

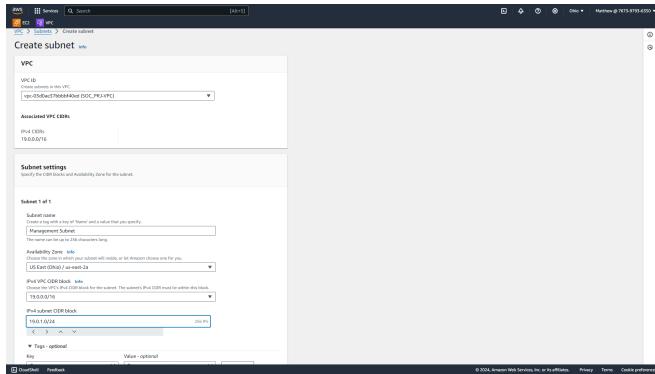
SOC Project Documentation

Create VPC

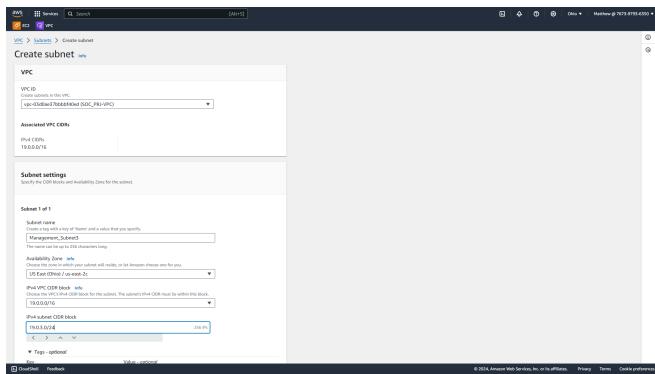
- Go to AWS(Log into root or IAM User account).
- Go to the **Services Search bar** on the top left and search for **VPC**.
- Create your VPC Name. **SOC_PRJ-VPC**
- Create your VPC IP Address. **(19.0.0.0/16)**
- Then Click **Create VPC**.

Create Subnets

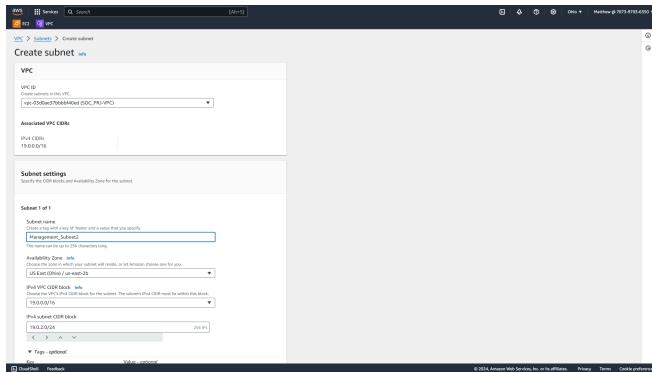
- Find Subnets in the VPC service on the left panel (**CLICK IT**)
- Click **create Subnet** on the top right.
- Click the VPC you create to connect your subnets to the VPC!
- Add the amount of subnets needed.
- Management Subnet:
 - AZ1: 19.0.1.0/24



- AZ2: 19.0.2.0/24



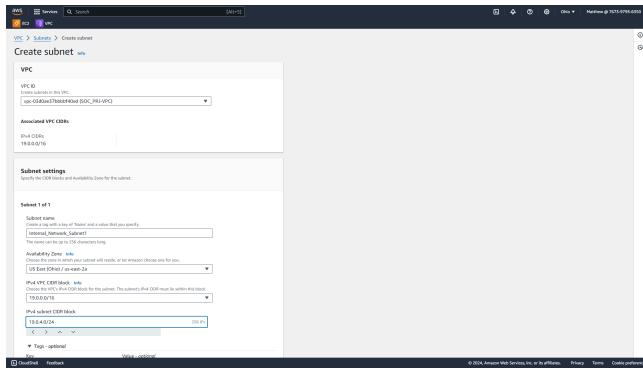
- AZ3: 19.0.3.0/24



- Internal Network Subnets:

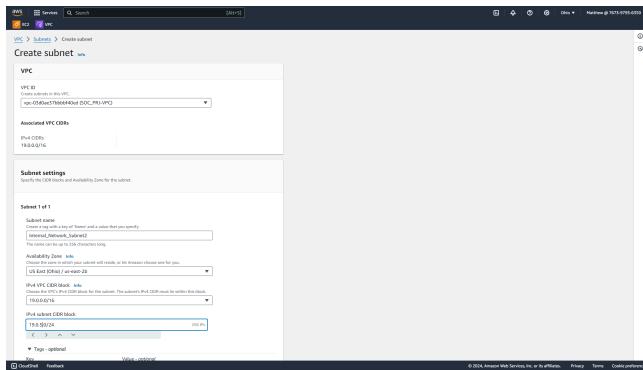
- Web Servers Subnet:

- AZ1: 19.0.4.0/24



- Application Servers Subnet:

- AZ2: 19.0.5.0/24



- Databases Subnet:

- AZ3: 19.0.6.0/24

VPC

VPC ID: vpc-0dab47b78f464619 (vpc-0dab47b78f464619)

Associated VPC CIDR: 19.0.0.0/16

Subnet settings: Specify the CIDR block and Availability Zone for the subnet.

