COLOMBIA POTENCIA DE LA VIDA

TIC

LECCIÓN 3: CONEXIÓN DEL ENTORNO DE RED DE AWS A INTERNET

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

Universidad Tecnológica de Pereira

CREACIÓN DE UNA SUBRED PÚBLICA

Gateway NAT

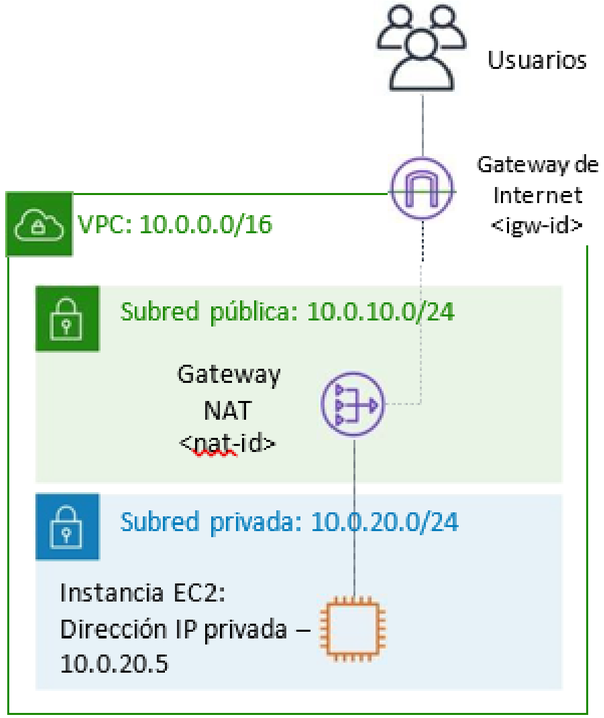
- Permiten que las instancias en una subred privada inicien el tráfico saliente hacia Internet u otros servicios de AWS.
- Impiden que las instancias privadas reciban solicitudes de conexión entrante desde Internet.

Tabla de enrutamiento pública

Destino	Objetivo
10.0.0.0/16	local
0.0.0.0/0	<igw-id>

Tabla de enrutamiento privada

Destino	Objetivo
10.0.0.0/16	local
0.0.0.0/0	<nat-id>



AHORA QUE SABE CÓMO DISEÑAR Y CREAR UN ENTORNO DE RED AISLADO PARA SUS CARGAS DE TRABAJO, BUSCARÁ CONECTARLO A INTERNET.

UNA GATEWAY DE INTERNET ES UN COMPONENTE DE VPC QUE PERMITE LA COMUNICACIÓN ENTRE LOS RECURSOS EN LA VPC Y EL INTERNET. SE ESCALA DE FORMA HORIZONTAL, ES REDUNDANTE Y CUENTA CON ALTA DISPONIBILIDAD. UNA GATEWAY DE INTERNET ADMITE EL TRÁFICO IPV4 E IPV6. ADEMÁS, CUMPLE DOS PROPÓSITOS. EN PRIMER LUGAR, PROPORCIONA UN OBJETIVO EN LAS TABLAS DE ENRUTAMIENTO DE LA VPC PARA EL TRÁFICO QUE SE PUEDE LLEVAR A INTERNET. EN SEGUNDO LUGAR, LA GATEWAY DE INTERNET REALIZA LA CONVERSIÓN DE LAS DIRECCIONES DE RED (NAT) PARA INSTANCIAS A LAS QUE SE ASIGNARON DIRECCIONES IPV4 PÚBLICAS.

PARA CONVERTIR UNA SUBRED EN PÚBLICA, PRIMERO DEBE CREAR UNA GATEWAY DE INTERNET Y ASOCIARLA A LA VPC.

DIRECCIONAMIENTO DEL TRÁFICO ENTRE RECURSOS DE VPC

- Las tablas de enrutamiento son necesarias para dirigir el tráfico entre los recursos de VPC.
- Cada VPC tiene una tabla de enrutamiento principal (predeterminada).
- Todas las subredes deben estar asociadas a una tabla de enrutamiento.
- Se pueden crear tablas de enrutamiento personalizadas.

