

# VPC-Peering

## 1. Create VPC-A

Your VPCs (2) [Info](#) Refresh Actions Create VPC

Filter VPCs

<input type="checkbox"/>	Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP
<input type="checkbox"/>	-	vpc-0a2b91a26ed02e516	Available	172.31.0.0/16	-	dopt-0
<input type="checkbox"/>	Sravani-VPC-A	vpc-055f0903a7b2f19ae	Available	10.100.0.0/16	-	dopt-0

## 2. Create 2 subnets in VPC-A (One private subnet and one public subnet)

You have successfully created 1 subnet: subnet-0e9d6e8d8f38b2af6 Close

Subnets (2) [Info](#) Refresh Actions Create subnet

Filter subnets

<input type="checkbox"/>	Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR
<input type="checkbox"/>	Sravani-VPCA-PrivSN	subnet-0d3405667c7b73cd0	Available	vpc-055f0903a7b2f19ae   Sra...	10.100.1.0/24	-
<input type="checkbox"/>	Sravani-VPCA-PubSN	subnet-0e9d6e8d8f38b2af6	Available	vpc-055f0903a7b2f19ae   Sra...	10.100.0.0/24	-

## 3. Create internet gateway

The following internet gateway was created: igw-01ef10d326c7dc9c8 - Sravani-IGW. You can now attach to a VPC to enable the VPC to communicate with the internet. Attach to a VPC Close

Internet gateways (1/1) [Info](#) Refresh Actions Create internet gateway

Filter internet gateways

<input checked="" type="checkbox"/>	Name	Internet gateway ID	State	VPC ID	Owner
<input checked="" type="checkbox"/>	Sravani-IGW	igw-01ef10d326c7dc9c8	Detached	-	738974081103

#### 4. Attach internet gateway to a VPC

VPC > Internet gateways > Attach to VPC (igw-01ef10d326c7dc9c8)

### Attach to VPC (igw-01ef10d326c7dc9c8) [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.

Q vpc-055f0903a7b2f19ae X

▶ AWS Command Line Interface command

Cancel

Attach internet gateway

#### 5. Create route tables

Route table rtb-04f1e4ae1ced7782a | SravaniVPCA-PubRT was created successfully. X

Route tables (4) [Info](#) Refresh Actions Create route table

Filter route tables

<input type="checkbox"/>	Name	Route table ID	Explicit subnet associat...	Edge associations	Main	VPC	Ow..
<input type="checkbox"/>	-	rtb-0c1d4dcee53b1c750	-	-	Yes	vpc-055f0903a7b2f19ae   Sra...	7389
<input type="checkbox"/>	-	rtb-04b02f1552ec9a346	-	-	Yes	vpc-0a2b91a26ed02e516	7389
<input type="checkbox"/>	SravaniVPCA-PrivRT	rtb-0a01a7716123a1895	-	-	No	vpc-055f0903a7b2f19ae   Sra...	7389
<input type="checkbox"/>	SravaniVPCA-PubRT	rtb-04f1e4ae1ced7782a	-	-	No	vpc-055f0903a7b2f19ae   Sra...	7389

#### 6. Associate subnets to route tables (Private-Private and Public-Public)

VPC > Route tables > rtb-04f1e4ae1ced7782a > Edit subnet associations

### Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (1/2)

Filter subnet associations

<input type="checkbox"/>	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
<input type="checkbox"/>	Sravani-VPCA-PrivSN	subnet-0d3405667c7b73cd0	10.100.1.0/24	-	Main (rtb-0c1d4dcee53b1c750)
<input checked="" type="checkbox"/>	Sravani-VPCA-PubSN	subnet-0e9d6e8d8f38b2af6	10.100.0.0/24	-	Main (rtb-0c1d4dcee53b1c750)

Selected subnets

subnet-0e9d6e8d8f38b2af6 / Sravani-VPCA-PubSN X

Cancel Save associations

VPC > Route tables > rtb-0a01a7716123a1895 > Edit subnet associations

### Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (1/2)

