

Amazon VPC Architecture Assignment

Prepared by: Vikram

Problem Statement

You work for XYZ Corporation and have been asked to create and set up distinct Amazon VPCs for the production and development teams.

Production Network

1. Design and build a 4-tier architecture.
2. Create 5 subnets — 4 private (app1, app2, dbcache, db) and 1 public (web).
3. Launch instances in all subnets and name them as per subnet name.
4. Allow dbcache instance and app1 subnet to send internet requests.
5. Manage Security Groups and NACLs.

Development Network

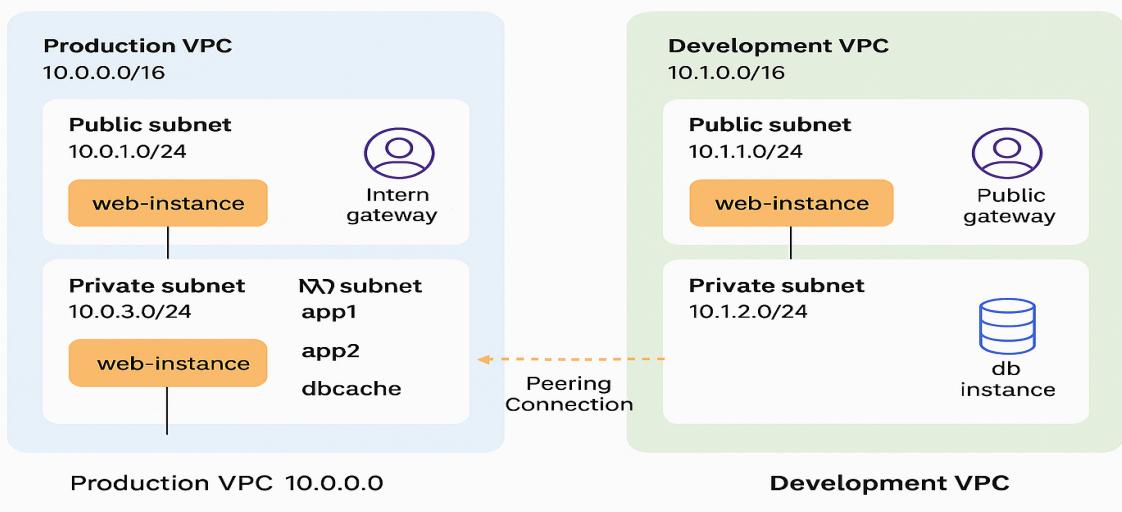
1. Design and build a 2-tier architecture with subnets (web and db).
2. Allow only web subnet to send internet requests.
3. Create peering connection between production and development networks.
4. Setup connection between db subnets of both production and development networks.

Architecture Overview

Two isolated VPCs were created: - **Production VPC:** 10.0.0.0/16 (4-tier architecture) - **Development VPC:** 10.1.0.0/16 (2-tier architecture)

A VPC Peering connection was created between the two VPCs to allow private communication between their DB subnets. The Production VPC includes a NAT Gateway for private subnets, while the Development VPC allows only the web subnet to access the internet.

AWS VPC Setup for Production and Development Environments



Step-by-Step Configuration

1. Create Production VPC (10.0.0.0/16)

- Create the following subnets:
- web (public)
- app1, app2, dbcache, db (private)
- Assign subnets across different Availability Zones for high availability.

The screenshot shows the AWS VPC console with the following details:

VPC ID: vpc-07dd6d9201b9f2852

State: Available

Block Public Access: Off

DNS hostnames: Disabled

DNS resolution: Enabled

Tenancy: default

Main network ACL: ad-0582b6fa3dc68f1da

Default VPC: No

IPv4 CIDR: 10.0.0.0/16

IPv6 pool: -

Network Address Usage metrics: Disabled

Route 53 Resolver DNS Firewall rule groups: -

Owner ID: 062250062838

Resource map: Shows 0 Subnets, 1 Route tables, and 0 Network Connections.

The screenshot shows the AWS Subnets console with the following details:

Subnets (5): prod web, prod app 1, prod app 2, prod dbcache, prod db

Last updated: less than a minute ago

Create subnet: button

Name	Subnet ID	State	VPC	Block Public...	IPv4 CIDR	IPv6 CIDR	IPv6 CIC
prod web	subnet-0c0aede159e57078e	Available	vpc-07dd6d9201b9f2852 pro...	Off	10.0.1.0/24	-	-
prod app 1	subnet-061e607352c89558d	Available	vpc-07dd6d9201b9f2852 pro...	Off	10.0.2.0/24	-	-
prod app 2	subnet-0f707bd709194457	Available	vpc-07dd6d9201b9f2852 pro...	Off	10.0.3.0/24	-	-
prod dbcache	subnet-0723633e0025f66d0	Available	vpc-07dd6d9201b9f2852 pro...	Off	10.0.4.0/24	-	-
prod db	subnet-00ca5a4fe43cc0578	Available	vpc-07dd6d9201b9f2852 pro...	Off	10.0.5.0/24	-	-

