Diseño multiVPC Cloud

Práctica Individual - GIRC

Aarón Escolano Candela

Introducción **2**
Enunciado 2
Diseño de infraestructura Cloud **2**
Overview 2
Recursos utilizados 3
VPCs 3
Gateways 3
Tabla de rutas 4
Internet GW VPC 4
Transit Gateway 5
Servicios 5
Production Web VPC 5
Staging Web VPC 5
Logs and Audit VPC 6
ERP VPC 6
Esquema General **6**
Características **8**
NAT GW 8
Transit GW 9
Escenarios **10**
Escenario 1: Conexión de un usuario a una instancia privada 10
Escenario 2: Conexión entre VPCs 11
Escenario 3: Conexión a Internet desde una VPC interna 11
Posibles mejoras **12**
Arquitectura distribuida en varias regiones 12
Aislamiento de las VPC 12
Bibliografía **14**

Introducción

Enunciado

En este trabajo se pretende afianzar los conocimientos estudiados en clase de teoría sobre la gestión y administración de redes Cloud. El trabajo consistirá en la definición de un escenario de red donde se requiere la interconexión de diferentes VPC's de un entorno cloud que se reparte en diferentes cuentas. El trabajo se realizará individualmente. Las tareas a realizar son las siguientes:

1.Diseña una solución de red donde se tienen que conectar las siguientes VPC's entre ellas.

A. VPC entorno de producción proyecto web.
B. VPC entorno de staging proyecto web.
C. VPC de auditoría y logs.
D. VPC de aplicación de ERP
E. VPC de salida a internet. Todas las VPC's deberán tener salida a través de los NAT Gateway de esta VPC.

2.Es necesario entregar un esquema de red con sus direccionamientos IP, así como las tablas de rutas y los servicios empleados. ¿Por qué se ha empleado un servicio y no otro?