Filter subnet associations

<input type="checkbox"/>	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
<input checked="" type="checkbox"/>	Sravani-VPCA-PrivSN	subnet-0d3405667c7b73cd0	10.100.1.0/24	-	Main (rtb-0c1d4dcee53b1c750)
<input type="checkbox"/>	Sravani-VPCA-PubSN	subnet-0e9d6e8d8f38b2af6	10.100.0.0/24	-	rtb-04f1e4ae1ced7782a / SravaniVPCA-PubRT

Selected subnets

subnet-0d3405667c7b73cd0 / Sravani-VPCA-PrivSN X

Cancel Save associations

7. Connect the public route table to internet gateway

VPC > Route tables > rtb-04f1e4ae1ced7782a > Edit routes

### Edit routes

Destination	Target	Status	Propagated
10.100.0.0/16	local	Active	No
0.0.0.0/0	igw-01ef10d326c7dc9c8	-	No

Add route

Cancel Preview Save changes

8. Create EC2 instances in public subnet and private subnet of first VPC, create security groups and select enable public ip along with instance creation:

Instances (2) Info

Find instance by attribute or tag (case-sensitive)

<input type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
<input type="checkbox"/>	Sravani-VPCA-PubInst	i-0761b0131abb6f0b6	Running	t2.micro	-	No alarms	ap-southeast-2a
<input type="checkbox"/>	Sravani-VPCA-PrivInst	i-03d45f6b614984881	Running	t2.micro	Initializing	No alarms	ap-southeast-2a

9. Security groups created along with instances:

Security Groups (2/4) Info

Filter security groups

<input type="checkbox"/>	Name	Security group ID	Security group name	VPC ID	Description	Owner
<input checked="" type="checkbox"/>	Sravani-VPCA-Publ...	sg-02079ff3b0307b083	Sravani-VPCA-PubInst-...	vpc-055f0903a7b2f19ae	Sravani-VPCA-PubInst-...	738974081103
<input type="checkbox"/>	-	sg-033f5ff541dd00cb0	default	vpc-0a2b91a26ed02e516	default VPC security gr...	738974081103
<input checked="" type="checkbox"/>	Sravani-VPCA-PrvIn...	sg-0664b5e20a2c4ca2a	Sravani-VPCA-PrivInst-SG	vpc-055f0903a7b2f19ae	Sravani-VPCA-PrivInst-SG	738974081103
<input type="checkbox"/>	-	sg-0b9b1b2b1de696ca8	default	vpc-055f0903a7b2f19ae	default VPC security gr...	738974081103

## 10. Edit inbound rules of security groups to have All ICMP-IPv4

EC2 > Security Groups > sg-02079ff3b0307b083 - Sravani-VPCA-PubInst-SG > 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-09e5e71adc494c6ef	SSH	TCP	22	Custom	Q	0.0.0.0/0 X Delete
-	All ICMP - IPv4	ICMP	All	Anywh...	Q	0.0.0.0/0 X Delete

Add rule

Cancel Preview changes Save rules

## 11. Connect to the public instance in the first VPC

```
ec2-user@ip-10-100-0-106:~  
svulupa1@SVULUPAPF17UKG8 MINGW64 ~/Downloads  
$ ssh -i "Sydney.pem" ec2-user@13.55.139.195  
The authenticity of host '13.55.139.195 (13.55.139.195)' can't be established.  
ECDSA key fingerprint is SHA256:IX3qxgywhH+AP+WFxJJKrb63Z1AjpLL+eP8tRGWGc0.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '13.55.139.195' (ECDSA) to the list of known hosts.  
  
  _ | _ | _ )  
  _ | ( _ /  Amazon Linux 2 AMI  
  _ | \ _ | _ |  
  
https://aws.amazon.com/amazon-linux-2/  
13 package(s) needed for security, out of 16 available  
Run "sudo yum update" to apply all updates.  
[ec2-user@ip-10-100-0-106 ~]$
```

## 12. Connect to private instance in the first VPC from within the public instance since private instance is not connected to the internet:

- Copy the pem file to the public instance:

```
PS C:\Users\svulupa1\Downloads> scp -i '.\Sydney.pem' -r '.\Sydney.pem' ec2-user@13.55.139.195:/home/ec2-user  
Sydney.pem  
100% 1674 6.1KB/s 00:00  
PS C:\Users\svulupa1\Downloads>
```

- Connect to the private instance from public instance using the public ip of the private instance

✓ Sravani-VPCA-PrvInst i-03d45f6b614984881 Running t2.micro 2/2 checks passed No alerts

Instance: i-03d45f6b614984881 (Sravani-VPCA-PrvInst)

Details Security Networking Storage Status checks Monitoring Tags

Instance summary Info

Instance ID	Public IPv4 address	Private IPv4 address
i-03d45f6b614984881 (Sravani-VPCA-PrvInst)	3.25.116.55   <a href="#">open address</a>	10.100.1.57

Private IPv4 address copied

- Modify key permissions and connect to private instance using private ip:

```
ec2-user@ip-10-100-1-57:~
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@          WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0664 for 'Sydney.pem' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "Sydney.pem": bad permissions
Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
[ec2-user@ip-10-100-0-106 ~]$ chmod 777 Sydney.pem
[ec2-user@ip-10-100-0-106 ~]$ ls
Sydney.pem
[ec2-user@ip-10-100-0-106 ~]$ ssh -i Sydney.pem ec2-user@10.100.1.57
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@          WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0777 for 'Sydney.pem' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "Sydney.pem": bad permissions
Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
[ec2-user@ip-10-100-0-106 ~]$ ^C
[ec2-user@ip-10-100-0-106 ~]$ chmod 400 Sydney.pem
[ec2-user@ip-10-100-0-106 ~]$ ssh -i Sydney.pem ec2-user@10.100.1.57

  _ | _ | _ )
  _ | ( _ | /   Amazon Linux 2 AMI
  _ | \ _ | _ |

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-100-1-57 ~]$
```

### 13. Create a second VPC

Your VPCs (3) Info

Filter VPCs

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP
Sravani-VPC-B	vpc-0c903f350f17cec5c	Available	10.200.0.0/16	-	dopt-0
-	vpc-0a2b91a26ed02e516	Available	172.31.0.0/16	-	dopt-0
Sravani-VPC-A	vpc-055f0903a7b2f19ae	Available	10.100.0.0/16	-	dopt-0

14. Create a private subnet in the above VPC

<input type="checkbox"/>	Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR
<input type="checkbox"/>	Srvani-VPC-B-Prv-SN	subnet-035f27f24c24574e5	Available	vpc-0c903f350f17cec5c   Srv...	10.200.1.0/24	-
<input type="checkbox"/>	Srvani-VPCA-PrvSN	subnet-0d3405667c7b73cd0	Available	vpc-055f0903a7b2f19ae   Sra...	10.100.1.0/24	-
<input type="checkbox"/>	Srvani-VPCA-PubSN	subnet-0e9d6e8d8f38b2af6	Available	vpc-055f0903a7b2f19ae   Sra...	10.100.0.0/24	-

15. Create a route table and associate the private subnet above to the route table from the subnet associations menu:

<input type="checkbox"/>	Name	Route table ID	Explicit subnet associat...	Edge associations	Main	VPC	Ow..
<input type="checkbox"/>	-	rtb-0ac0d1c3a556e2065	-	-	Yes	vpc-0c903f350f17cec5c   Srv...	7389
<input type="checkbox"/>	-	rtb-0c1d4dcee53b1c750	-	-	Yes	vpc-055f0903a7b2f19ae   Sra...	7389
<input type="checkbox"/>	-	rtb-04b02f1552ec9a346	-	-	Yes	vpc-0a2b91a26ed02e516	7389
<input type="checkbox"/>	SrvaniVPCA-PrvRT	rtb-0a01a7716123a1895	subnet-0d3405667c7b7...	-	No	vpc-055f0903a7b2f19ae   Sra...	7389
<input type="checkbox"/>	SrvaniVPCA-PubRT	rtb-04f1e4ae1ced7782a	subnet-0e9d6e8d8f38b...	-	No	vpc-055f0903a7b2f19ae   Sra...	7389
<input type="checkbox"/>	SrvaniVPCB-PrvRT	rtb-00d64f190eb323b5e	subnet-035f27f24c2457...	-	No	vpc-0c903f350f17cec5c   Srv...	7389

Change which subnets are associated with this route table.