2. Create Development VPC (10.1.0.0/16)

- Create subnets:
- web (public)
- db (private)

You successfully created vpc-0b8e6496e14fc587c / development vpc

vpc-0b8e6496e14fc587c / development vpc

Actions ▾

Details		Info	
VPC ID	vpc-0b8e6496e14fc587c	State	Available
DNS resolution	Enabled	Tenancy	default
Main network ACL	acl-068ee18bf81d73811	Default VPC	No
IPv6 CIDR (Network border group)	-	Network Address Usage metrics	Disabled
		Block Public Access	Off
		DHCP option set	dopt-017e3521298e97eee
		IPv4 CIDR	10.1.0.0/16
		Route 53 Resolver DNS Firewall rule groups	-
		DNS hostnames	Disabled
		Main route table	rtb-02022daf0bc1d0aab
		IPv6 pool	-
		Owner ID	062250062838

Resource map | CIDRs | Flow logs | Tags | Integrations

Resource map

Show all details

VPC	Subnets (0)	Route tables (1)	Network Connections (0)
Your AWS virtual network	Subnets within this VPC	Route network traffic to resources	Connections to other networks
development vpc		rtb-02022daf0bc1d0aab	

Subnets (2) Info

Last updated less than a minute ago

Actions ▾ Create subnet

Find subnets by attribute or tag

Name : dev-web X Name : dev-db X Clear filters

1

Name	Subnet ID	State	VPC	Block Public...	IPv4 CIDR	IPv6 CIDR	IPv6 CIC
dev-web	subnet-065eb1fb7480cd92f	Available	vpc-0b8e6496e14fc587c deve...	Off	10.1.0.0/24	-	-
dev-db	subnet-0ec36006e9e634c7e	Available	vpc-0b8e6496e14fc587c deve...	Off	10.1.2.0/24	-	-

3. Attach Internet Gateways

- Create and attach an Internet Gateway (IGW) to both VPCs.

Internet gateway igw-05dbb2196694b10b1 successfully attached to vpc-07dd6d9201b9f2852

igw-05dbb2196694b10b1 / prod igw

Actions ▾

Details Info

Internet gateway ID igw-05dbb2196694b10b1	State Attached	VPC ID vpc-07dd6d9201b9f2852 production vpc	Owner 062250062838
--	-------------------	--	-----------------------

Tags

Search tags

Key	Value
Name	prod igw

Manage tags

Internet gateway igw-0bed3ff66250128d6 successfully attached to vpc-0b8e496e14fc587c

igw-0bed3ff66250128d6 / dev-igw

Actions ▾

Details Info

Internet gateway ID igw-0bed3ff66250128d6	State Attached	VPC ID vpc-0b8e496e14fc587c development vpc	Owner 062250062838
--	-------------------	--	-----------------------

Tags

Search tags

Key	Value
Name	dev-igw

Manage tags

4. Create NAT Gateway (Production VPC only)

- Allocate a new **Elastic IP**.
- Create a **NAT Gateway** in the Production public subnet (web).
- Attach the allocated Elastic IP to the NAT Gateway.

The screenshot shows two separate AWS management interfaces side-by-side.

Elastic IP Addresses: This interface displays a single allocated Elastic IP address (52.203.123.70) in a table. The table columns include Name, Allocated IPv4 address, Type, Allocation ID, Reverse DNS record, Associated instance ID, and Private IP address. The row for the IP 52.203.123.70 has a Public IP type and an allocation ID of eipalloc-01cabad137cff7d3.

NAT Gateways: This interface shows a single NAT gateway named nat-012fc16e909ec025f in the prod-ngw VPC. The NAT gateway ID is nat-012fc16e909ec025f and its ARN is amazsec2:us-east-1:062250062838:natgateway/nat-012fc16e909ec025f. It is connected to a public subnet (subnet-0c0aeade159e57078e). The primary public IP is 52.203.123.70 and the primary private IP is 10.0.1.233. The state is Pending.

Secondary IPv4 addresses: This section indicates that no secondary IPv4 addresses are available for this NAT gateway.