Diseño de infraestructura Cloud

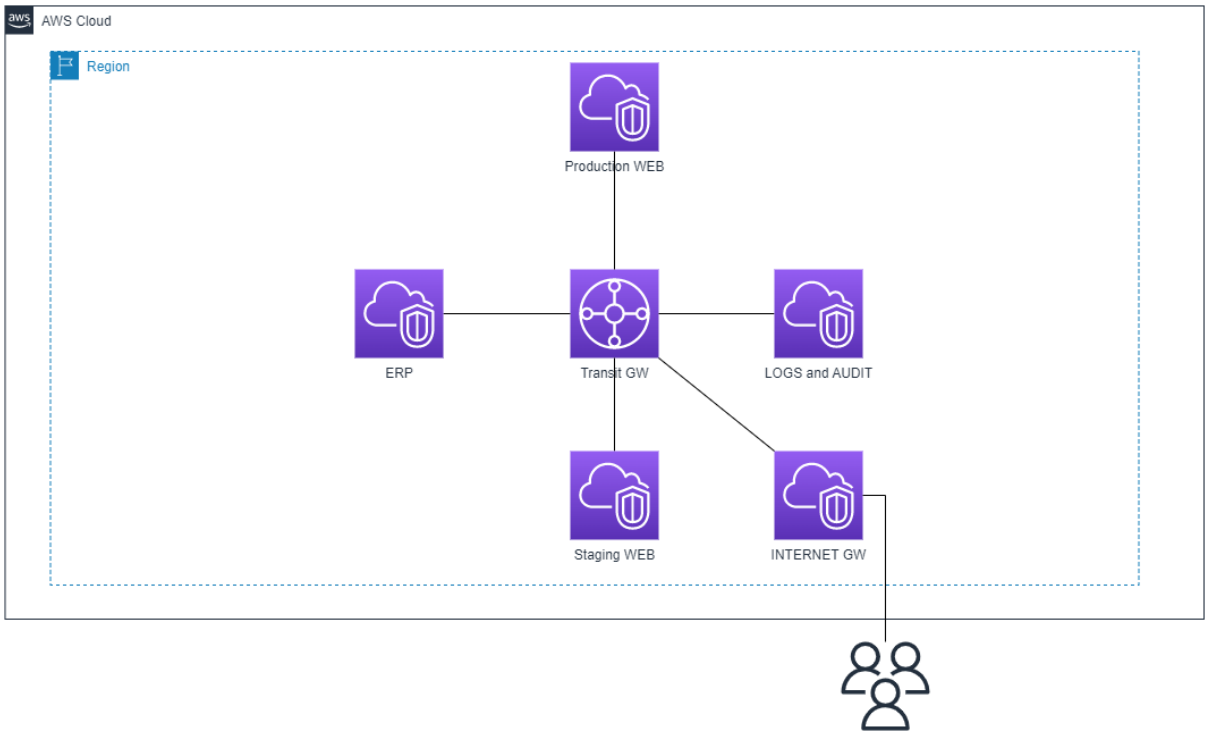
Overview

El siguiente diagrama muestra los componentes más importantes que forman parte de la arquitectura a desarrollar. Las diferentes VPC de nuestra arquitectura tendrán conectividad a internet utilizando la VPC de internet GW que, a través de una NAT GW pública y una Internet GW, proporcionará conexión a internet. Por otro lado, los usuarios también podrán acceder a los servicios internos desde internet mediante un host bastión alojado en la VPC de internet.

La interconexión de VPC 's se realizará utilizando un Transit GW. Configuraremos la tabla de rutas para permitir la conexión entre las diferentes VPCs. Todo el tráfico hacia internet se enviará a la VPC Internet GW. La NAT GW de la VPC Internet GW redirigirá todo el tráfico a la Internet GW.

Main Network Overview

All VPC's connected using an AWS Transit Gateway



Este esquema simplificado nos muestra que la transit gateway funcionará cómo un router entre todas las VPC. Por otro lado, las rutas que crearemos seguirán la siguiente estratégia: Centralized outbound routing to the internet. Esto significa que todos los paquetes deberán pasar necesariamente por la Internet GW.

Recursos utilizados

VPCs

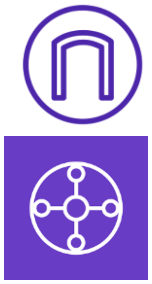
La arquitectura estará formada por cinco VPCs con IPs que no se sobreponen.

- La Internet GW VPC tendrá dos subredes. Una subred pública con una NAT GW y un host bastión y una subred privada con una interfaz elástica para la conexión con la Transit GW.
- Las demás VPCs tendrán dos subredes privadas con instancias ec2 para el funcionamiento de los servicios.

Gateways

- Utilizaremos una **NAT GW** para poder proporcionar conexión a internet a todos los dispositivos que **no** tienen una ip pública. Connectivity type: public, para poder reenviar los paquetes al internet GW.

- Utilizaremos una **Internet GW** para que la NAT GW redirija todo el tráfico hacia internet y para que los usuarios puedan acceder al host bastión desde internet a la ip pública del Internet GW.
- El **Transit GW** nos permitirá conectar todas las VPC entre sí para funcionar cómo si fuera un router. De entre todas las opciones disponibles para realizar dicha interconexión, es la más sencilla de configurar porque no necesitamos ninguna aplicación adicional cómo una VPN y porque la tabla de rutas es más sencilla que utilizando VPC Peering.



- **Host Bastion**. Para que los usuarios puedan acceder desde internet a las instancias en las subredes privadas.

Tabla de rutas

Internet GW VPC

CIDR: 10.0.0.0/16

La subred privada es la que estará conectada mediante una interfaz de red elástica a la transit GW. La primera ruta permite que el tráfico entre instancias en la propia subred sea posible y la segunda entrada permite que todo el tráfico proveniente de la Transit GW hacia internet se redirija a la NAT GW en la subred pública. La subred pública tiene la entrada 0.0.0.0 para permitir el tráfico hacia internet y la entrada 11.0.0.0/14 para permitir el tráfico desde el host bastión hacia los servicios.

IG VPC Private Route Table	
Prefix	Next Target
10.0.0.0/16	local
0.0.0.0/0	NAT GW

IG VPC Public Route Table	
Prefix	Next Target
10.0.0.0/16	local
11.0.0.0/14	Transit GW 1
0.0.0.0/0	INTERNET GW

Transit Gateway

La tabla de rutas de la transit GW funciona cómo si fuera un router. Existe una entrada para cada VPC con destino el attachment o interfaz de red conectado a la Transit GW.