**Available subnets (1/1)**

<input checked="" type="checkbox"/>	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
<input checked="" type="checkbox"/>	Srvani-VPC-B-Prv-SN	subnet-035f27f24c24574e5	10.200.1.0/24	-	rtb-00d64f190eb323b5e / SrvaniVPCB-PrvRT

**Selected subnets**

subnet-035f27f24c24574e5 / Srvani-VPC-B-Prv-SN

Cancel Save associations

16. Create instance in the second VPC using the auto enable ip and creating a new security group:

<input type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
<input type="checkbox"/>	Srvani-VPCA-PubInst	i-0761b0131abb6f0b6	Running	t2.micro	2/2 checks passed	No alarms	ap-southeast-2a
<input type="checkbox"/>	Srvani-VPCA-PrvInst	i-03d45f6b614984881	Running	t2.micro	2/2 checks passed	No alarms	ap-southeast-2a
<input type="checkbox"/>	Srvani-VPCB-PrvInst	i-0b68e08198a9c391c	Running	t2.micro	Initializing	No alarms	ap-southeast-2a

## 17. Edit the security group to enable All ICMPIPv4

EC2 > Security Groups > sg-0305e7c878aa2e909 - Sravani-VPCB-PrvSN-SG > Edit inbound rules

### Edit inbound rules [Info](#)

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

#### Inbound rules [Info](#)

Security group rule ID	Type <a href="#">Info</a>	Protocol <a href="#">Info</a>	Port range <a href="#">Info</a>	Source <a href="#">Info</a>	Description - optional <a href="#">Info</a>	
sgr-0afce10d0719e88ca	SSH	TCP	22	Custom		Delete
-	All ICMP - IPv4	ICMP	All	Anywh...		Delete

[Add rule](#)

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

## 18. Create Peering connection using the following settings:

### Peering connection settings

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

Sravani-VPC-Peering

**Select a local VPC to peer with**

VPC ID (Requester)

vpc-055f0903a7b2f19ae (Sravani-VPC-A)

VPC CIDRs for vpc-055f0903a7b2f19ae (Sravani-VPC-A)

CIDR	Status	Status reason
10.100.0.0/16	Associated	-

**Select another VPC to peer with**

Account

My account

Another account

Region

This Region (ap-southeast-2)

Another Region

VPC ID (Acceptor)

vpc-0c903f350f17cec5c (Sravani-VPC-B)

19. Accept the pending request for the peering connection:

The screenshot shows the AWS console interface for 'Peering connections (1/1)'. A table lists a single connection with the status 'Pending acceptance'. An 'Actions' dropdown menu is open, highlighting the 'Accept request' option.

Name	Peering connection ID	Status	Requester VPC
Sravani-VPC-P...	pcx-0b39bf57f14a930f6	Pending acceptance	vpc-055f0903a7b2f19ae / Sra...

The screenshot shows the same AWS console interface, but the status of the peering connection is now 'Active'. The 'Actions' dropdown menu is closed.

Name	Peering connection ID	Status	Requester VPC	Acceptor VPC	Requester CIDI
Sravani-VPC-P...	pcx-0b39bf57f14a930f6	Active	vpc-055f0903a7b2f19ae / Sra...	vpc-0c903f350f17cec5c / Sra...	10.100.0.0/16

20. Update the route tables of both the private subnets of first and second VPC to make a connection from one to the other

- Route table of first VPC private subnet

The screenshot shows the 'Edit routes' page for a route table. The table below shows the current routes. A new route for destination 10.200.1.0/24 is being added with target pcx-0b39bf57f14a930f6.

Destination	Target	Status	Propagated
10.100.0.0/16	local	Active	No
10.200.1.0/24	pcx-0b39bf57f14a930f6	-	No

- Route table of second VPC private subnet

The screenshot shows the 'Edit routes' page for a route table. The table below shows the current routes. A new route for destination 10.100.1.0/24 is being added with target pcx-0b39bf57f14a930f6.

