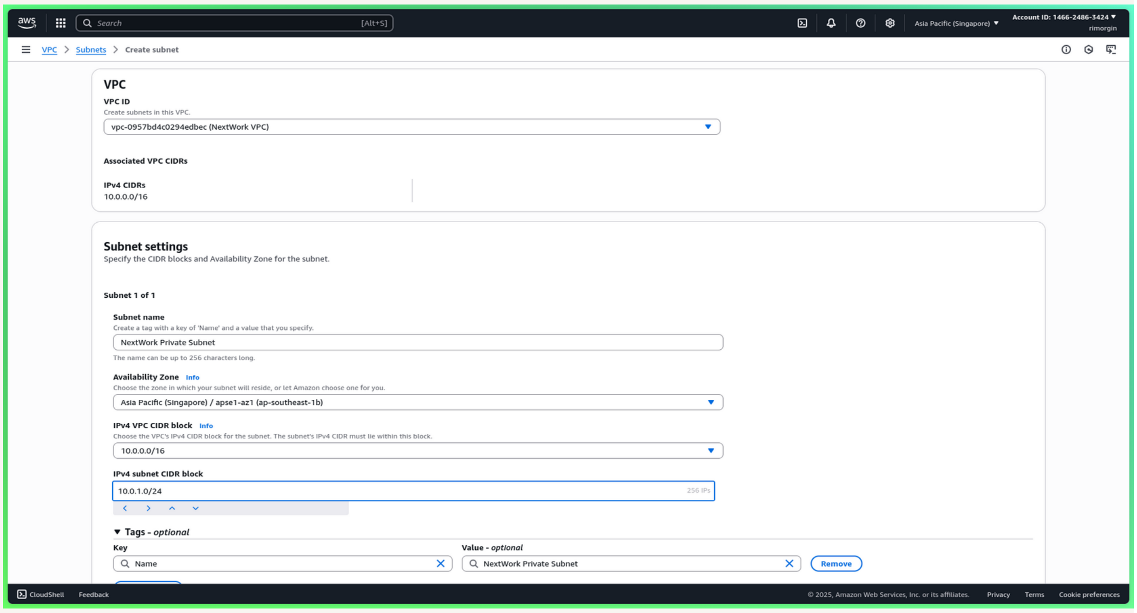
nextwork.org

Creating a Private Subnet

Sean Calderon


aws
Search [Alt+S]
Asia Pacific (Singapore)
Account ID: 1466-2486-3424
rimorgin
VPC > Subnets > Create subnet
Info
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

VPC

VPC ID
Create subnets in this VPC.
vpc-0957bd4c0294edbec (NextWork VPC)

Associated VPC CIDRs

IPv4 CIDRs
10.0.0.0/16

Subnet settings
Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.
NextWork Private Subnet
The name can be up to 256 characters long.

Availability Zone
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
Asia Pacific (Singapore) / apse1-az1 (ap-southeast-1b)

IPv4 VPC CIDR block
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.
10.0.0.0/16

IPv4 subnet CIDR block
10.0.1.0/24 256 IPs

▼ **Tags** - *optional*

Key	Value - *optional*	
Name	NextWork Private Subnet	Remove

Introducing Today's Project!

What is Amazon VPC?

Amazon VPC is the best fit for creating an infrastructure where the requirements should have a resource containing data that needs to be protected and only a certain resource can access that data.

How I used Amazon VPC in this project

In today's project, I used Amazon VPC to create private subnets, setup dedicated routing table and NACL to demonstrate public subnets and private subnets must have their own dedicated settings and properties in order to achieve security-in-the-cloud.

This project took me...