Práctica recomendada: Utilice tablas de enrutamiento personalizadas para cada subred.

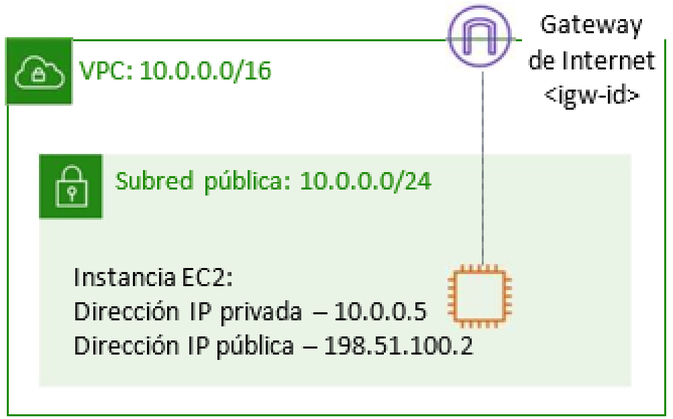
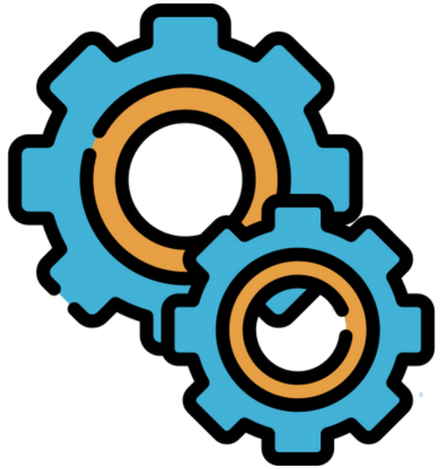


Tabla de enrutamiento pública

Destino	Objetivo
10.0.0.0/16	local
0.0.0.0/0	<igw-id>

DESPUÉS DE CONFIGURAR LA GATEWAY DE INTERNET, EL SIGUIENTE PASO ES ACTUALIZAR LA TABLA DE ENRUTAMIENTO CORRESPONDIENTE A LA SUBRED QUE DESEAS CONECTAR A INTERNET. UNA TABLA DE ENRUTAMIENTO CONTIENE UN CONJUNTO DE INSTRUCCIONES LLAMADAS RUTAS, QUE DETERMINAN LA DIRECCIÓN HACIA LA CUAL SE DIRIGE EL TRÁFICO DE RED.

AL CREAR UNA VPC, AUTOMÁTICAMENTE SE LE ASIGNA UNA TABLA DE ENRUTAMIENTO PRINCIPAL. INICIALMENTE, ESTA TABLA DE ENRUTAMIENTO PRINCIPAL (Y TODAS LAS DEMÁS EN LA VPC) CONTIENE SOLO UNA RUTA LOCAL QUE PERMITE LA COMUNICACIÓN ENTRE LOS RECURSOS DENTRO DE LA VPC. ESTA RUTA LOCAL NO PUEDE SER MODIFICADA. CUANDO LANZAS UNA INSTANCIA EN LA VPC, LA RUTA LOCAL SE APLICA AUTOMÁTICAMENTE A ESA INSTANCIA, ELIMINANDO LA NECESIDAD DE AGREGARLA MANUALMENTE A LA TABLA DE ENRUTAMIENTO. SIN EMBARGO, ES POSIBLE CREAR TABLAS DE ENRUTAMIENTO ADICIONALES PERSONALIZADAS PARA LA VPC.



