

Transit Gateway

A *transit gateway* is a network transit hub that you can use to interconnect your virtual private clouds (VPCs) and on-premises networks. As your cloud infrastructure expands globally, inter-Region peering connects transit gateways together using the AWS Global Infrastructure. All network traffic between AWS data centers is automatically encrypted at the physical layer.



The problem with VPC peering & Transit VPC

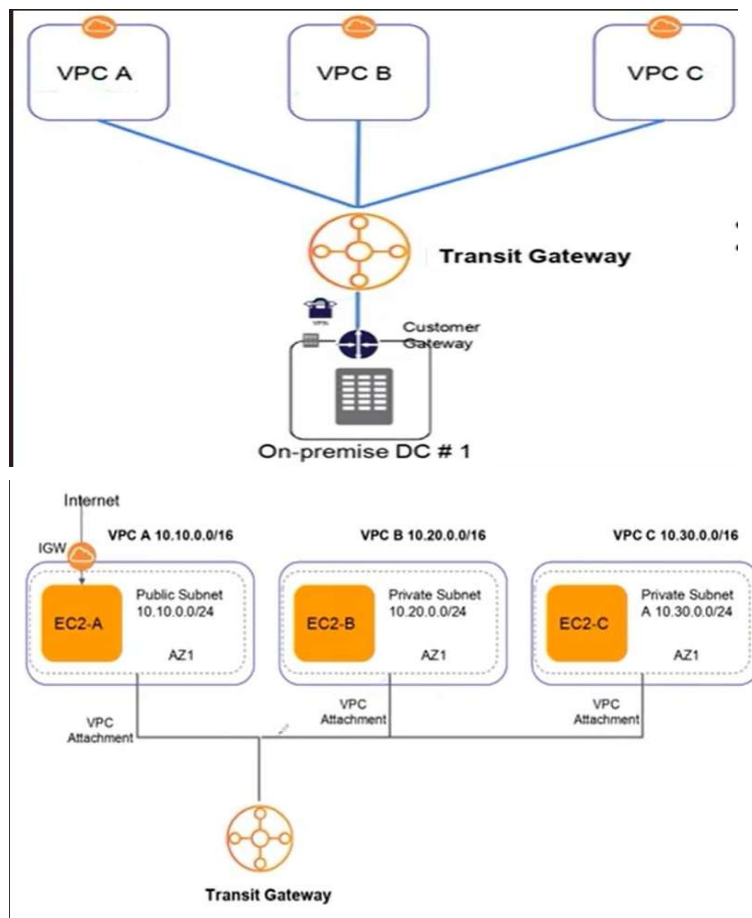
VPC Peering:

- Point-to-point connection between VPCs
- Non transitive traffic flow
- Separate connection for each VPC for on-premise VPN or Direct Connect

Transit VPC:

- Instance based (Cisco CSR 1000V)
- Additional EC2 cost
- Software Licensing cost
- Availability issues
- Bandwidth limitations of EC2

Here we're doing hands-on based on the below diagrams:



Select VPC from AWS console and Create VPC

[VPC](#) > [Your VPCs](#) > Create VPC

Create VPC [Info](#)

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.

VPC settings

Resources to create [Info](#)
Create only the VPC resource or the VPC and other networking resources.

☒ VPC only
 ☐ VPC and more

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

VPC A

IPv4 CIDR block [Info](#)

☒ IPv4 CIDR manual input
☐ IPAM-allocated IPv4 CIDR block

IPv4 CIDR

10.10.0.0/16

IPv6 CIDR block [Info](#)

☒ No IPv6 CIDR block
☐ IPAM-allocated IPv6 CIDR block
☐ Amazon-provided IPv6 CIDR block
☐ IPv6 CIDR owned by me

Tenancy [Info](#)

Default

Then click on Create VPC.

In a similar way , create other 2 CPCs naming VPC B and VPC C with 10.20.0.0/16 . 10.30.0.0/16 as IP addresses respectively.