Subnet 1 of 1:

- Subnet name:** AZ1_Subnet1 (Create a new name or reuse an existing one.)
- Availability Zone:** US East (N. Virginia) (The subnet can be in the same or a different availability zone.)
- IPv4 CIDR block:** 19.0.7.0/24 (The subnet must have a CIDR block that doesn't overlap with other subnets in the VPC. The subnet's IPv4 CIDR must be within this block.)
- IPv4 subnet CIDR block:** 19.0.7.0/24 (The subnet must have a CIDR block that doesn't overlap with other subnets in the VPC. The subnet's IPv4 CIDR must be within this block.)
- Tags (optional):** (Add tags)

- DMZ (Demilitarized Zone) Subnet:

- AZ1: 19.0.7.0/24

VPC

VPC ID: vpc-0dab47b78f464619 (vpc-0dab47b78f464619)

Associated VPC CIDR: 19.0.0.0/16

Subnet settings: Specify the CIDR block and Availability Zone for the subnet.

Subnet 1 of 1:

- Subnet name:** AZ1_Subnet2 (Create a new name or reuse an existing one.)
- Availability Zone:** US East (N. Virginia) (The subnet can be in the same or a different availability zone.)
- IPv4 CIDR block:** 19.0.8.0/24 (The subnet must have a CIDR block that doesn't overlap with other subnets in the VPC. The subnet's IPv4 CIDR must be within this block.)
- IPv4 subnet CIDR block:** 19.0.8.0/24 (The subnet must have a CIDR block that doesn't overlap with other subnets in the VPC. The subnet's IPv4 CIDR must be within this block.)
- Tags (optional):** (Add tags)

- AZ2: 19.0.8.0/24

VPC

VPC ID: vpc-0dab47b78f464619 (vpc-0dab47b78f464619)

Associated VPC CIDR: 19.0.0.0/16

Subnet settings: Specify the CIDR block and Availability Zone for the subnet.

Subnet 1 of 1:

- Subnet name:** AZ2_Subnet1 (Create a new name or reuse an existing one.)
- Availability Zone:** US East (N. Virginia) (The subnet can be in the same or a different availability zone.)
- IPv4 CIDR block:** 19.0.9.0/24 (The subnet must have a CIDR block that doesn't overlap with other subnets in the VPC. The subnet's IPv4 CIDR must be within this block.)
- IPv4 subnet CIDR block:** 19.0.9.0/24 (The subnet must have a CIDR block that doesn't overlap with other subnets in the VPC. The subnet's IPv4 CIDR must be within this block.)
- Tags (optional):** (Add tags)

- AZ3: 19.0.9.0/24

VPC

VPC ID: vpc-0dab47b78f464619 (vpc-0dab47b78f464619)

Associated VPC CIDR: 19.0.0.0/16

Subnet settings: Specify the CIDR block and Availability Zone for the subnet.

Subnet 1 of 1:

- Subnet name:** AZ3_Subnet1 (Create a new name or reuse an existing one.)
- Availability Zone:** US East (N. Virginia) (The subnet can be in the same or a different availability zone.)
- IPv4 CIDR block:** 19.0.10.0/24 (The subnet must have a CIDR block that doesn't overlap with other subnets in the VPC. The subnet's IPv4 CIDR must be within this block.)
- IPv4 subnet CIDR block:** 19.0.10.0/24 (The subnet must have a CIDR block that doesn't overlap with other subnets in the VPC. The subnet's IPv4 CIDR must be within this block.)
- Tags (optional):** (Add tags)

- Intrusion Detection/Prevention Subnet:

- AZ1: 19.0.10.0/24

VPC
VPC ID: vpc-05d8e077b44646c9
Associated VPC CENs:
None
Subnet settings
Specify the CIDR block and Availability Zone for the subnet.

Subnet 1 of 1
Subnet name:
Availability Zone:
IPv4 CIDR block:
Tags: optional

- AZ2: 19.0.11.0/24

VPC
VPC ID: vpc-05d8e077b44646c9
Associated VPC CENs:
None
Subnet settings
Specify the CIDR block and Availability Zone for the subnet.

Subnet 1 of 1
Subnet name:
Availability Zone:
IPv4 CIDR block:
Tags: optional

- AZ3: 19.0.12.0/24

VPC
VPC ID: vpc-05d8e077b44646c9
Associated VPC CENs:
None
Subnet settings
Specify the CIDR block and Availability Zone for the subnet.

Subnet 1 of 1
Subnet name:
Availability Zone:
IPv4 CIDR block:
Tags: optional

- VPN Gateway Subnet:

- AZ1: 19.0.13.0/24

VPC > Subnets > Create subnet

Create subnet

VPC
VPC Subnets in this VPC
vpc-05d8e778744640c0 (soc_pru_vpc)

Associated VPC CDBs
IPv4 CDBs
93.0.0.0/16

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

Subnet 1 of 1

Subnet name
Create a long with a mix of 'Name' and a value that you specify.
VPC Gateway Subnet
The name can be up to 255 characters long.

Availability Zone
US East (Ohio) / us-east-2a
This is the availability zone the subnet will reside in, or let Amazon choose one for you.

IPv4 VPC CIDR block
Specify the IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must be within this block.
192.0.0.0/16

IPv4 subnet CIDR block
192.168.0.0/24
Specify the IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must be within this block.
192.168.0.0/24

Tags - optional

- AZ2: 19.0.14.0/24

VPC > Subnets > Create subnet

Create subnet

VPC
VPC Subnets in this VPC
vpc-05d8e778744640c0 (soc_pru_vpc)

Associated VPC CDBs
IPv4 CDBs
93.0.0.0/16

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

Subnet 1 of 1

Subnet name
Create a long with a mix of 'Name' and a value that you specify.
VPC Gateway Subnet
The name can be up to 255 characters long.

