# Postwork

# 1. Objetivo 🎯

* Conocer y configurar un entorno de red con subred pública y privada como piedra angular en el establecimiento de una infraestructura.

# 2. Requisitos 📋

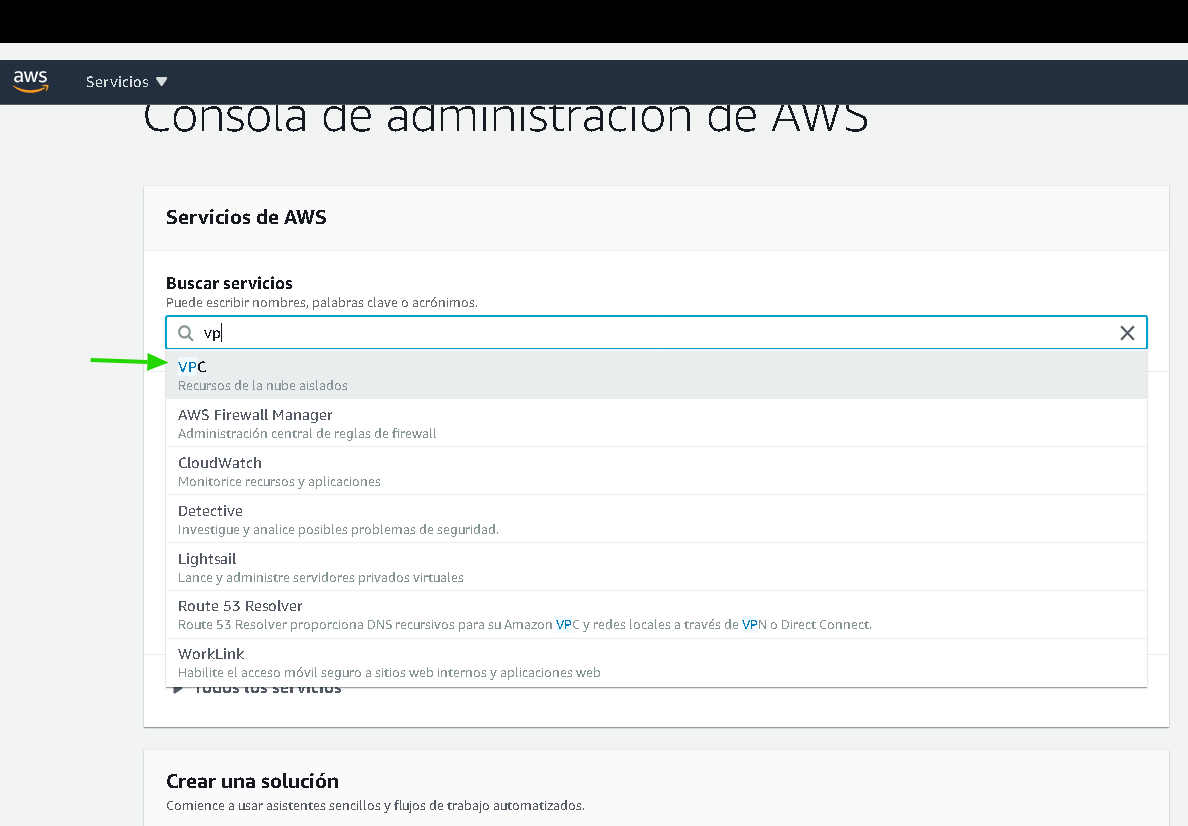
* Acceso a AWS Console.
* Diagrama del proyecto a la mano.
* Calculadora CIDR

# 3. Desarrollo 📑

Antes de generar un esquema de red y subredes es necesaria la generación de un diagrama con los elementos principales a fin de conocer los requerimientos de red de estos. En el diagrama del proyecto se identifican como elementos dependientes de una VPC o red a la base de datos RDS, las instancias EC2 y balanceadores de carga.

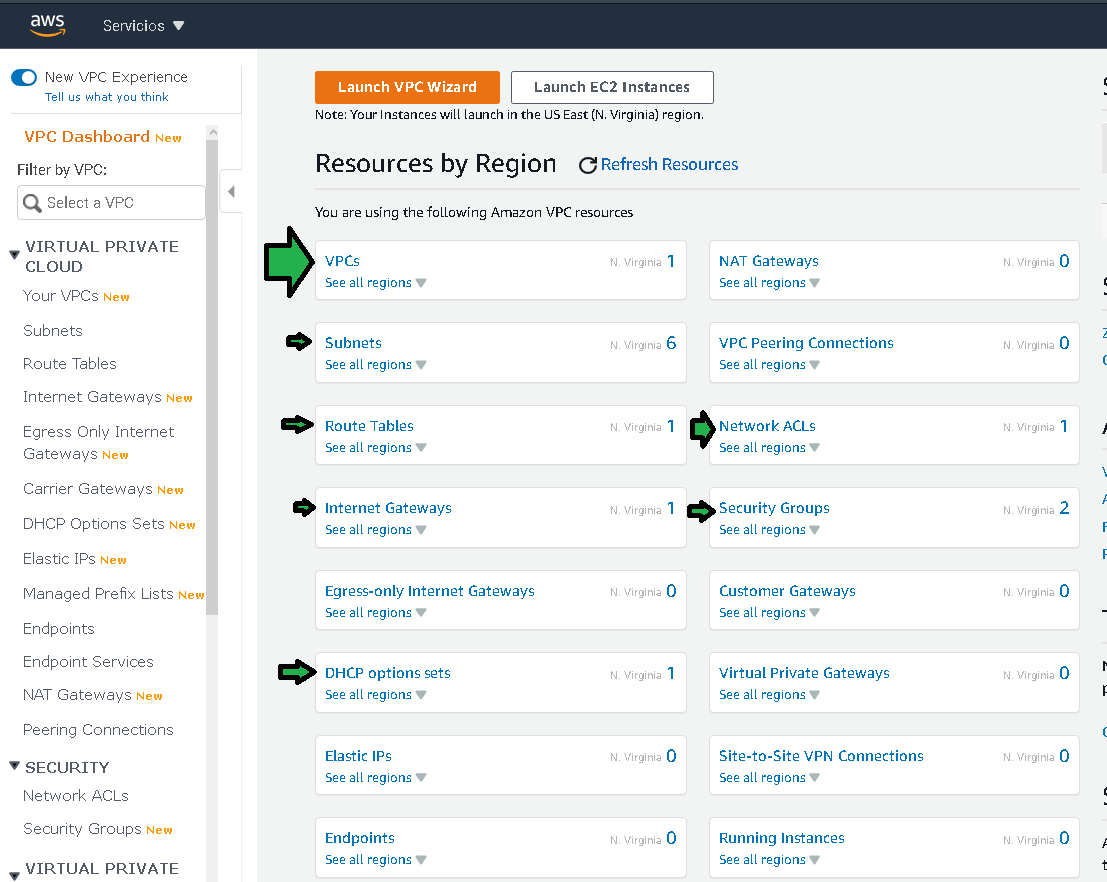
Para generar un esquema DMZ donde la capa de persistencia de datos (bases de datos) sean inaccesibles desde el mundo exterior se requerirá generar una res pública y privada. La red pública puede ser alcanzada por cualquier dispositivo desde internet, la red privada no puede ser alcanzada desde internet directamente.

1. Acceder a la sección VPC desde la consola de administración de AWS.

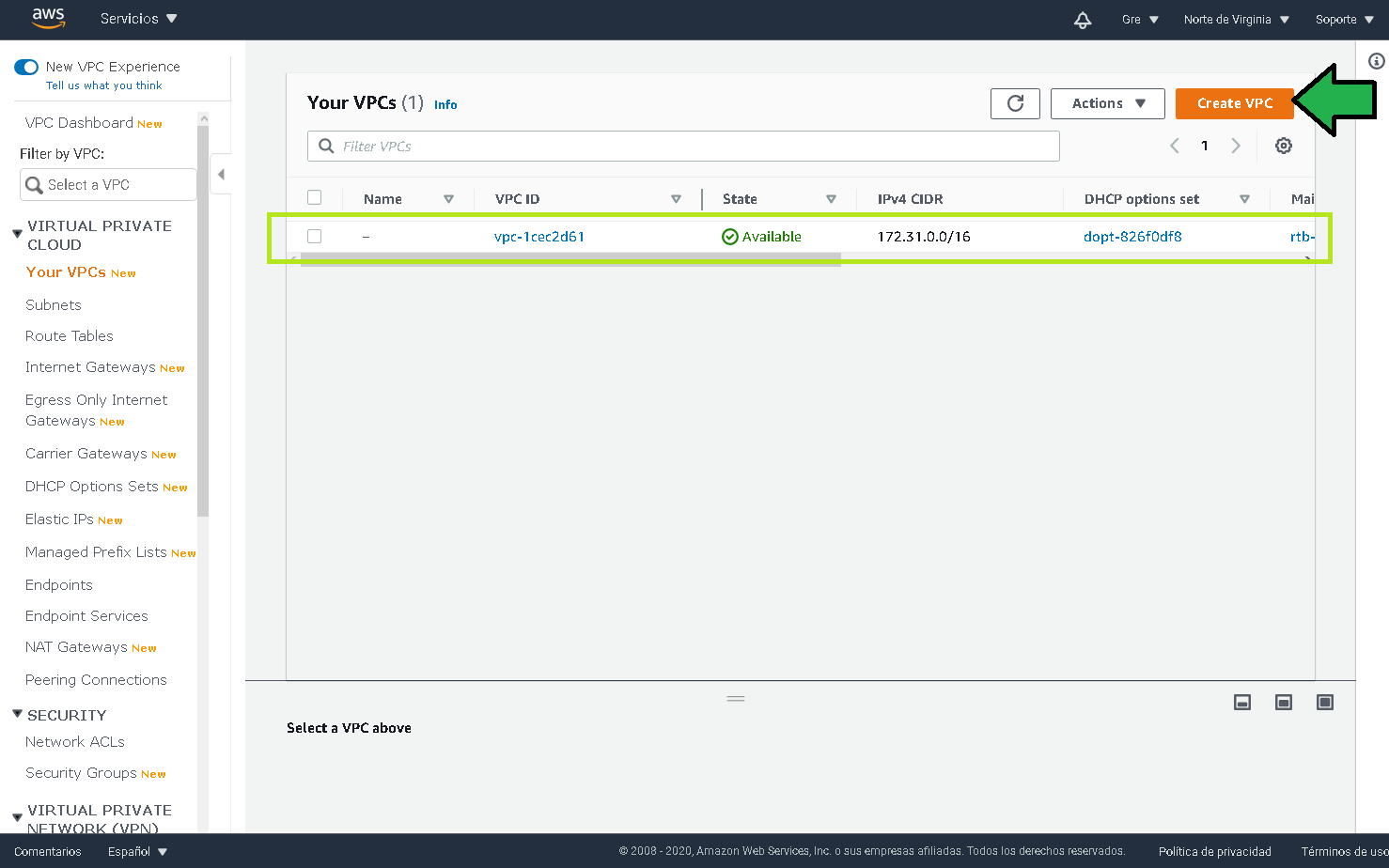
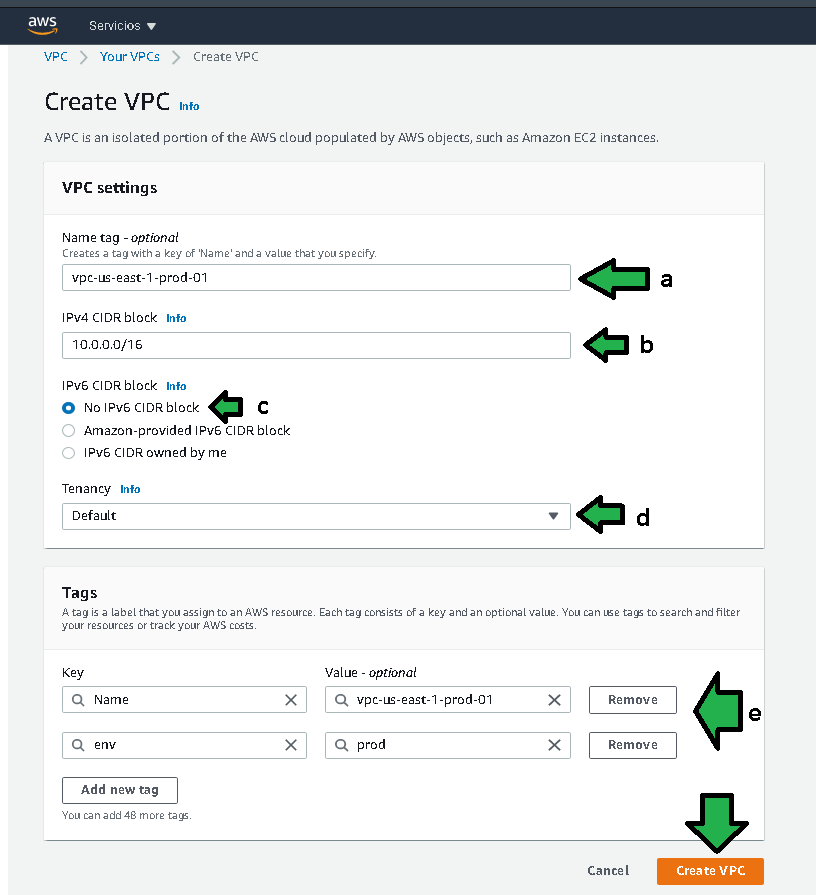


