VPC Architecture & VPC Peering Connection

1. Overview

This architecture represents two Virtual Private Clouds (VPCs):
- VPC-SIT (10.0.0.0/16): Primary VPC with web and database layers.
- VPC-SIT-2 (11.0.0.0/16): Secondary VPC with only a database subnet.

These VPCs are connected via VPC Peering to enable private communication between components.

2. CIDR Ranges

Component	CIDR Block
VPC-SIT	10.0.0.0/16
WEB-SUBNET	10.0.1.0/24
DB-SUBNET	10.0.2.0/24
VPC-SIT-2	11.0.0.0/16
DB-SUBNET-2	11.0.1.0/24

3. Subnets

In VPC-SIT:

- WEB-SUBNET (10.0.1.0/24):
  - Contains instances with both public and private IPs.
  - Accessible from the internet (via Internet Gateway).

- DB-SUBNET (10.0.2.0/24):
  - Private subnet for database instances.
  - No public IPs; requires NAT for outbound internet.

In VPC-SIT-2:

- DB-SUBNET-2 (11.0.1.0/24):
  - Private subnet.
  - Communicates with DB in VPC-SIT via VPC Peering.

4. VPC Peering Setup

1. Create Peering Connection between VPC-SIT and VPC-SIT-2.
2. Accept Peering Request from the other VPC.

3. Update Route Tables in both VPCs:
  - VPC-SIT route table: Add route to 11.0.0.0/16 via peering connection.
  - VPC-SIT-2 route table: Add route to 10.0.0.0/16 via peering connection.

5. Route Tables

Example routes:

Subnet	Routes Included
WEB-SUBNET	0.0.0.0/0 → Internet Gateway 11.0.0.0/16 → VPC Peering
DB-SUBNET	0.0.0.0/0 → NAT Gateway 11.0.0.0/16 → VPC Peering
DB-SUBNET-2	0.0.0.0/0 → NAT Gateway (if needed) 10.0.0.0/16 → VPC Peering

6. NAT Gateway

- Placed in WEB-SUBNET (public subnet).
- Purpose: Allows private subnets (DB-SUBNET) to access the internet without exposing their private IPs.
- Elastic IP: Allocate and associate to the NAT Gateway.

7. Internet Gateway (IGW)

- Attached to VPC-SIT.
- Enables WEB-SUBNET to access the internet and receive inbound traffic.
- Route 0.0.0.0/0 in web subnet route table points to IGW.

8. Elastic IP (EIP)

- Assigned to:
  - NAT Gateway: Required for stable outbound internet access.
  - EC2 instance (optional) in WEB-SUBNET: If you need a fixed public IP.

9. Security Groups

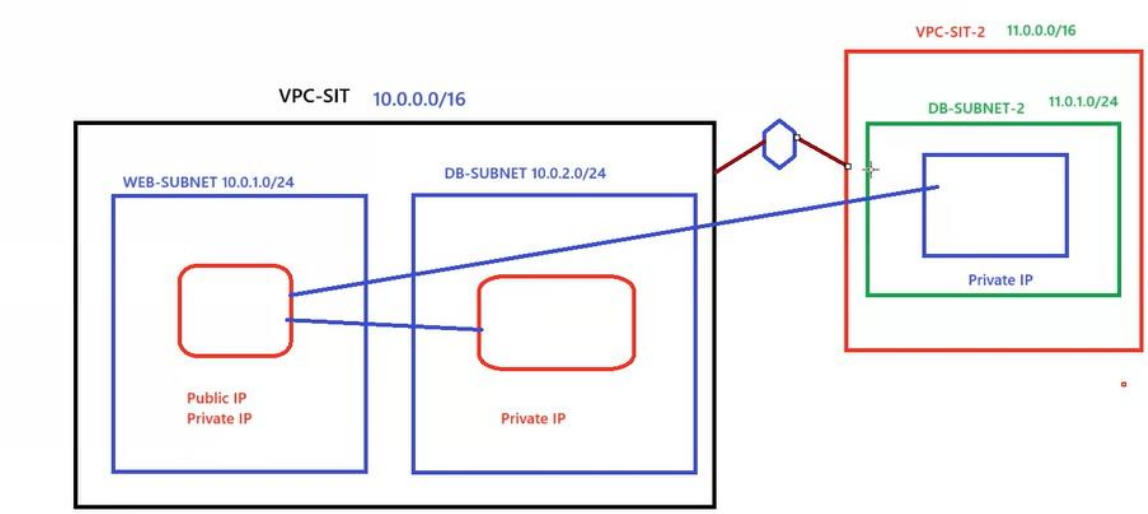
- WEB Instance SG: Allows HTTP/HTTPS and SSH from internet.
- DB Instance SG: Allows MySQL (or relevant DB port) only from WEB-SUBNET and VPC-SIT-2.