Availability Zone
US East (Ohio) / us-east-2a
This is the availability zone the subnet will reside in, or let Amazon choose one for you.

IPv4 VPC CIDR block
Specify the IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must be within this block.
192.0.0.0/16

IPv4 subnet CIDR block
192.168.1.0/24
Specify the IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must be within this block.
192.168.1.0/24

Tags - optional

- AZ3: 19.0.15.0/24

VPC > Subnets > Create subnet

Create subnet

VPC
VPC Subnets in this VPC
vpc-05d8e778744640c0 (soc_pru_vpc)

Associated VPC CDBs
IPv4 CDBs
93.0.0.0/16

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

Subnet 1 of 1

Subnet name
Create a long with a mix of 'Name' and a value that you specify.
Backup_and_Recovery_Subnet
The name can be up to 255 characters long.

Availability Zone
US East (Ohio) / us-east-2a
This is the availability zone the subnet will reside in, or let Amazon choose one for you.

IPv4 VPC CIDR block
Specify the IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must be within this block.
192.0.0.0/16

IPv4 subnet CIDR block
192.168.0.0/24
Specify the IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must be within this block.
192.168.0.0/24

Tags - optional

- Backup and Recovery Subnet:

- AZ1: 19.0.16.0/24

VPC > Subnets > Create subnet

Create subnet

VPC
VPC Subnets in this VPC
vpc-05d8e778744640c0 (soc_pru_vpc)

Associated VPC CDBs
IPv4 CDBs
93.0.0.0/16

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

Subnet 1 of 1

Subnet name
Create a long with a mix of 'Name' and a value that you specify.
Backup_and_Recovery_Subnet
The name can be up to 255 characters long.

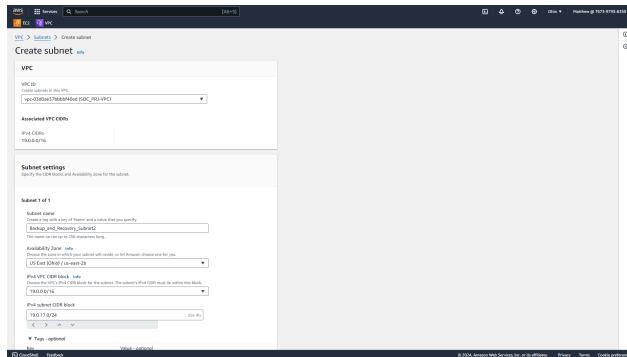
Availability Zone
US East (Ohio) / us-east-2a
This is the availability zone the subnet will reside in, or let Amazon choose one for you.

IPv4 VPC CIDR block
Specify the IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must be within this block.
192.0.0.0/16

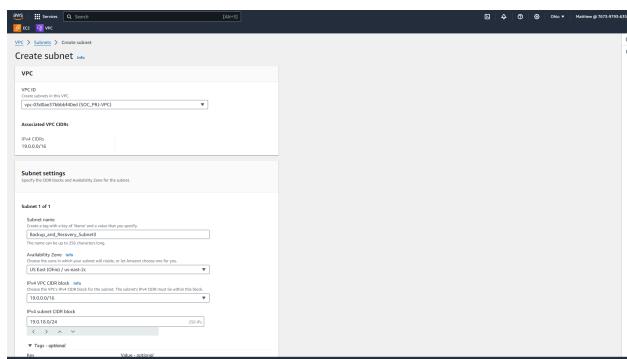
IPv4 subnet CIDR block
192.168.0.0/24
Specify the IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must be within this block.
192.168.0.0/24

Tags - optional

- AZ2: 19.0.17.0/24

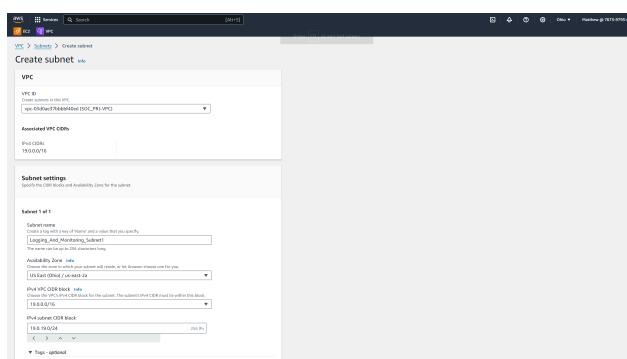


- AZ3: 19.0.18.0/24

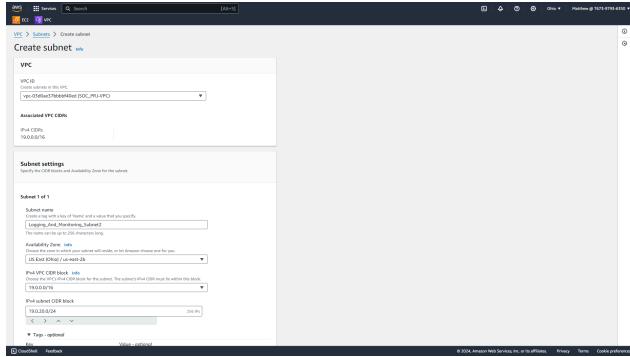


- Logging and Monitoring Subnet:

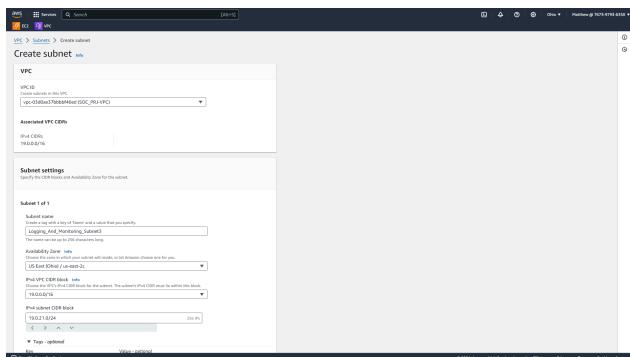
- AZ1: 19.0.19.0/24



- AZ2: 19.0.20.0/24



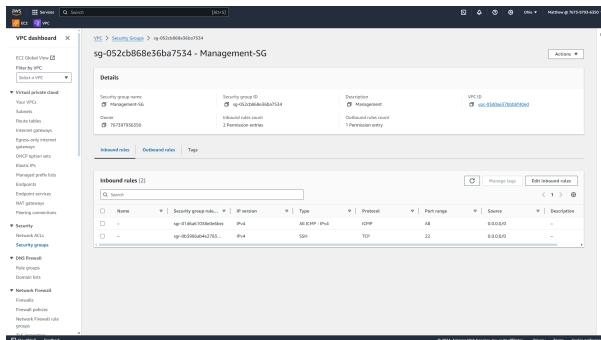
- AZ3: 19.02.0/24



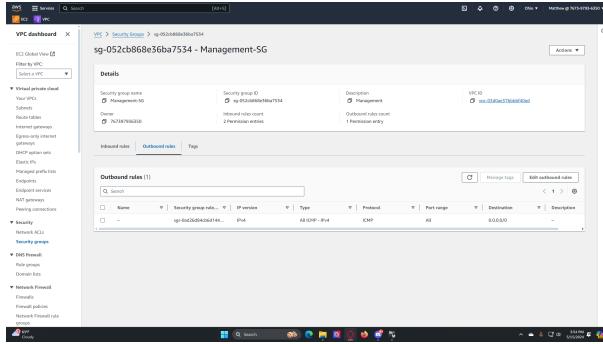
Create Security Groups

Management Security Group

- Click Create Security Group on the top right
 - Type in the name()
 - Type in a description
 - Connect it to your VPC
 - Set Inbound Rules()

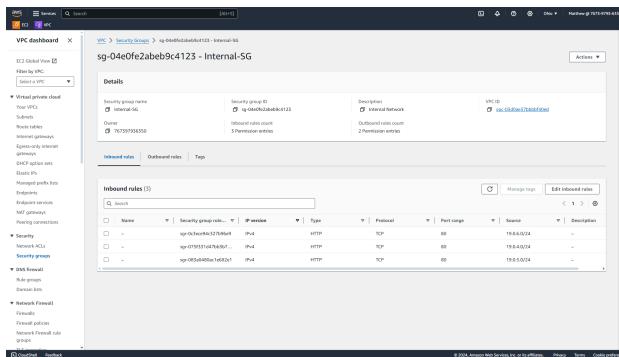


- Set Outbound rules()

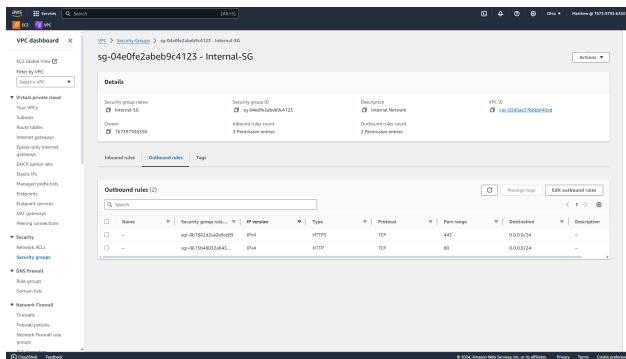


Internal Network Security Group

- Click Create Security Group on the top right
- Type in the name()
- Type in a description
- Connect it to your VPC
- Set Inbound Rules()



- Set Outbound rules()



DMZ (Demilitarized Zone) Security Group

- Click Create Security Group on the top right
- Type in the name()

- Type in a description
- Connect it to your VPC
- Set Inbound Rules()

Details

Name	Security group rule ID	IP version	Type	Protocol	Port range	Source	Description
sg-08e052e3bdbf2473f	sg-08e052e3bdbf2473f	IPv4	HTTPS	TCP	443	0.0.0.0/0	
	sg-0c17030d0c5f4	IPv4	SMTP	TCP	25	0.0.0.0/0	
	sg-025824bc05701...	IPv4	HTTP	TCP	80	0.0.0.0/0	

- Set Outbound rules()

Outbound rules (1)

Name	Security group rule ID	IP version	Type	Protocol	Port range	Destinations	Description
sg-08e052e3bdbf2473f	sg-08e052e3bdbf2473f	IPv4	TCP	TCP	52	0.0.0.0/0	

Intrusion Detection/Prevention Security Group

- Click Create Security Group on the top right
- Type in the name()
- Type in a description
- Connect it to your VPC
- Set Inbound Rules()

