DigitalHouse>

Certified Tech Developer
The Ultimate Degree

Infraestructura I

VPC en AWS

Funcionamiento

Amazon Virtual Private Cloud (**VPC**) brinda un completo control sobre su entorno de redes virtuales, incluidas la ubicación de los **recursos**, la **conectividad** y la **seguridad**.

El primer paso es crear tu VPC. Luego, se puede agregar recursos, como instancias de Amazon Elastic Compute Cloud (**EC2**) y Amazon Relational Database Service (**RDS**). Por último, podés definir cómo se comunican tus VPC entre sí, entre cuentas, zonas de disponibilidad (**AZ**) o regiones. En este caso, el tráfico de red se comparte entre dos VPC dentro de cada región.

Características de Amazon VPC

Amazon Virtual Private Cloud proporciona características que se pueden utilizar para aumentar y mejorar la seguridad de la nube privada virtual (VPC):

- **Analizador de accesibilidad:** es una herramienta de análisis de configuración estática que permite analizar y depurar la accesibilidad de red entre dos recursos en la VPC. Después de especificar los recursos de destino y origen en la VPC, el analizador de accesibilidad produce detalles salto por salto de la ruta virtual entre ellos cuando son accesibles e identifica el componente que genera un bloqueo cuando no son accesibles.

- **Registros de flujos de la VPC:** puede monitorear los registros de flujo de la VPC entregados a Amazon S3 o Amazon CloudWatch para obtener una visibilidad operativa de las dependencias de red y los patrones de tráfico, detectar anomalías y evitar filtraciones de datos, y solucionar problemas de configuración y conectividad de la red. Los metadatos enriquecidos de los registros de flujo ayudan a adquirir información adicional sobre quién inició las conexiones TCP, así como el destino y el

origen reales a nivel de paquete para el tráfico que fluye a través de capas intermedias, como la gateway de NAT. También puede archivar los registros de flujo para ayudar a cumplir ciertos requisitos de conformidad.

- **Replicación de tráfico de VPC:** la replicación de tráfico de VPC permite copiar el tráfico de red de una interfaz de red elástica de instancias de Amazon EC2 y, tras ello, enviar el tráfico a dispositivos de monitoreo y seguridad fuera de banda para la inspección profunda de paquetes. Con la replicación de tráfico de VPC, se puede detectar anomalías de seguridad y de red, obtener información operativa, implementar controles de seguridad y conformidad, y solucionar problemas. La replicación de tráfico de VPC es una característica que proporciona acceso directo a los paquetes de red que fluyen a través de la VPC.

- **Direccionamiento de entrada:** esto permite dirigir todo el tráfico de entrada y de salida que fluye a/desde un gateway de Internet (**IGW**) o gateway privada virtual (VGW) a la interfaz de red elástica de una instancia de EC2 específica. Con esta característica, se puede configurar una nube privada virtual para enviar todo el tráfico a una IGW, una VGW o la instancia de EC2 antes de que el tráfico alcance las cargas de trabajo empresariales.