COLOMBIA POTENCIA DE LA VIDA

TIC

CADA SUBRED DENTRO DE LA VPC DEBE ESTAR ASOCIADA A UNA TABLA DE ENRUTAMIENTO PARA CONTROLAR SU DIRECCIONAMIENTO. SI NO SE ASIGNA EXPLÍCITAMENTE UNA SUBRED A UNA TABLA DE ENRUTAMIENTO ESPECÍFICA, SE ASOCIARÁ AUTOMÁTICAMENTE A LA TABLA DE ENRUTAMIENTO PRINCIPAL Y UTILIZARÁ SUS REGLAS. AUNQUE UNA SUBRED PUEDE ESTAR ASOCIADA SOLO A UNA TABLA DE ENRUTAMIENTO A LA VEZ, MÚLTIPLES SUBREDES PUEDEN COMPARTIR LA MISMA TABLA DE ENRUTAMIENTO.

PARA UNA GESTIÓN MÁS DETALLADA DE LAS RUTAS Y DESTINOS, PUEDES CREAR TABLAS DE ENRUTAMIENTO PERSONALIZADAS PARA CADA SUBRED. ESTO PERMITE UNA CONFIGURACIÓN MÁS ESPECÍFICA Y ADAPTADA A TUS NECESIDADES.

PARA ENVIAR TRÁFICO NO LOCAL A TRAVÉS DE LA GATEWAY DE INTERNET HACIA INTERNET, CREE UNA RUTA CON DESTINO 0.0.0.0/0 Y OBJETIVO<IGW-ID> EN LA TABLA DE ENRUTAMIENTO ASOCIADA A LA SUBRED.

TALENTO TECH

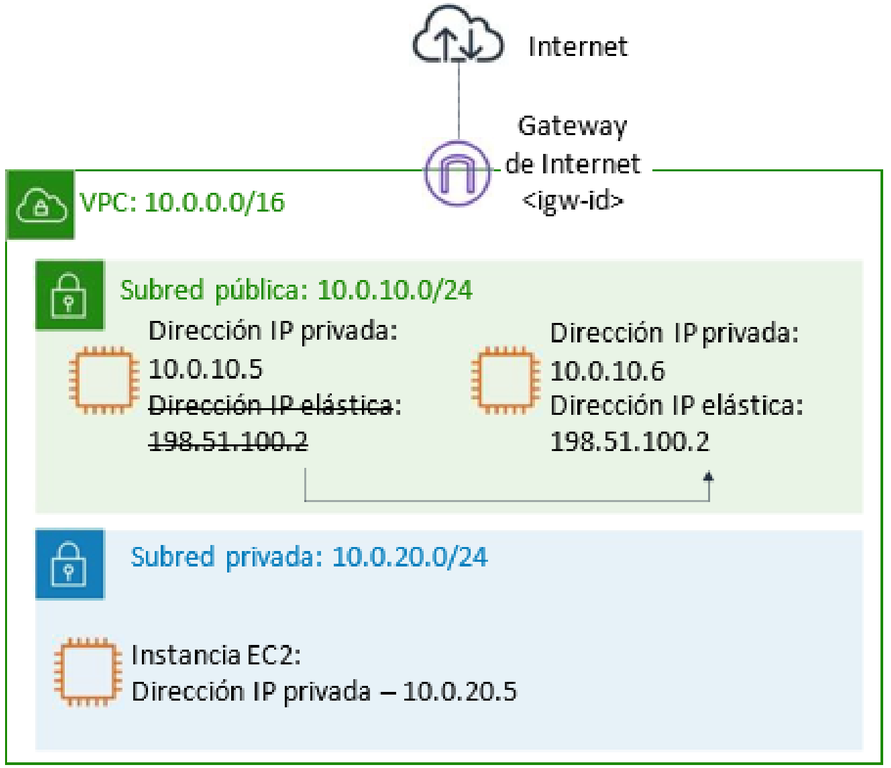
AZ | PROYECTOS EDUCATIVOS

UTP Universidad Tecnológica de Pereira

REASIGNACIÓN DE UNA DIRECCIÓN IP DE UNA INSTANCIA A OTRA

Direcciones IP elásticas

- Son direcciones IPv4 públicas y estáticas que se asocian a su cuenta de AWS.
- Se pueden asociar a una instancia o una interfaz de red elástica.
- Se pueden reasignar a otra instancia en su cuenta.
- Son útiles para la redundancia cuando no se pueden usar los balanceadores de carga.