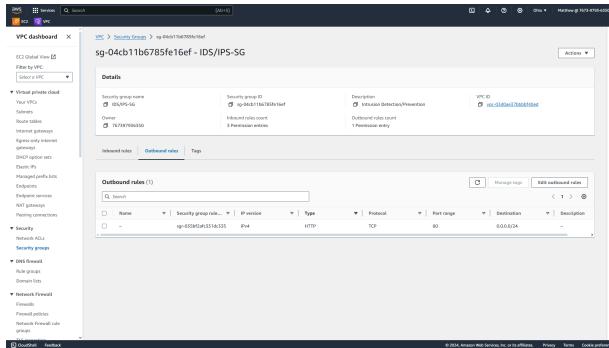
Details

Name	Security group ID	Description	VPC ID
sg-04cb11b6785fe16ef	sg-04cb11b6785fe16ef	Intrusion Detection/Prevention	vpc-0cd8ac1b0ab1d01d

Inbound rules (3)

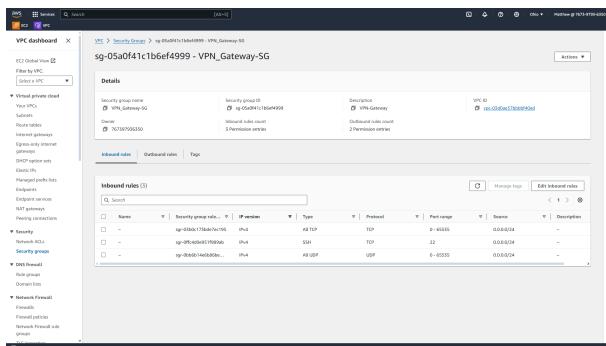
Name	Security group rule ID	IP version	Type	Protocol	Port range	Source	Description
sg-04cb11b6785fe16ef	sg-04cb11b6785fe16ef	IPv4	All traffic	All	192.168.0.0/16		
	sg-04cb11b6785fe16ef	IPv4	All traffic	All	192.168.0.0/16		
	sg-04cb11b6785fe16ef	IPv4	All traffic	All	192.168.0.0/16		

- Set Outbound rules()

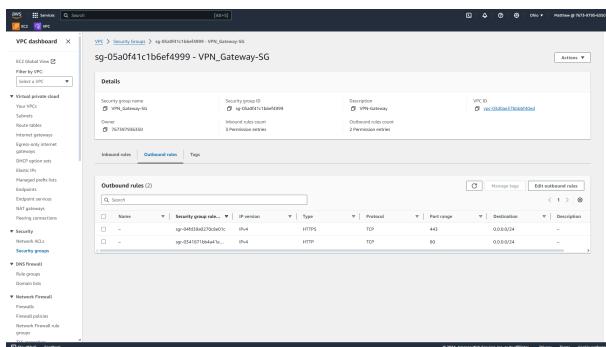


VPN Gateway Security Group

- Click Create Security Group on the top right
- Type in the name()
- Type in a description
- Connect it to your VPC
- Set Inbound Rules()



- Set Outbound rules()



Backup and Recovery Security Group

- Click Create Security Group on the top right
- Type in the name()
- Type in a description
- Connect it to your VPC

- Set Inbound Rules()

Name	Security group rule ID	Type	Protocol	Port range	Source	Description
sg-01837d94aac611343	sg-01837d94aac611343	IP	TCP	2323	192.168.0.24	
sg-0446dbf9ef416140	sg-0446dbf9ef416140	IP	TCP	2349	192.168.0.24	
sg-0111515a27c73c	sg-0111515a27c73c	IP	TCP	2349	192.168.0.24	

- Set Outbound rules()

Name	Security group rule ID	Type	Protocol	Port range	Destination	Description
sg-01837d94aac611343	sg-01837d94aac611343	IP	NFS	2049	192.168.0.24	

Logging and Monitoring Security Group

- Click Create Security Group on the top right
- Type in the name()
- Type in a description
- Connect it to your VPC
- Set Inbound Rules()

Name	Security group rule ID	Type	Protocol	Port range	Source	Description
sg-078c0da059afdd043	sg-078c0da059afdd043	IP	TCP	2323	192.168.0.24	
sg-078c0da059afdd043	sg-078c0da059afdd043	IP	TCP	2349	192.168.0.24	
sg-078c0da059afdd043	sg-078c0da059afdd043	IP	TCP	2355	192.168.0.24	

- Set Outbound rules()

Setting up NACLs

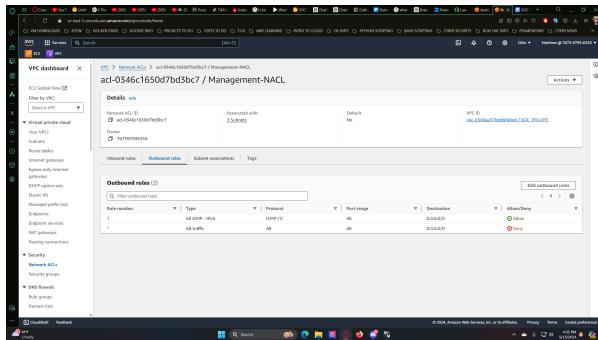
Go to the NACLs in the subsections of the VPC

Management NACL

- Click Create Network ACL on the top right
- Type in the name()
- Connect it to your VPC
- Add any tags related to the NACL
- Set the Subnet associations()

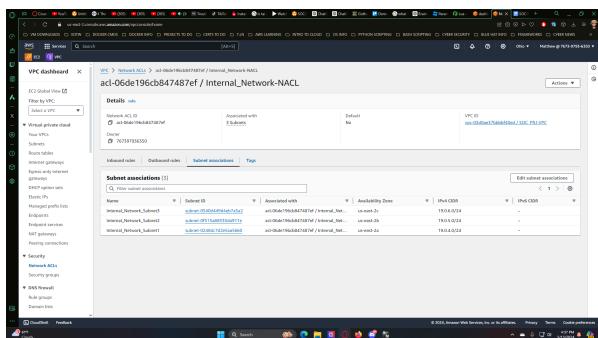
- Set Inbound Rules()