5. Configure Route Tables and Associations

- Production VPC:

- Public Route Table `web` subnet IGW (0.0.0.0/0)
- Private Route Table (with NAT) `app1`, `dbcache` subnets NAT Gateway (0.0.0.0/0)
- Private Route Table (no NAT) `app2`, `db` subnets No internet access

You have successfully updated subnet associations for rtb-07dbc3b6afe1bd71f / prod-public-rt.

rtb-07dbc3b6afe1bd71f / prod-public-rt

Details Info

Route table ID rtb-07dbc3b6afe1bd71f	Main <input type="checkbox"/> No	Explicit subnet associations subnet-0c0ae0e159e57078e / prod web	Edge associations -
VPC vpc-07dd6d9201b9f2852 production vpc	Owner ID 062250062838		

Routes Subnet associations Edge associations Route propagation Tags

Routes (2)

Destination	Target	Status	Propagated	Route Origin
0.0.0.0/0	igw-05ddb2196694b10b1	Active	No	Create Route
10.0.0.0/16	local	Active	No	Create Route Table

You have successfully updated subnet associations for rtb-04ced5999cb64e15f / prod-private-with-nat-rt.

rtb-04ced5999cb64e15f / prod-private-with-nat-rt

Details Info

Route table ID rtb-04ced5999cb64e15f	Main <input type="checkbox"/> No	Explicit subnets 2 subnets subnet-061e607352c89558d / prod app 1 subnet-0723633e0025f66d0 / prod dbcache	Edge associations -
VPC vpc-07dd6d9201b9f2852 production vpc	Owner ID 062250062838		

Routes Subnet associations Edge associations Route propagation Tags

Routes (2)

Destination	Target	Status	Propagated	Route Origin
0.0.0.0/0	nat-012fc16e909ec025f	Active	No	Create Route
10.0.0.0/16	local	Active	No	Create Route Table

rtb-0ae92bde5ee9a57c0 / prod-private-with-no-nat-rt

Actions ▾

Details Info

Route table ID rtb-0ae92bde5ee9a57c0	Main <input type="checkbox"/> No	Explicit subnets 2 subnets subnet-0f707bdf709194457 / prod app 2 subnet-00ca5a4fe43cc0578 / prod db	Edge associations -
VPC vpc-07dd6d9201b9f2852 production vpc	Owner ID 062250062838		

Routes Subnet associations Edge associations Route propagation Tags

Routes (1)

Destination	Target	Status	Propagated	Route Origin
10.0.0.0/16	local	Active	No	Create Route Table

• Development VPC:

- Public Route Table  subnet IGW (0.0.0.0/0)
- Private Route Table  db subnet No internet access

You have successfully updated subnet associations for rtb-00a56ec60af488906 / dev-public rt.

rtb-00a56ec60af488906 / dev-public rt

[Actions ▾](#)

Details Info		Explicit subnet associations		Edge associations																									
Route table ID  rtb-00a56ec60af488906	Main  No	subnet-065eb1fb7480cd92f / dev-web	-	-																									
VPC vpc-0b8e6496e14fc587c development vpc	Owner ID  062250062838																												
Routes Subnet associations Edge associations Route propagation Tags																													
Routes (2) <table border="1"> <thead> <tr> <th colspan="5">Both ▾ Edit routes</th> </tr> <tr> <th colspan="5"> Filter routes</th> </tr> <tr> <th>Destination</th> <th>▼ Target</th> <th>Status</th> <th>▼ Propagated</th> <th>▼ Route Origin</th> </tr> </thead> <tbody> <tr> <td>0.0.0.0/0</td> <td>igw-0bed3ff66250128d6</td> <td> Active</td> <td>No</td> <td>Create Route</td> </tr> <tr> <td>10.1.0.0/16</td> <td>local</td> <td> Active</td> <td>No</td> <td>Create Route Table</td> </tr> </tbody> </table>					Both ▾ Edit routes					 Filter routes					Destination	▼ Target	Status	▼ Propagated	▼ Route Origin	0.0.0.0/0	igw-0bed3ff66250128d6	 Active	No	Create Route	10.1.0.0/16	local	 Active	No	Create Route Table
Both ▾ Edit routes																													
 Filter routes																													
Destination	▼ Target	Status	▼ Propagated	▼ Route Origin																									
0.0.0.0/0	igw-0bed3ff66250128d6	 Active	No	Create Route																									
10.1.0.0/16	local	 Active	No	Create Route Table																									