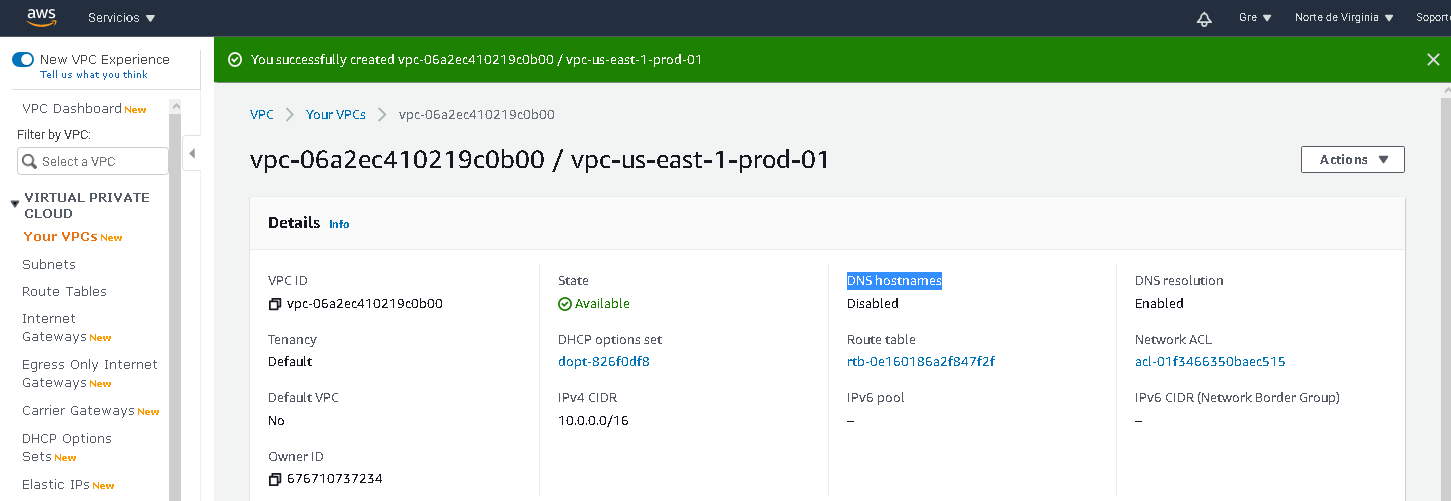
pw1-access-vpn.png

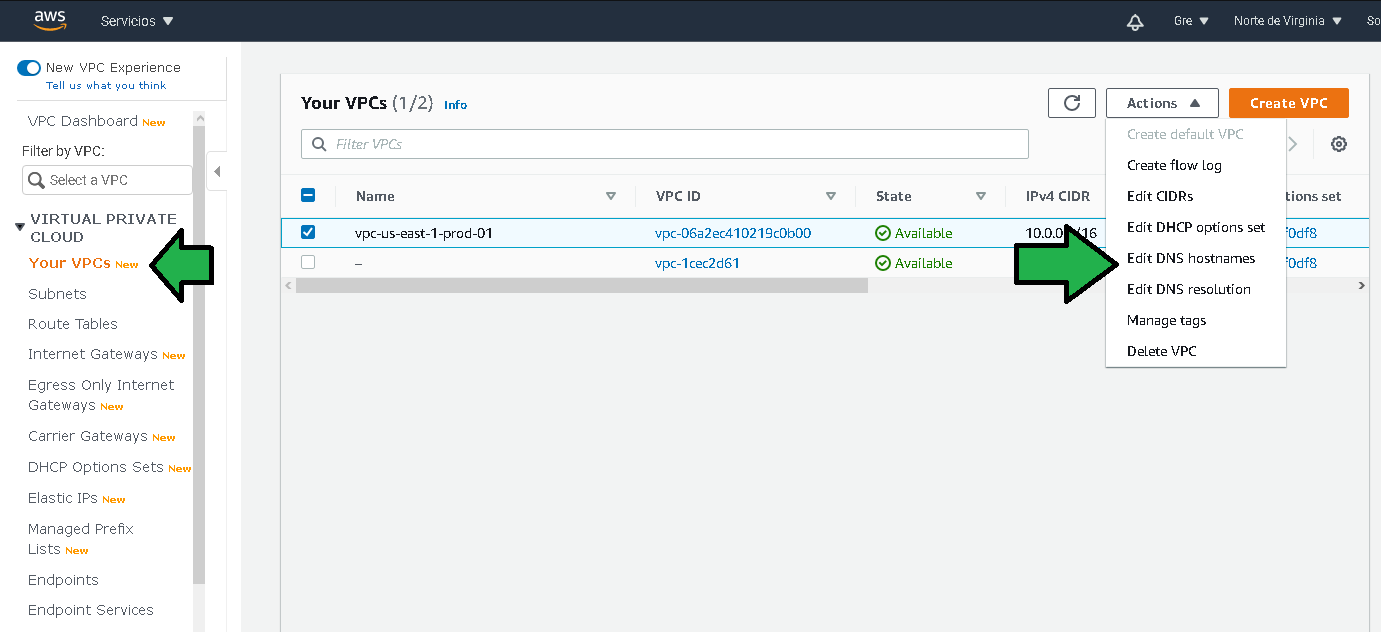
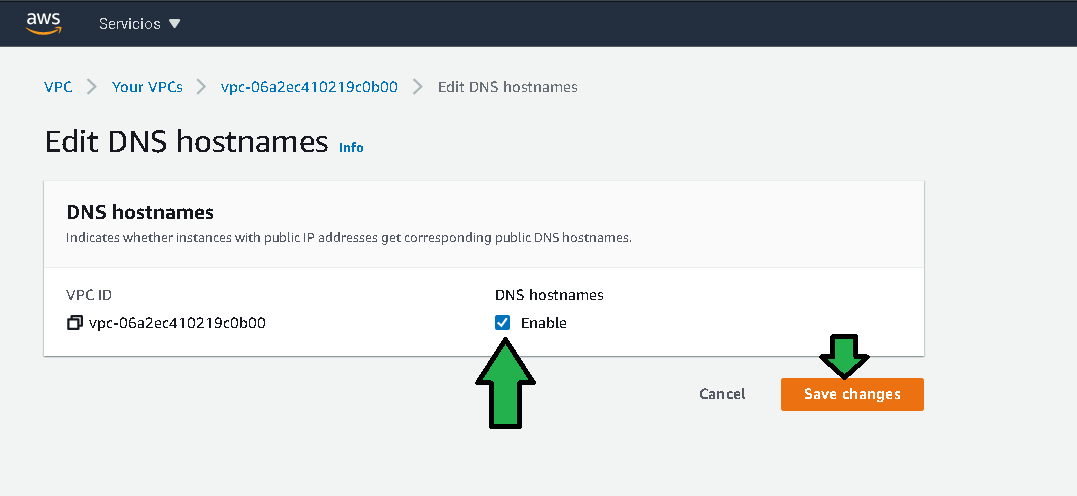
1. Se observan ya algunos dispositivos a pesar de no haber configurado nada previamente, esto sucede ya que todas las regiones tienen una VPC por defecto, para que esta VPC funcione se hay dispositivos adicionales que deben ser configurados como Security Groups, DHCP, Routing Table, Internet Gateway y Network ACL. Dar click en “VPCs”

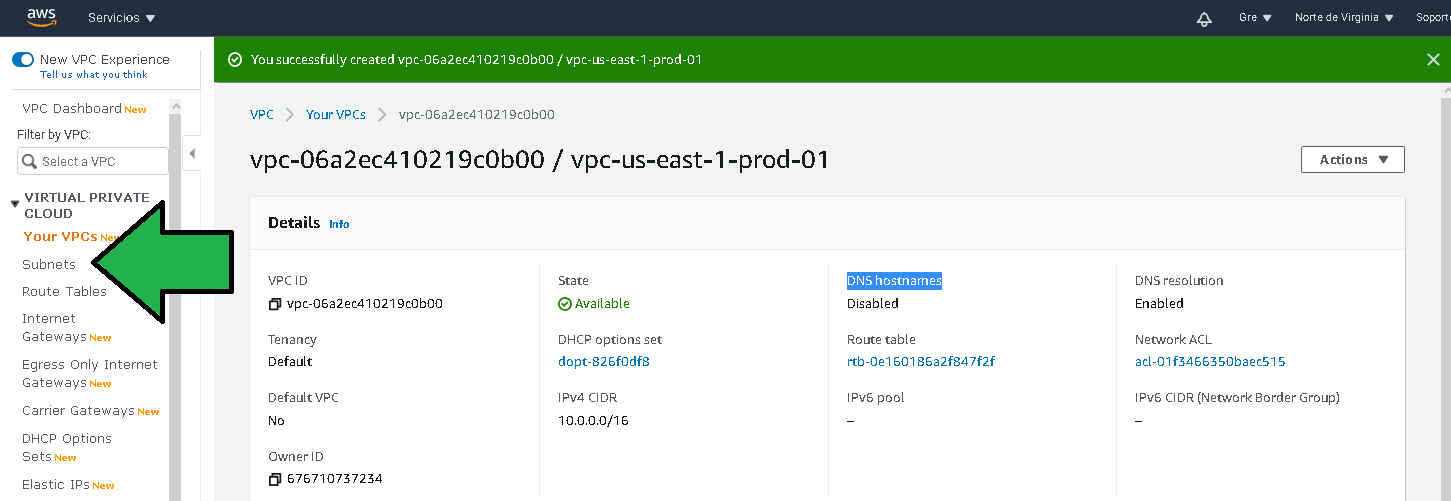


pw1-dispositivos-default.png

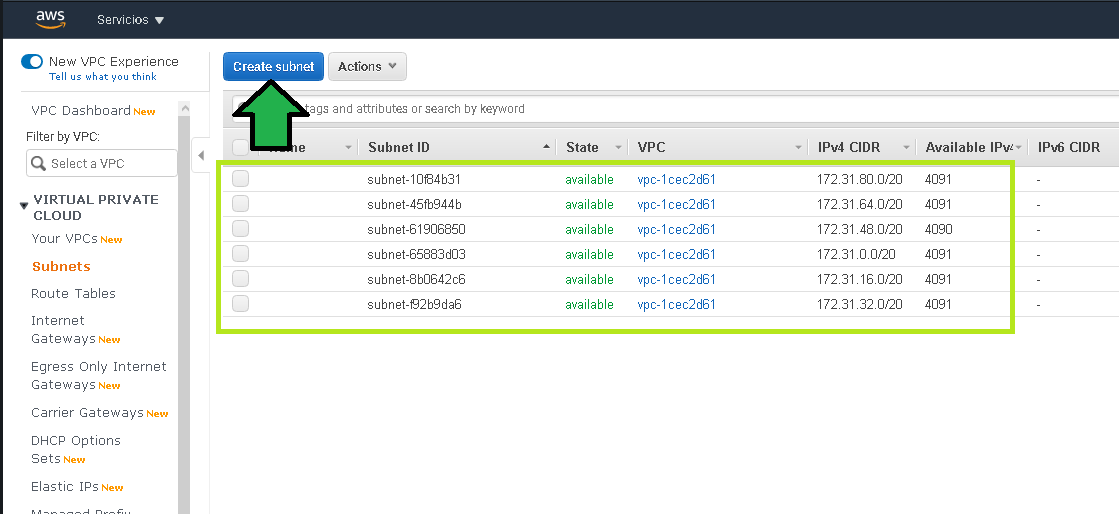
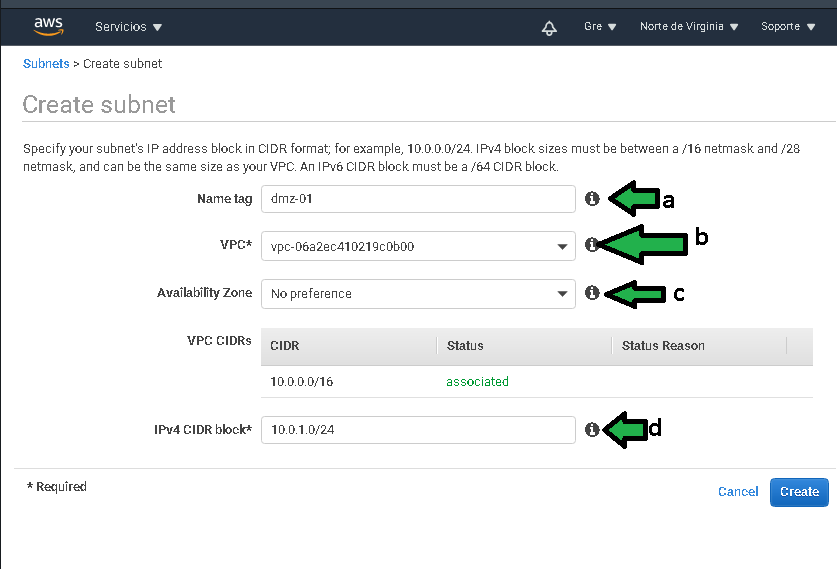
1. Se accederá al panel de redes VPC, se observará una red VPC por defecto, dar clic en “Create VPC” 
2. Se establecen:
3. Nombre de la VPC, se recomienda un nombre descriptivo, en este caso se hace referencia a la región a la que pertenece y el entorno en este producción, una forma de segmentar entornos de desarrollo y stagging es por medio de redes VPC.
4. Se debe asignar el bloque de direcciones IP que tendrá la red completa, para el ejemplo, esta red con máscara 16 dará para configurar aproximadamente 256 redes con 256 direcciones IP disponibles en cada red. (Es aproximado por que AWS tomas algunas IP para su gestión interna, se recomienda en este punto interactuar con la calculadora IP)
5. No se usará IPv6
6. Se selecciona la opción default para decir a AWS que no se desea hardware de red dedicado.
7. Asignar alguna Tag con fines administrativos y de identificación. 