- Set Outbound rules()

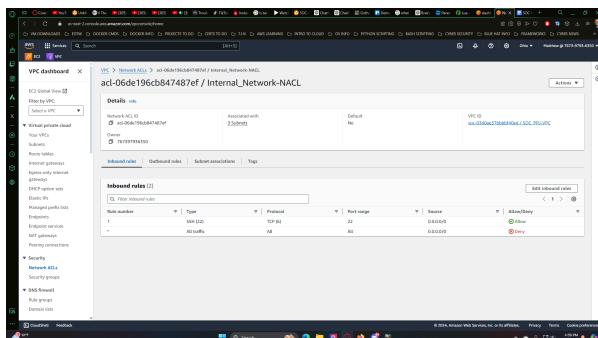


Internal Network NACL

- Click Create Network ACL on the top right
- Type in the name()
- Connect it to your VPC
- Add any tags related to the NACL
- Set the Subnet associations()



- Set Inbound Rules()



- Set Outbound rules()

DMZ (Demilitarized Zone) NACL

- Click Create Network ACL on the top right
- Type in the name()
- Connect it to your VPC
- Add any tags related to the NACL
- Set the Subnet associations()

- Set Inbound Rules()

- Set Outbound rules()

Rule number	Type	Protocol	Port range	Destination	Action
1	HTTP (80)	TCP (6) All	0.0.0.0/0	All	Allow
+	All traffic	All	0.0.0.0/0	All	Deny

Intrusion Detection/Prevention NACL

- Click Create Network ACL on the top right
- Type in the name()
- Connect it to your VPC
- Add any tags related to the NACL
- Set the Subnet associations()

Subnet	Subnet ID	Associated with	Availability Zone	Port range	IPV4 CIDR
EC2-Optimized Subnet	subnet-01234567890123456	acl-0dc0623cbd3df7b7a / IDS/IPS-NACL	us-east-1a	153.11.0.0/24	-
EC2-Optimized Subnet	subnet-01234567890123456	acl-0dc0623cbd3df7b7a / IDS/IPS-NACL	us-east-1b	153.12.0.0/24	-
EC2-Optimized Subnet	subnet-01234567890123456	acl-0dc0623cbd3df7b7a / IDS/IPS-NACL	us-east-1c	153.13.0.0/24	-

- Set Inbound Rules()

Rule number	Type	Protocol	Port range	Source	Action
1	HTTP (80)	TCP (6) All	0.0.0.0/0	All	Allow
2	HTTPS (443)	TCP (6) All	443	0.0.0.0/0	Allow
+	All traffic	All	0.0.0.0/0	All	Deny

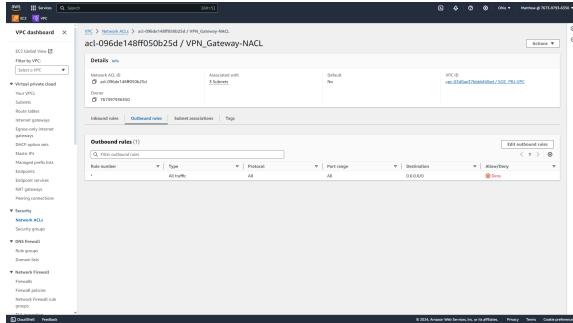
- Set Outbound rules()

VPN Gateway NACL

- Click Create Network ACL on the top right
- Type in the name()
- Connect it to your VPC
- Add any tags related to the NACL
- Set the Subnet associations()

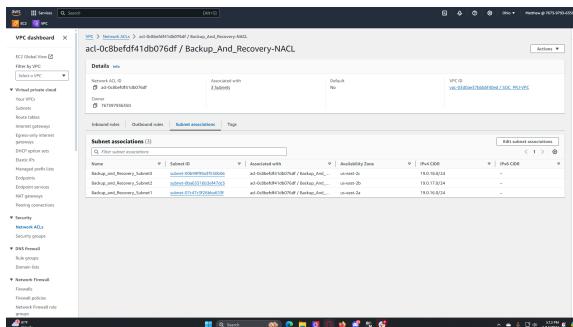
- Set inbound Rules()

- Set Outbound rules()

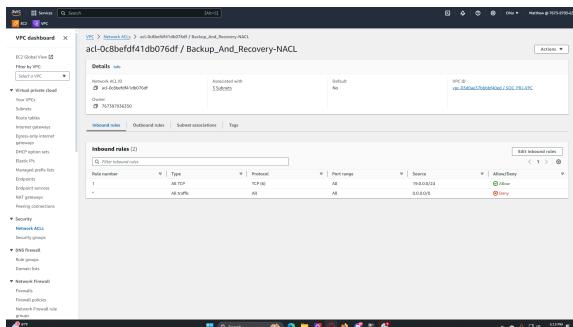


Backup and Recovery NACL

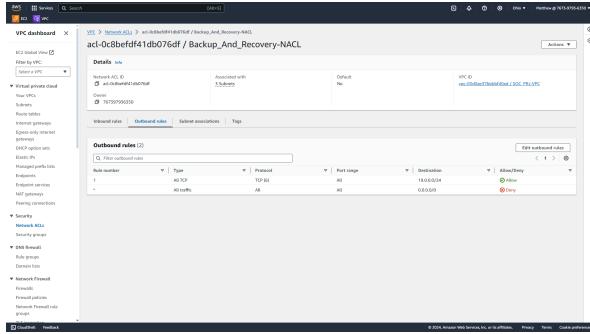
- Click Create Network ACL on the top right
- Type in the name()
- Connect it to your VPC
- Add any tags related to the NACL
- Set the Subnet associations()