Transit GW Route Table	
CIDR	Next Target
10.0.0.0/16	Attachment de **Internet GW VPC**
11.0.0.0/16	Attachment de **Production Web VPC**
11.1.0.0/16	Attachment de **Staging Web VPC**
11.2.0.0/16	Attachment de **Logs and Audit VPC**
11.3.0.0/16	Attachment de **ERP VPC**
0.0.0.0/0	Attachment de **Internet GW VPC**

Servicios

CIDR: 11.0.0.0/14

Production Web VPC

CIDR: 11.0.0.0/16

Production Web Private Route Table	
Prefix	Next Target
11.0.0.0/16	local
0.0.0.0/0	Transit GW

Staging Web VPC

CIDR: 11.1.0.0/16

Production Web Private Route Table	
Prefix	Next Target
11.1.0.0/16	local
0.0.0.0/0	Transit GW

Logs and Audit VPC

CIDR: 11.2.0.0/16

Production Web Private Route Table	
Prefix	Next Target
11.2.0.0/16	local
0.0.0.0/0	Transit GW

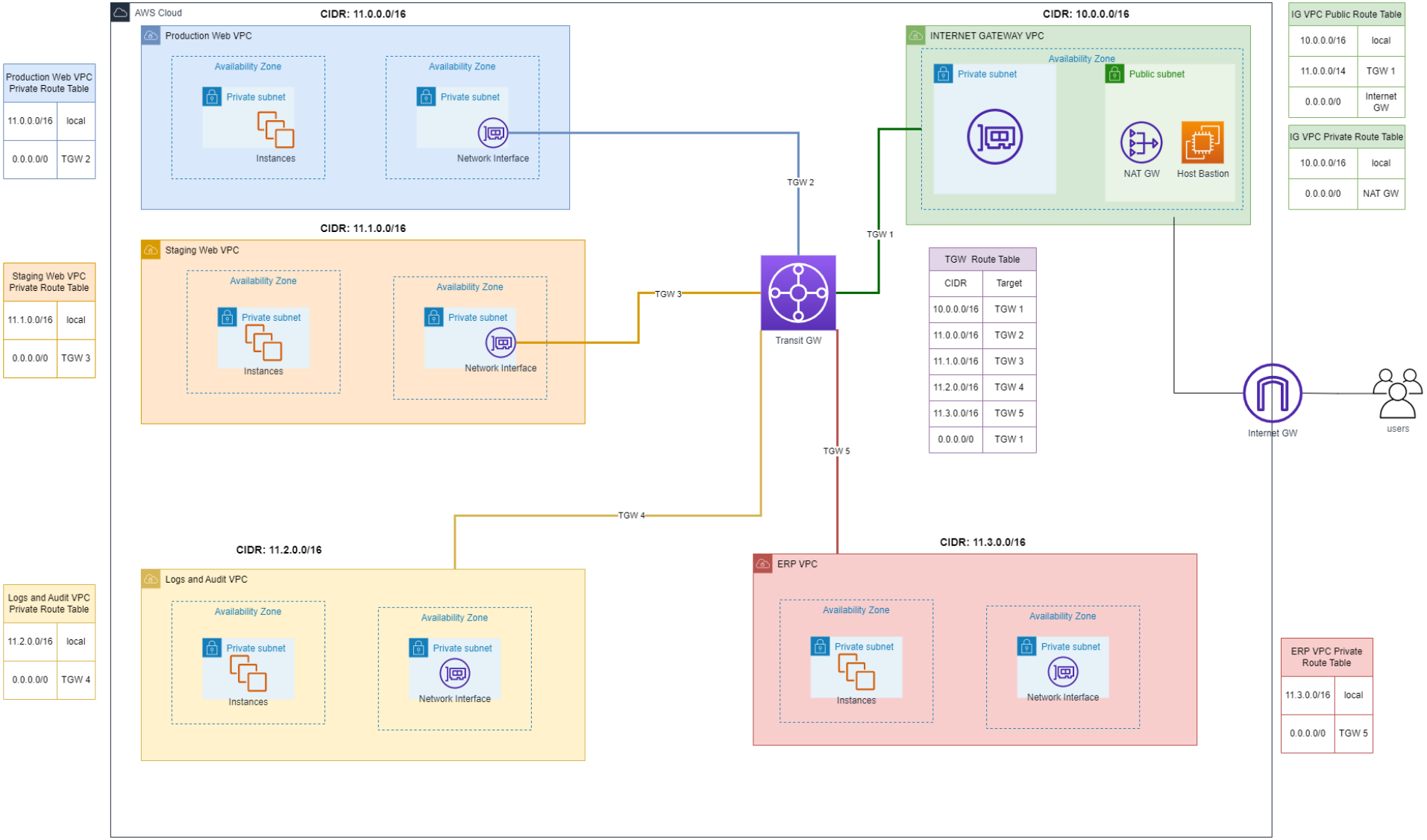
ERP VPC

CIDR: 11.3.0.0/16

Production Web Private Route Table	
Prefix	Next Target
11.3.0.0/16	local
0.0.0.0/0	Transit GW