Your VPCs (4) [Info](#)

Find resources by attribute or tag

	Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP option set	Main route table	Main netw
<input type="checkbox"/>	Default	vpc-0901e48909247ddcb	Available	172.31.0.0/16	-	dopt-029001ef65421c8...	rtb-05c161c1bb365f6	acl-0f38b...
<input type="checkbox"/>	VPC A	vpc-02c77757ccac5757d	Available	10.10.0.0/16	-	dopt-029001ef65421c8...	-	-
<input type="checkbox"/>	VPC B	vpc-002c8d51809e98dd7	Available	10.20.0.0/16	-	dopt-029001ef65421c8...	-	-
<input type="checkbox"/>	VPC C	vpc-011a9434def19f493	Available	10.30.0.0/16	-	dopt-029001ef65421c8...	-	-

From the diagram , we can see VPC A is public and VPC B & C are private. So we need to configure Internet GateWay for VPC A.

Click on Internet Gateway from the LHS panel and click on create Internet Gateway.

[VPC](#) > [Internet gateways](#) > Create internet gateway

Create internet gateway [Info](#)

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.

Internet gateway settings

Name tag

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

VPC-A-IGW

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

Q Name

Value - optional

Q VPC-A-IGW

Remove

Add new tag

You can add 49 more tags.

Cancel

Create internet gateway

Now select the newly created IGW and select Attach to VPC from Actions.

Internet gateways (1/2) Info						Actions Create internet gateway	
Q Filter internet gateways						View details	
						Attach to VPC	
						Detach from VPC	
						Manage tags	
						Delete internet gateway	
<input type="checkbox"/>	Name	Internet gateway ID	State	VPC ID	Owner		
<input type="checkbox"/>	Default	igw-029e689907e172658	Attached	vpc-0901e48909247ddcb Default	598823471631		
<input checked="" type="checkbox"/>	VPC-A-IGW	igw-089bbe41e4c57b23	Detached	-	598823471631		

Select VPC A from drop down and click on Attach internet gateway

[VPC](#) > [Internet gateways](#) > Attach to VPC (igw-01443e5f8f3595425)

Attach to VPC (igw-01443e5f8f3595425) [Info](#)

VPC

Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.

Available VPCs

Attach the internet gateway to this VPC.

► **AWS Command Line Interface command**

[Cancel](#) [Attach internet gateway](#)

Next we need to create Subnets, for that click on Subnets from the LHS panel and click on create subnet for VPC A as per below:

VPC

VPC ID
Create subnets in this VPC.

vpc-02c77757ccac5757d (VPC A) ▼

Associated VPC CIDRs

IPv4 CIDRs

10.10.0.0/16

Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.

VPC-A-Public-Subnet1

The name can be up to 256 characters long.

Availability Zone [Info](#)
Choose the zone in which your subnet will reside, or let Amazon choose one for you.

US East (Ohio) / us-east-2a ▼

IPv4 CIDR block [Info](#)

10.10.1.0/24 ✕

► **Tags - optional**

Remove

Add new subnet

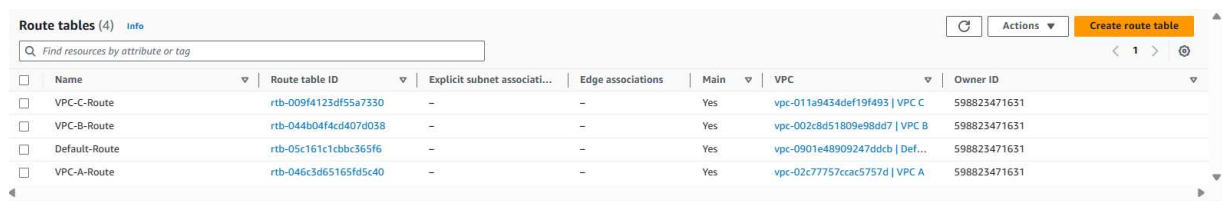
Likewise , we have to create 3 subnets for each VPC. I have created with the info below:

VPC-A-Public-Subnet1
10.10.1.0/24

VPC-B-Private-Subnet1
10.20.1.0/24

VPC-C-Private-Subnet1
10.30.1.0/24

Now we need to add the route tables , Click on Route Tables from the LHS panel and click on create route table.