DESPUÉS DE CONFIGURAR LA CONEXIÓN A INTERNET, ES IMPORTANTE GARANTIZAR QUE TUS INSTANCIAS TENGAN DIRECCIONES IP PÚBLICAS O ELÁSTICAS.

LAS DIRECCIONES IP ELÁSTICAS SON DIRECCIONES IPV4 PÚBLICAS Y ESTÁTICAS DISEÑADAS ESPECÍFICAMENTE PARA ENTORNOS DE COMPUTACIÓN EN LA NUBE DINÁMICA. PUEDES ASOCIAR UNA DIRECCIÓN IP ELÁSTICA A CUALQUIER INSTANCIA O INTERFAZ DE RED ELÁSTICA, INDEPENDIENTEMENTE DE LA VPC DE TU CUENTA. CON UNA DIRECCIÓN IP ELÁSTICA, TIENES LA CAPACIDAD DE SOLUCIONAR RÁPIDAMENTE ERRORES EN LAS INSTANCIAS AL REASIGNAR LA DIRECCIÓN A OTRA INSTANCIA DENTRO DE TU VPC. ASOCIAR UNA DIRECCIÓN IP ELÁSTICA A LA INTERFAZ DE RED TIENE UNA VENTAJA SOBRE ASOCIARLA DIRECTAMENTE A LA INSTANCIA, YA QUE TE PERMITE TRANSFERIR TODOS LOS ATRIBUTOS DE LA INTERFAZ DE RED DE UNA INSTANCIA A OTRA EN UN SOLO PASO.

CONEXIÓN DE SUBREDES PRIVADAS A INTERNET

Gateway NAT

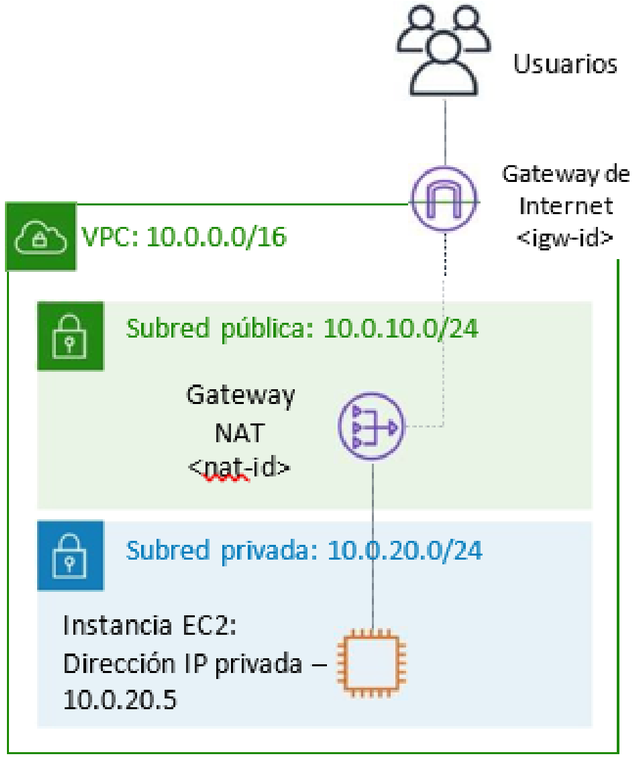
- Permiten que las instancias en una subred privada inicien el tráfico saliente hacia Internet u otros servicios de AWS.
- Impiden que las instancias privadas reciban solicitudes de conexión entrante desde Internet.