[Actions ▾](#)

rtb-0ef3552c5614966d5 / dev-private rt

Details Info		Explicit subnet associations		Edge associations																				
Route table ID  rtb-0ef3552c5614966d5	Main  No	subnet-0ec36006e9e634c7e / dev-db	-	-																				
VPC vpc-0b8e6496e14fc587c development vpc	Owner ID  062250062838																							
Routes Subnet associations Edge associations Route propagation Tags																								
Routes (1) <table border="1"> <thead> <tr> <th colspan="5">Both ▾ Edit routes</th> </tr> <tr> <th colspan="5"> Filter routes</th> </tr> <tr> <th>Destination</th> <th>▼ Target</th> <th>Status</th> <th>▼ Propagated</th> <th>▼ Route Origin</th> </tr> </thead> <tbody> <tr> <td>10.1.0.0/16</td> <td>local</td> <td> Active</td> <td>No</td> <td>Create Route Table</td> </tr> </tbody> </table>					Both ▾ Edit routes					 Filter routes					Destination	▼ Target	Status	▼ Propagated	▼ Route Origin	10.1.0.0/16	local	 Active	No	Create Route Table
Both ▾ Edit routes																								
 Filter routes																								
Destination	▼ Target	Status	▼ Propagated	▼ Route Origin																				
10.1.0.0/16	local	 Active	No	Create Route Table																				

6. Launch EC2 Instances

- Use **Amazon Linux 2 AMI**.
- Assign **key pairs** for SSH access.
- Public instances (web) Enable Auto-assign Public IP.
- Private instances (app1, app2, dbcache, db) Disable Public IP.
- Assign correct **Security Groups** and **Subnets**.

The screenshot shows the AWS CloudWatch Metrics Insights search interface. At the top, there's a search bar with placeholder text "Find Metric by name or metric type (case-sensitive)" and a dropdown menu set to "All metrics". Below the search bar is a table with columns: Metric name, Metric namespace, Value, Unit, and Last updated. The table contains several rows of metric data, such as "AWS/CloudWatch Metrics: /aws/lambda/functions/lambda-function-invocations", "AWS/CloudWatch Metrics: /aws/lambda/functions/lambda-function-invocations", and "AWS/CloudWatch Metrics: /aws/lambda/functions/lambda-function-invocations". The last row is highlighted in yellow. At the bottom of the table, there's a "Next" button with a page number "1" and a "Last" button.

The screenshot shows the AWS CloudWatch Metrics Insights search interface with filters applied. At the top, there's a search bar with placeholder text "Find Metric by name or metric type (case-sensitive)" and a dropdown menu set to "All metrics". Below the search bar is a table with columns: Metric name, Metric namespace, Value, Unit, and Last updated. The table contains several rows of metric data, such as "AWS/CloudWatch Metrics: /aws/lambda/functions/lambda-function-invocations", "AWS/CloudWatch Metrics: /aws/lambda/functions/lambda-function-invocations", and "AWS/CloudWatch Metrics: /aws/lambda/functions/lambda-function-invocations". The last row is highlighted in yellow. At the bottom of the table, there's a "Next" button with a page number "1" and a "Last" button.

VPC Peering Connection & Routing Configuration

Step 1 — Create and Accept Peering Connection

- Go to VPC Console Peering Connections Create Peering Connection.
- Requester: Production VPC
- Acceptor: Development VPC
- Accept request after creation.

The screenshot shows the AWS VPC Peering Connection details page for a connection named 'pcx-038a737af5f56ee1d / prod-dev-peer'. The top banner indicates the connection has been established. The main table provides detailed information about both the requester and accepter VPCs, including their respective owner IDs, VPC IDs, CIDRs, and regions. The 'DNS' tab is selected, showing DNS settings for both VPCs, which are currently disabled. An 'Edit DNS settings' button is available for each VPC.

Details		Info	
Requester owner ID	062250062838	Acceptor owner ID	062250062838
Peering connection ID	pcx-038a737af5f56ee1d	Requester VPC	vpc-07dd6d9201b9f2852 / production vpc
Status	Active	Requester CIDRs	10.0.0.0/16
Expiration time	-	Requester Region	N. Virginia (us-east-1)
		Acceptor VPC	vpc-0b8e6496e14fc587c / development vpc
		Acceptor CIDRs	10.1.0.0/16
		Acceptor Region	N. Virginia (us-east-1)

DNS | Route tables | Tags

DNS settings

Requester VPC ([vpc-07dd6d9201b9f2852 / production vpc](#)) [Info](#)

Allow accepter VPC to resolve DNS of hosts in requester VPC to private IP addresses

Disabled

Acceptor VPC ([vpc-0b8e6496e14fc587c / development vpc](#)) [Info](#)

Allow requester VPC to resolve DNS of hosts in accepter VPC to private IP addresses

Disabled

Step 2 — Edit Route Tables for Peering

- **Production Private (db subnet):** Route 10.1.0.0/16 Peering Connection ID
- **Development Private (db subnet):** Route 10.0.0.0/16 Peering Connection ID
- **Optional:** Add same route in `prod-public-rt` for testing.