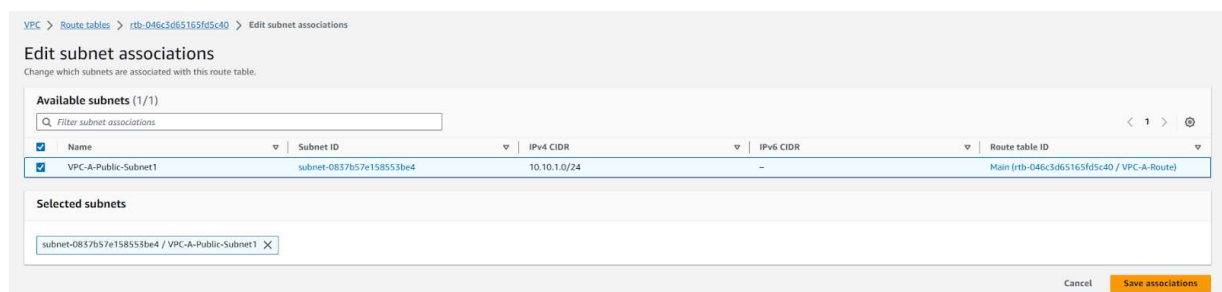


Route tables (4) Info

Find resources by attribute or tag

<input type="checkbox"/>	Name	Route table ID	Explicit subnet associati...	Edge associations	Main	VPC	Owner ID
<input type="checkbox"/>	VPC-C-Route	rtb-009f4123df55a7330	-	-	Yes	vpc-011a9434def19f493 VPC C	598823471631
<input type="checkbox"/>	VPC-B-Route	rtb-044b04f4cd407d038	-	-	Yes	vpc-002c8d51809e98dd7 VPC B	598823471631
<input type="checkbox"/>	Default-Route	rtb-05c161c1cbbc365f6	-	-	Yes	vpc-0901e48909247ddcb Def...	598823471631
<input type="checkbox"/>	VPC-A-Route	rtb-046c3d65165fd5c40	-	-	Yes	vpc-02c77757ccac5757d VPC A	598823471631

Next we have to associate the subnet with routing table. For that select VPC-A-Route -> Click on Subnet associations -> Edit subnet associations , then select VPC-A-Public-Subnet1 -> Save associations.



VPC > Route tables > rtb-046c3d65165fd5c40 > Edit subnet associations

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (1/1)

Filter subnet associations

<input checked="" type="checkbox"/>	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
<input checked="" type="checkbox"/>	VPC-A-Public-Subnet1	subnet-0837b57e158553be4	10.10.1.0/24	-	Main (rtb-046c3d65165fd5c40 / VPC-A-Route)

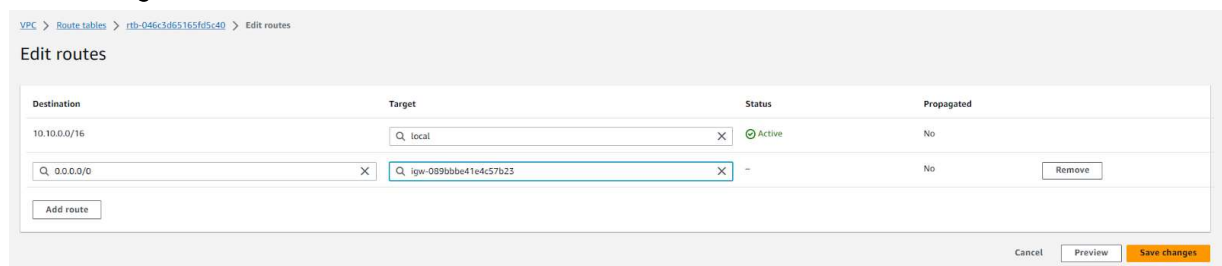
Selected subnets

subnet-0837b57e158553be4 / VPC-A-Public-Subnet1 X

Cancel Save associations

Do the same for VPC-B-Route and VPC-C-Route.

Select the VPC-A-Route and go to Routes->Edit routes and add as per below , then click on save changes.



VPC > Route tables > rtb-046c3d65165fd5c40 > Edit routes

Edit routes

Destination	Target	Status	Propagated
10.10.0.0/16	local	Active	No
0.0.0.0/0	igw-0990bbe41e4c57b23	-	No

Add route

Cancel Preview Save changes

We're all set in the VPC part , Now select EC2 from AWS console and create 2 instances as per above diagram.