Tabla de enrutamiento pública

Destino	Objetivo
10.0.0.0/16	local
0.0.0.0/0	<igw-id>

Tabla de enrutamiento privada

Destino	Objetivo
10.0.0.0/16	local
0.0.0.0/0	<nat-id>



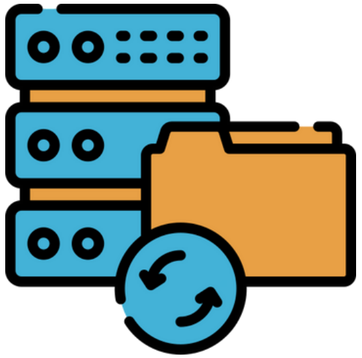
PARA HABILITAR LA CONEXIÓN DE LAS INSTANCIAS EN LA SUBRED PRIVADA A INTERNET O A OTROS SERVICIOS DE AWS, ES NECESARIO CONFIGURAR UNA GATEWAY DE TRADUCCIÓN DE DIRECCIONES DE RED (NAT). ESTA GATEWAY NAT PERMITE QUE LAS INSTANCIAS EN LA SUBRED PRIVADA ACCEDAN A INTERNET Y A OTROS SERVICIOS DE AWS, MIENTRAS QUE AL MISMO TIEMPO IMPIDE QUE INTERNET INICIE CONEXIONES CON ESAS INSTANCIAS.

PARA CREAR UNA GATEWAY NAT, SE DEBE ESPECIFICAR LA SUBRED PÚBLICA DONDE SE UBICARÁ LA GATEWAY. ADEMÁS, ES NECESARIO ASIGNAR UNA DIRECCIÓN IP ELÁSTICA PARA ASOCIARLA A LA GATEWAY NAT. UNA VEZ QUE SE HAYA CREADO LA GATEWAY NAT, ES NECESARIO ACTUALIZAR LA TABLA DE ENRUTAMIENTO ASOCIADA A UNA O MÁS SUBREDES PRIVADAS, PARA QUE EL TRÁFICO DESTINADO A INTERNET SEA DIRIGIDO HACIA LA GATEWAY NAT. DE ESTA MANERA, LAS INSTANCIAS EN LAS SUBREDES PRIVADAS PODRÁN ESTABLECER COMUNICACIÓN CON INTERNET DE FORMA SEGURA Y CONTROLADA.

EJEMPLOS DE CASOS DE USO DE SUBREDES (1 DE 2)

INSTANCIAS DE ALMACÉN DE DATOS

INSTANCIAS DE PROCESAMIENTO POR LOTES



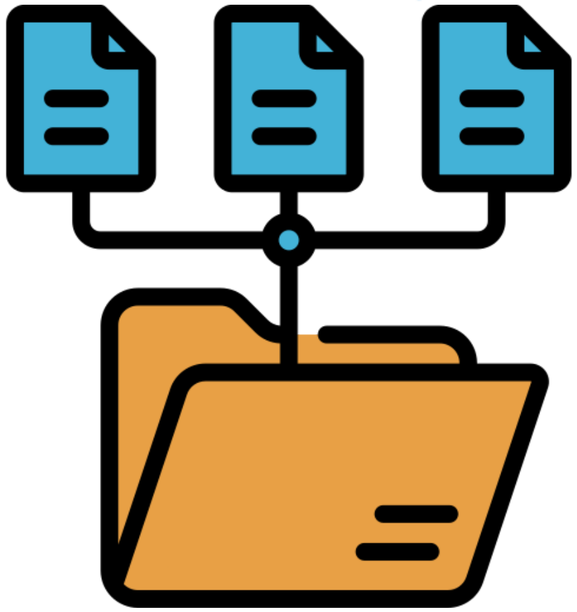
INSTANCIAS DE BACKNED

INSTANCIAS DE APLICACIONES WEB

TÓMATE UN MOMENTO PARA REFLEXIONAR SOBRE SI LAS INSTANCIAS DE ESTOS EJEMPLOS DEBERÍAN SER UBICADAS EN UNA SUBRED PÚBLICA O EN UNA PRIVADA.