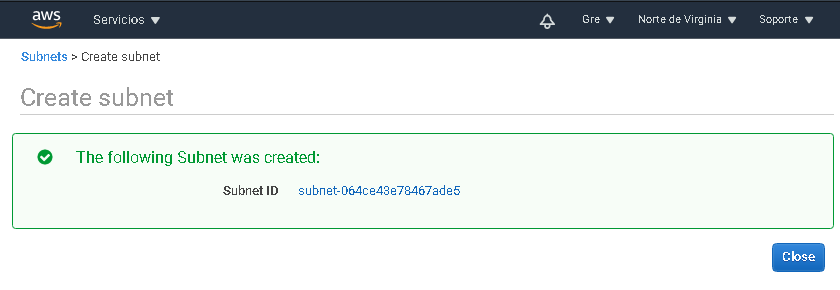
Después de algunos segundos la VPC ha sido creada. 

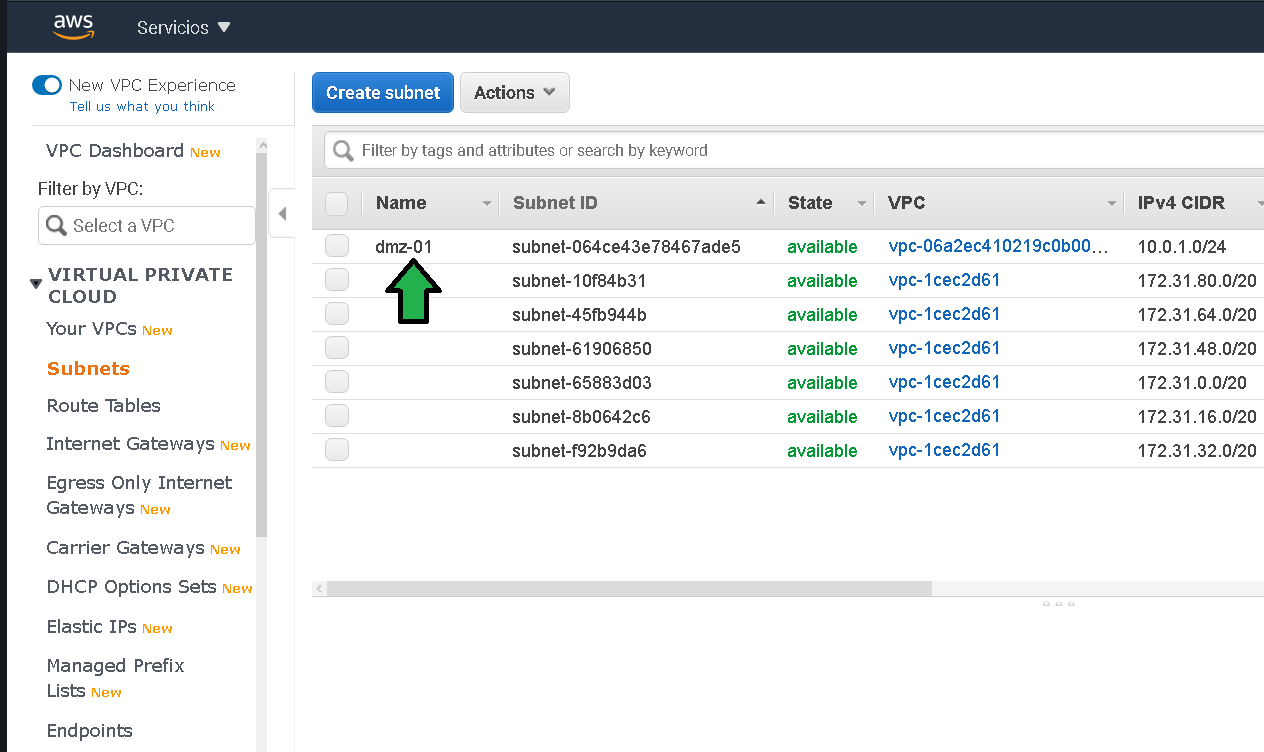
1. Habrá que habilitar la asociación entre nombres de dominio públicos y privados en correspondencia a IPv4 pública e IPv4 privada. Click en “Edit DNS hostnames” 
2. Habilitar finalmente la asociación DNS. 
3. Para la generación de la res pública se deberá seleccionar “Subnets”



pw1-choose-subnets.png

1. Se observan varias subredes, observando el espacio de direcciones IP de cada una y la VPC a la que pertenecen se deduce que son redes de la VPC por defecto. Se deberá dar click en “Create Subnet” 
2. Se establecen los siguientes valores para la configuración de la primera red pública:
3. El nombre que la red tendrá.
4. La VPC a la que pertenecerá esta subred, seleccionar la VPC recién generada.
5. Se permite que AWS seleccione la zona de disponibilidad.
6. Se establece el tamaño de una subred, para este caso se establece un bloque con máscara 24 lo que quiere decir que este bloque tendrá 256 direcciones IP disponibles (marca menos porque AWS toma algunas para gestión interna). Cabe mencionar que este es solo un bloque de direcciones de los 256 que se pueden hacer por la mascara 16 seleccionada para la VPC. 

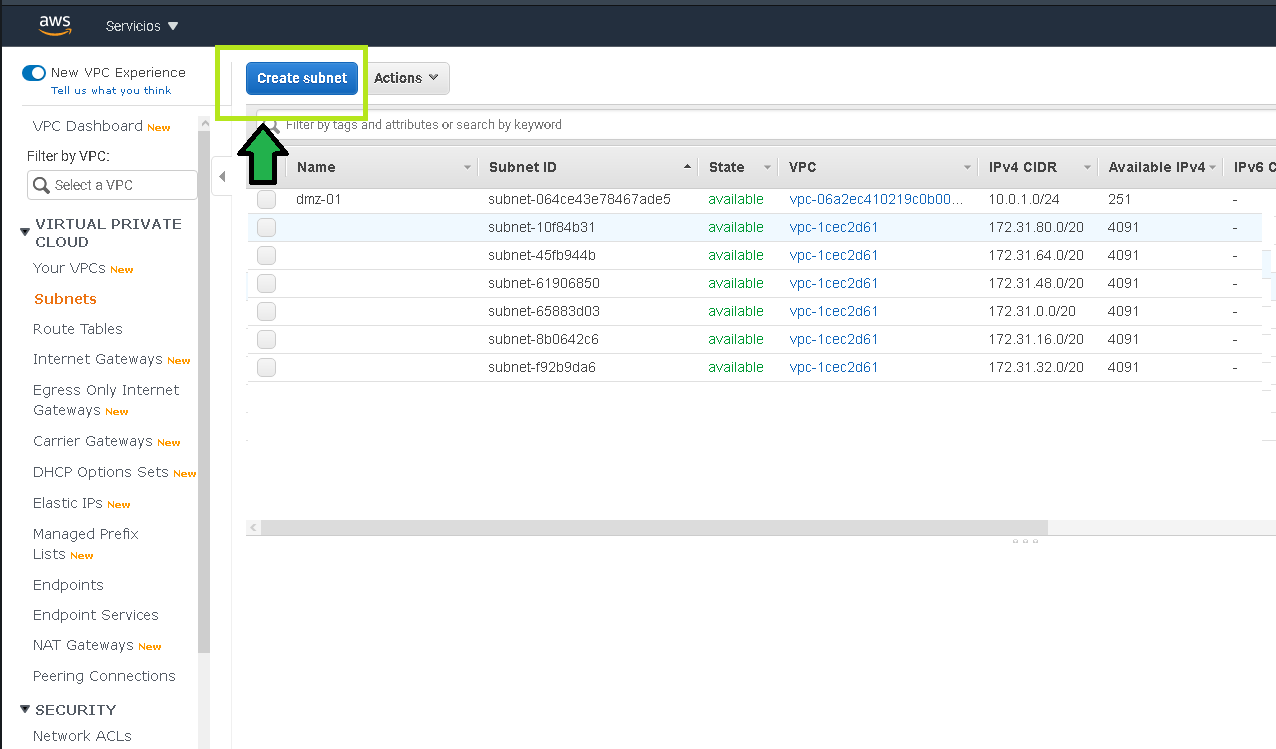
Después de algunos segundos la red es creada. 



pw1-public-subnet-done.png

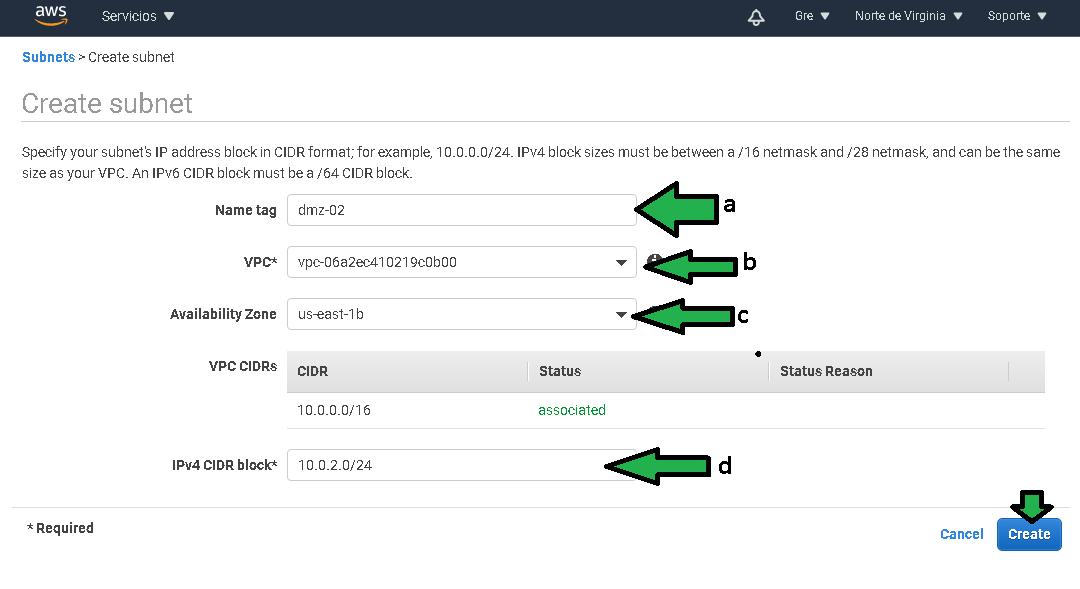
Se requiere generar una segunda red pública para dar servicio por medio del balanceador de cargas.

Dar click en “Create Subnet”



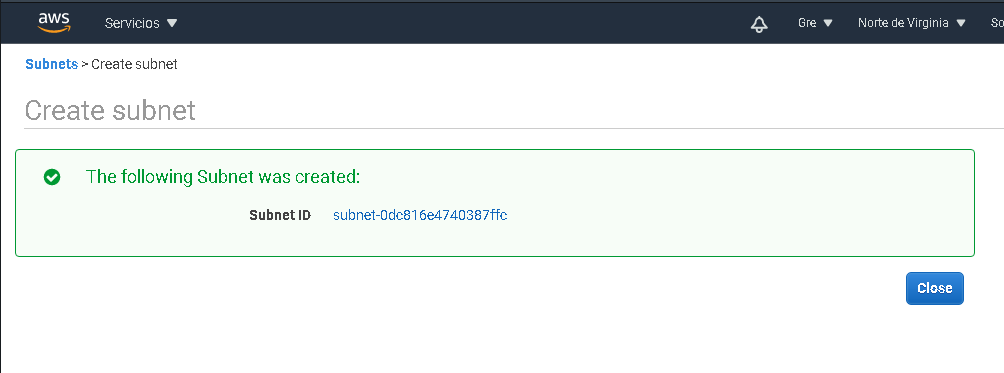
pw1-add-second-public-subnet.png

Luego establecer las configuraciones como: a) Establecer un nombre de la subred descriptivo. b) Especificar la red VPC a la que pertenecerá la subred. c) Escoger la zona de disponibilidad distinta a la zona de disponibilidad de la red creada anterior en este ejercicio. d) Establecer el espacio de direcciones IP disponibles para los servicios que se conecten a esta subred.



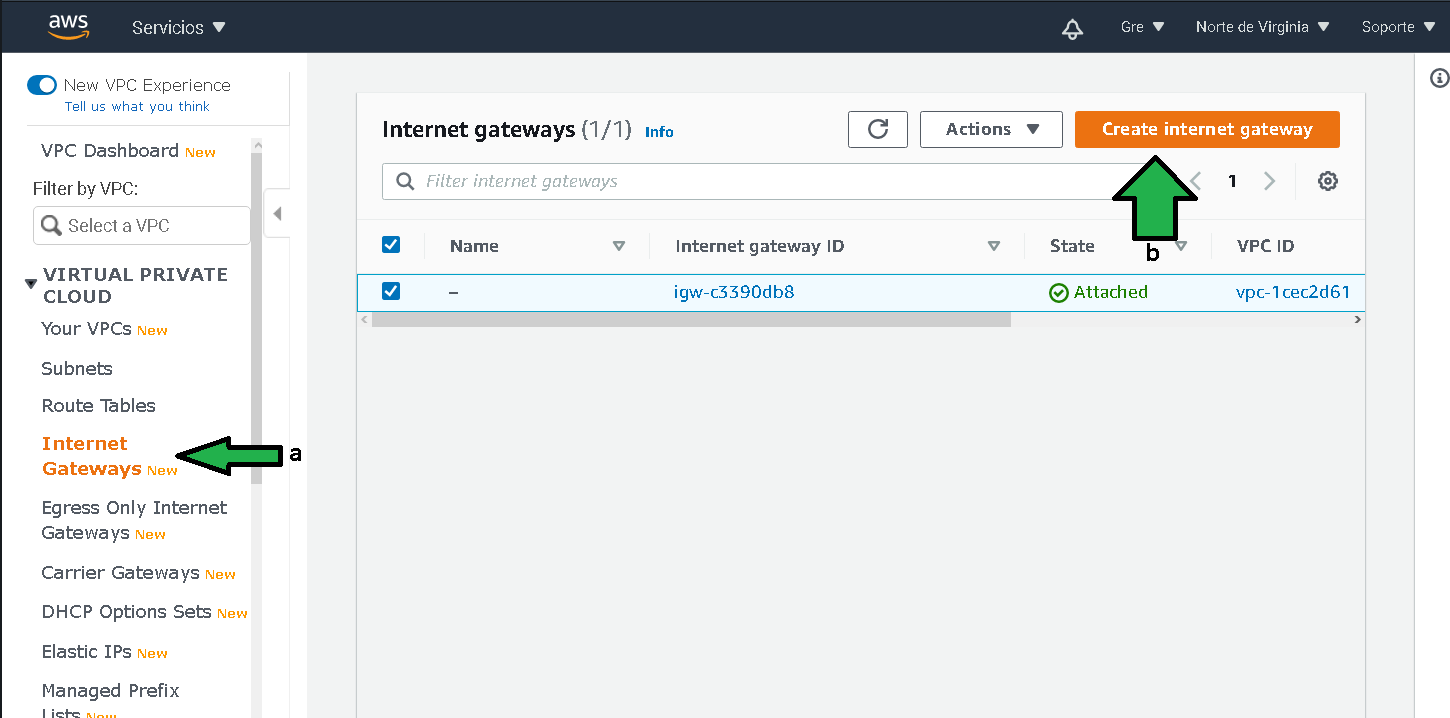
pw1-add-subnet-public-configure.png

Después de algunos segundos la subred es creada.