Destination	Target	Status	Propagated
10.200.0.0/16	local	Active	No
10.100.1.0/24	pcx-0b39bf57f14a930f6	Active	No



21. Ping the private subnet instance of the second VPC from the private subnet instance of the first VPC now after adding the routes.

```
[ec2-user@ip-10-100-1-57 ~]$ pwd
/home/ec2-user
[ec2-user@ip-10-100-1-57 ~]$ ping 10.200.1.103
PING 10.200.1.103 (10.200.1.103) 56(84) bytes of data:
64 bytes from 10.200.1.103: icmp_seq=1 ttl=255 time=0.460 ms
64 bytes from 10.200.1.103: icmp_seq=2 ttl=255 time=0.507 ms
64 bytes from 10.200.1.103: icmp_seq=3 ttl=255 time=0.483 ms
64 bytes from 10.200.1.103: icmp_seq=4 ttl=255 time=0.442 ms
64 bytes from 10.200.1.103: icmp_seq=5 ttl=255 time=0.445 ms
64 bytes from 10.200.1.103: icmp_seq=6 ttl=255 time=0.500 ms
64 bytes from 10.200.1.103: icmp_seq=7 ttl=255 time=0.481 ms
64 bytes from 10.200.1.103: icmp_seq=8 ttl=255 time=0.654 ms
64 bytes from 10.200.1.103: icmp_seq=9 ttl=255 time=0.445 ms
64 bytes from 10.200.1.103: icmp_seq=10 ttl=255 time=0.506 ms
64 bytes from 10.200.1.103: icmp_seq=11 ttl=255 time=0.448 ms
^C
--- 10.200.1.103 ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 10239ms
rtt min/avg/max/mdev = 0.442/0.488/0.654/0.059 ms
[ec2-user@ip-10-100-1-57 ~]$
```

22. Connect from the instance in first VPC private subnet1 to the instance in second VPC private subnet 1
- Copy the pem file from the instance in public subnet of the first VPC to the instance in private subnet of the first VPC

```
[ec2-user@ip-10-100-0-106 ~]$ scp -i Sydney.pem -r Sydney.pem ec2-user@10.100.1.57:/home/ec2-user/
r
Sydney.pem                               100% 1674   495.2KB/s   00:00
```

- Connect to the private subnet machine of the first VPC from public subnet of the first VPC

```
[ec2-user@ip-10-100-0-106 ~]$ ssh -i Sydney.pem ec2-user@10.100.1.57
Last login: Fri Oct 28 06:04:18 2022 from 10.100.0.106

  _ | _ | _ )
  _ | ( _ /   Amazon Linux 2 AMI
  _ | \ _ | _ |

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-100-1-57 ~]$ cd /home/ec2-user/
[ec2-user@ip-10-100-1-57 ~]$ ls
Sydney.pem
[ec2-user@ip-10-100-1-57 ~]$ chmod 400 Sydney.pem
[ec2-user@ip-10-100-1-57 ~]$
```

- c. Now, connect to the private subnet machine of the first VPC to the private subnet instance of the second VPC using the private ip

```
[ec2-user@ip-10-100-1-57 ~]$ ssh -i Sydney.pem ec2-user@10.200.1.103
[ec2-user@ip-10-100-1-57 ~]$ ssh -i Sydney.pem ec2-user@10.200.1.103
The authenticity of host '10.200.1.103 (10.200.1.103)' can't be established.
ECDSA key fingerprint is SHA256:jFHoUGqreWSfH6JfHeeRLInejCU+nhaqWNVVYDIM+Qo.
ECDSA key fingerprint is MD5:9e:4c:ed:97:c8:46:59:8e:c6:b8:5c:ea:34:aa:e9:0f.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.200.1.103' (ECDSA) to the list of known hosts.

  _ | _ | _ )
  _ | ( _ | /   Amazon Linux 2 AMI
  _ | \ _ | _ |

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-200-1-103 ~]$
```