rtb-0ef3552c5614966d5 / dev-private rt

Routes (3)				
Both ▾ Edit routes				
Destination	Target	Status	Propagated	Route Origin
10.0.0.0/16	pcx-038a737af5f56ee1d	Active	No	Create Route
10.0.5.0/24	pcx-038a737af5f56ee1d	Active	No	Create Route
10.1.0.0/16	local	Active	No	Create Route Table

rtb-0ae92bde5ee9a57c0 / prod-private-with no nat rt

Routes (3)				
Both ▾ Edit routes				
Destination	Target	Status	Propagated	Route Origin
10.0.0.0/16	local	Active	No	Create Route Table
10.1.0.0/16	pcx-038a737af5f56ee1d	Active	No	Create Route
10.1.2.0/24	pcx-038a737af5f56ee1d	Active	No	Create Route

© 2025, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

rtb-07dbc3b6afe1bd71f / prod-public-rt

Updated routes for rtb-07dbc3b6afe1bd71f / prod-public-rt successfully

► Details

Actions ▾

Details		Info	
Route table ID	rtb-07dbc3b6afe1bd71f	Main	No
VPC	vpc-07dd6d9201b9f2852 production vpc	Owner ID	062250062838
Explicit subnet associations	subnet-0c0aeede159e57078e / prod web		
Edge associations	-		

Routes Subnet associations Edge associations Route propagation Tags

Routes (3)				
Both ▾ Edit routes				
Destination	Target	Status	Propagated	Route Origin
0.0.0.0/0	igw-05ddb2196694b10b1	Active	No	Create Route
10.0.0.0/16	local	Active	No	Create Route Table
10.1.0.0/16	pcx-038a737af5f56ee1d	Active	No	Create Route

Connectivity Testing

1. SSH into **Production Web** instance.
2. Ping Production DB private IP: ping 10.0.x.x
3. Ping Development DB private IP: ping 10.1.x.x
4. SSH into **Development Web** instance.
5. Ping Development DB private IP to confirm internal connectivity.

Expected Results: - Prod web Internet access - Prod app1/dbcache Internet via NAT - Dev web Internet access - Private DBs No internet access

```
'`#`          Amazon Linux 2023
`~\`###`\
`~\`###`\
`~\`###`\
`~\`#/`__> https://aws.amazon.com/linux/amazon-linux-2023
`~`v~'`->
`~~`/
`~~`/`_`/`_
`~/`m/`_`/`_
Last login: Tue Oct 14 03:04:10 2025 from 106.200.170.76
[ec2-user@ip-10-0-1-123 ~]$ ls
[ec2-user@ip-10-0-1-123 ~]$ ping -c 10.0.5.33
ping: invalid argument: '10.0.5.33'
[ec2-user@ip-10-0-1-123 ~]$ ping 10.0.5.33
PING 10.0.5.33 (10.0.5.33) 56(84) bytes of data.
64 bytes from 10.0.5.33: icmp_seq=250 ttl=127 time=0.193 ms
64 bytes from 10.0.5.33: icmp_seq=251 ttl=127 time=0.185 ms
64 bytes from 10.0.5.33: icmp_seq=252 ttl=127 time=0.183 ms
64 bytes from 10.0.5.33: icmp_seq=253 ttl=127 time=0.252 ms
64 bytes from 10.0.5.33: icmp_seq=254 ttl=127 time=0.180 ms
64 bytes from 10.0.5.33: icmp_seq=255 ttl=127 time=0.173 ms
64 bytes from 10.0.5.33: icmp_seq=256 ttl=127 time=0.188 ms
64 bytes from 10.0.5.33: icmp_seq=257 ttl=127 time=0.189 ms
64 bytes from 10.0.5.33: icmp_seq=258 ttl=127 time=0.184 ms
64 bytes from 10.0.5.33: icmp_seq=259 ttl=127 time=0.210 ms
64 bytes from 10.0.5.33: icmp_seq=260 ttl=127 time=0.224 ms
64 bytes from 10.0.5.33: icmp_seq=261 ttl=127 time=0.189 ms
64 bytes from 10.0.5.33: icmp_seq=262 ttl=127 time=0.186 ms
64 bytes from 10.0.5.33: icmp_seq=263 ttl=127 time=0.248 ms
64 bytes from 10.0.5.33: icmp_seq=264 ttl=127 time=0.181 ms
64 bytes from 10.0.5.33: icmp_seq=265 ttl=127 time=0.192 ms
64 bytes from 10.0.5.33: icmp_seq=266 ttl=127 time=0.194 ms
64 bytes from 10.0.5.33: icmp_seq=267 ttl=127 time=0.180 ms
64 bytes from 10.0.5.33: icmp_seq=268 ttl=127 time=0.233 ms
```

```
[ec2-user@ip-10-0-1-123 ~]$ ls
[ec2-user@ip-10-0-1-123 ~]$ ping 10.1.2.68
PING 10.1.2.68 (10.1.2.68) 56(84) bytes of data.
^C
--- 10.1.2.68 ping statistics ---
604 packets transmitted, 0 received, 100% packet loss, time 627080ms

[ec2-user@ip-10-0-1-123 ~]$ ping 10.1.2.68
PING 10.1.2.68 (10.1.2.68) 56(84) bytes of data.
64 bytes from 10.1.2.68: icmp_seq=171 ttl=127 time=0.552 ms
64 bytes from 10.1.2.68: icmp_seq=172 ttl=127 time=0.210 ms
64 bytes from 10.1.2.68: icmp_seq=173 ttl=127 time=0.184 ms
64 bytes from 10.1.2.68: icmp_seq=174 ttl=127 time=0.208 ms
64 bytes from 10.1.2.68: icmp_seq=175 ttl=127 time=0.176 ms
```

```

\ \ #      Amazon Linux 2023
\ \ ##i
#/
-/ -/
--/ , /-
-/r

[ec2-user@ip-10-1-1-123 ~]$ ping 10.1.2.68
PING 10.1.2.68 (10.1.2.68) 56(84) bytes of data.
64 bytes from 10.1.2.68 (16.1.26) icmp=seq=1 ttl=200 ms
64 bytes from 10.1.2.68 (16.1.26) icmp=seq=2 ttl=127 ms
64 bytes from 10.1.2.68 (16.1.26) icmp=seq=3 ttl=127 ms
64 bytes from 10.1.2.68 (16.1.26) icmp=seq=4 ttl=127 ms
64 bytes from 10.1.2.68 (16.1.26) icmp=seq=5 ttl=127 ms
64 bytes from 10.1.2.68 (16.1.26) icmp=seq=6 ttl=127 ms
64 bytes from 10.1.2.68 (16.1.26) icmp=seq=7 ttl=127 ms
64 bytes from 10.1.2.68 (16.1.26) icmp=seq=8 ttl=127 ms
64 bytes from 10.1.2.68 (16.1.26) icmp=seq=9 ttl=127 ms
--- ping statistics -iP6
10 packets transmitted, 10 received, 0% packet loss, time 9014ms
rtt min/avg/max/mdev = 0.171/0.193/0.233/0.019 ms