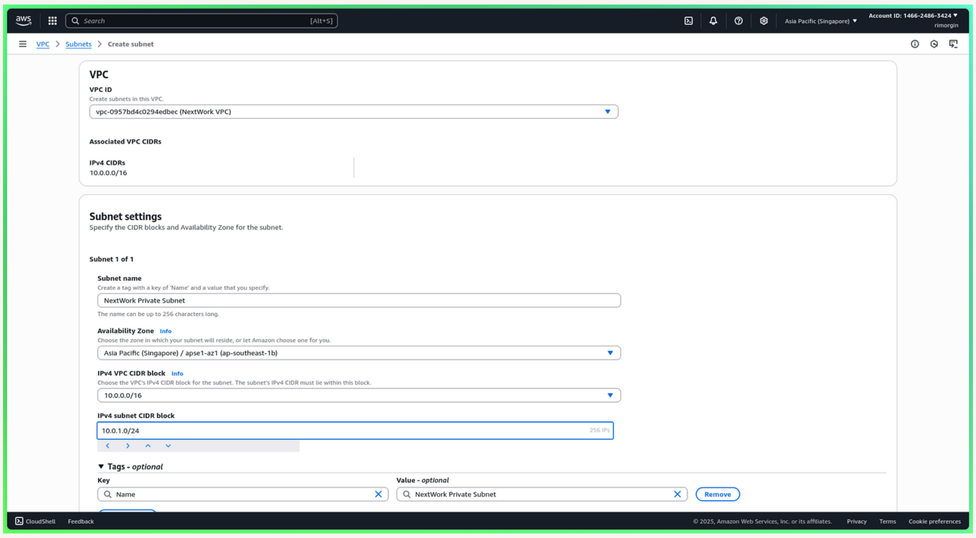
This project took me approximately 15 minutes. Setting up private subnet and its dedicated route table and NACL is taken with just a few clicks!

Private vs Public Subnets

The difference between public and private subnets is that a public subnet has public routable traffic whereas private does not have the means to route traffic going to the internet.

Having private subnets are useful because it is a way to protect essential resources that must not be exposed to the internet such as a database containing SPII or any sensitive data stored on it.

My private and public subnets cannot have the same network subnet/prefix because overlapping and conflicting subnets may cause problems on routing traffic.



VPC

VPC ID
Create subnets in this VPC.
vpc-0957bd4c0294edbec (NextWork VPC)

Associated VPC CIDRs

IPv4 CIDRs
10.0.0.0/16

Subnet settings
Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.
NextWork Private Subnet
The name can be up to 256 characters long.

Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
Asia Pacific (Singapore) / apse1-az1 (ap-southeast-1b)

IPv4 VPC CIDR block Info
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.
10.0.0.0/16

IPv4 subnet CIDR block
10.0.1.0/24 256 IPs

▼ Tags - *optional*

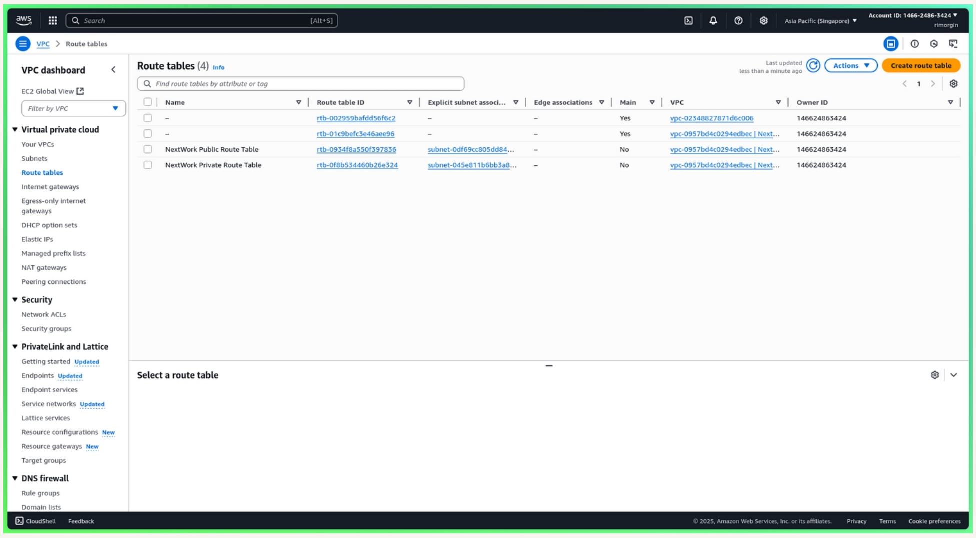
Key	Value - *optional*
Name	NextWork Private Subnet

A dedicated route table

By default, my private subnet is associated with a default route table when I created my custom VPC.