- Set Inbound Rules()

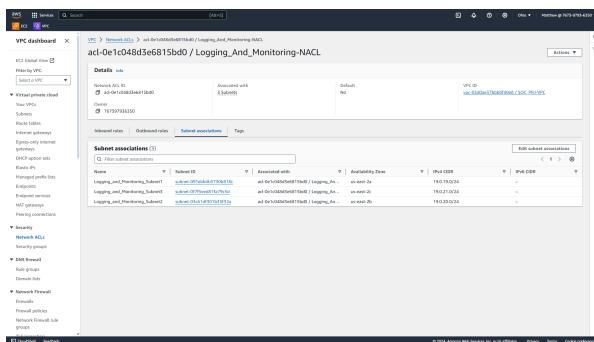


- Set Outbound rules()

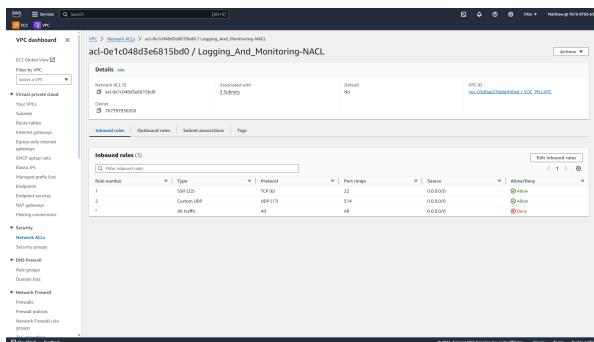


Logging and Monitoring NACL

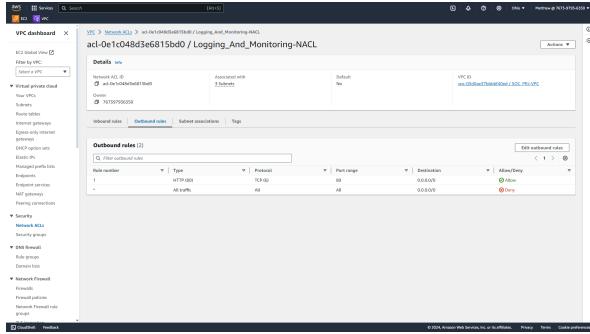
- Click Create Network ACL on the top right
- Type in the name()
- Connect it to your VPC
- Add any tags related to the NACL
- Set the Subnet associations()



- Set inbound Rules()

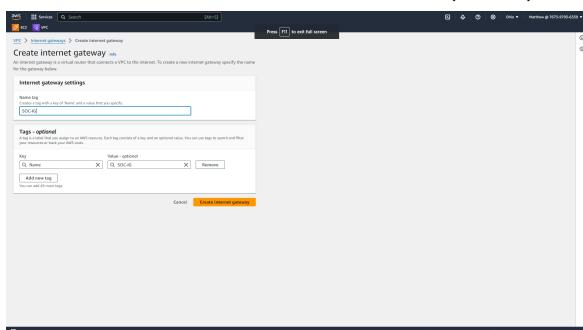


- Set Outbound rules()



Internet Gateway

- Go to the Internet gateway in the subsection of the VPC (click it)
- Go to the top right and click Create Internet Gateway
- Give it a name()
- Click Create Internet Gateway
- Attach Internet Gateway to your VPC



Route Table

Look to the left where the subsections of the VPC are and Click on Route Tables

Management Route Table

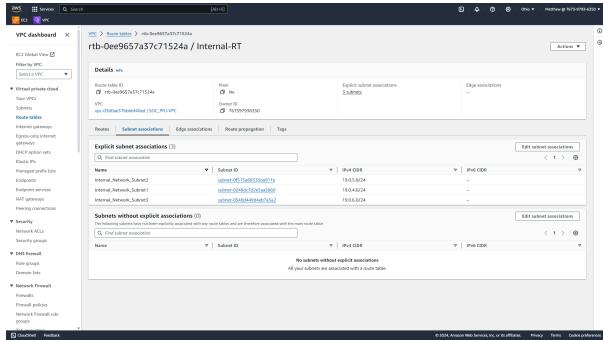
- Click create route table on the top right
- Put the route table name()
- And select the VPC
- Click Create route table
- Edit the Routes()

- Associate the appropriate subnet associations()

Internal Route Table

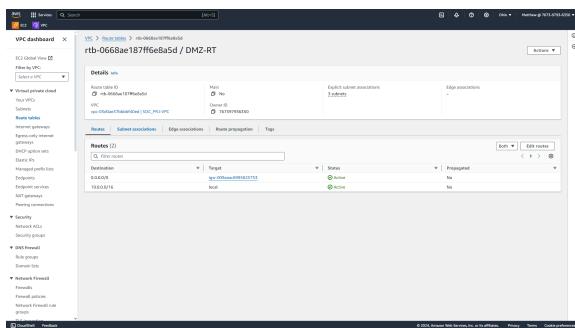
- Click create route table on the top right
- Put the route table name()
- And select the VPC
- Click Create route table
- Edit the Routes()

- Associate the appropriate subnet associations()