EJEMPLOS DE CASOS DE USO DE SUBREDES (2 DE 2)

INSTANCIAS DE ALMACÉN DE DATOS	INSTANCIAS DE PROCESAMIENTO POR LOTES	INSTANCIAS DE BACKNED	INSTANCIAS DE APLICACIONES WEB
SUBRED PRIVADA	SUBRED PRIVADA	SUBRED PRIVADA	SUBRED PÚBLICA Y PRIVADA



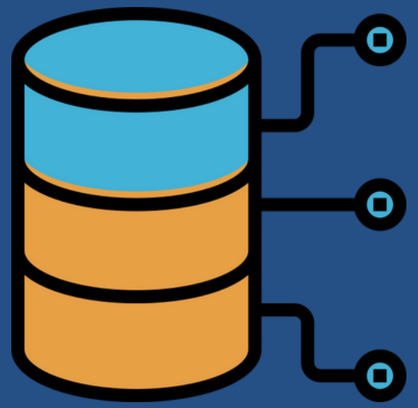
LAS INSTANCIAS DEDICADAS AL ALMACENAMIENTO DE DATOS, PROCESAMIENTO POR LOTES Y BACKEND DEBEN SER UBICADAS EN SUBREDES PRIVADAS. POR OTRO LADO, LAS INSTANCIAS DE LA CAPA WEB PUEDEN SER COLOCADAS EN SUBREDES PÚBLICAS. SIN EMBARGO, SE RECOMIENDA POR PARTE DE AWS QUE LAS INSTANCIAS DE LA CAPA WEB SEAN ALOJADAS DENTRO DE SUBREDES PRIVADAS, UBICADAS DETRÁS DE UN BALANCEADOR DE CARGA QUE SE ENCUENTRE EN UNA SUBRED PÚBLICA. EN CIERTOS ESCENARIOS, ES NECESARIO ASOCIAR DIRECCIONES IP ELÁSTICAS DIRECTAMENTE A LAS INSTANCIAS DE LAS APLICACIONES WEB (AUNQUE TAMBIÉN ES POSIBLE ASOCIAR UNA IP ELÁSTICA A UN BALANCEADOR DE CARGA). EN TALES CASOS, LAS INSTANCIAS DE LAS APLICACIONES WEB DEBEN SER UBICADAS EN SUBREDES PÚBLICAS.

COLOMBIA POTENCIA DE LA VIDA

TIC

SERVIDORES BASTIÓN

SE TRATA DE UN SERVIDOR CUYO PROPÓSITO ES BRINDAR ACCESO A UNA RED PRIVADA DESDE UNA RED EXTERNA.

