



St. JOSEPH'S
GROUP OF INSTITUTIONS
OMR, CHENNAI - 119



Placement Empowerment Program

Cloud Computing and DevOps Centre

SECURE ACCESS WITH A BASTION HOST

(Set up a bastion host in a public subnet to securely access instances in a private subnet)

NAME: NIDHISHA A DHAS

DEPARTMENT: AML

INTRODUCTION:

A 'bastion host' is a special-purpose server used to securely access resources in a private network from an external network, like the internet. It acts as a jump server or gateway for managing instances that do not have direct internet access.

Why Use a Bastion Host?

- Secure access: Prevents exposing all private servers to the internet.
- Controlled entry point: Only the bastion host is accessible from the internet.
- Better security: Reduces the attack surface by limiting SSH access to one server.
- Logging & Monitoring: You can track who accesses internal instances via the bastion.

IMPORTANCE:

- Secure Access to Private Network.
- Reduced Attack Surface - Instead of exposing multiple instances to the internet, only the bastion host is accessible.
- Reduces the chances of brute-force attacks, malware infections, or unauthorized access.
- Enhances Network Segmentation - Separates public-facing components (bastion) from private infrastructure.

STEP BY STEP OVERVIEW:

Step 1: CREATE VPC

- Login into your AWS console and navigate to VPC dashboard and create your own VPC.
- Specify the name tag, IPv4 CIDR block (10.0.0.0/16), IPv6 CIDR (optional)
- Then click create.

aws [Search] [Alt+S] Asia Pacific (Mumbai) Nidhisha A Dhas

VPC > Your VPCs > vpc-02529547f8d9ed11a

VPC dashboard < EC2 Global View [?] Filter by VPC: [v]

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
Security groups

PrivateLink and Lattice
Getting started [Updated](#)
Endpoints [Updated](#)
Endpoint services

You successfully created vpc-02529547f8d9ed11a / my-vpc

vpc-02529547f8d9ed11a / my-vpc [Actions]

Details [Info]

VPC ID vpc-02529547f8d9ed11a	State Available	Block Public Access Off	DNS hostnames Disabled
DNS resolution Enabled	Tenancy default	DHCP option set dopt-02776c26c09898d34	Main route table rtb-00ce348503926292a
Main network ACL acl-0a6197940d871c26b	Default VPC No	IPv4 CIDR 10.0.0.0/16	IPv6 pool -
IPv6 CIDR (Network border group) -	Network Address Usage metrics Disabled	Route 53 Resolver DNS Firewall rule groups -	Owner ID 941377153200

[Resource map](#) | [CIDRs](#) | [Flow logs](#) | [Tags](#) | [Integrations](#)

Resource map [Info]

VPC [Show details](#)
Your AWS virtual network

my-vpc

Subnets (0)
Subnets within this VPC

Route tables (1)
Route network traffic to resources

rtb-00ce348503926292a

Network connections (0)
Connections to other networks

Step 2: CREATE A PUBLIC SUBNETS

- Click on create subnets and select the VPC you have just created.
- Create a public subnet with CIDR block of 10.0.1.0/24.
- Enable the 'auto-assign' public IP.

aws [Search] [Alt+S] Asia Pacific (Mumbai) Nidhisha A Dhas

VPC dashboard < EC2 Global View [?] Filter by VPC: [v]

Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only Internet gateways
DHCP option sets

Subnets (1) [Info] Last updated less than a minute ago [Actions] [Create subnet](#)

Find resources by attribute or tag

Subnet ID: subnet-024f051296ad776ac [X] [Clear filters](#)

<input type="checkbox"/>	Name	Subnet ID	State	VPC	Block Public...	IPv4 CIDR	IPv6 CIDR
<input type="checkbox"/>	public	subnet-024f051296ad776ac	Available	vpc-02529547f8d9ed11a my-...	Off	10.0.1.0/24	-

Step 3: CREATE A PRIVATE SUBNET

- Click on create subnets and select the VPC you have just created.
- Create a private subnet with CIDR block of 10.0.2.0/24.
- Don't enable the 'auto-assign' public IP.