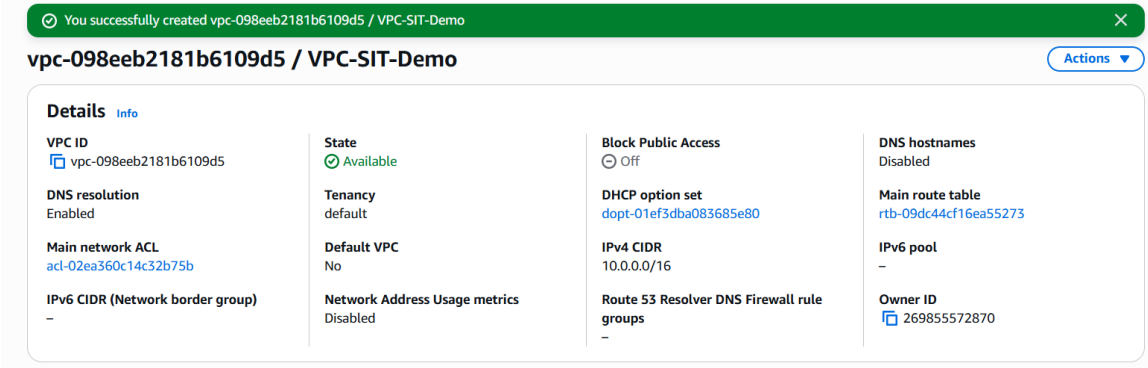
10. Flow Summary

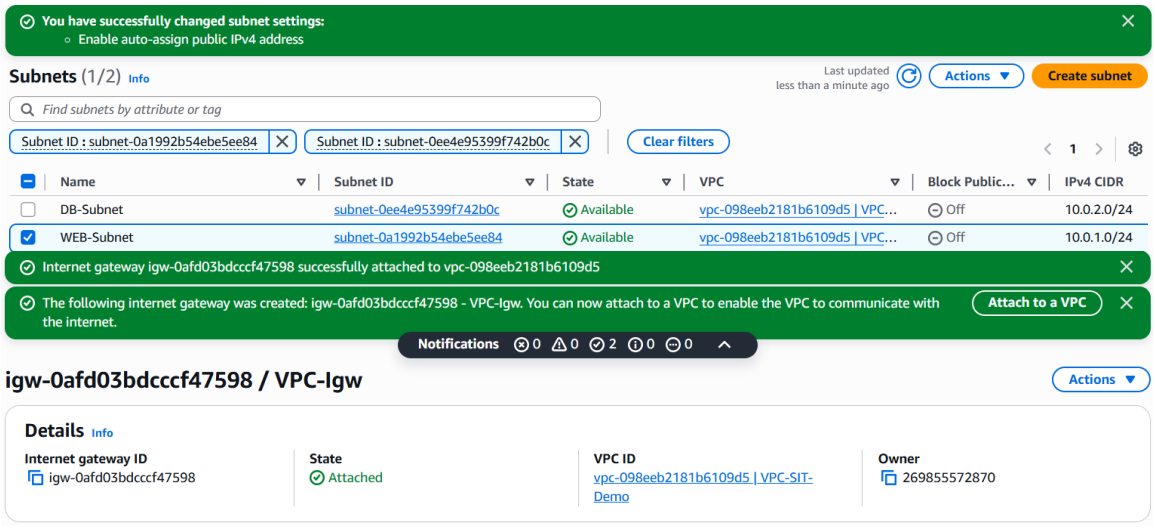
1. Public users access web server in WEB-SUBNET via public IP.
2. Web server communicates with DB-SUBNET and DB-SUBNET-2 via private IPs.