Esquema General

Architecture MultiVPCs



Production Web VPC Private Route Table	
11.0.0.0/16	local
0.0.0.0/0	TGW 2

Staging Web VPC Private Route Table	
11.1.0.0/16	local
0.0.0.0/0	TGW 3

Logs and Audit VPC Private Route Table	
11.2.0.0/16	local
0.0.0.0/0	TGW 4

TGW Route Table	
CIDR	Target
10.0.0.0/16	TGW 1
11.0.0.0/16	TGW 2
11.1.0.0/16	TGW 3
11.2.0.0/16	TGW 4
11.3.0.0/16	TGW 5
0.0.0.0/0	TGW 1

IG VPC Public Route Table	
10.0.0.0/16	local
11.0.0.0/14	TGW 1
0.0.0.0/0	Internet GW

IG VPC Private Route Table	
10.0.0.0/16	local
0.0.0.0/0	NAT GW

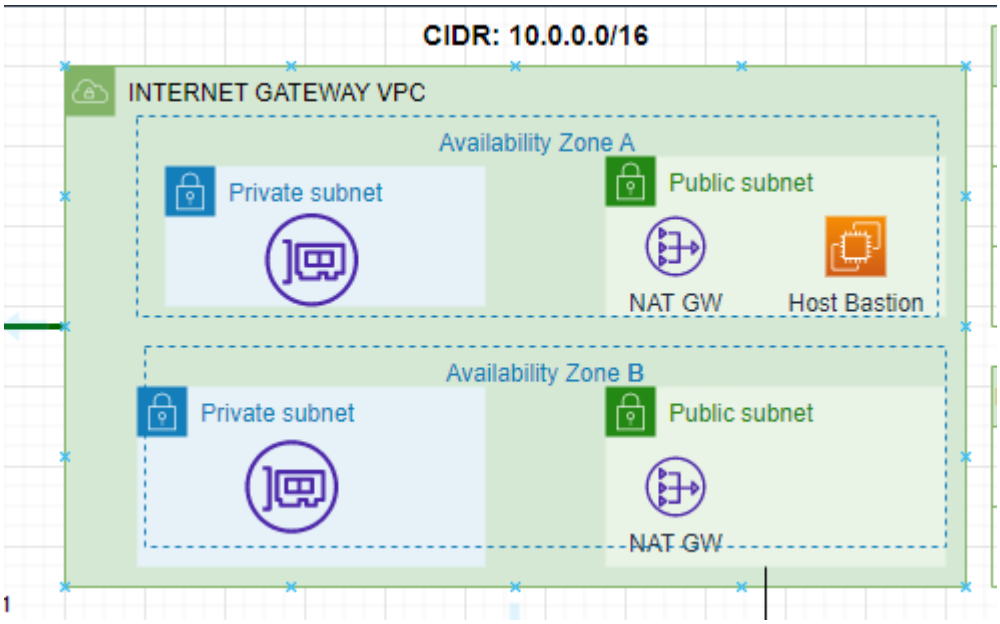
ERP VPC Private Route Table	
11.3.0.0/16	local
0.0.0.0/0	TGW 5

Características

NAT GW

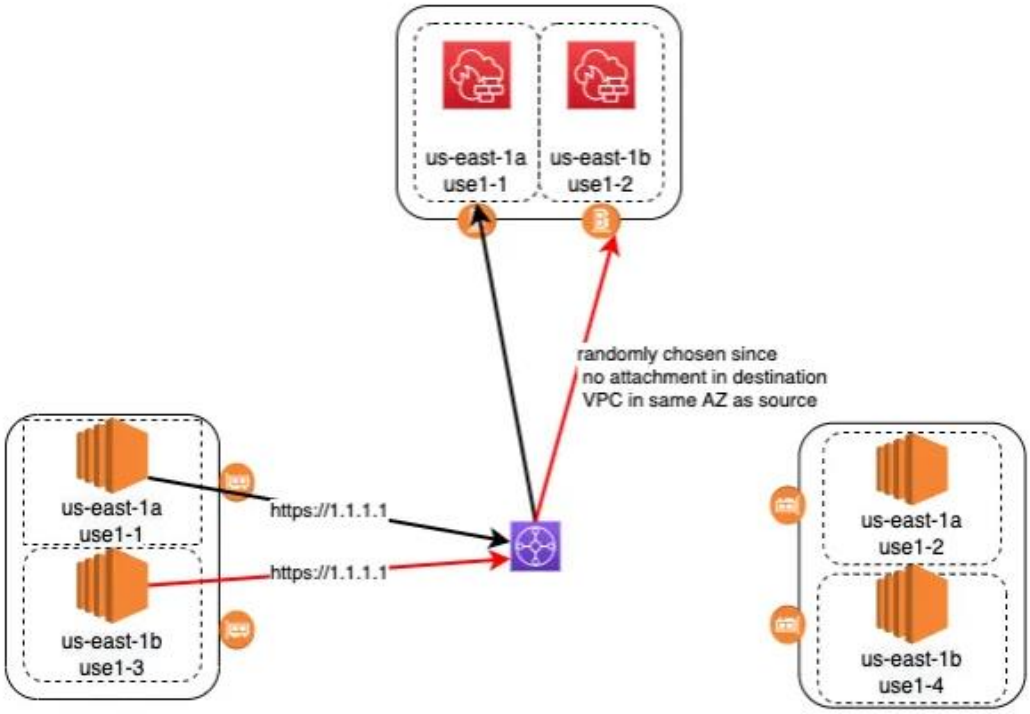
- Es capaz de manejar un tráfico de 5 Gbps de ancho de banda y escala automáticamente hasta 100 Gbps.
- Procesa un millón de paquetes por segundo y escala automáticamente hasta diez millones de paquetes por segundo.