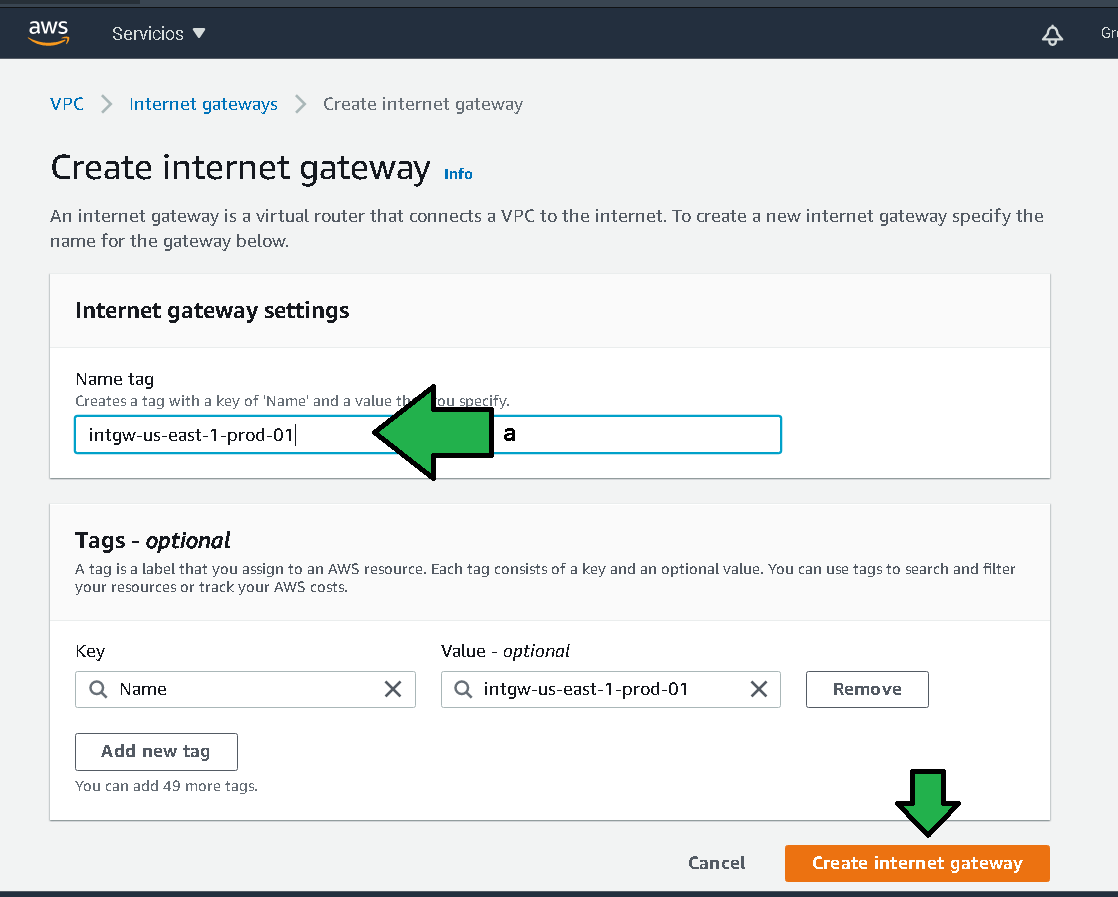


pw1-subred-publica-02-done.png

1. Para dar acceso a la red pública desde internet y hacia internet hay que crear un Internet Gateway.

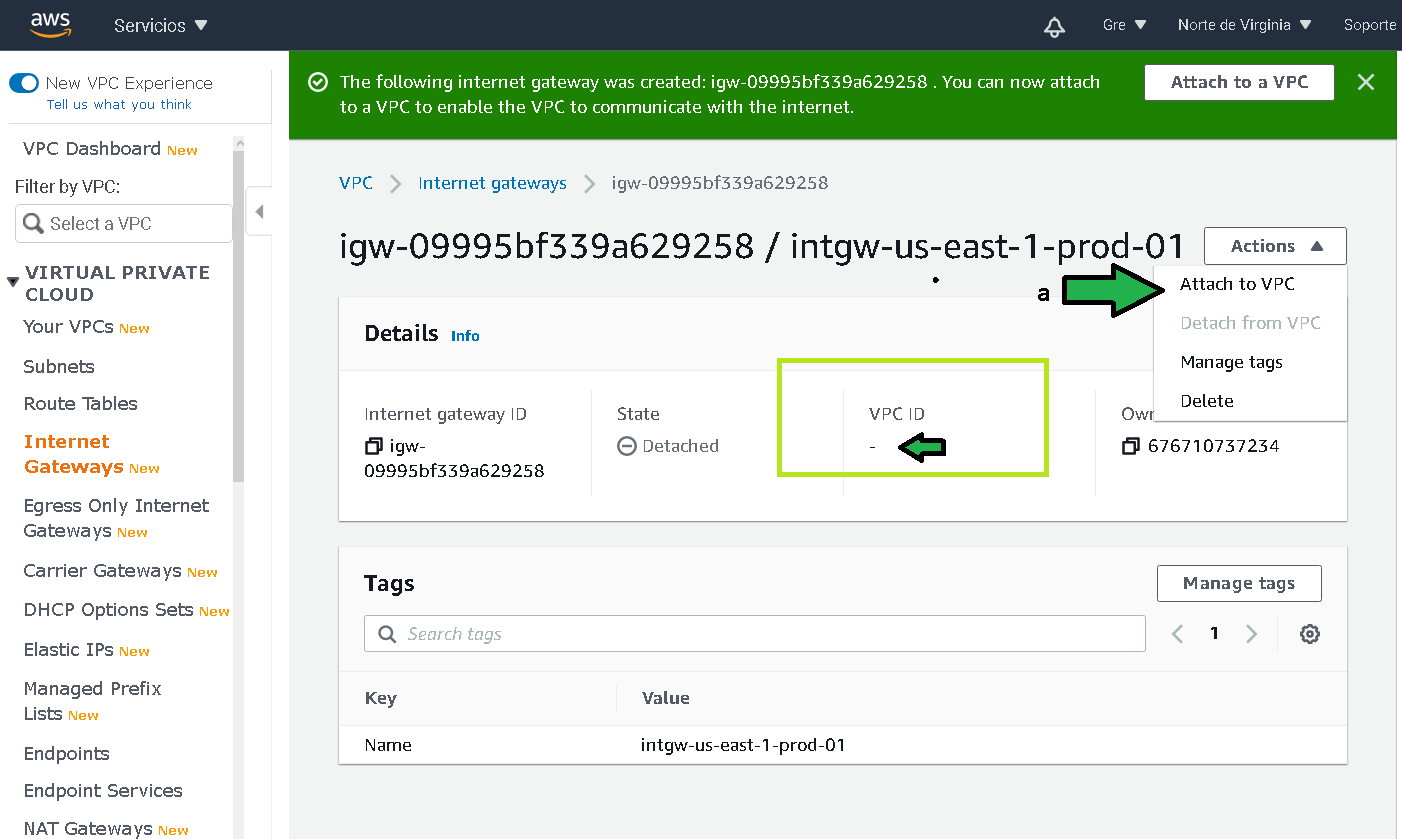
Habrá que dirigirse al menú izquierdo a la parte de “Internet Gateway” (a), después hacer click en “Create internet gateway”. 

1. Establecer un nombre al internet gateway, click en “Create internet gateway” para generarlo.

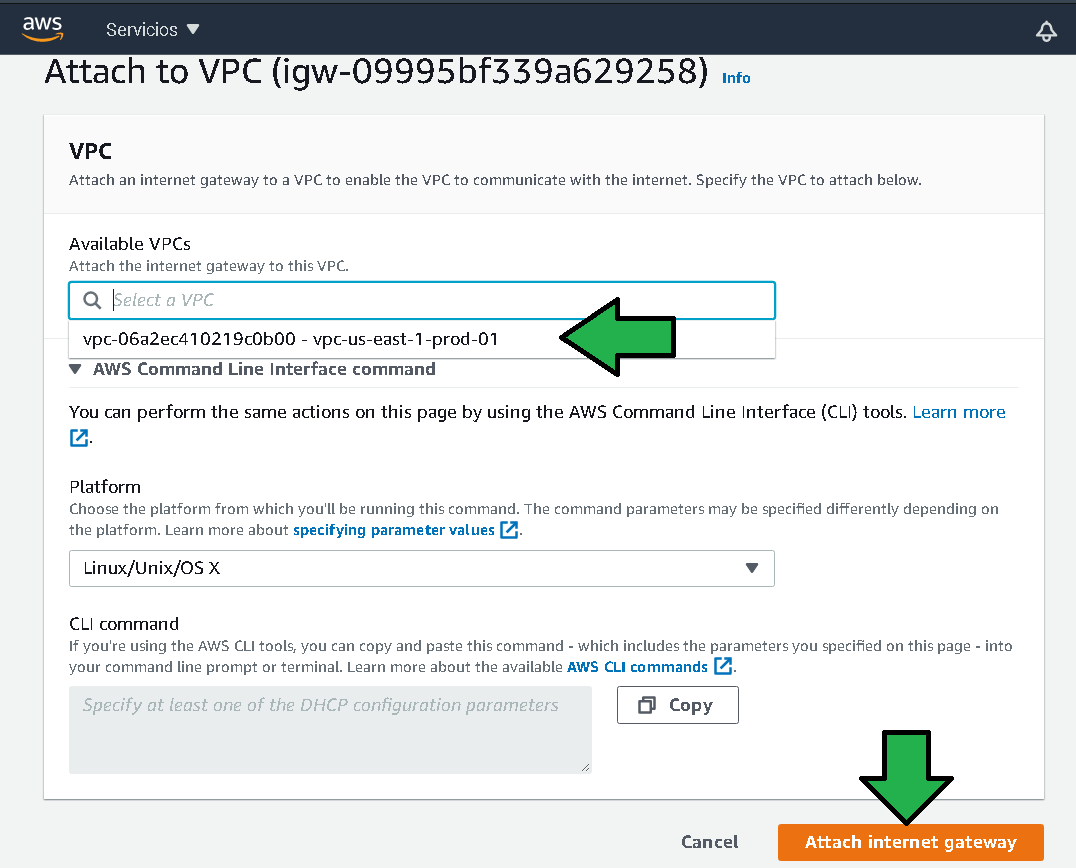


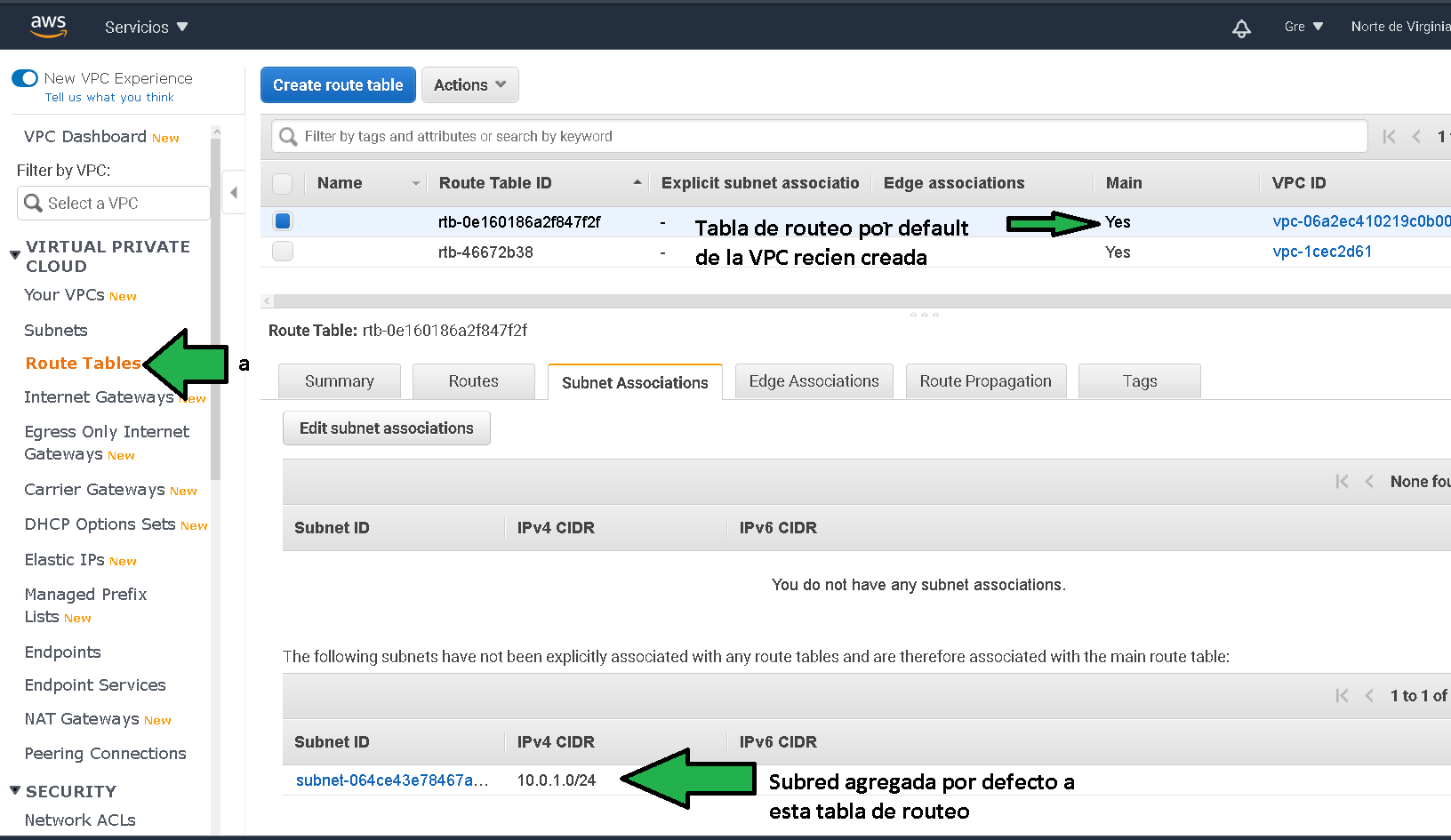
pw1-create-ig-name.png

1. Una vez creado el Internet Gateway (a.k.a IG) se puede observar que no se encuentra asociado a ninguna red VPC, para asociarlo habrá que hacer click en “Attach in VPC” (a)

