



Creating a Private Subnet



Ivan Delgadillo Fernandez

The screenshot shows the AWS Subnets page with a success message: "You have successfully created 1 subnet: subnet-03c0147ba8f4b4c9f". The table lists one subnet:

| Name | Subnet ID | State | VPC | IPv4 CIDR | IPv6 CIDR |
|------------------------------|--------------------------|-----------|-------------------------------------|-------------|-----------|
| SubnetPrivate-IvanDelgadillo | subnet-03c0147ba8f4b4c9f | Available | vpc-0b8dd2afc7f5ee566 VPC-Ivan... | 10.0.2.0/24 | - |

The subnet details page is shown for "subnet-03c0147ba8f4b4c9f / SubnetPrivate-IvanDelgadillo". The "Details" tab is selected, displaying the following information:

| Subnet ID | Subnet ARN | State | IPv4 CIDR |
|--------------------------|--|---------------------------------|---|
| subnet-03c0147ba8f4b4c9f | arn:aws:ec2:us-east-1:600627346491:subnet/subnet-03c0147ba8f4b4c9f | Available | 10.0.2.0/24 |
| Available IPv4 addresses | IPv6 CIDR association ID | Availability Zone | Route table |
| 251 | - | us-east-1b | rtb-0be65521e8f4476e5 PublicRouteTable-IvanDelgadillo |
| Availability Zone ID | VPC | Auto-assign public IPv4 address | Auto-assign IPv6 address |
| use1-sz4 | vpc-0b8dd2afc7f5ee566 VPC-IvanDelgadillo | No | No |
| Network ACL | Network border group | | |
| - | us-east-1 | | |



Ivan Delgadillo Fernandez

NextWork Student

NextWork.org

Introducing Today's Project!

What is Amazon VPC?

Amazon Virtual Private Cloud (Amazon VPC) gives you full control over your virtual networking environment, including resource placement, connectivity, and security.

How I used Amazon VPC in this project

Used to create Private and Public Subnets

One thing I didn't expect in this project was...

I didn't expect configure NACL.

This project took me...

33 Minutes



Ivan Delgadillo Fernandez

NextWork Student

NextWork.org

Private vs Public Subnets

Public subnet – The subnet has a direct route to an internet gateway. Resources in a public subnet can access the public internet. Private subnet – The subnet does not have a direct route to an internet gateway. Resources in a private subnet require

For example, it's very common for engineers to set up an EC2 instance hosting their web app in a public subnet, but keep the database of customers and login details in a private subnet.

My private and public subnets cannot have the same CIDR

The screenshot shows the AWS Subnets console with a success message: "You have successfully created 1 subnet: subnet-03c0147ba8f4b4c9f". The main table lists one subnet:

| Name | Subnet ID | State | VPC | IPv4 CIDR | IPv6 CIDR |
|------------------------------|--------------------------|-----------|----------------------------------|-------------|-----------|
| SubnetPrivate-IvanDelgadillo | subnet-03c0147ba8f4b4c9f | Available | vpc-0b8dd2afc7f5ee566 VPC-I... | 10.0.2.0/24 | - |

The subnet details page for "subnet-03c0147ba8f4b4c9f / SubnetPrivate-IvanDelgadillo" is shown. The "Details" tab is selected, displaying the following information:

| Subnet ID | Subnet ARN | State | IPv4 CIDR |
|--------------------------|--|--------------------------|---|
| subnet-03c0147ba8f4b4c9f | arn:aws:ec2:us-east-1:600627346491:subnet/subnet-03c0147ba8f4b4c9f | Available | 10.0.2.0/24 |
| Available IPv4 addresses | - | IPv6 CIDR | - |
| 251 | - | VPC | vpc-0b8dd2afc7f5ee566 VPC-IvanDelgadillo |
| Availability Zone ID | use1-az4 | Network border group | Auto-assign public IPv4 address |
| Network ACL | - | us-east-1 | No |
| Default Route table | - | Route table | rtb-0be65521e8f4476e5 PublicRouteTable-IvanDelgadillo |
| | | Auto-assign IPv6 address | No |