Si estas especificaciones fuesen insuficientes se podría modificar la arquitectura de la siguiente manera:



De esta forma obtenemos más ancho de banda. La Transit Gateway redirigirá los paquetes a la subred que tenga la misma zona de disponibilidad que donde se originó el paquete.

Aquí muestro un ejemplo. Si se envía un paquete desde la zona de disponibilidad us-east-1a, la transit gateway redirigirá el paquete a esa zona de disponibilidad en el destino. En cambio, si se envía un paquete desde la zona de disponibilidad us-east-1b, al no existir esa zona en el destino, la transit gateway la eligirá de forma aleatoria. Esto ocurrirá si el modo Appliance está desactivado. En caso contrario, appliance mode activado,se eliminará el paquete.



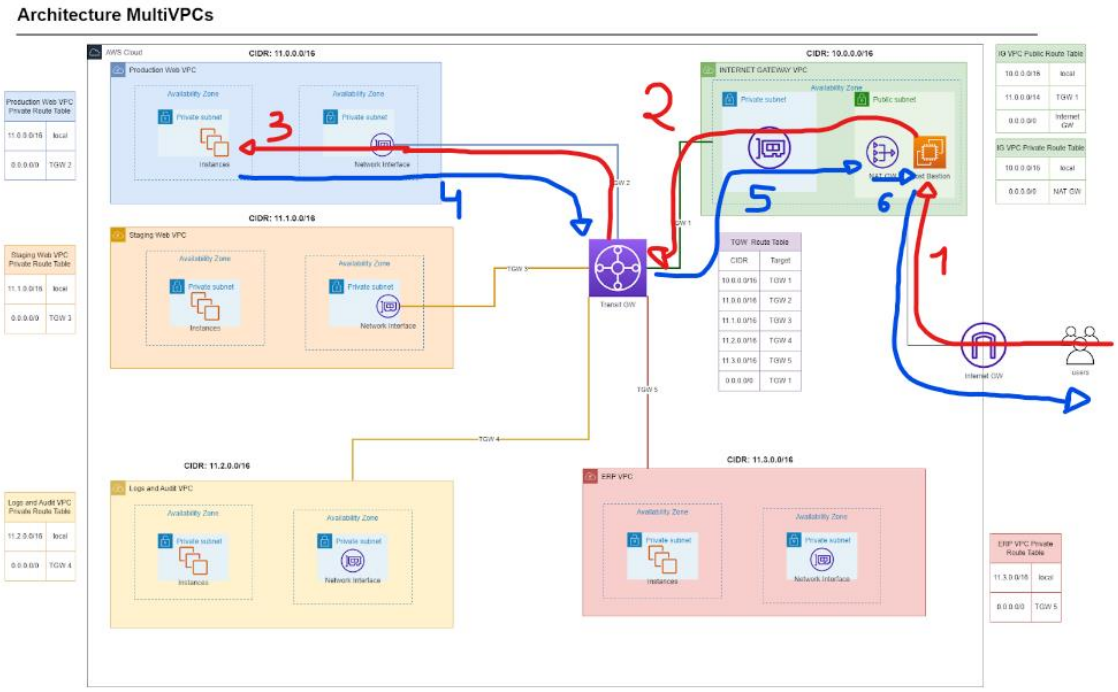
- Soporta los siguientes protocolos: TCP, UDP, y ICMP.