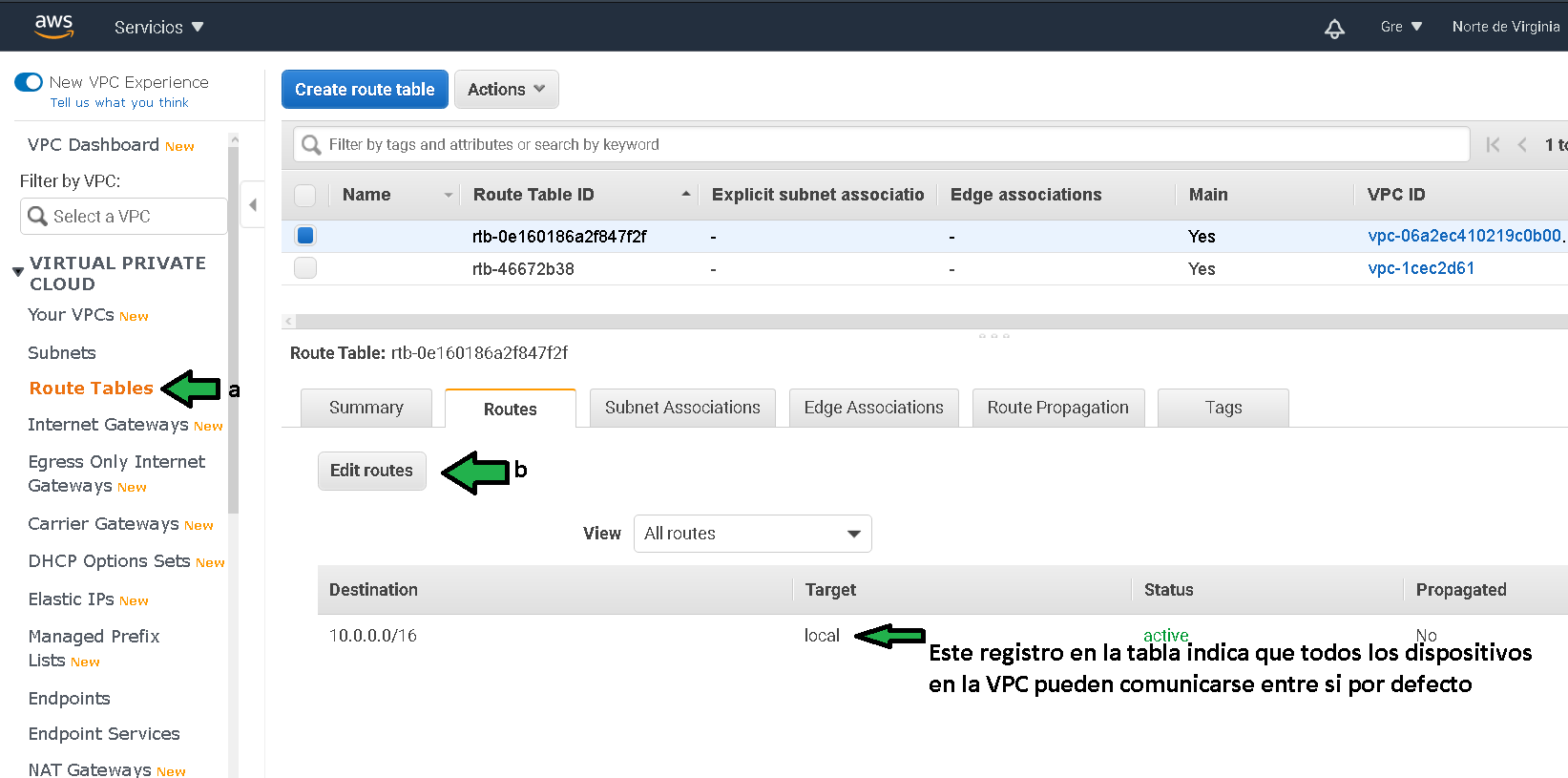
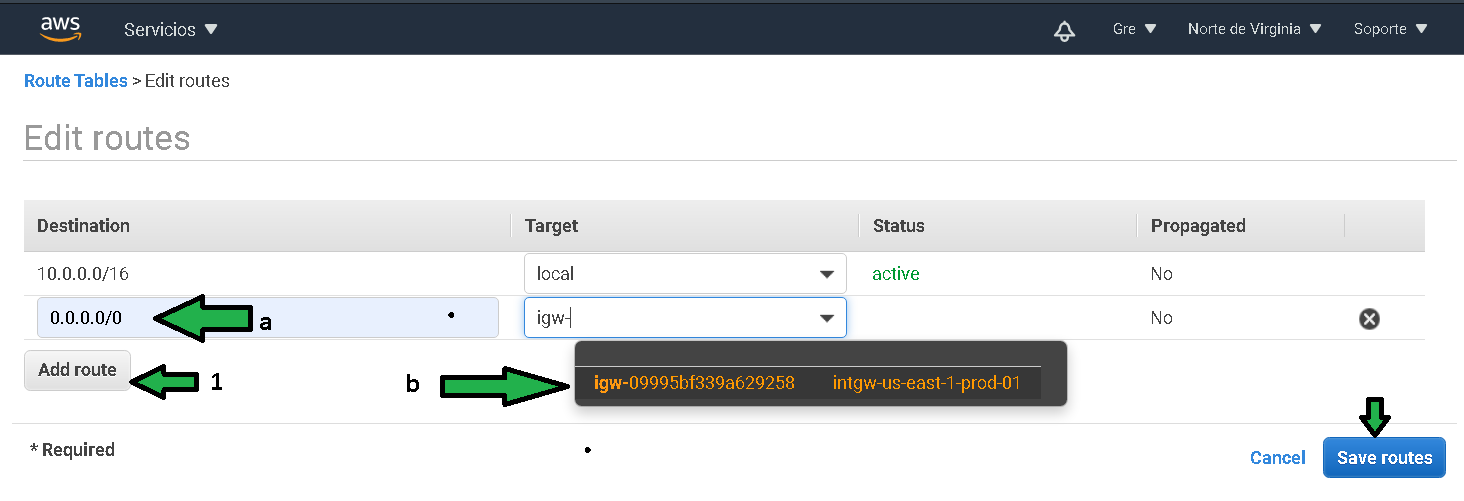


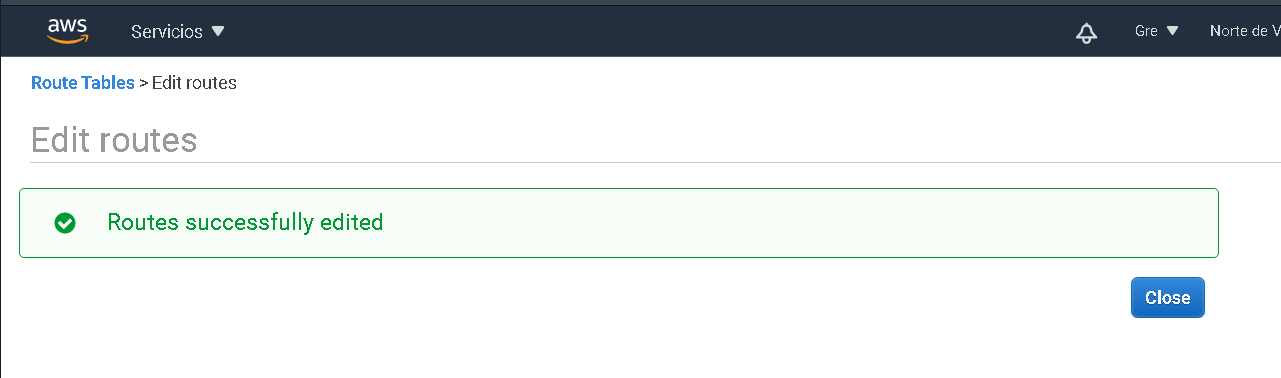
pw1-attach-ig-to-vpc.png

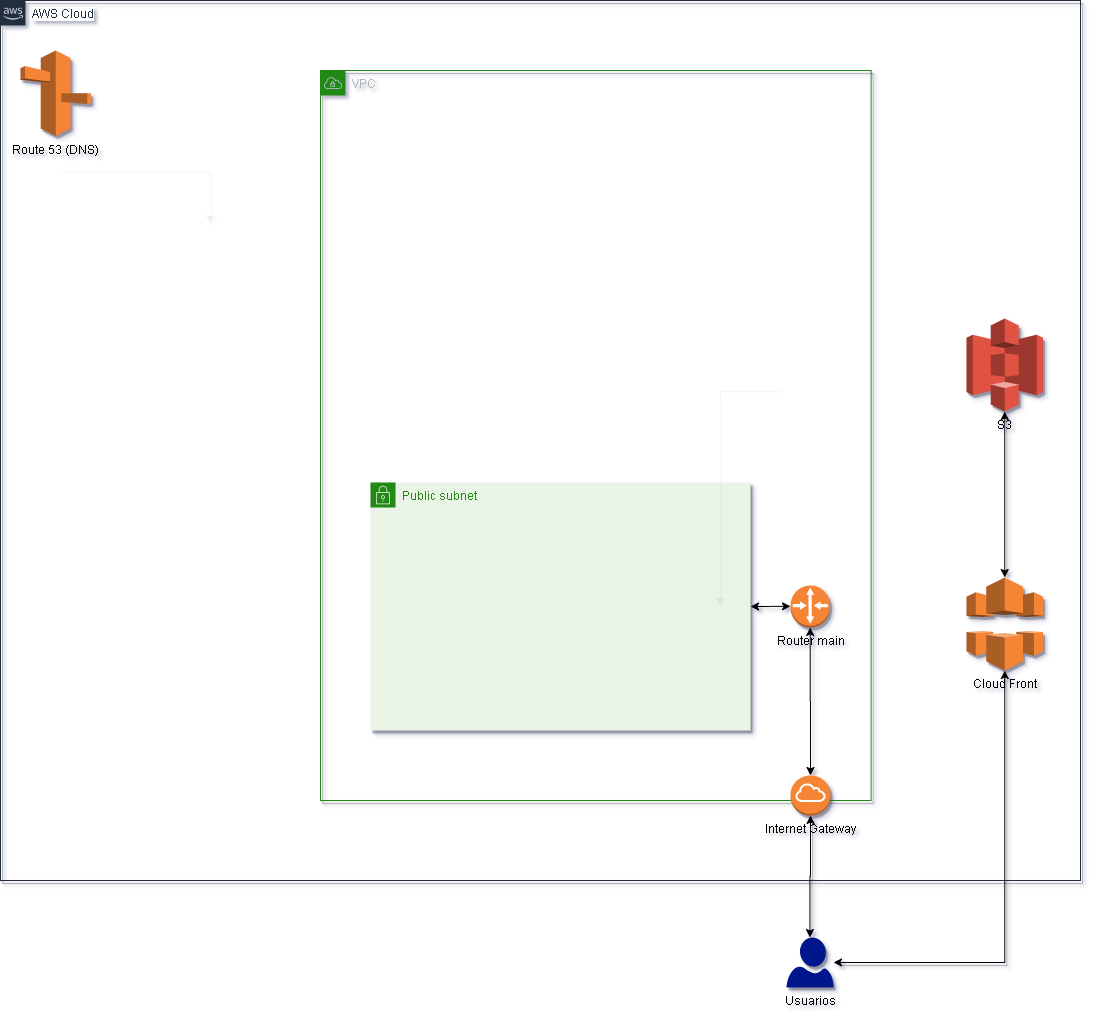
1. Seleccionar la VPC acabada de crear y dar click en “Attach internet gateway” 
2. En este punto se ha configurado la subred que debe tener acceso desde y hacia internet por medio de un Internet Gateway. Es momento de redirigir el tráfico que no es local hacia el Internet Gateway para dar salida a internet. Por defecto todos los dispositivos agregados a una subred se pueden comunicar entre ellos pero en caso de requerir acceso al repositorio de Ubuntu de actualizaciones para actualizar el sistema operativo en http://archive.ubuntu.com/ubuntu el tráfico simplemente no alcanzará la URL por que no se ha especificado el mecanismo para redirigir el tráfico. Al generar la VPC se genera una tabla de routeo por defecto, y cada vez que se genera una subred la subred es asociada a esta tabla de routeo por defecto. La tabla de routeo por defecto tiene lo necesario para comunicar los los dispositivos en la misma red. Al ingresar a las Tablas de Routeo en el menú (a) se pueden ver los detalles.