Launch an instance [Info](#)

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags [Info](#)

Name








VPC-A-Public

[Add additional tags](#)

▼ Application and OS Images (Amazon Machine Image) [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Quick Start

						 Browse more AMIs Including AMIs from AWS, Marketplace and the Community
---	---	---	---	---	---	---

Amazon Machine Image (AMI)

Configure Network Settings as below:

▼ Network settings Info

VPC - required Info

vpc-02c77757ccac5757d (VPC A)
10.10.0.0/16

↻

Subnet Info

subnet-0837b57e158553be4 VPC-A-Public-Subnet1
VPC: vpc-02c77757ccac5757d Owner: 598823471631 Availability Zone: us-east-2a
IP addresses available: 251 CIDR: 10.10.1.0/24

↻ Create new subnet

Auto-assign public IP Info

Enable

Firewall (security groups) Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☒ Create security group

☐ Select existing security group

Security group name - required

VPC-A

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and . _ - / () # , @ [] + = & ; { } ! \$ *

Description - required Info

VPC-A

Inbound Security Group Rules

▼ Security group rule 1 (TCP, 22, 103.203.73.60/32)

Remove

Type Info	Protocol Info	Port range Info
ssh	TCP	22
Source type Info	Name Info	Description - optional Info
My IP	<div>Add CIDR, prefix list or security</div> <div>103.203.73.60/32 X</div>	e.g. SSH for admin desktop

And launch the instance.
Now create VPC-B-Private as below:

▼ Network settings

Info

VPC - required

Info

vpc-002c8d51809e98dd7 (VPC B)

10.20.0.0/16

▼

↻

Subnet

Info

subnet-0b7bdf9b79dac2085

VPC-B-Private-Subnet1

▼

VPC: vpc-002c8d51809e98dd7

Owner: 598823471631

Availability Zone: us-east-2a

IP addresses available: 251

CIDR: 10.20.1.0/24)

↻

Create new subnet

↗

Auto-assign public IP

Info

Disable

▼

Firewall (security groups)

Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☒ Create security group

☐ Select existing security group

Security group name - required

VPC-B

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and . _ - / () # , @ [] + = & ; { } ! \$ *

Description - required

Info

VPC-B

Inbound Security Group Rules

▼ Security group rule 1 (All, All, 10.0.0.0/8)

Remove

Type

Info

All traffic

▼

Protocol

Info

All

Port range

Info

All

Source type

Info

Custom

▼

Source

Info

Q Add CIDR, prefix list or security

10.0.0.0/8

×

Description - optional

Info

e.g. SSH for admin desktop

Rest all settings are default or same as VPC-A-Public. Then create one more instance same as VPC-B-Private.

Also create one more inbound rule in VPC-A-Public as shown below:

EC2 > Security Groups > sg-02e1bd04e22740376 - VPC-A > Edit inbound rules

Edit inbound rules info

Inbound rules control the incoming traffic that's allowed to reach the instance.

Security group rule ID	Type <small>info</small>	Protocol <small>info</small>	Port range <small>info</small>	Source <small>info</small>	Description - optional <small>info</small>	
sg-00f3cd4d64bab6fb6	SSH	TCP	22	Custom	10.20.1.233	Delete
-	All traffic	All	All	Custom	10.0.0.0/8	Delete

[Add rule](#)

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

Once the instances are up and running , take the ssh connection and login as root. Then from VPC-A-Public , check if the private IPs of VPC-B-Private and VPC-C-Private are reachable. It should not be reachable as below:

```
[root@ip-10-10-1-23 ec2-user]# ping 10.20.1.233
PING 10.20.1.233 (10.20.1.233) 56(84) bytes of data.
^C
--- 10.20.1.233 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4130ms

[root@ip-10-10-1-23 ec2-user]# ping 10.30.1.49
PING 10.30.1.49 (10.30.1.49) 56(84) bytes of data.
^C
--- 10.30.1.49 ping statistics ---
6 packets transmitted, 0 received, 100% packet loss, time 5192ms

[root@ip-10-10-1-23 ec2-user]#
```

Now we need to connect VPCs among each other.

Go to VPC and click on Transit Gateway.

Create Transit Gateway as shown below

VPC > Transit gateways > Create transit gateway

Create transit gateway [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 - *optional*

Name tag

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

Description [Info](#)

Set the description of your transit gateway to help you identify it in the future.