```

Security Groups

Security Groups work like firewalls for EC2 instances. They control what kind of traffic is allowed **in and out**.

Production VPC

Security Group	Purpose	Inbound Rules	Outbound Rules
web-sg	Web server	Allow SSH (22) & HTTP (80) from anywhere	Allow all traffic
app1-sg	Application tier	Allow HTTP (80) from web-sg	Allow all traffic (for NAT)
app2-sg	Internal tier	Allow internal traffic only from app1/app2	Allow all traffic
dbcache-sg	Cache server	Allow 3306 (MySQL) from app1/app2	Allow all traffic (via NAT)
db-sg	Database	Allow 3306 (MySQL) from app1/app2; ICMP from dev-db-sg	Allow all traffic

Development VPC

Security Group	Purpose	Inbound Rules	Outbound Rules
dev-web-sg	Web server	Allow SSH (22) & HTTP (80) from anywhere	Allow all traffic
dev-db-sg	Database	Allow 3306 (MySQL) & ICMP from Production DB SG	Allow all traffic

sg-098ef94232b64630c - launch-wizard-1 Actions ▾

Details			
Security group name launch-wizard-1	Security group ID sg-098ef94232b64630c	Description launch-wizard-1 created 2023-10-14T02:20:16.139Z	VPC ID vpc-07dd6d9201b9f2852
Owner 062250062838	Inbound rules count 3 Permission entries	Outbound rules count 1 Permission entry	

[Inbound rules](#) | [Outbound rules](#) | [Sharing - new](#) | [VPC associations - new](#) | [Tags](#)

Inbound rules (3)										
<input type="button" value="Manage tags"/> <input type="button" value="Edit inbound rules"/> ◀ 1 ▶ ⌂										
<input type="text" value="Search"/>										
Name	Security group rule ID	IP version	Type	Protocol	Port range	Source	Description			
-	sgr-0b2ff8c7f06846f68	IPv4	HTTPS	TCP	443	0.0.0.0/0	-			
-	sgr-02298871d6def45b2	IPv4	SSH	TCP	22	0.0.0.0/0	-			
-	sgr-046495960c2db1eec	IPv4	HTTP	TCP	80	0.0.0.0/0	-			

sg-03bcf2601140c346c - launch-wizard-2

[Actions ▾](#)