pw-route1-review-default-routing.png

1. Para redireccionar el tráfico habrá que ir al menú “Route Tables” (a), de ahí dar click en “Edit routes” (b) 
2. Agregar una nueva ruta en “Add route” (1), generando el nuevo registro con destino 0.0.0.0/0 (a) apuntando el tráfico hacia el Internet Gateway (b). Hay que notar como nombrar los elementos con una nomenclatura lo suficientemente explícita ayuda a la hora de configurar. Dar click en “Save routes” 

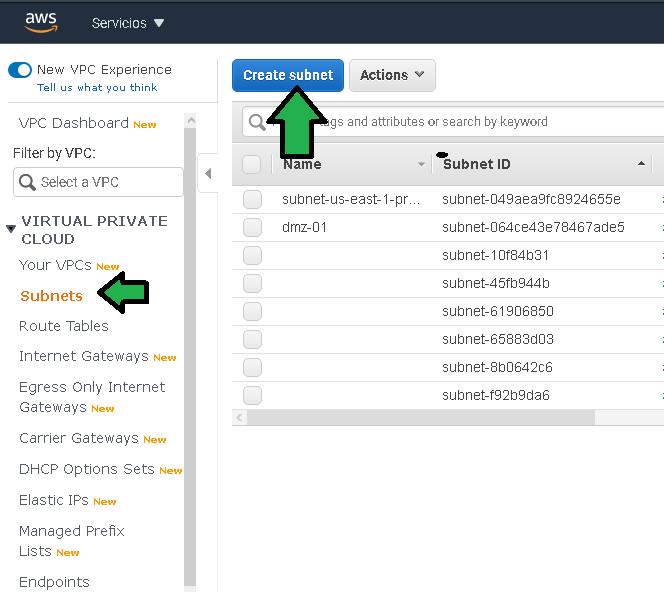
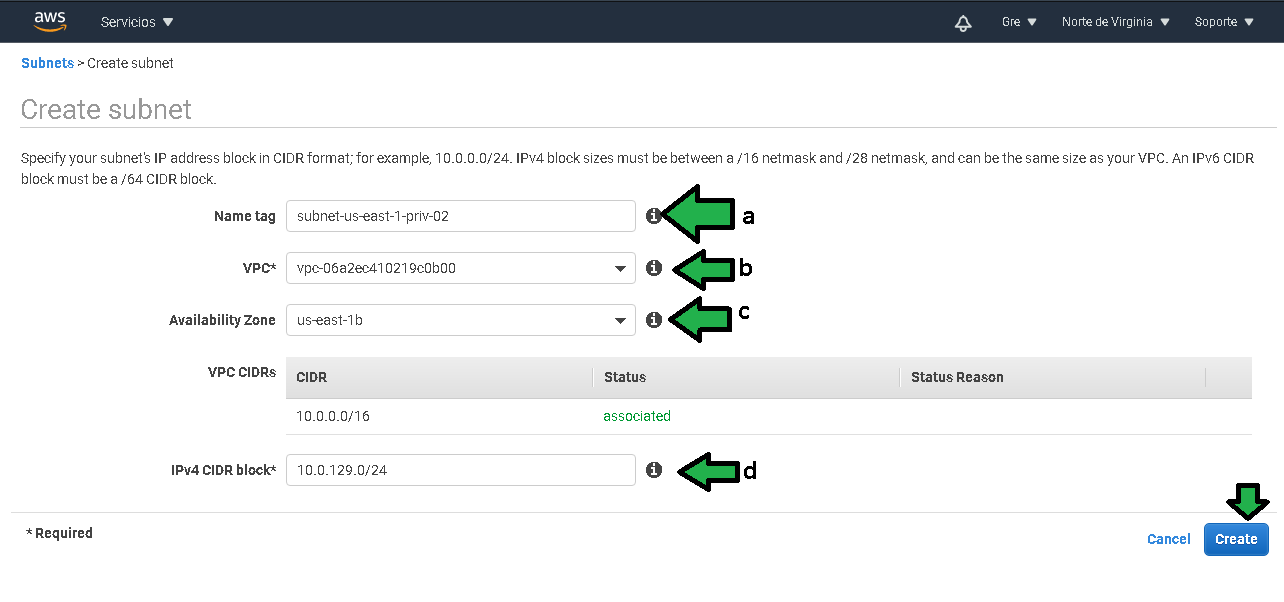
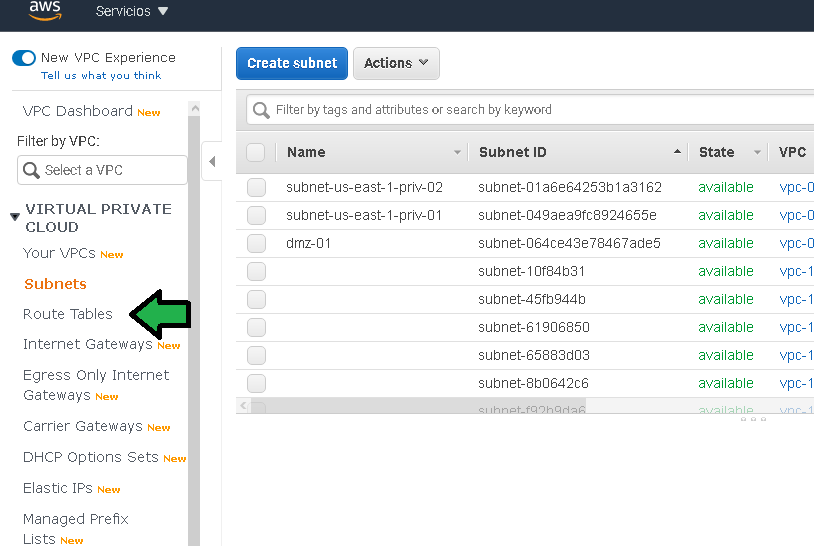
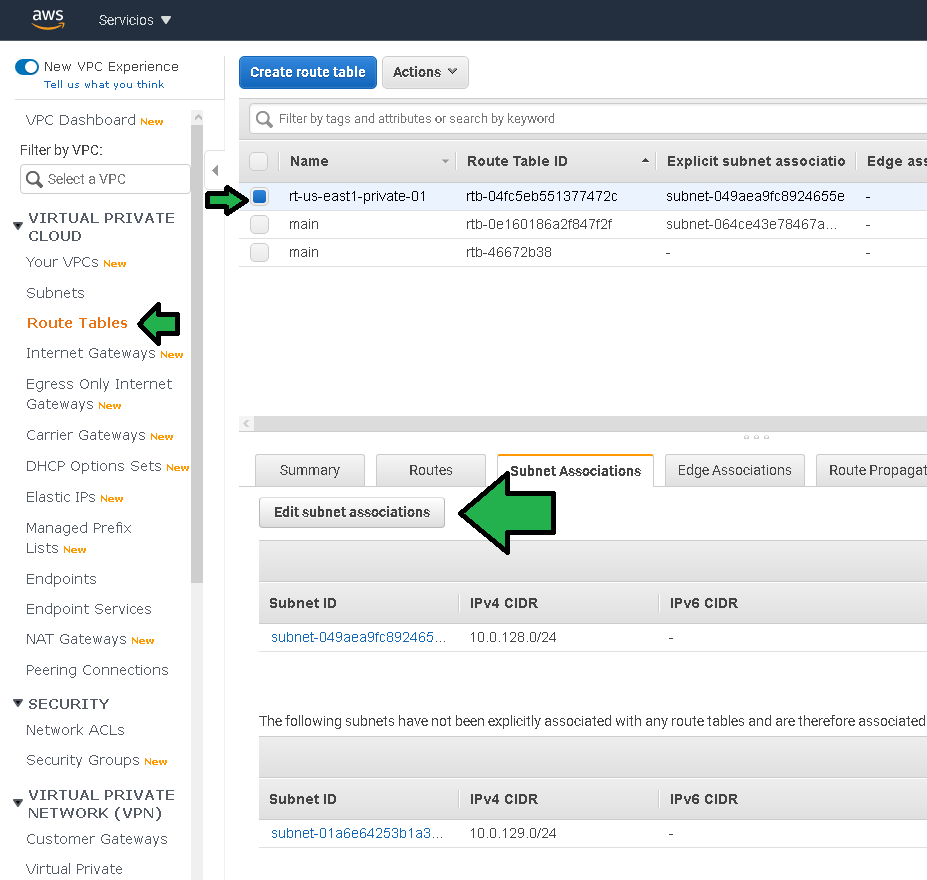
 Con este cambio todo el tráfico que no sea local (no vaya dirigido a una ip de la red 10.0.0.0/16 en este caso) será dirigido al Internet Gateway dando acceso hacia y desde internet.

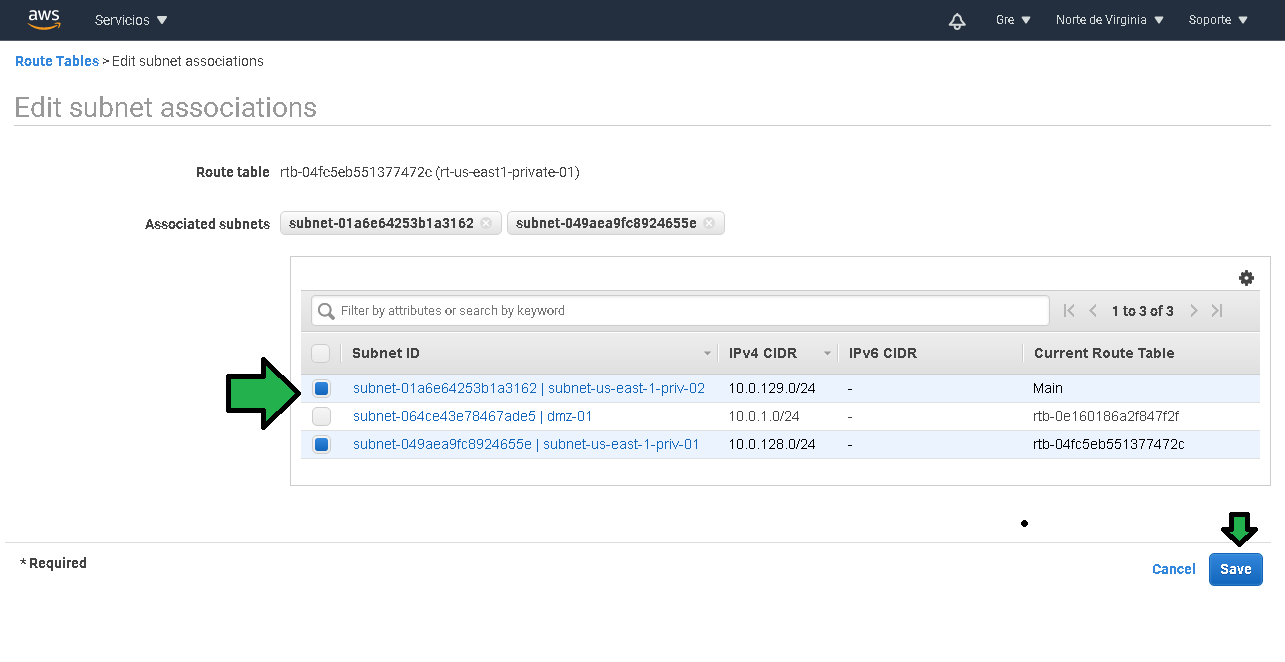
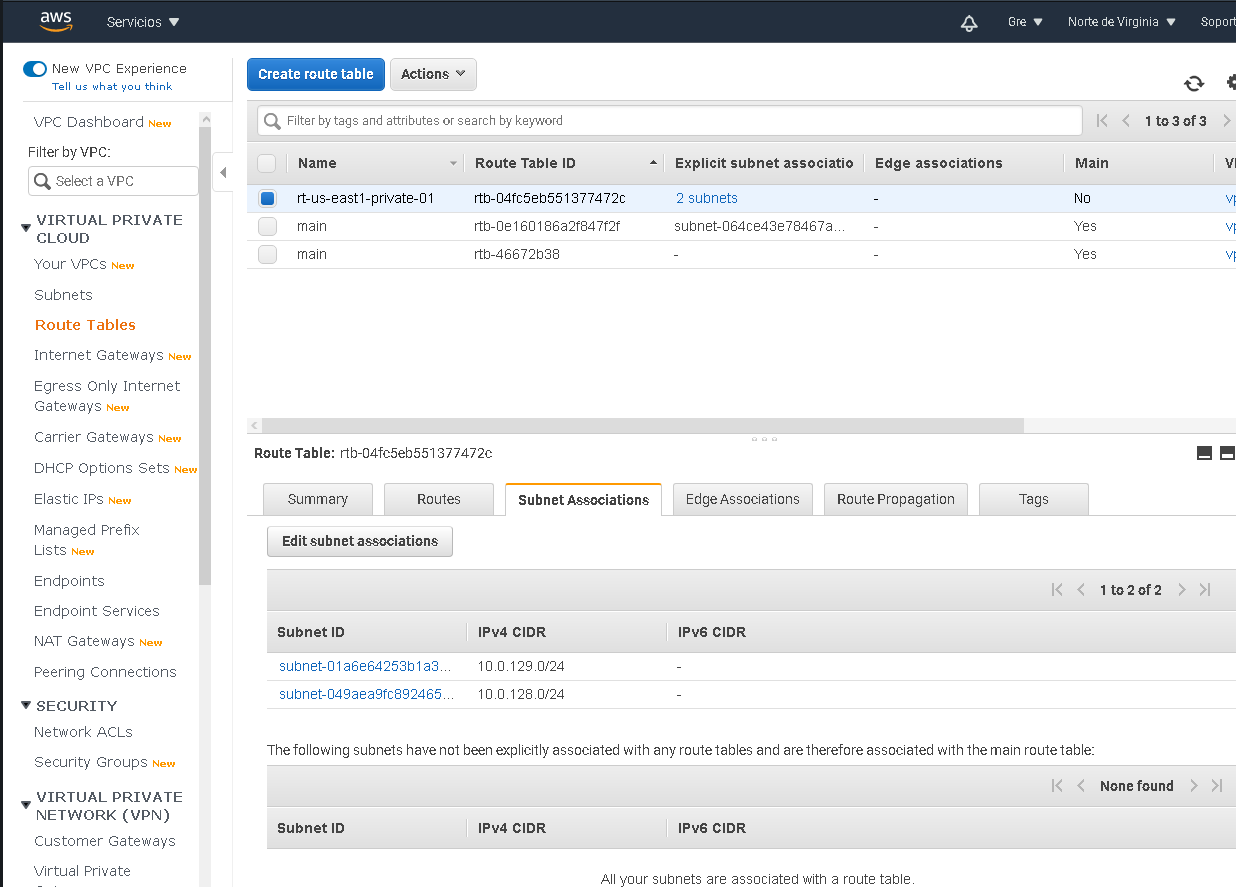
Hasta ahora el avance en el proyecto es el siguiente. ¡Felicidades! # TODO Actualizar esta imagen 

