Nadia Arellano González
Actividad Módulo 3- Sesión 4

Caso: Imagina que eres el administrador de redes de una empresa llamada TechSecure, la cual necesita conectar su red local en la oficina principal con su infraestructura en AWS. Además, algunos empleados trabajan de forma remota, por lo que es necesario habilitar un acceso seguro para ellos.

Requerimientos técnicos:

1. **Conexión Segura entre la Red Local y AWS**

   Para comenzar, en la consola de AWS, accedí al servicio Virtual Private Network (VPN) y creé un VPN Gateway, que representa el extremo en la nube. Luego configuré un Customer Gateway, que representa el extremo en la red local de TechSecure, indicando su IP pública estática. Ambos extremos fueron enlazados mediante una conexión VPN, la cual se establece automáticamente una vez que ambas configuraciones están activas y los parámetros coinciden.

   Durante la configuración, definí los parámetros clave del túnel IPSec:

   - **Método de cifrado:** utilicé AES-256, un estándar robusto que garantiza que los datos sean ilegibles para terceros.
   - **Autenticación:** se aplicó SHA-256 como algoritmo hash para verificar la integridad de los datos, y el uso de claves compartidas (pre-shared keys) para autenticar ambos extremos.
   - **Fase de IKE:** configurada para negociar los métodos de seguridad.
   - **Protocolos utilizados:** se habilitaron ESP (Encapsulating Security Payload) para cifrar el contenido de los paquetes, y AH (Authentication Header) para verificar su autenticidad.

   En cuanto a la red, configuré una **VPC en AWS** con subredes privadas y públicas, asegurándome de que las rutas entre la red local y la subred privada de AWS estuvieran correctamente definidas en las tablas de ruteo. Así, el tráfico entre ambos entornos fluye de manera cifrada, confiable y segura, cumpliendo con los estándares corporativos de seguridad de TechSecure.

2. **Acceso Remoto para Empleados**

   Desde la consola de AWS, accedí al servicio Client VPN y creé una nueva conexión, asociándola a la VPC previamente configurada. Como parte de esta configuración, generé un archivo de configuración OpenVPN (.ovpn), el cual se distribuirá a cada empleado autorizado para que puedan conectarse desde sus dispositivos.

   Para la autenticación de los usuarios remotos, opté por el método basado en certificados gestionados mediante AWS Certificate Manager (ACM), garantizando que solo los dispositivos que cuenten con un certificado válido puedan acceder a la red. Este método se complementa con la autenticación de usuarios a través de Active Directory (AWS Directory Service), lo que permite aplicar controles adicionales como autenticación multifactor (MFA) y políticas de grupo.

3. **Protocolos de Seguridad**

   En ambos escenarios —el túnel IPSec VPN y el Client VPN— utilicé como protocolo de cifrado el estándar AES-256 (Advanced Encryption Standard), que proporciona un alto nivel de seguridad al cifrar los datos antes de su transmisión. Este algoritmo es resistente a ataques de fuerza bruta y es recomendado por organismos internacionales de ciberseguridad. Además, para asegurar la integridad de los datos durante el transporte, apliqué SHA-256 (Secure Hash Algorithm 256 bits) como función hash. Esto permite detectar cualquier alteración del contenido transmitido.

   Respecto a la autenticación de usuarios y dispositivos, para la conexión IPSec VPN entre la red local y AWS utilicé pre-shared keys (PSK) combinadas con autenticación basada en certificados. En el caso del acceso remoto mediante Client VPN, implementé AWS Directory Service con Active Directory, permitiendo así que los usuarios se autentiquen con sus credenciales corporativas. Esta integración facilita además la aplicación de políticas de acceso, autenticación multifactor (MFA) y gestión centralizada de permisos.

El siguiente diagrama **(Imagen_1)** representa la arquitectura de red propuesta para la empresa TechSecure, integrando una conexión segura entre la red local de la oficina principal y la infraestructura en AWS mediante un túnel IPSEC VPN, junto con el acceso remoto de empleados a través de un Client VPN.

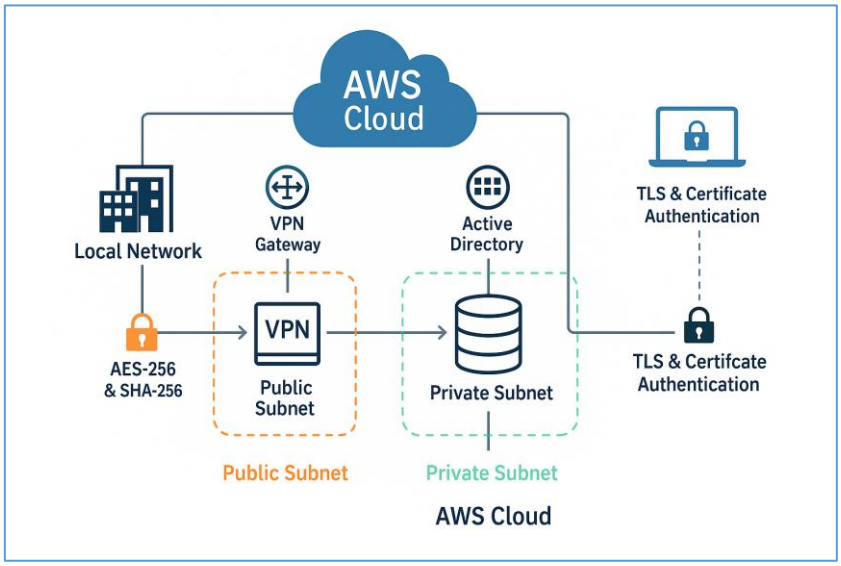

Imagen_1: Diagrama de la red que muestra la estructura propuesta.