Transit GW

- Alta disponibilidad de serie.

Escenarios

Escenario 1: Conexión de un usuario a una instancia privada



Paso 1: Paquete desde el usuario hasta el host bastión pasando por la Internet GW (Origin) 79.266.124.44 -> (Public IP Host bastión)44.192.54.100

Paso 2: Paquete desde el host bastión hacia la vpc destino. Se salta la NAT GW.

(Private IP Host bastión) 10.0.0.1 -> (Private IP Instance in VPC destiny) 11.0.0.1

Paso 3: Paquete redirigido desde la Transit GW hacia la vpc

(Private IP Host bastión) 10.0.0.1 -> (Private IP Instance in VPC destiny) 11.0.0.1

Paso 4: Paquete respuesta

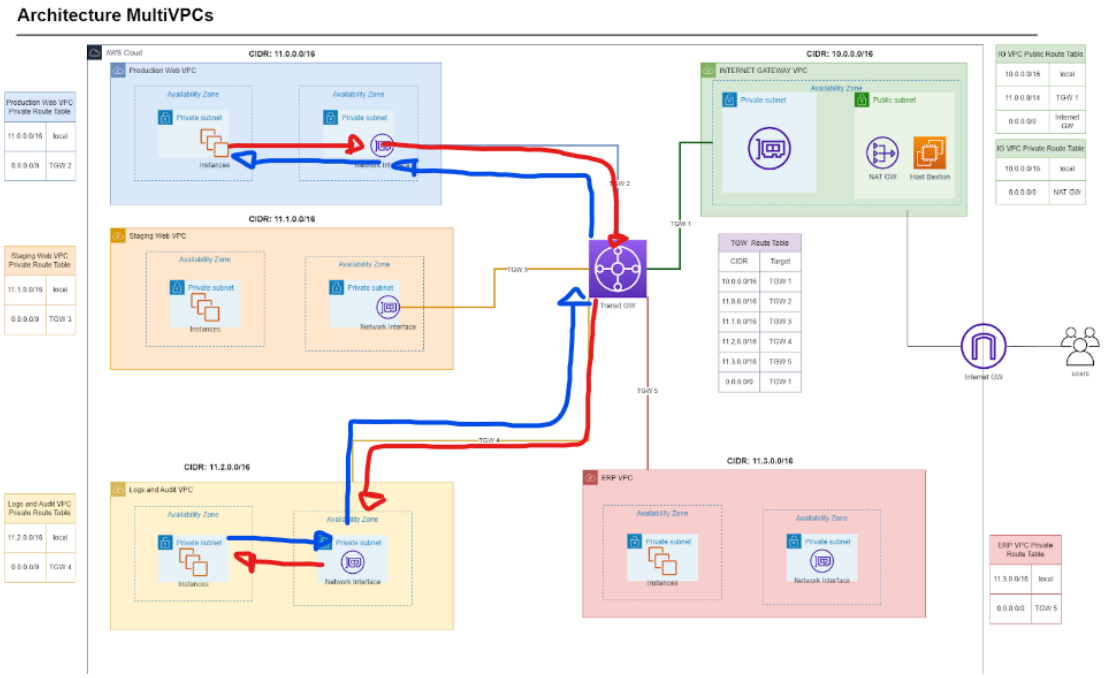
(Private IP Instance) 11.0.0.1 -> (Private IP Host Bastión) 10.0.0.1