Details

Security group name launch-wizard-2	Security group ID sg-03bcf2601140c346c	Description launch-wizard-2 created 2025-10-14T02:23:04.582Z	VPC ID vpc-07dd6d9201b9f2852
Owner 062250062838	Inbound rules count 2 Permission entries	Outbound rules count 1 Permission entry	

[Inbound rules](#) | [Outbound rules](#) | [Sharing - new](#) | [VPC associations - new](#) | [Tags](#)

Inbound rules (2)

<input type="checkbox"/>	Name	Security group rule ID	IP version	Type	Protocol	Port range	Source	Description
<input type="checkbox"/>	-	sgr-090b5cf6a56490fb	-	HTTP	TCP	80	sg-098ef94232b64630c...	-
<input type="checkbox"/>	-	sgr-0a26b1823af425f51	IPv4	SSH	TCP	22	0.0.0.0/0	-

sg-0d97d7a7e8773fe96 - launch-wizard-4

[Actions ▾](#)

Details

Security group name launch-wizard-4	Security group ID sg-0d97d7a7e8773fe96	Description launch-wizard-4 created 2025-10-14T02:24:05.2012Z	VPC ID vpc-07dd6d9201b9f2852
Owner 062250062838	Inbound rules count 2 Permission entries	Outbound rules count 1 Permission entry	

[Inbound rules](#) | [Outbound rules](#) | [Sharing - new](#) | [VPC associations - new](#) | [Tags](#)

Inbound rules (2)

<input type="checkbox"/>	Name	Security group rule ID	IP version	Type	Protocol	Port range	Source	Description
<input type="checkbox"/>	-	sgr-0291c72d3fa0f0fb	IPv4	SSH	TCP	22	0.0.0.0/0	-
<input type="checkbox"/>	-	sgr-0fb55d9b5cf60d847	-	MySQL/Aurora	TCP	3306	sg-03bcf2601140c346c...	-

sg-0727c38521ba07a1b - launch-wizard-5

[Actions ▾](#)

Details

Security group name launch-wizard-5	Security group ID sg-0727c38521ba07a1b	Description launch-wizard-5 created 2025-10-14T02:24:46.198Z	VPC ID vpc-07dd6d9201b9f2852
Owner 062250062838	Inbound rules count 2 Permission entries	Outbound rules count 1 Permission entry	

[Inbound rules](#) | [Outbound rules](#) | [Sharing - new](#) | [VPC associations - new](#) | [Tags](#)

Inbound rules (2)

<input type="checkbox"/>	Name	Security group rule ID	IP version	Type	Protocol	Port range	Source	Description
<input type="checkbox"/>	-	sgr-08e2bcb3f4fce6e1e	-	MySQL/Aurora	TCP	3306	sg-03bcf2601140c346c...	-
<input type="checkbox"/>	-	sgr-021623e99eefffa3	IPv4	SSH	TCP	22	0.0.0.0/0	-

sg-0a9c1be73860085f3 - launch-wizard-7

[Actions ▾](#)

Details		Security group ID		Description		VPC ID	
Security group name launch-wizard-7		sg-0a9c1be73860085f3		launch-wizard-7 created 2025-10-14T02:46:33.614Z		vpc-0b8e6496e14fc587c Edit	
Owner 062250062838		Inbound rules count 2 Permission entries		Outbound rules count 1 Permission entry			

[Inbound rules](#) | [Outbound rules](#) | [Sharing - new](#) | [VPC associations - new](#) | [Tags](#)

Inbound rules (2)

<input type="checkbox"/>	Name	Security group rule ID	IP version	Type	Protocol	Port range	Source	Description
<input type="checkbox"/>	-	sgr-053ea24698f937405	IPv4	MySQL/Aurora	TCP	3306	10.0.0/24	-
<input type="checkbox"/>	-	sgr-0727b81f351498f14	IPv4	SSH	TCP	22	0.0.0.0/0	-

[Manage tags](#) | [Edit inbound rules](#)

sg-0727c38521ba07a1b - launch-wizard-5

[Actions ▾](#)

Inbound security group rules successfully modified on security group sg-0727c38521ba07a1b | launch-wizard-5

[Details](#)

sg-0727c38521ba07a1b - launch-wizard-5

[Actions ▾](#)

Details		Security group ID		Description		VPC ID	
Security group name launch-wizard-5		sg-0727c38521ba07a1b		launch-wizard-5 created 2025-10-14T02:24:46.198Z		vpc-07dd6d9201b9f2852 Edit	
Owner 062250062838		Inbound rules count 3 Permission entries		Outbound rules count 1 Permission entry			

[Inbound rules](#) | [Outbound rules](#) | [Sharing - new](#) | [VPC associations - new](#) | [Tags](#)