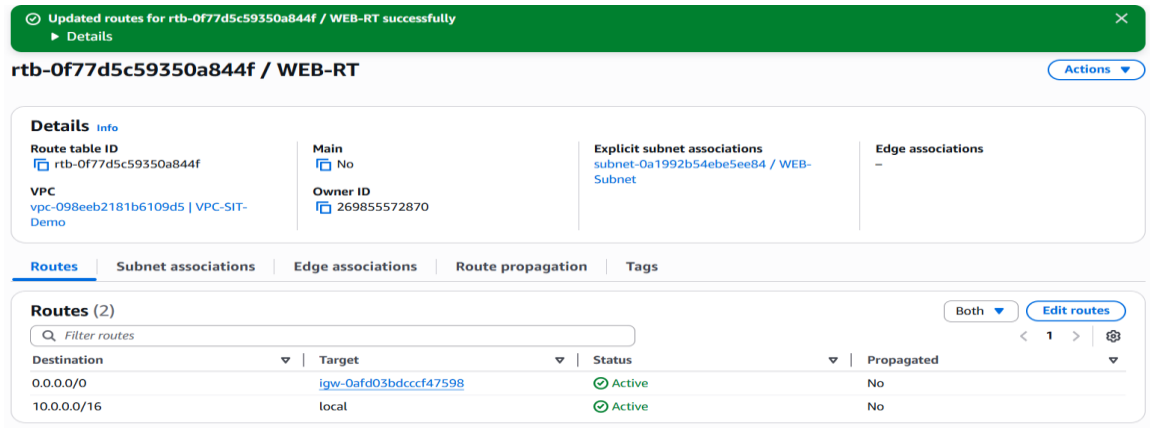
3. VPC Peering allows web servers to talk to DB in another VPC.
4. NAT Gateway allows DB-SUBNET instances to pull updates from the internet securely.

Lab-Work (Demo Architecture): -










```
2025-06-17  16:46.41  /drives/c/Users/Ayush Singh/Downloads  ssh -i "test-key-1.pem" ec2-user@13.127.197.236
ssh: connect to host 13.127.197.236 port 22: Connection timed out

2025-06-17  16:47.06  /drives/c/Users/Ayush Singh/Downloads  ssh -i "test-key-1.pem" ec2-user@13.127.197.236
Warning: Permanently added '13.127.197.236' (ED25519) to the list of known hosts.
X11 forwarding request failed on channel 0
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       /m/'
[ec2-user@ip-10-0-1-225 ~]$ ping 10.0.2.100
PING 10.0.2.100 (10.0.2.100) 56(84) bytes of data.
64 bytes from 10.0.2.100: icmp_seq=1 ttl=127 time=2.27 ms
64 bytes from 10.0.2.100: icmp_seq=2 ttl=127 time=1.12 ms
64 bytes from 10.0.2.100: icmp_seq=3 ttl=127 time=1.16 ms
64 bytes from 10.0.2.100: icmp_seq=4 ttl=127 time=1.04 ms
64 bytes from 10.0.2.100: icmp_seq=5 ttl=127 time=1.15 ms
64 bytes from 10.0.2.100: icmp_seq=6 ttl=127 time=1.42 ms

--- 10.0.2.100 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5004ms
rtt min/avg/max/mdev = 1.038/1.360/2.267/0.421 ms
```

```
[ec2-user@ip-10-0-1-225 ~]$ vi test-key-1.pem
[ec2-user@ip-10-0-1-225 ~]$ chmod 400 test-key-1.pem
[ec2-user@ip-10-0-1-225 ~]$ ssh -i "test-key-1.pem" ec2-user@10.0.2.100
The authenticity of host '10.0.2.100 (10.0.2.100)' can't be established.
ED25519 key fingerprint is SHA256:iOUedTkFTjB5P6eQeW6TT/KPA2ljaK+MJqaXafer3ac.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.100' (ED25519) to the list of known hosts.
       #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
[ec2-user@ip-10-0-2-100 ~]$ exit
logout
Connection to 10.0.2.100 closed.
[root@ip-10-0-1-225 ~]# ping google.com
PING google.com (142.250.183.110) 56(84) bytes of data.
64 bytes from bom12s13-in-f14.1e100.net (142.250.183.110): icmp_seq=1 ttl=114 time=1.97 ms
64 bytes from bom12s13-in-f14.1e100.net (142.250.183.110): icmp_seq=2 ttl=114 time=2.00 ms
64 bytes from bom12s13-in-f14.1e100.net (142.250.183.110): icmp_seq=3 ttl=114 time=2.57 ms

--- google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 1.968/2.181/2.572/0.276 ms
```