Configure the transit gateway

Amazon side Autonomous System Number (ASN) [Info](#)

☒ DNS support [Info](#)

☒ VPN ECMP support [Info](#)

☒ Default route table association [Info](#)

☒ Default route table propagation [Info](#)

☐ Multicast support [Info](#)

Select Transit gateway attachment from LHS panel and create Transit gateway attachment for every VPCs.

Give a name and select the transit gateway as shown below:

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](#)

Attachment type [Info](#)

Then configure the attachment as below:

VPC attachment

Select and configure your VPC attachment.

☒ DNS support [Info](#)

☐ IPv6 support [Info](#)

☐ Appliance Mode support [Info](#)

VPC ID

Select the VPC to attach to the transit gateway.

vpc-02c77757ccac5757d (VPC A) ▼

Subnet IDs [Info](#)

Select the subnets in which to create the transit gateway VPC attachment.

☒ us-east-2a

subnet-0837b57e158553be4 (VPC-A-Public-Sub... ▼

☐ us-east-2b

No subnet available

☐ us-east-2c

No subnet available

subnet-0837b57e158553be4 ✕

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.

Key

Q Name ✕

Value - optional

Q VPC A ✕

Remove

Add new tag

You can add 49 more tags.

Cancel

Create transit gateway attachment

Sameway create another 2 attachments for VPC B and VPC C.

Select Transit gateway route tables from the LHS panel and go to the routes , we can see the VPC CIDR have been listed there.

Routes (3)									
Filter routes									
<input type="checkbox"/>	CIDR	Attachment ID	Resource ID	Resource type	Route type	Route state	Prefix list ID		
<input type="checkbox"/>	10.10.0.0/16	tgw-attach-0204f02950a18d928	vpc-02c77757ccac5757d	VPC	Propagated	Active	-		
<input type="checkbox"/>	10.20.0.0/16	tgw-attach-09426ce1aa7f8372e	vpc-002c8d51809e98dd7	VPC	Propagated	Active	-		
<input type="checkbox"/>	10.30.0.0/16	tgw-attach-04844306da274fbc9	vpc-011a9434def19f493	VPC	Propagated	Active	-		

Now go to Route Tables, select VPC A and add route as shown below:

VPC > Route tables > rtb-046c3d65165f05c40 > Edit routes

Edit routes

Destination	Target	Status	Propagated
10.10.0.0/16	local	Active	No
0.0.0.0/0	igw-069bbbe41e4c57b23	Active	No
10.0.0.0/8	tgw-07e5e02b7985a1bbf	-	No

Update the same for VPC B and VPC C.

Now check the connectivity from VPC-A-Public , check if the private IPs of VPC-B-Private and VPC-C-Private are reachable.

```
[root@ip-10-10-1-23 ec2-user]#  
[root@ip-10-10-1-23 ec2-user]# ping 10.20.1.233  
PING 10.20.1.233 (10.20.1.233) 56(84) bytes of data.  
64 bytes from 10.20.1.233: icmp_seq=1 ttl=126 time=1.12 ms  
64 bytes from 10.20.1.233: icmp_seq=2 ttl=126 time=0.546 ms  
64 bytes from 10.20.1.233: icmp_seq=3 ttl=126 time=0.638 ms  
^C  
--- 10.20.1.233 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2079ms  
rtt min/avg/max/mdev = 0.546/0.766/1.115/0.249 ms  
[root@ip-10-10-1-23 ec2-user]#  
[root@ip-10-10-1-23 ec2-user]#  
[root@ip-10-10-1-23 ec2-user]#  
[root@ip-10-10-1-23 ec2-user]# ping 10.30.1.49  
PING 10.30.1.49 (10.30.1.49) 56(84) bytes of data.  
64 bytes from 10.30.1.49: icmp_seq=1 ttl=126 time=0.836 ms  
64 bytes from 10.30.1.49: icmp_seq=2 ttl=126 time=0.746 ms  
64 bytes from 10.30.1.49: icmp_seq=3 ttl=126 time=0.768 ms  
64 bytes from 10.30.1.49: icmp_seq=4 ttl=126 time=0.658 ms  
^C  
--- 10.30.1.49 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3097ms  
rtt min/avg/max/mdev = 0.658/0.752/0.836/0.063 ms  
[root@ip-10-10-1-23 ec2-user]#
```

We can see it is reachable. This is how the Transit gateway works..!!!!