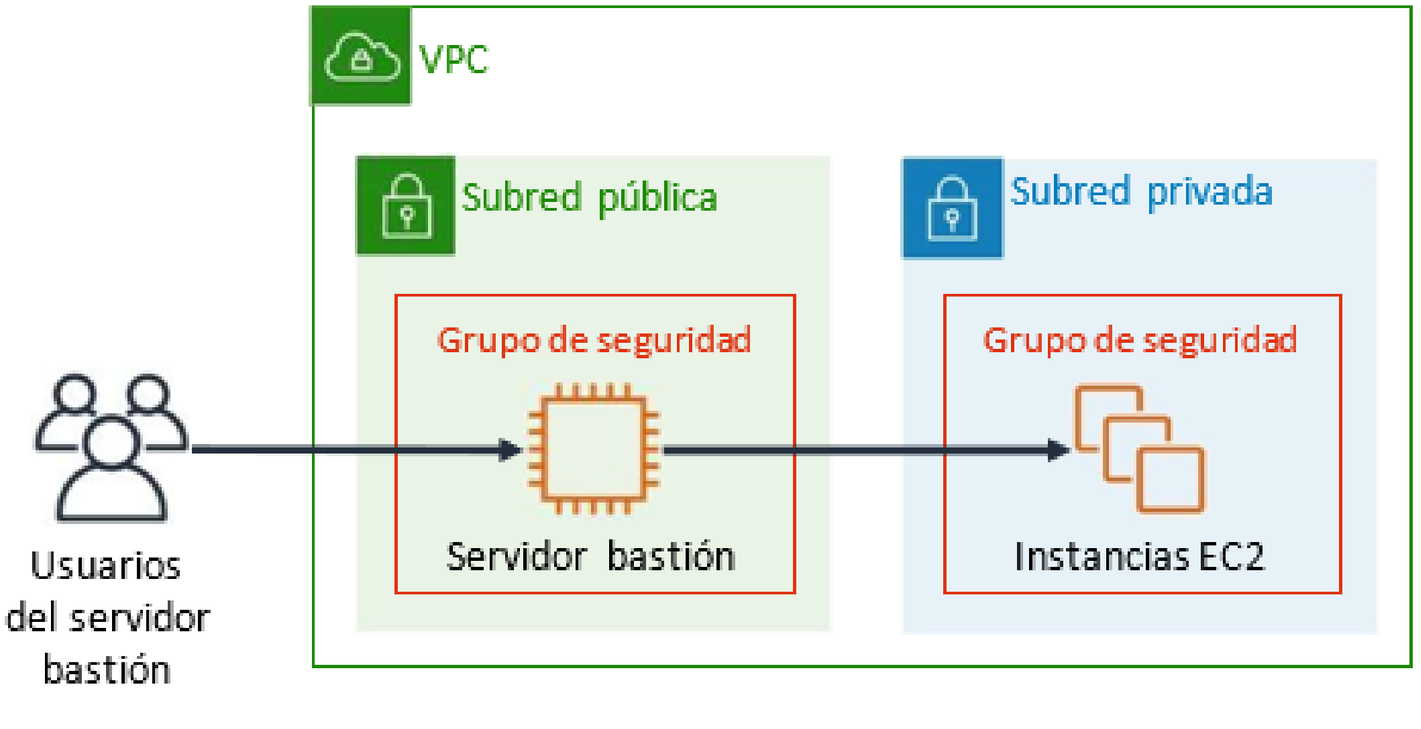


DEBE MINIMIZAR LAS POSIBILIDADES DE INTRUSIÓN.

TALENTO TECH

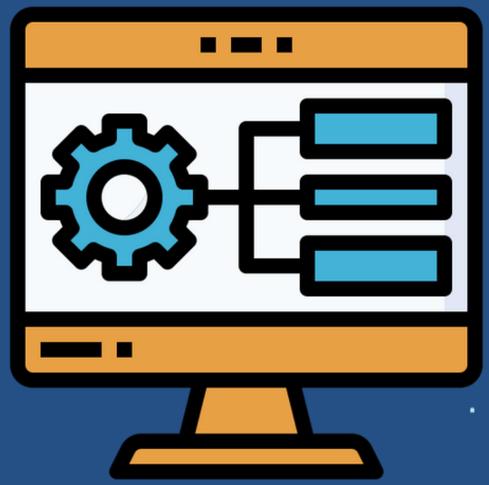
AZ | PROYECTOS EDUCATIVOS

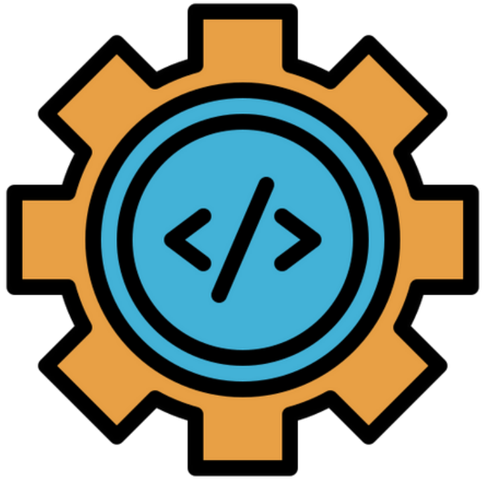
UTP Universidad Tecnológica de Pereira


VPC
Subred pública
Subred privada
Grupo de seguridad
Grupo de seguridad
Usuarios del servidor bastión
Servidor bastión
Instancias EC2

UN SERVIDOR BASTIÓN ES UN SERVIDOR DISEÑADO PARA FACILITAR EL ACCESO A UNA RED PRIVADA DESDE UNA RED EXTERNA, COMO INTERNET. LA FUNCIÓN PRINCIPAL DE UN SERVIDOR BASTIÓN ES REDUCIR EL RIESGO DE INTRUSIÓN Y ATAQUES EN LOS RECURSOS DE LA RED PRIVADA.