NAT gateway nat-02685f06d6a25e798 | VPC-Ngw was created successfully.

nat-02685f06d6a25e798 / VPC-Ngw

Actions

Details

NAT gateway ID nat-02685f06d6a25e798	**Connectivity type** Public	**State** Pending	**State message** Info –
NAT gateway ARN arn:aws:ec2:ap-south-1:269855572870:natgateway/nat-02685f06d6a25e798	**Primary public IPv4 address** –	**Primary private IPv4 address** –	**Primary network interface ID** –
VPC vpc-098eeb2181b6109d5 / VPC-SIT-Demo	**Subnet** subnet-0a1992b54ebe5ee84 / WEB-Subnet	**Created** Tuesday, June 17, 2025 at 17:08:42 GMT+5:30	**Deleted** –

vpc-0606601a354c249ef / VPC-SIT-Demo-2

Details Info

VPC ID vpc-0606601a354c249ef	**State** Available	**Block Public Access** Off	**DNS hostnames** Disabled
DNS resolution Enabled	**Tenancy** default	**DHCP option set** dopt-01ef3dba083685e80	**Main route table** rtb-02ccaeaa24ac0d7f0
Main network ACL acl-0cdec85f5e4dbcc10	**Default VPC** No	**IPv4 CIDR** 11.0.0.0/16	**IPv6 pool** –
IPv6 CIDR (Network border group) –	**Network Address Usage metrics** Disabled	**Route 53 Resolver DNS Firewall rule groups** –	**Owner ID** 269855572870

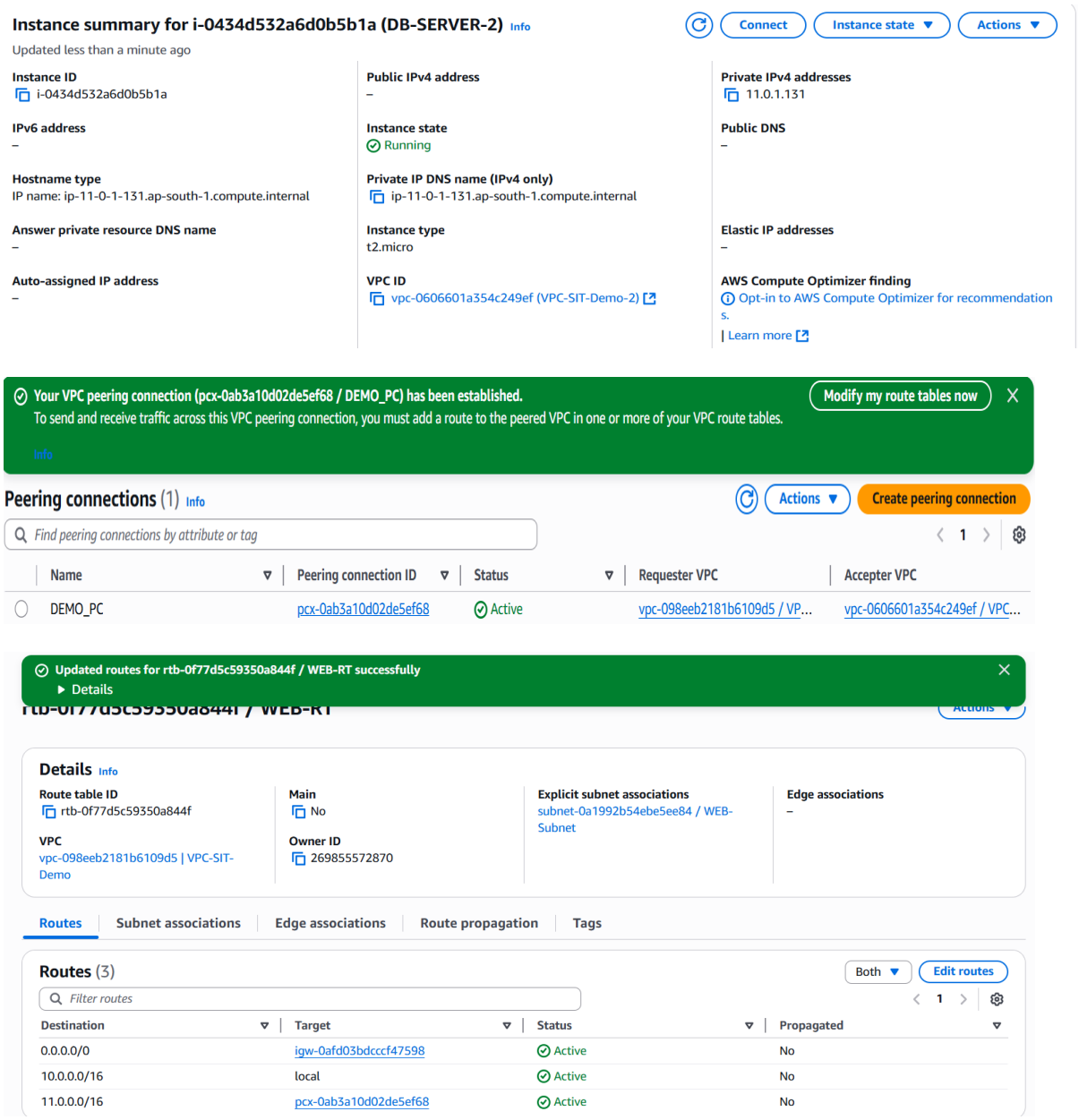
You have successfully updated subnet associations for rtb-0d7035f742f0ad11d / DB-RT-2.