Ivan Delgadillo Fernandez

NextWork Student

NextWork.org

A dedicated route table

By default, my private subnet is associated with subnet explicit

I had to set up a new route table because I need separate CIDR between Public Subnet and Private Subnet

My private subnet's dedicated route table only has one inbound and one outbound rule that allows traffic only with private IPs in VPC

Route tables (1/3) [Info](#)

Last updated [less than a minute ago](#) [Actions](#) [Create route table](#)

| Name | Route table ID | Explicit subnet associ... | Edge associations | Main | VPC | Own... |
|--|---------------------------------------|--|-------------------|------|---|-----------|
| - | rtb-00c281bbcdad1f700 | - | - | Yes | vpc-09e590b2738c761ee | 600627... |
| PublicRouteTable-IvanDelgadillo | rtb-0be65521e8f4476e5 | subnet-066127ae77ede4... | - | Yes | vpc-0b8dd2afc7f5ee566 VPC-IvanDelgad... | 600627... |
| <input checked="" type="checkbox"/> PrivateRouteTable-IvanDelgadillo | rtb-04502d51aa7067f53 | - | - | No | vpc-0b8dd2afc7f5ee566 VPC-IvanDelgad... | 600627... |

rtb-04502d51aa7067f53 / PrivateRouteTable-IvanDelgadillo

[Details](#) [Routes](#) [Subnet associations](#) [Edge associations](#) [Route propagation](#) [Tags](#)

Details

| | | | |
|---|--|-----------------------------------|------------------------|
| Route table ID rtb-04502d51aa7067f53 | Main <input type="checkbox"/> No | Explicit subnet associations - | Edge associations - |
| VPC vpc-0b8dd2afc7f5ee566 VPC-IvanDelgadillo | Owner ID 600627346491 | | |



Ivan Delgadillo Fernandez

NextWork Student

NextWork.org

A new network ACL

By default, my private subnet is associated with nothing, I have to associate with my Private Subnet

To restricts traffic and protects private subnet!

My new network ACL has two simple rules Rule 100 that allow all traffic from source any

The screenshot shows the AWS Network ACLs console. At the top, a message says "You have successfully updated outbound rules for acl-0ef127da1e502cd36 / PrivateNetworkACL-IvanDelgadillo". Below this is a table of Network ACLs:

| Name | Network ACL ID | Associated with | Default | VPC ID | Inbound rules count |
|--|---|--|---------|--|---------------------|
| - | acl-06573268ec7bf1f2c | 6 Subnets | Yes | vpc-09e590b2738c761ee | 2 Inbound rules |
| - | acl-0465bfecc90cda9b83 | subnet-03c0147ba8f4b4c9f / SubnetPrivate-Iv... | Yes | vpc-0b8dd2afc7f5ee566 / VPC-IvanDel... | 2 Inbound rules |
| PublicNetworkACL-IvanDelgadillo | acl-0ee470d70d9bf5ca | subnet-066127ae77ede4a72 / SubnetPublic-Iv... | No | vpc-0b8dd2afc7f5ee566 / VPC-IvanDel... | 2 Inbound rules |
| <input checked="" type="checkbox"/> PrivateNetworkACL-IvanDelgadillo | <input checked="" type="checkbox"/> acl-0ef127da1e502cd36 | - | No | vpc-0b8dd2afc7f5ee566 / VPC-IvanDel... | 2 Inbound rules |

Below the table, a specific Network ACL is selected: "acl-0ef127da1e502cd36 / PrivateNetworkACL-IvanDelgadillo". The "Inbound rules" tab is active, showing two rules:

| Rule number | Type | Protocol | Port range | Source | Allow/Deny |
|-------------|-------------|----------|------------|-----------|------------|
| 100 | All traffic | All | All | 0.0.0.0/0 | Allow |
| * | All traffic | All | All | 0.0.0.0/0 | Deny |



NextWork.org

Everyone should be in a job they love.

Check out nextwork.org for
more projects