POR EJEMPLO, IMAGINEMOS QUE NECESITAS PERMITIR CONEXIONES DESDE UNA RED EXTERNA A INSTANCIAS DE LINUX UBICADAS EN UNA SUBRED PRIVADA DE TU VPC A TRAVÉS DE SECURE SHELL (SSH). EN ESTE CASO, PUEDES EMPLEAR UN SERVIDOR BASTIÓN PARA MITIGAR EL RIESGO ASOCIADO CON ESTAS CONEXIONES EXTERNAS SSH A LAS INSTANCIAS DE LA SUBRED PRIVADA. NORMALMENTE, UN SERVIDOR BASTIÓN SE EJECUTA EN UNA INSTANCIA EC2 UBICADA EN UNA SUBRED PÚBLICA DE LA VPC. LAS INSTANCIAS DE LINUX EN LA SUBRED PRIVADA SE CONFIGURAN CON UN GRUPO DE SEGURIDAD QUE PERMITE EL ACCESO SSH DESDE EL GRUPO DE SEGURIDAD ASOCIADO AL SERVIDOR BASTIÓN. LOS USUARIOS QUE NECESITAN ACCEDER A LAS INSTANCIAS DE LINUX SE CONECTAN PRIMERO AL SERVIDOR BASTIÓN Y LUEGO PUEDEN ESTABLECER CONEXIÓN CON LAS INSTANCIAS DE LINUX.





AUNQUE ESTA ARQUITECTURA PUEDE SER PERSONALIZADA PARA ADAPTARSE A TUS NECESIDADES ESPECÍFICAS, ES IMPORTANTE QUE EL SERVIDOR BASTIÓN SEA LA ÚNICA FUENTE DE TRÁFICO SSH PARA TUS INSTANCIAS DE LINUX, LO QUE AYUDA A MANTENER LA SEGURIDAD DE TU RED.

PARA OBTENER MÁS INFORMACIÓN ACERCA DE ESTA ARQUITECTURA, CONSULTE LA PUBLICACIÓN DE BLOG HOW TO RECORD SSH SESSIONS ESTABLISHED THROUGH A BASTION HOST. SI DESEA APRENDER A IMPLEMENTAR UN SERVIDOR BASTIÓN LINUX EN UN ENTORNO DE VPC EN AWS, COMPLETE SERVIDORES BASTIÓN DE LINUX EN AWS QUICK START.

COLOMBIA POTENCIA DE LA VIDA

TIC

ESTOS SON ALGUNOS DE LOS APRENDIZAJES CLAVE DE ESTA SECCIÓN DEL MÓDULO:

UNA GATEWAY DE INTERNET PERMITE LA COMUNICACIÓN ENTRE INSTANCIAS DE LA VPC E INTERNET.

LAS TABLAS DE ENRUTAMIENTO CONTROLAN EL TRÁFICO DE LA SUBRED O LA GATEWAY.

LAS DIRECCIONES IP ELÁSTICAS SON DIRECCIONES IPV4 PÚBLICAS Y ESTÁTICAS QUE SE PUEDEN ASOCIAR A UNA INSTANCIA O UNA INTERFAZ DE RED ELÁSTICA.

SE PUEDEN REASIGNAR A OTRA INSTANCIA EN SU CUENTA.

LAS GATEWAY NAT PERMITEN QUE LAS INSTANCIAS DE LA SUBRED PRIVADA INICIEN EL TRÁFICO SALIENTE HACIA INTERNET U OTROS SERVICIOS DE AWS.

UN SERVIDOR BASTIÓN ES UN SERVIDOR CUYO PROPÓSITO ES PROPORCIONAR ACCESO A UNA RED PRIVADA DESDE UNA RED EXTERNA, COMO INTERNET.

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

UTP Universidad Tecnológica de Pereira