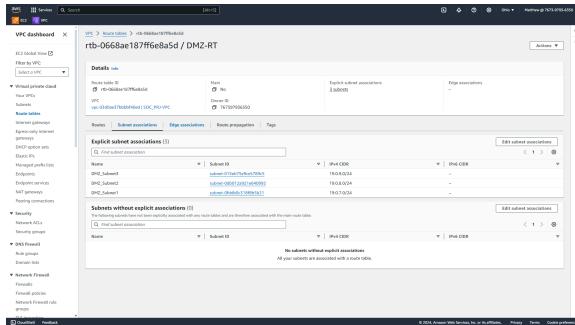


DMZ Route Table

- Click create route table on the top right
- Put the route table name()
- And select the VPC
- Click Create route table
- Edit the Routes()

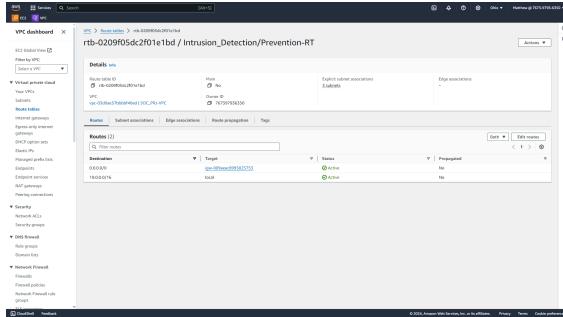


- Associate the appropriate subnet associations()

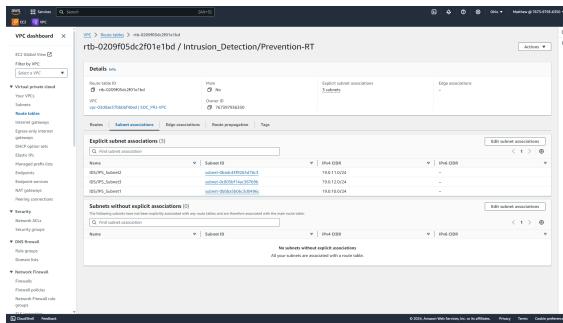


Intrusion Detection/Prevention Route Table

- Click create route table on the top right
- Put the route table name()
- And select the VPC
- Click Create route table
- Edit the Routes()

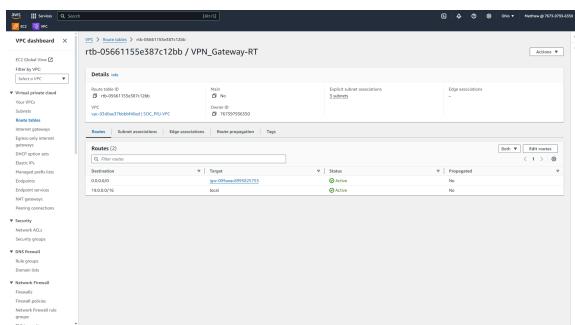


- Associate the appropriate subnet associations()

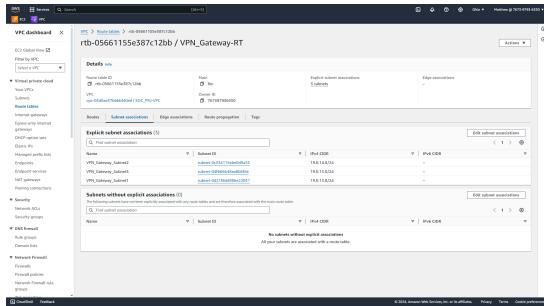


VPN Gateway Route Table

- Click create route table on the top right
- Put the route table name()
- And select the VPC
- Click Create route table
- Edit the Routes()

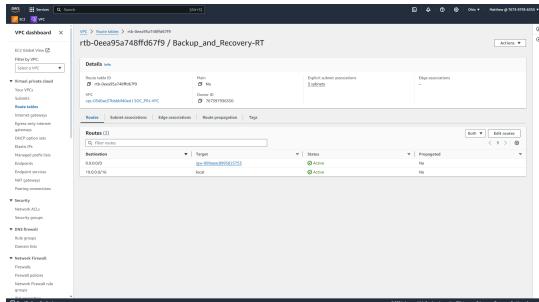


- Associate the appropriate subnet associations()

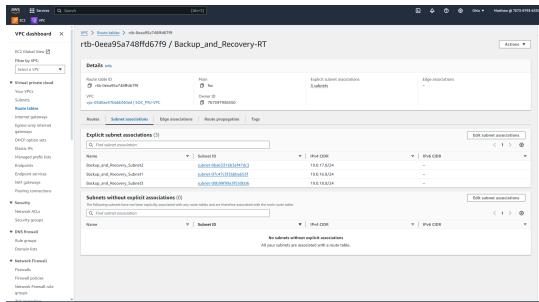


Backup and Recovery Route Table

- Click create route table on the top right
- Put the route table name()
- And select the VPC
- Click Create route table
- Edit the Routes()

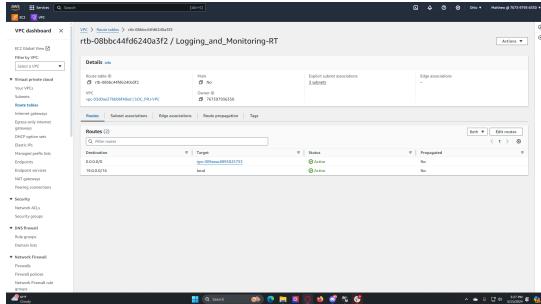


- Associate the appropriate subnet associations()



Logging and Monitoring Route Table

- Click create route table on the top right
- Put the route table name()
- And select the VPC
- Click Create route table
- Edit the Routes()



- Associate the appropriate subnet associations()