Paso 5: Paquete respuesta redirigido desde Transit GW a la NAT GW

(Private IP Instance) 11.0.0.1 -> (Private IP Host Bastión) 10.0.0.1

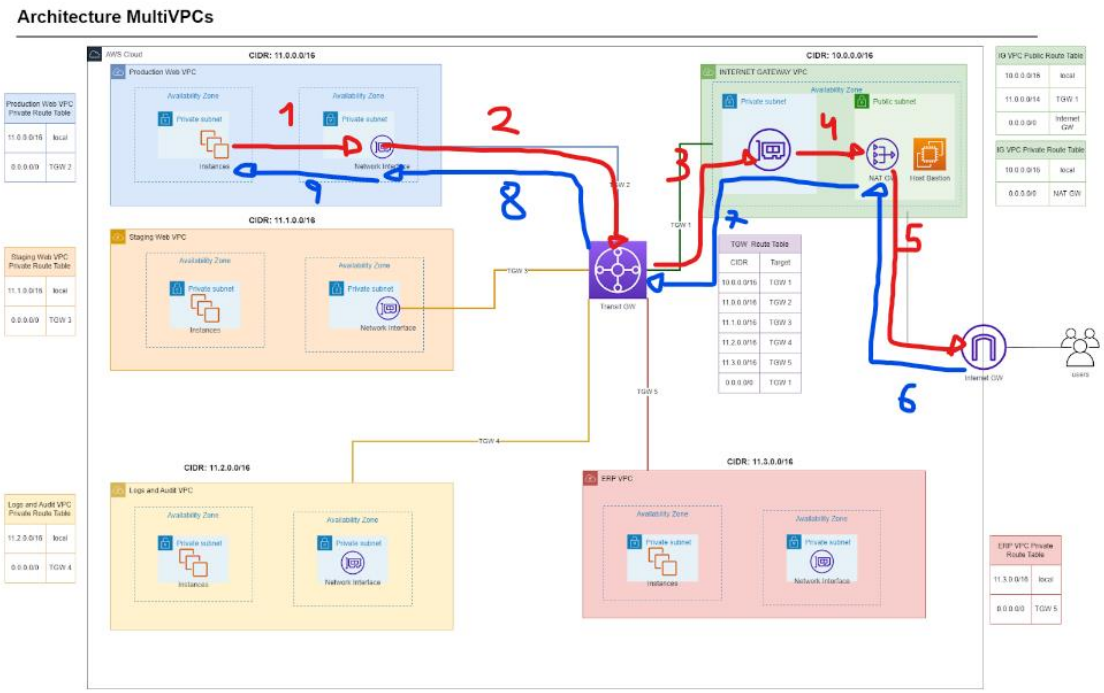
Paso 6: Paquete respuesta redirigido desde NAT GW a Host bastión
Paso 7: Paquete respuesta hacia el usuario
(Public IP Host bastión)44.192.54.100 -> (Public IP User) 79.266.124.44

Escenario 2: Conexión entre VPCs



Las tablas de rutas de la VPC azul envía todos los paquetes no dirigidos a la propia vpc a la transit GW. La transit GW se encarga de enviar los paquetes a la VPC correspondiente.

