ec2-user@ip-172-41-144-120 ~]\$ telnet 10.200.2.250 22*  
*Trying 10.200.2.250...*

Connected to 10.200.2.250.  
Escape character is '^]'.  
SSH-2.0-OpenSSH\_8.0

*From OCI Sydney VM : 10.100.1.35 to :*

*AWS us-east-1 Instance IP : 172.31.91.251*

*[opc@ords-secondary ~]\$ curl -v telnet://172.31.91.251:22*

*\* Rebuilt URL to: telnet://172.31.91.251:22/*

*\* Trying 172.31.91.251...*

*\* TCP\_NODELAY set*

*\* Connected to 172.31.91.251 (172.31.91.251) port 22 (#0)*

*AWS us-west-1 Instance IP : 172.41.144.120*

*[opc@ords-secondary ~]\$ curl -v telnet://172.41.144.120:22*

*\* Rebuilt URL to: telnet://172.41.144.120:22/*

*\* Trying 172.41.144.120...*

*\* TCP\_NODELAY set*

*\* Connected to 172.41.144.120 (172.41.144.120) port 22 (#0)*

*OCI Melbourne VM : 10.200.2.250*

*[opc@ords-secondary ~]\$ curl -v telnet://10.200.2.250:22*

*\* Rebuilt URL to: telnet://10.200.2.250:22/*

*\* Trying 10.200.2.250...*

*\* TCP\_NODELAY set*

*\* Connected to 10.200.2.250 (10.200.2.250) port 22 (#0)*

SSH-2.0-OpenSSH\_8.0

*From OCI Melbourne VM : 10.200.2.250 to :*

*AWS us-east-1 Instance IP : 172.31.91.251*

*[opc@instance-20250324-2246 ~]\$ curl -v telnet://172.31.91.251:22*

*\* Rebuilt URL to: telnet://172.31.91.251:22/*

*\* Trying 172.31.91.251...*

*\* TCP\_NODELAY set*

*\* Connected to 172.31.91.251 (172.31.91.251) port 22 (#0)*

*AWS us-west-1 Instance IP : 172.41.144.120*

*[opc@instance-20250324-2246 ~]\$ curl -v telnet://172.41.144.120:22*

*\* Rebuilt URL to: telnet://172.41.144.120:22/*

*\* Trying 172.41.144.120...*

*\* TCP\_NODELAY set*

*\* Connected to 172.41.144.120 (172.41.144.120) port 22 (#0)*

*OCI Sydney VM : 10.100.1.35*

*[opc@instance-20250324-2246 ~]\$ curl -v telnet://10.100.1.35:22*

*\* Rebuilt URL to: telnet://10.100.1.35:22/*

*\* Trying 10.100.1.35...*

*\* TCP\_NODELAY set*

*\* Connected to 10.100.1.35 (10.100.1.35) port 22 (#0)*

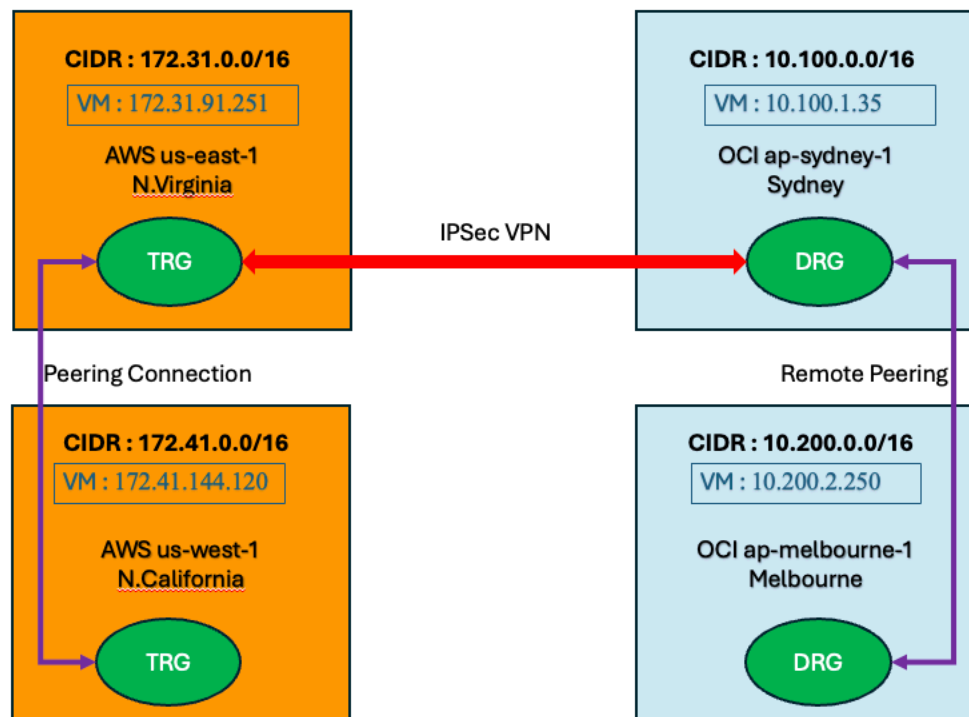
## Connectivity Tests:

Source Instance	Destination Instance	Test Method	Result
AWS us-east-1 (172.31.91.251)	OCI Sydney (10.100.1.35)	SSH/Telnet	✓ Pass
AWS us-east-1 (172.31.91.251)	OCI Melbourne (10.200.2.250)	SSH/Telnet	✓ Pass
AWS us-west-1 (172.41.144.120)	OCI Sydney (10.100.1.35)	SSH/Telnet	✓ Pass
AWS us-west-1 (172.41.144.120)	OCI Melbourne (10.200.2.250)	SSH/Telnet	✓ Pass
OCI Sydney (10.100.1.35)	AWS us-east-1 (172.31.91.251)	SSH/Telnet	✓ Pass
OCI Sydney (10.100.1.35)	AWS us-west-1 (172.41.144.120)	SSH/Telnet	✓ Pass
OCI Melbourne (10.200.2.250)	AWS us-east-1 (172.31.91.251)	SSH/Telnet	✓ Pass
OCI Melbourne (10.200.2.250)	AWS us-west-1 (172.41.144.120)	SSH/Telnet	✓ Pass

### SUMMARY

We've now created routing and connection over port 22 from all regions in AWS(x2) to all regions in OCI (x2) using Transit Routing Gateway in AWS and Dynamic Routing Gateway in OCI.

TRG are paired with Peering connections; DRG are paired with Remote Peering Connection. IPsec Tunnel in OCI has Import Route Distribution Added for the IPsec Tunnel connection. AWS TRG has Route Table Static routes added for OCI and other AWS region.



All the route rules, security group, security list in this Whitepaper for both AWS and OCI is only tested for port 22. For any other ports ensure you add the required tcp or udp ports in each of the security groups in AWS and security list in OCI.

## Conclusion

This whitepaper outlines an extendable multi-cloud routing architecture integrating AWS Transit Gateway and OCI DRG. By leveraging site-to-site VPNs, dynamic BGP routing, and remote peering connections, enterprises can achieve scalable and secure connectivity across multiple AWS and OCI regions.

This solution provides the following benefits:

- **Scalability:** Extendable to additional regions and VPCs.
- **Security:** Encrypted connectivity using IPSec VPN.
- **Resilience:** High availability with redundant tunnels and peering.
- **Operational Efficiency:** Centralized routing management across multiple cloud regions.

## REFERENCES

[https://docs.oracle.com/en-us/iaas/Content/Network/Tasks/vpn\\_to\\_aws.htm](https://docs.oracle.com/en-us/iaas/Content/Network/Tasks/vpn_to_aws.htm)  
<https://docs.aws.amazon.com/vpc/latest/tgw/tgw-peering-create.html>  
<https://docs.aws.amazon.com/vpc/latest/tgw/tgw-peering.html>  
<https://docs.aws.amazon.com/vpc/latest/tgw/tgw-peering-add-route.html>  
<https://www.ateam-oracle.com/post/setting-up-secure-sitetosite-vpn-connectivity-from-oci-to-aws-transit-gateway>  
<https://medium.com/@ystatit/azure-ipsec-vpn-to-oci-plus-oci-remote-peering-0b09e62e50a2>