Inbound rules (3)

<input type="checkbox"/>	Name	Security group rule ID	IP version	Type	Protocol	Port range	Source	Description
<input type="checkbox"/>	-	sgr-08e2bc3f4fce6e1e	-	MySQL/Aurora	TCP	3306	sg-03b0cf2601140c346c...	-
<input type="checkbox"/>	-	sgr-02ae227827f4b4654	IPv4	MySQL/Aurora	TCP	3306	10.1.2.0/24	-
<input type="checkbox"/>	-	sgr-021623e99eefffac3	IPv4	SSH	TCP	22	0.0.0.0/0	-

[Manage tags](#) | [Edit inbound rules](#)

sg-0727c38521ba07a1b - launch-wizard-5



X

ⓘ Inbound security group rules successfully modified on security group (sg-0727c38521ba07a1b | launch-wizard-5)
[Details](#)

sg-0727c38521ba07a1b - launch-wizard-5

Actions ▾

Details

Security group name	launch-wizard-5	Security group ID	sg-0727c38521ba07a1b	Description	launch-wizard-5 created 2025-10-14T02:24:46.198Z	VPC ID	vpc-07dd6d9201bf2852
Owner	062250062838	Inbound rules count	4 Permission entries	Outbound rules count	1 Permission entry		

[Inbound rules](#) | [Outbound rules](#) | [Sharing - new](#) | [VPC associations - new](#) | [Tags](#)

Inbound rules (4)

<input type="checkbox"/>	Name	Security group rule ID	IP version	Type	Protocol	Port range	Source	Description
<input type="checkbox"/>	-	sgr-08e2bcb3f4fce6e1e	-	MySQL/Aurora	TCP	3306	sg-03bcfd2601140c346c...	-
<input type="checkbox"/>	-	sgr-02ae227827f4b4654	IPv4	MySQL/Aurora	TCP	3306	10.1.2.0/24	-
<input type="checkbox"/>	-	sgr-0f51cdfba6e9eb86	IPv4	All ICMP - IPv4	ICMP	All	10.0.1.0/24	-
<input type="checkbox"/>	-	sgr-021623e99eefffac3	IPv4	SSH	TCP	22	0.0.0.0/0	-

sg-0a9c1be73860085f3 - launch-wizard-7



ⓘ Inbound security group rules successfully modified on security group (sg-0a9c1be73860085f3 | launch-wizard-7)
[Details](#)

sg-0a9c1be73860085f3 - launch-wizard-7

Actions ▾

Details

Security group name	launch-wizard-7	Security group ID	sg-0a9c1be73860085f3	Description	launch-wizard-7 created 2025-10-14T02:46:33.614Z	VPC ID	vpc-0b8e6496e14fc587c
Owner	062250062838	Inbound rules count	3 Permission entries	Outbound rules count	1 Permission entry		

[Inbound rules](#) | [Outbound rules](#) | [Sharing - new](#) | [VPC associations - new](#) | [Tags](#)

Inbound rules (3)

<input type="checkbox"/>	Name	Security group rule ID	IP version	Type	Protocol	Port range	Source	Description
<input type="checkbox"/>	-	sgr-053ea24698f937405	IPv4	MySQL/Aurora	TCP	3306	10.0.5.0/24	-
<input type="checkbox"/>	-	sgr-03bd707825fc4abe3	IPv4	All ICMP - IPv4	ICMP	All	10.0.0.0/16	-
<input type="checkbox"/>	-	sgr-0727b81f351498f14	IPv4	SSH	TCP	22	0.0.0.0/0	-

Network ACLs (Simplified)

NACLs are an extra layer of security at the **subnet level**. Think of them as “rules for the entire street,” while security groups are “rules for each house.”

Public Subnet NACL

- **Inbound:** Allow 22 (SSH), 80 (HTTP), 443 (HTTPS) from 0.0.0.0/0
- **Outbound:** Allow all (0.0.0.0/0)

Private Subnet NACL

- **Inbound:** Allow traffic only from internal subnets (10.0.0.0/8, 10.1.0.0/8)
- **Outbound:** Allow response traffic (1024–65535)

Verification & Validation

- Check instance reachability per subnet.
- Confirm NAT Gateway traffic for app1 and dbcache.
- Confirm peering communication between DBs.
- Verify route associations and security rules.

Final Result: All configurations function as expected. Production and Development networks are isolated yet securely connected via peering, with controlled internet access and validated routing.

Conclusion

The setup successfully demonstrates two independent VPCs (Production and Development) with secure, tiered design and controlled communication through peering. Internet access policies, NAT configuration, and private routing were validated through connectivity tests and audits.