Escenario 3: Conexión a Internet desde una VPC interna

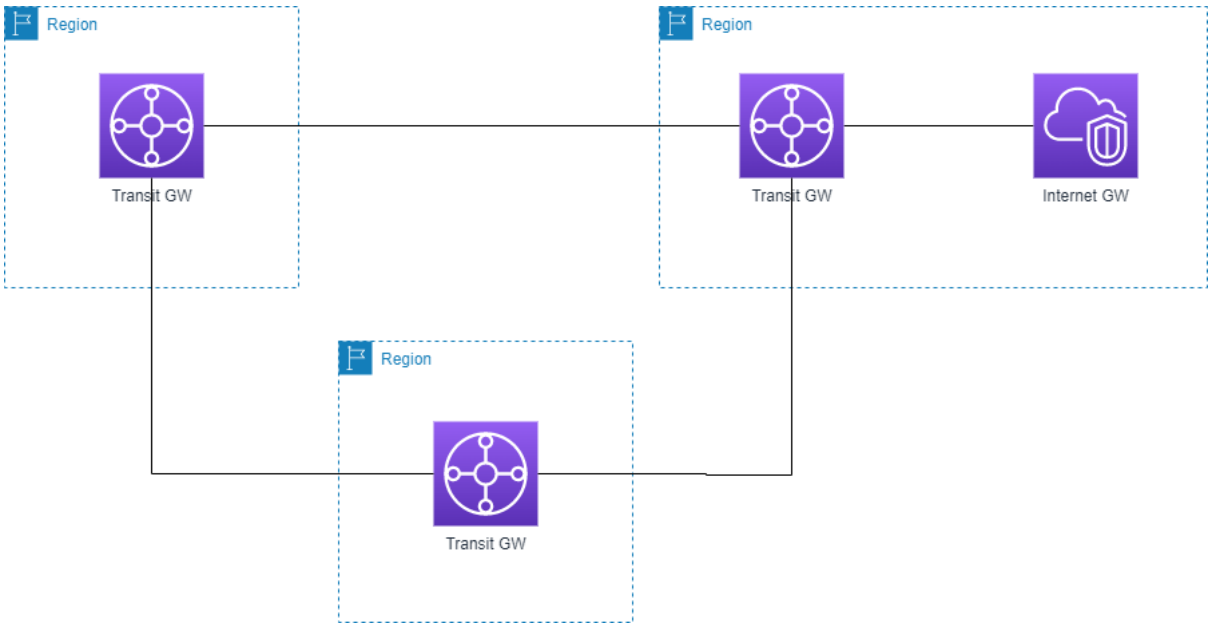


En este escenario la NAT GW es fundamental para el correcto funcionamiento de la arquitectura. Los paquetes se originan en las subredes privadas. Estos paquetes son enviados a la transit GW y esta se encarga de reenviarlos a los servidores destino. Gracias a que la transit GW tiene una IP Pública, los servidores podrán contestar a estas peticiones con la ip destino la NAT GW. Una vez el paquete del servidor haya vuelto a la NAT GW, esta traducirá el paquete y lo enviará a la ip privada correspondiente.

Posibles mejoras

Arquitectura distribuida en varias regiones

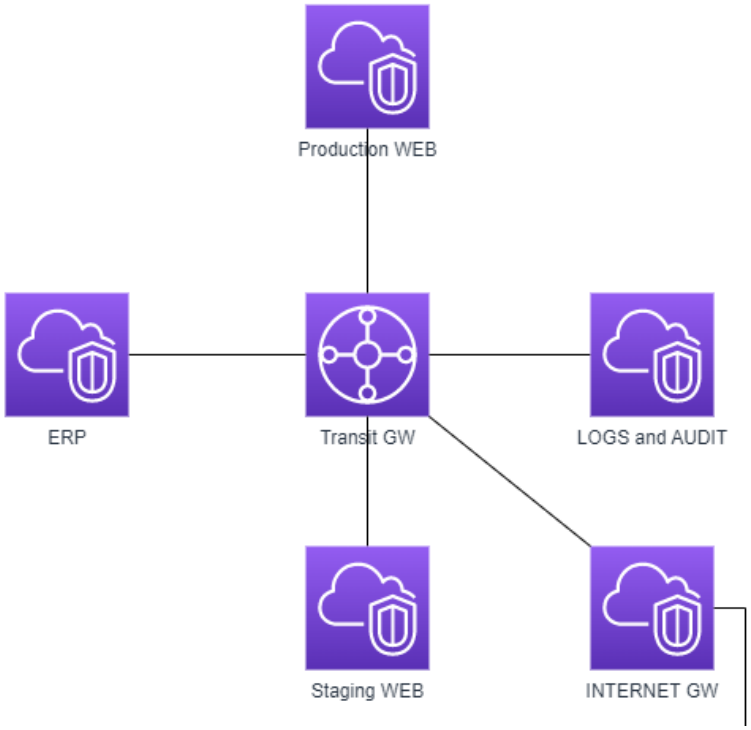
Si quisieramos ampliar la arquitectura para añadir VPCs que se encontraran en múltiples regiones podríamos añadir una transit GW en cada region y conectarlas entre ellas con peering connections.



Las tablas de rutas serían muy similares a las mostradas con el esquema general, con la única diferencia de que existiría una capa adicional de redirecciones.

Aislamiento de las VPC

El hecho de que las diferentes VPCs internas puedan comunicarse entre sí puede suponer un riesgo para la seguridad. Una posible mejora podría ser aislar la comunicación entre VPCs y sólo permitir el tráfico hacia la VPC de internet.



Para aplicar este escenario, la transit GW tendría dos tablas de rutas:

Tabla de rutas para el attachment de la INTERNET GW:

Internet GW attachment Transit GW ROUTE TABLE	
CIDR	Next Target
11.0.0.0/16	Attachment de **Production Web VPC**
11.1.0.0/16	Attachment de **Staging Web VPC**
11.2.0.0/16	Attachment de **Logs and Audit VPC**
11.3.0.0/16	Attachment de **ERP VPC**

Esta tabla se aplicará en los paquetes que vayan desde la Internet GW hacia las otras VPCs.

Tabla de rutas para todos los demás attachment, es decir todas las VPCs diferentes a la de internet

The rest VPCs Transit GW ROUTE TABLE	
CIDR	Next Target
0.0.0.0/0	Attachment de **Internet GW VPC**

Se aplicará cuando los paquetes salgan de las vpc de servicios .

Bibliografía

- What is a transit gateway
- Amazon VPC-to-Amazon VPC connectivity options
- Transit gateway
- https://catalog.workshops.aws/networking/en-US/intermediate/2-tgw-vpns/60-tgw-routing
- https://aws.amazon.com/blogs/architecture/field-notes-working-with-route-tables-in-aws-transit-gateway/