rtb-0d7035f742f0ad11d / DB-RT-2

Actions

Details Info

Route table ID rtb-0d7035f742f0ad11d	**Main** No	**Explicit subnet associations** subnet-063d9927ceed23fb1 / DB-SUBNET-2	**Edge associations** –
VPC vpc-0606601a354c249ef | VPC-SIT-Demo-2	**Owner ID** 269855572870		


Instance summary for i-0434d532a6d0b5b1a (DB-SERVER-2) Info
Connect
Instance state
Actions
Updated less than a minute ago
Instance ID
i-0434d532a6d0b5b1a
IPv6 address
–
Hostname type
IP name: ip-11-0-1-131.ap-south-1.compute.internal
Answer private resource DNS name
–
Auto-assigned IP address
–
Public IPv4 address
–
Instance state
Running
Private IP DNS name (IPv4 only)
ip-11-0-1-131.ap-south-1.compute.internal
Instance type
t2.micro
VPC ID
vpc-0606601a354c249ef (VPC-SIT-Demo-2)
Private IPv4 addresses
11.0.1.131
Public DNS
–
Elastic IP addresses
–
AWS Compute Optimizer finding
Opt-in to AWS Compute Optimizer for recommendations.
Learn more
Your VPC peering connection (pcx-0ab3a10d02de5ef68 / DEMO_PC) has been established.
To send and receive traffic across this VPC peering connection, you must add a route to the peered VPC in one or more of your VPC route tables.
Info
Modify my route tables now
Peering connections (1) Info
Actions
Create peering connection
Find peering connections by attribute or tag
Name
Peering connection ID
Status
Requester VPC
Accepter VPC
DEMO_PC
pcx-0ab3a10d02de5ef68
Active
vpc-098eeb2181b6109d5 / VP...
vpc-0606601a354c249ef / VPC...
Updated routes for rtb-0f77d5c59350a844f / WEB-RT successfully
Details
Details Info
Route table ID
rtb-0f77d5c59350a844f
VPC
vpc-098eeb2181b6109d5 | VPC-SIT-Demo
Main
No
Owner ID
269855572870
Explicit subnet associations
subnet-0a1992b54ebe5ee84 / WEB-Subnet
Edge associations
–
Routes
Subnet associations
Edge associations
Route propagation
Tags
Routes (3)
Both
Edit routes
Filter routes
Destination
Target
Status
Propagated
0.0.0.0/0
igw-0afd03bdcccf47598
Active
No
10.0.0.0/16
local
Active
No
11.0.0.0/16
pcx-0ab3a10d02de5ef68
Active
No

----------X----------