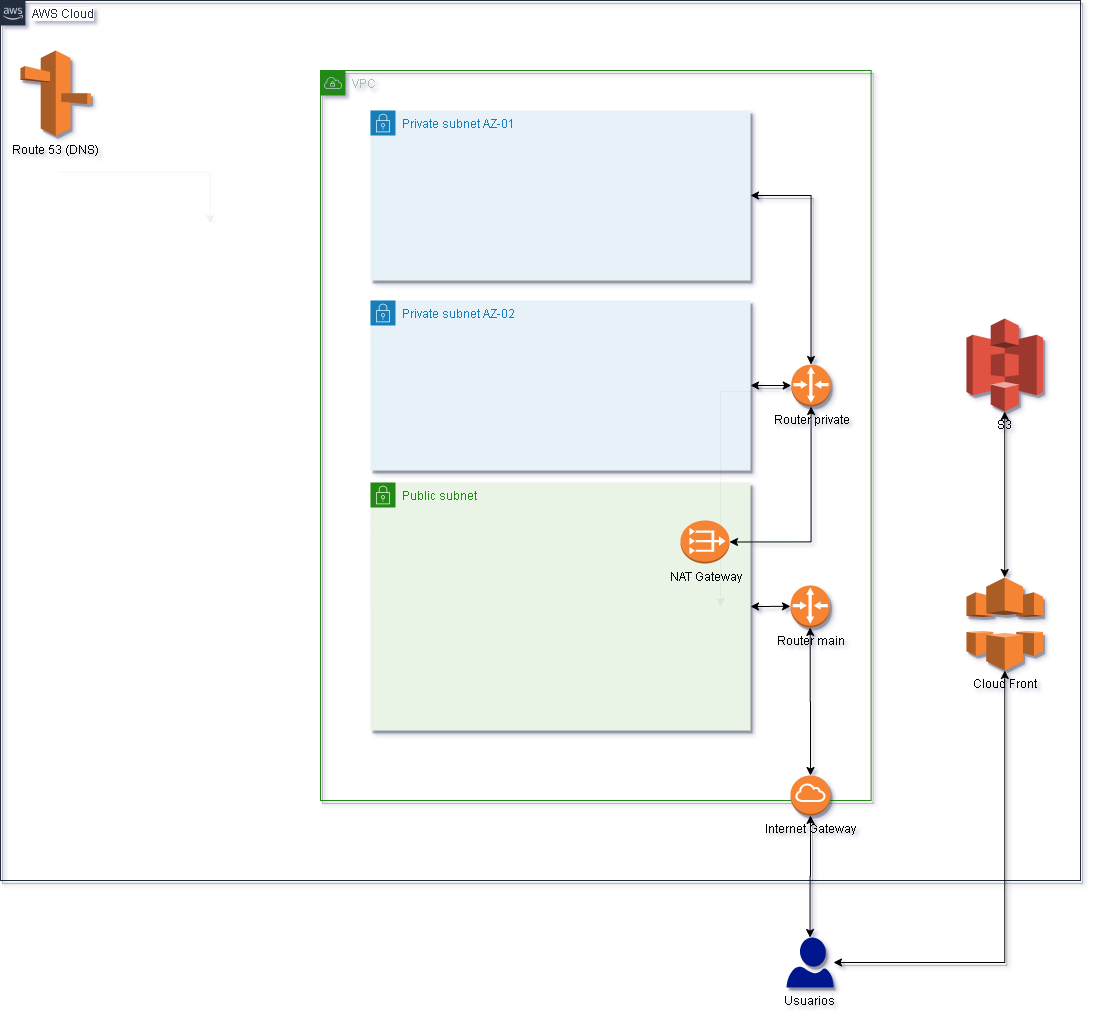
|  |
| --- |
| Hay que generar un par de subredes privadas, las subredes privadas no tienen acceso desde internet directo. |
| Para generar una subred privada se deben seguir los siguientes pasos: |
| 1. Ingresar al servicio de VPC, ir a la sección en el menú “Subnets” y luego click en “Create subnet” |
| pw1-create-subnet-private.png |
| 2. Configurar: a) Establecer un nombre descriptivo a la subred. b) Seleccionar la VPC donde se asociará la subnet privada, seleccionar la VPC recién creada. c) Esta vez no se le dejará la decisión a AWS de que zona de disponibilidad usar. Seleccionar la primera en la lista. d) Se debe establecer el tamaño del bloque de direcciones IP que contendrá la red privada. Hay que notar que el bloque comienza en la dirección 128, la idea es dejar los primeros (0-127) 128 bloques disponibles para redes publicas y los restantes (128-256) para redes privadas. pw1-private-subnet-01.png |
| pw1-subred-private-created.png |
| 3. Para que las subredes tengan acceso a internet con el fin de instalar software o parches de seguridad es necesario habilitar un “NAT Gateway”, para lo cual ir al menú “NAT Gateway” después click en “Create NAT gateway”. |
| pw1-resume-nat-gateway.png |
| 4. Configurar el NAT Gateway con lo siguiente: a) Se debe establecer un nombre descriptivo para el Nat Gateway. b) Seleccionar la subred **pública**. c) En NAT Gateway requiere una dirección IP pública, para generarla dar click en “Allocate Elastic IP”, generada la IP aparecerá un mensake de confirmación (d). Click al final en “Create NAT gateway” |
| pw1-create-gateway.png pw1-nat-gw-done.png |
| 5. Ya generado el NAT Gateway, habrá que decir como redireccionar el tráfico que no es de red interno hacia el NAT Gateway, para lo que hay que generar un nuevo router, dar click en el menú “Route Tables”. pw1-menu-router-01.png |
| 6. Se debe agregar una nueva tabla de routeo en “Create route table” pw1-resume-route-tables.png |
| 7. Configurar con: a) Agregar un nombre descriptivo a la tabla de routeo. b) Seleccionar la VPC a la que se asociará el router, seleccionar la VPC recién creada. |
| pw1-create-route-table-config.png |
| pw1-route-table-private-done.png |
| 8. Creado el router se debe configurar para redirigir el trafico. Seleccionar el nuevo router y dar click en “Edit routes” |
| pw-edit-routes-private.png |
| 9. Configurar las rutas como: a) Agregar la IP 0.0.0.0/0 con la que se especifica que cualquier tráfico que no sea perteneciente a la red de la VPC sea manejado por esta nueva regla. b) Seleccionar el NAT Gateway recién creado. pw1-add-new-route-private.png |
| pw1-route-private-edited-done.png |
| 10. Ahora se debe asociar explícitamente al Router la subred para que maneje su tráfico. a) Dar click en la pestaña “Subnet Associations” b) Dar click en “Edit subnet Associations” |
| pw1-edit-asociation-resume.png |
| 12. Seleccionar la subred privada manejada por esta tabla de routeo. pw1-add-subnet-to-route-table.png |
| Hasta ahora este es el estado del proyecto: |
| # TODO Actualizar imagen pw1-add-private-subnet |

Se debe generar una segunda subred en una zona de disponibilidad distinta al paso 2 inciso c) en la generación de la subred privada.

Para generar la segunda subred:

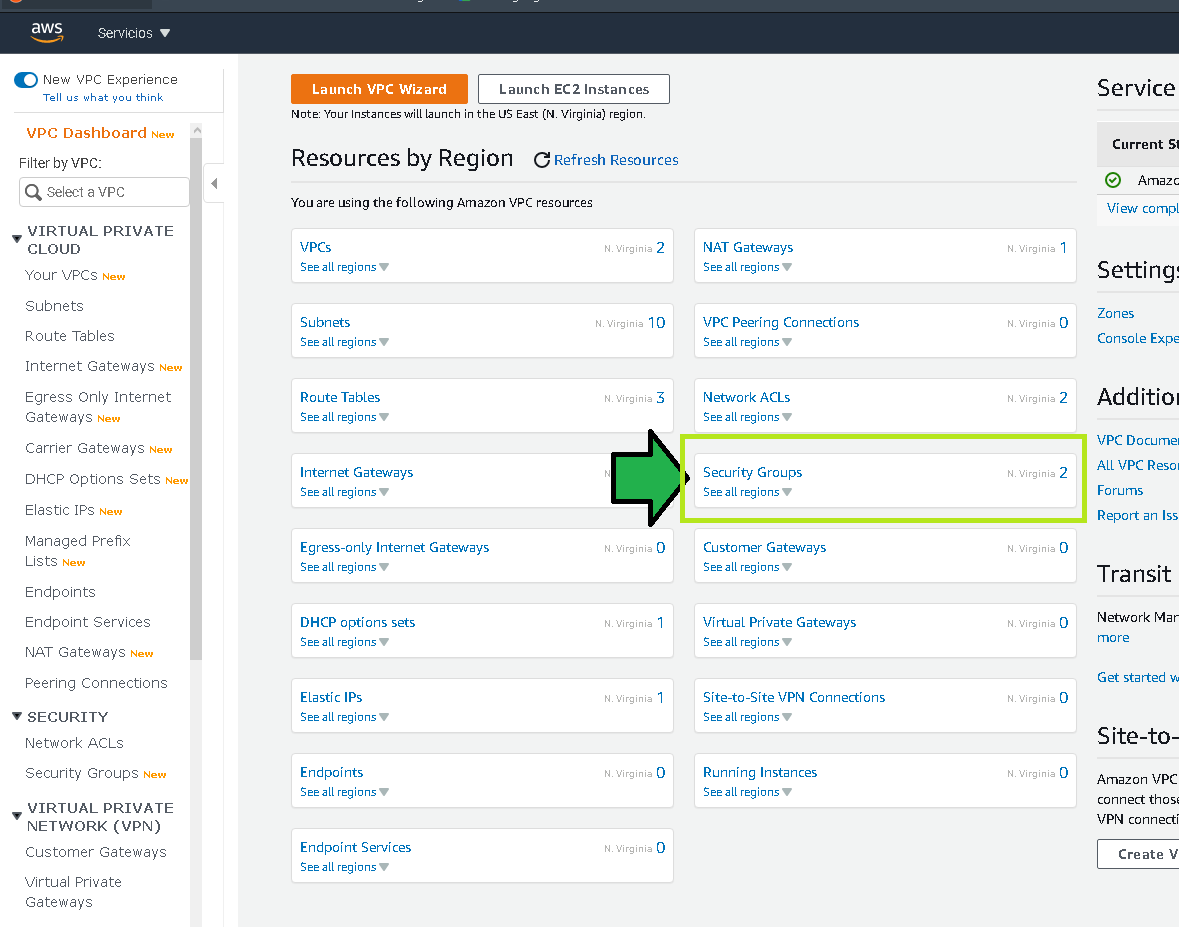
1. Click en “Create Subnet” 
2. Configurar la subred como:
3. Asignar un nombre a la subred.
4. Seleccionar la VPC a la que estará asociada la subred.
5. Seleccionar una zona de disponibilidad distinta a la zona de disponibilidad de la red privada creada previamente.
6. Se asigna el bloque de direcciones IP que la subred tendrá, para se asigna el bloque 129, recordar que del bloque 128 al 256 se designa para subredes privadas. 
7. Ir al la sección re tablas de routeo. 
8. Editar la asociación de la subred a la tabla de routeo que manejará el trágico hacia el NAT Gateway. 
9. Se debe seleccionar la nueva subred privada.