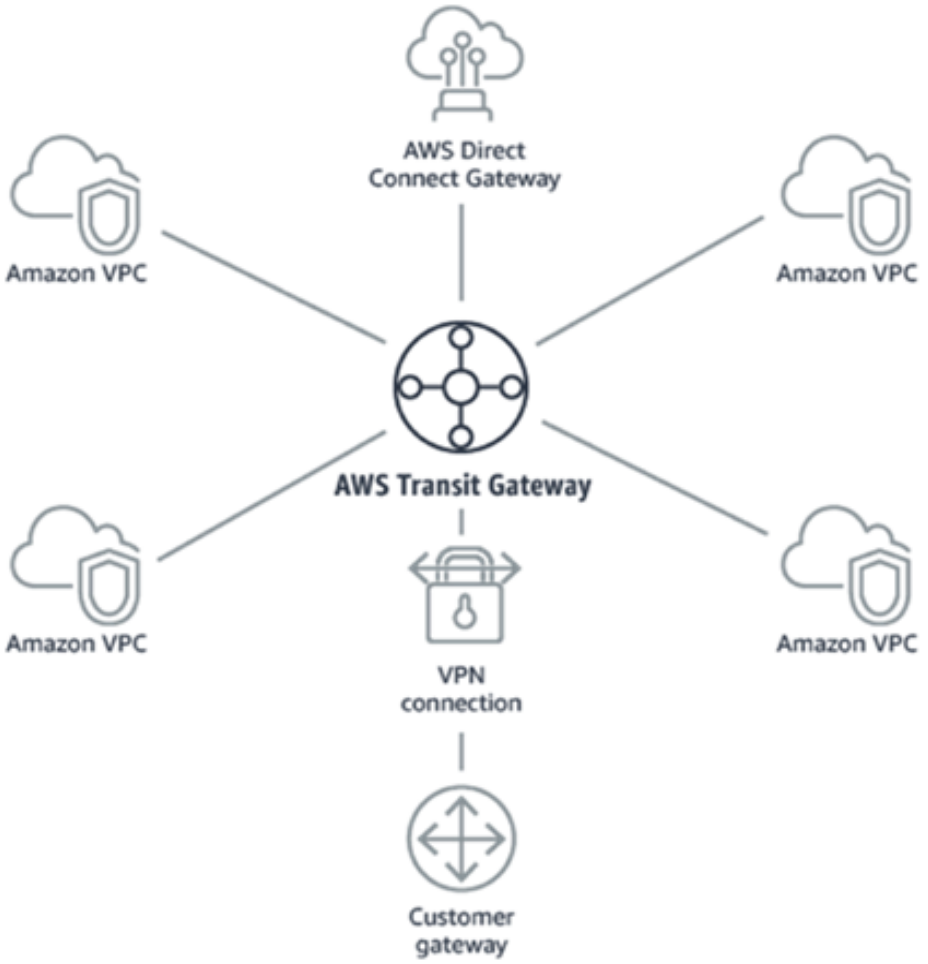
- **Grupos de seguridad:** los grupos de seguridad funcionan como un firewall para instancias de Amazon EC2 asociadas. Controlan el tráfico de entrada y de salida a nivel de instancia. Al lanzar una instancia, se la puede asociar a uno o más grupos de seguridad creados. Cada instancia dentro de la VPC puede pertenecer a un conjunto diferente de grupos de seguridad. Si no se especifica un grupo de seguridad al lanzar la instancia, esta se asocia automáticamente al grupo de seguridad predeterminado de la VPC.

- **Lista de control de acceso de red:** una lista de control de acceso (**ACL**) de red es una capa de seguridad opcional para la VPC que actúa como un firewall para controlar el tráfico entrante y saliente de una o más subredes. Se puede configurar ACL de red con reglas similares a las de los grupos de seguridad para agregar una capa de seguridad adicional a la VPC.

Uso de otros recursos de AWS con Amazon VPC

Hay varios recursos que se pueden utilizar con la nube privada virtual (VPC):

❖ **AWS Transit Gateway:** permite conectar fácilmente las VPC de Amazon, las cuentas de AWS y las redes en las instalaciones a una única gateway.



Optimiza la VPC y hace fácilmente escalable la infraestructura. Dirige todo el tráfico de cada VPC o VPN y le brinda un lugar para monitorear.

❖ **AWS Private Link:** sirve para establecer conectividad privada entre las VPC y los servicios alojados en AWS o en las instalaciones, sin exponer los datos a Internet.

❖ **AWS Network Firewall:** permite implementar seguridad en las redes en las VPC de Amazon de manera sencilla y clara.

❖ **AWS VPN:** posibilita extender las redes en las instalaciones a la nube y acceder a ellas de forma segura desde cualquier lugar:

- **AWS Client VPN:** es un servicio de VPN completamente administrado y elástico que aumenta o disminuye automáticamente en función de sus requisitos. Debido a que es una solución de VPN en la nube, no necesita instalar y administrar soluciones basadas en hardware o software, ni intentar estimar cuántos usuarios remotos puede admitir a la vez.

- **AWS Site-to-Site VPN:** crea una conexión segura entre su centro de datos o sucursal y sus recursos de la nube de AWS. Para aplicaciones distribuidas globalmente, la opción Accelerated Site-to-Site VPN proporciona un rendimiento todavía mayor gracias al funcionamiento con AWS Global Accelerator.

❖ **Gateway de traducción de direcciones de red (NAT):** proporciona que las cargas de trabajo de la subred privada de la VPC obtengan acceso a Internet, a la vez que evita que Internet inicialice una conexión con esas instancias.

Conclusión

La declaración de la misión de Amazon establece que concentran sus esfuerzos en "**ofrecer a nuestros clientes los precios más bajos posibles, la mejor selección disponible y la mayor comodidad**". La visión no puede estar más clara y, por eso, trabaja para convertirse en "**la compañía más centrada en el cliente del mundo**".

Teniendo en cuenta estos valores, son unos de los proveedores de cloud más elegidos por las empresas para montar su infraestructura. Estos servicios nos ofrecen una mayor seguridad en nuestra VPC, facilitan el acceso y despliegue de la misma.