Subnets (1) Info

Find resources by attribute or tag

Subnet ID: subnet-0b80a0fd3dc6f1f89 Clear filters

Name	Subnet ID	State	VPC	Block Public...	IPv4 CIDR	IPv6 CIDR
private	subnet-0b80a0fd3dc6f1f89	Available	vpc-02529547f8d9ed11a my-...	Off	10.0.2.0/24	-

Step 4: CREATE THE INTERNET GATEWAY

- Go to the Internet Gateways and click on Internet gateway.
- Name it and attach it to the VPC that we have created.

igw-00f658dcf526976a9 / my-gateway

The following internet gateway was created: igw-00f658dcf526976a9 - my-gateway. You can now attach to a VPC to enable the VPC to communicate with the internet. Attach to a VPC

Details Info

Internet gateway ID igw-00f658dcf526976a9	State Detached	VPC ID -	Owner 941377153200
--	-------------------	-------------	-----------------------

Tags

Key	Value
Name	my-gateway

Attach to VPC (igw-00f658dcf526976a9) 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-02529547f8d9ed11a

AWS Command Line Interface command

Cancel Attach internet gateway

igw-00f658dcf526976a9 / my-gateway

Internet gateway igw-00f658dcf526976a9 successfully attached to vpc-02529547f8d9ed11a

Details Info

Internet gateway ID igw-00f658dcf526976a9	State Attached	VPC ID vpc-02529547f8d9ed11a my-vpc	Owner 941377153200
--	-------------------	--	-----------------------

Tags

Key	Value
Name	my-gateway

Step 5: CREATE PUBLIC ROUTE TABLE

- Go to route table- click on ‘create route table’.
- Specify the name and associate it with the public subnet.
- Add destination and target to the route table.
- Click create.

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

rtb-0b25cf1fbacebbb07 / sample Actions ▼

You have successfully updated subnet associations for rtb-0b25cf1fbacebbb07 / sample. ✕

Details info

Route table ID rtb-0b25cf1fbacebbb07

VPC vpc-08b45a9670bdd87aa | vpc-1

Main No

Owner ID 941377153200

Explicit subnet associations 2 subnets

Edge associations -

Routes Subnet associations Edge associations Route propagation Tags

Routes (1) Both ▼ Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No

Step 4: LAUNCH BASTION HOST

- Go to the EC2 dashboard and launch two EC2 instances by specifying the instance name, AMI and Instance Type.
- Under the ‘network settings’, select your VPC and select the public subnet and the private subnet respectively for both the instances.
- Enable the auto assign Public IP for the public EC2 and disable it for the private EC2 instance.
- Also, create the Security groups for the instances.
- Now, click on launch instance.

EC2 <

Dashboard

EC2 Global View

Events

Instances

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Instances (1/2) Info Info

Last updated less than a minute ago ⌚ Connect Instance state ▼ Actions ▼ Launch instances ▼

All states ▼

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IP
private-ec2	i-0e3660541ef044cfd	Running	t2.micro	2/2 checks passed	View alarms +	ap-south-1b	-	-
public-ec2	i-01565f3af2f715fd5	Running	t2.micro	2/2 checks passed	View alarms +	ap-south-1a	-	43.205

Inbound Security Group Rules

▼ Security group rule 1 (TCP, 22, 0.0.0.0/0)

Remove

Type | Info

ssh

Protocol | Info

TCP

Port range | Info

22

Source type | Info

Anywhere

Source | Info

Q Add CIDR, prefix list or security group

0.0.0.0/0 X

Description - optional | Info

e.g. SSH for admin desktop

Add security group rule

► Advanced network configuration

Step 5: CONNECT THE PRIVATE INSTANCE TO THE BASTION HOST

- Open the PowerShell and give the following command to change the directory.

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Arulldhas> cd downloads
PS C:\Users\Arulldhas\downloads> |
```

- To connect the private instance copy the ssh command from the private instance and paste it in the PowerShell.

```
C:\TEST>ssh -i "my-test-pair.pem" ec2-user@ec2-15-207-248-31.ap-south-1.compute.amazonaws.com

#####
##### Amazon Linux 2023
#####
##### https://aws.amazon.com/linux/amazon-linux-2023
#####
```

CONCLUSION:

By completing this PoC, you will be able to:

- Create a Bastion host that enhances the security to access resources in a private network from an external network, like the internet.