I had to set up a new route table because the default route table specified is the main route table which is the public route table and has a route to the internet.

My private subnet's dedicated route table only has one inbound and one outbound rule that allows any traffic.



Route tables (4) Info

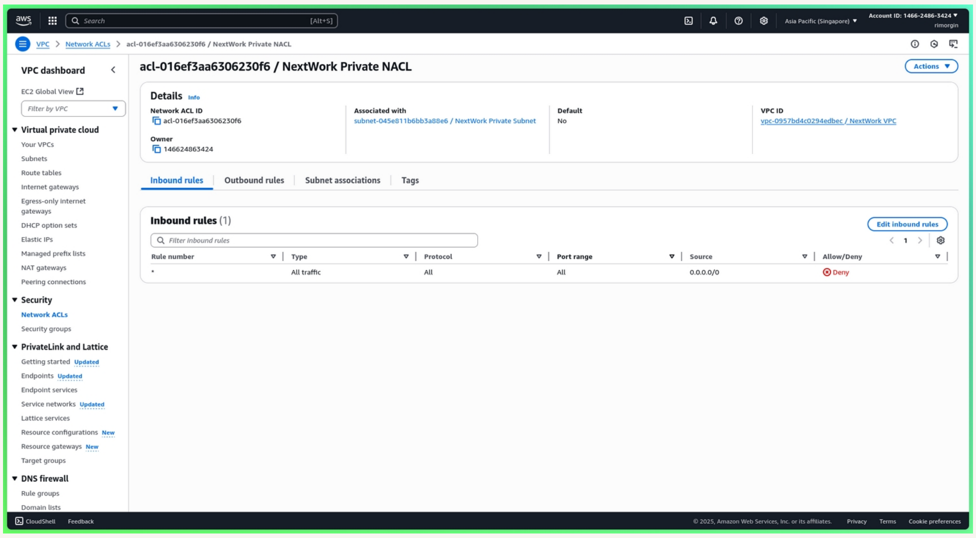
Name	Route table ID	Explicit subnet associ...	Edge associations	Main	VPC	Owner ID
–	rtb-002959bafdd56f6c2	–	–	Yes	vpc-02348827871d6c006	146624863424
–	rtb-01c9befc3e46aee96	–	–	Yes	vpc-0957bd4c0294edbec | Next...	146624863424
NextWork Public Route Table	rtb-0934f8a550f397836	subnet-0df69cc805dd84...	–	No	vpc-0957bd4c0294edbec | Next...	146624863424
NextWork Private Route Table	rtb-0f8b534460b26e324	subnet-045e811b6bb3a8...	–	No	vpc-0957bd4c0294edbec | Next...	146624863424

A new network ACL

By default, my private subnet is associated with a NACL too that is also associated with public subnet.

I set up a dedicated network ACL for my private subnet because setting the same NACL doesn't guarantee privacy and may cause breach of security especially if the data is extremely sensitive and must have utmost privacy and confidentiality.

My new network ACL has two simple rules, one for deny for traffic inbound and one for deny for traffic outbound.



acl-016ef3aa6306230f6 / NextWork Private NACL

Details Info

Network ACL ID: acl-016ef3aa6306230f6

Associated with: subnet-045e811b6bb3a88e6 / NextWork Private Subnet

Default: No

VPC ID: vpc-0957bd4c0294edbec / NextWork VPC

Owner: 146624863424

Inbound rules (1)

Rule number	Type	Protocol	Port range	Source	Allow/Deny
*	All traffic	All	All	0.0.0.0/0	⊗ Deny

The place to learn & showcase your skills

Check out nextwork.org for more projects