El estatus del proyecto es el siguiente hasta este punto. Prácticamente todo el esquema de red esta listo para seguir construyendo sobre el. # TODO Actualizar imagen 

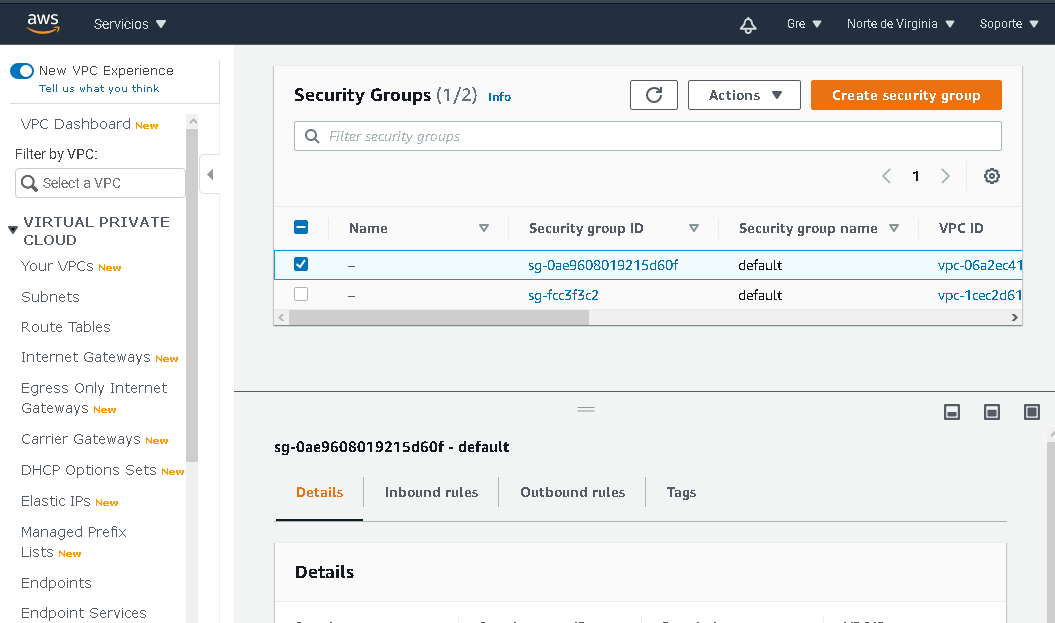
Por último en esta sección se configurarán los grupos de seguridad que darán acceso al tráfico de red a las instancias EC2 y las instancias RDS.

1. Seleccionar “Security Groups”



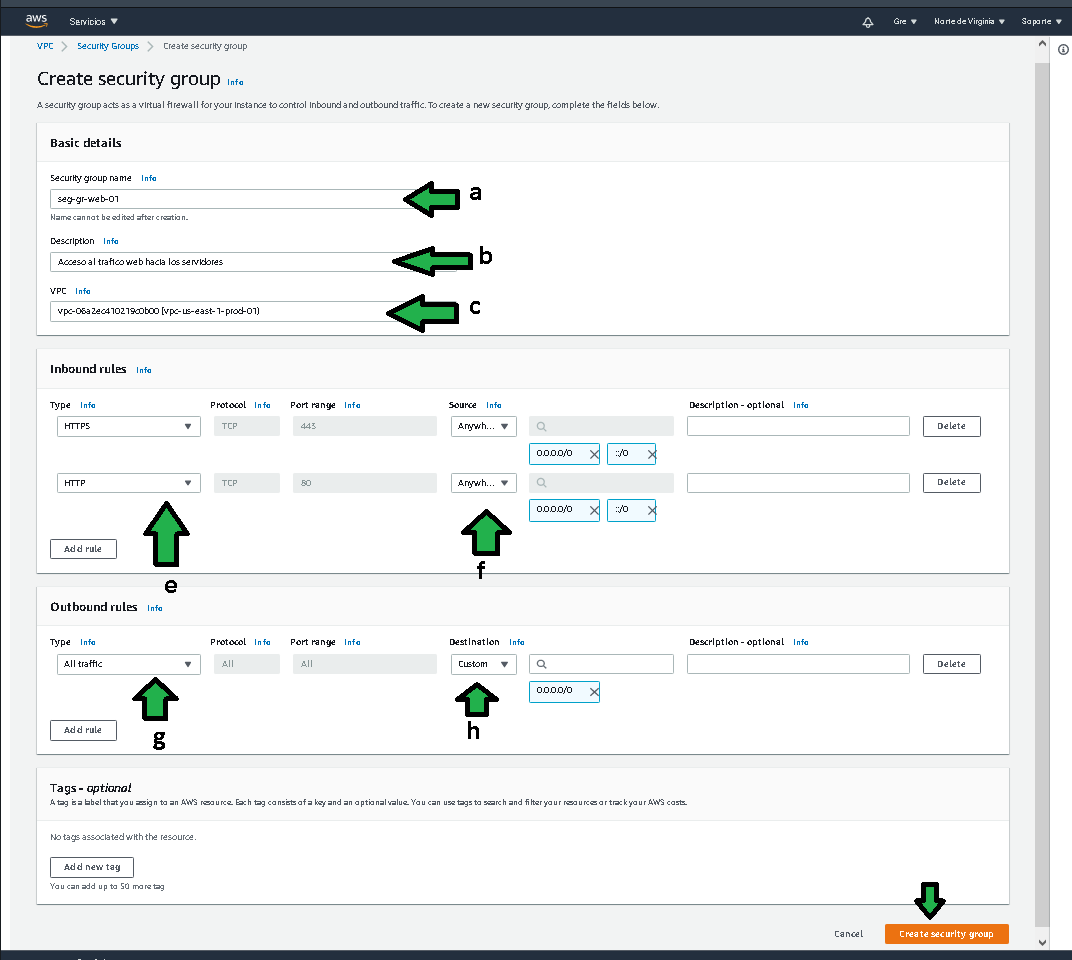
pw1-security-groups-access.png

1. Click en “Create Security Group”

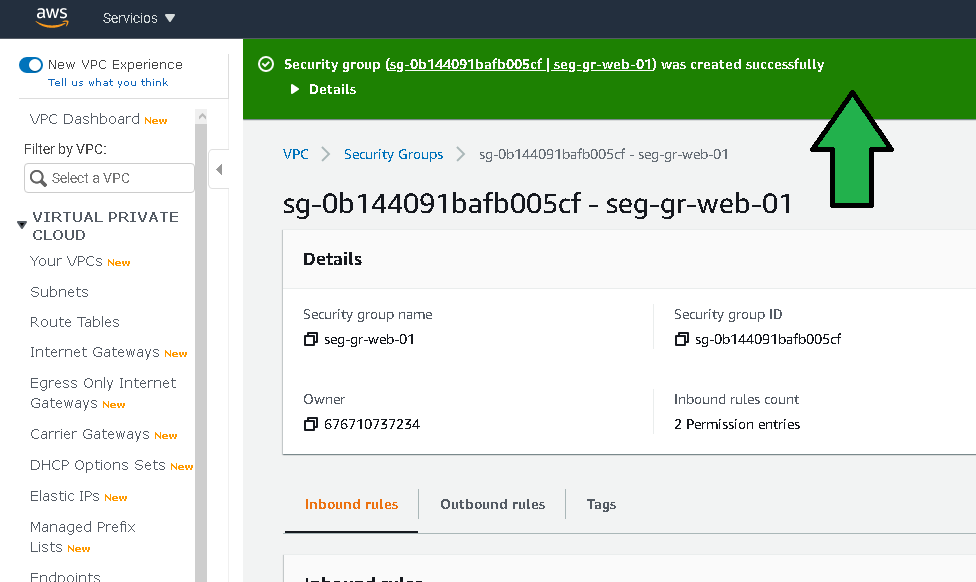


pw1-create-security-group.png

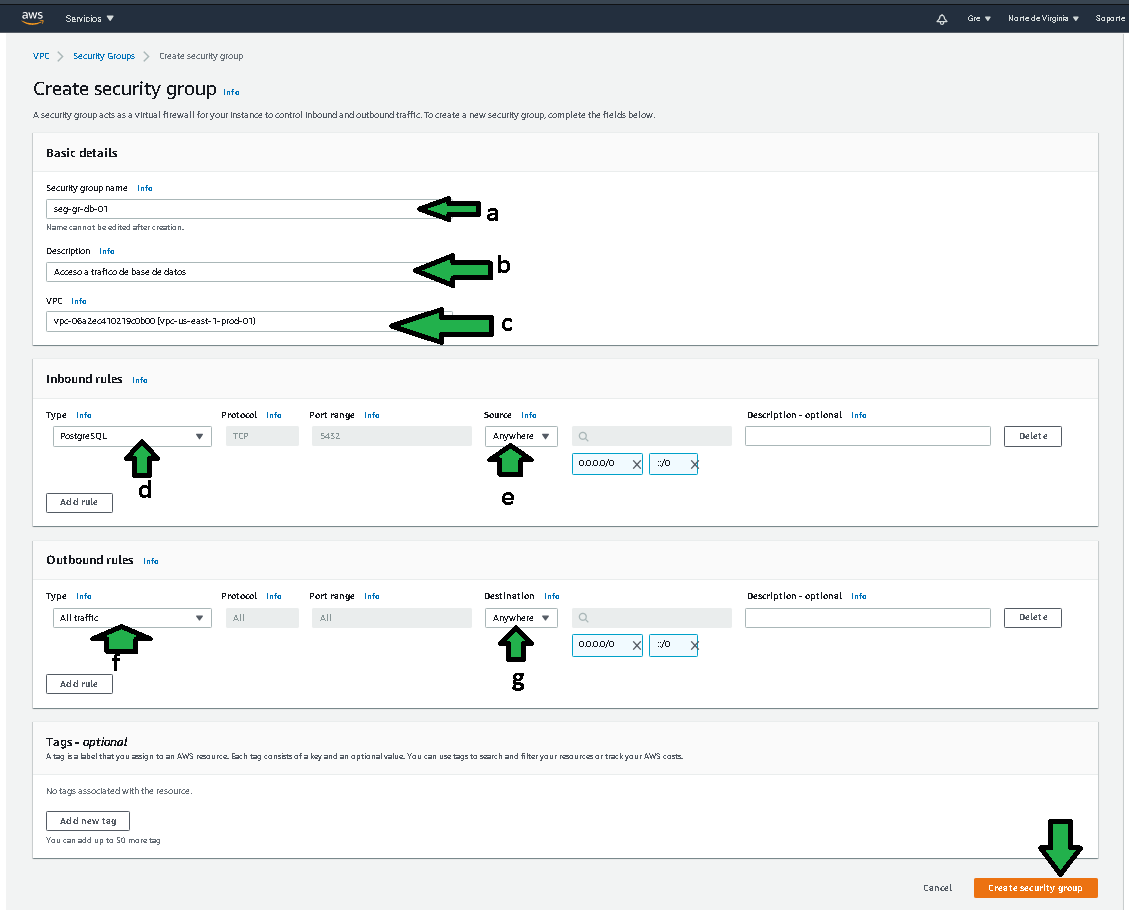
1. Configurar el grupo de seguridad como: a), b) Establecer un nombre descriptivo así como una descripción,
2. Seleccionar la red VPC a la cual pertenecerá la regla de seguridad. d), e) Establecer el tipo de tráfico permitido de entrada hacia AWS desde una fuente (source). f), g) Establecer el tráfico que se permitirá de salida y hacia donde se podrá conectar desde AWS, se recomienda dejar abierto el tráfico por temas de actualizaciones y descarga de software.

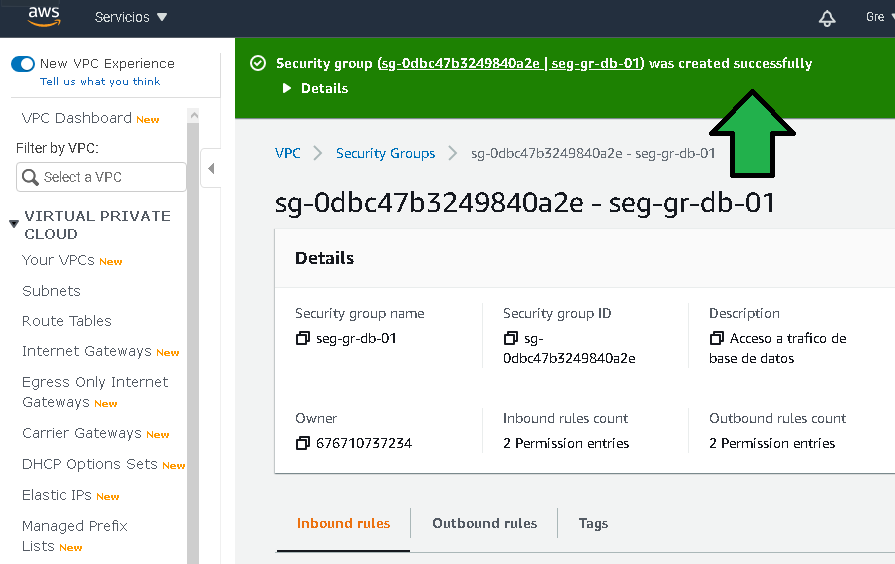


pw1-add-security-group-web.png



pw-seg-group-web-01-done.png

1. Generar un nuevo grupo de seguridad para el tráfico de base de datos de Postgres. a), b) Establecer un nombre descriptivo así como una descripción del grupo de seguridad.
2. Seleccionar la red VPC a la cual pertenecerá la regla de seguridad. d), e) Establecer el tipo de tráfico permitido de entrada hacia AWS desde una fuente (source), para este caso se permitirá acceso de Postgres (puerto 5432) desde cualquier origen. f), g) Establecer el tráfico que se permitirá de salida y hacia donde se podrá conectar desde AWS, se recomienda dejar abierto el tráfico por temas de actualizaciones y descarga de software. 



pw-seg-group-db-01-done.png

1. Generar un nuevo grupo de seguridad para el tráfico de conexión SSH. a), b) Establecer un nombre descriptivo así como una descripción del grupo de seguridad.
2. Seleccionar la red VPC a la cual pertenecerá la regla de seguridad. d), e) Establecer el tipo de tráfico permitido de entrada hacia AWS desde una fuente (source), para este caso se permitirá acceso SSH (puerto 22) desde cualquier origen. f), g) Establecer el tráfico que se permitirá de salida y hacia donde se podrá conectar desde AWS, se recomienda dejar abierto el tráfico por temas de actualizaciones y descarga de software. 