Nombre de la materia:
Fundamento de telecomunicaciones

Nombre de la licenciatura:
SISTEMAS COMPUTACIONALES

Nombre del alumno(a):
ALAN GERARDO GIJON AGOSTO

Número de control:
18530390

Nombre de la tarea: Investigación (SIEM)

Unidad #: nombre de la unidad:

Nombre del profesor(a):
ING. ISMAEL JIMENEZ SANCHEZ

Fecha:

AWS VPN

Una VPN típica puede tener una red de área local (LAN) principal en la sede central corporativa de una empresa, otras LAN en oficinas o instalaciones remotas, y usuarios individuales que se conectan desde el campo.

Una VPN es una red privada que utiliza una red pública (por lo general, Internet) para conectar sitios o usuarios remotos entre sí. En vez de utilizar una conexión real dedicada como línea arrendada, una VPN utiliza conexiones "virtuales" enrutadas a través de Internet desde la red privada de la empresa hacia el empleado o el sitio remoto.

¿Qué constituye una VPN?

Hay dos tipos de VPN comunes.

- Acceso remoto: también denominada Red telefónica privada virtual (VPDN), se trata de una conexión de usuario a LAN utilizada por una empresa que posee empleados que necesitan conectarse a la red privada desde distintas ubicaciones remotas. Normalmente, una empresa que desea configurar una VPN de acceso remoto grande proporciona algún tipo de cuenta telefónica de Internet a sus usuarios mediante un proveedor de servicios de Internet (ISP). Luego, los teletrabajadores pueden marcar un número 1-800 para conectarse a Internet y usar su software de cliente VPN para acceder a la red corporativa. Un buen ejemplo de una empresa que necesita una VPN de acceso remoto sería una firma grande con cientos de miembros del personal de ventas en el campo. Las VPN de acceso remoto permiten conexiones seguras y cifradas entre la red privada de una empresa y los usuarios remotos a través de un proveedor de servicios de terceros.

- Sitio a sitio: mediante el uso de equipos exclusivos y cifrados a gran escala, una empresa puede conectar varios sitios fijos a través de una red pública como Internet. Cada sitio solo necesita una conexión local a la misma red pública, lo cual ahorra dinero en extensas líneas arrendadas privadas. Las VPN de sitio a sitio también se pueden clasificar en intranets o extranets. Una VPN de sitio a sitio desarrollada entre oficinas de la misma empresa se denomina VPN intranet, mientras que una VPN desarrollada para conectar la empresa con su partner o cliente se denomina VPN extranet.

Una VPN bien diseñada puede beneficiar mucho a una empresa. Por ejemplo, puede:

- Ampliar la conectividad geográfica

- Reducir costos operativos en relación a WAN tradicionales
- Reducir los tiempos de tránsito y los costos de viaje de usuarios remotos
- Mejorar la productividad
- Simplificar la topología de la red
- Proporcionar oportunidades de redes globales
- Proporcionar soporte para el tele trabajador
- Proporcionar un Retorno de la inversión (ROI) más rápido que la WAN tradicional

Un dispositivo de gateway de cliente es un dispositivo físico o de software que usted posee o administra en la red local (en su extremo de una conexión de Site-to-Site VPN). Usted o el administrador de red tienen que configurar el dispositivo para que funcione con la conexión de Site-to-Site VPN.

En el siguiente diagrama se muestra su red, el dispositivo de gateway de cliente y la conexión de VPN que va a una gateway privada virtual (asociada a su VPC). Las dos líneas entre el dispositivo de gateway de cliente y la gateway privada virtual representan los túneles para la conexión de VPN. Si se produce un error del dispositivo en AWS, su conexión de VPN cambiará automáticamente al segundo túnel para que su acceso no se vea interrumpido. Cada cierto tiempo, AWS también lleva a cabo un mantenimiento rutinario en la conexión de VPN, lo que podría desactivar uno de los dos túneles de la conexión de VPN durante un breve periodo de tiempo. Para obtener más información, consulte Sustitución de los puntos de enlace de un túnel de Site-to-Site VPN. Por lo tanto, al configurar el dispositivo de gateway de cliente, es importante que configure ambos túneles.

Si desea ver los pasos necesarios para configurar una conexión de VPN, consulte Introducción. Durante este proceso, tiene que crear un recurso de gateway de cliente en AWS que proporciona información a AWS sobre el dispositivo, como la dirección IP pública. Para obtener más información, consulte Opciones de la gateway de cliente para su conexión de Site-to-Site VPN. El recurso de gateway de cliente en AWS no configura ni crea el dispositivo de gateway de cliente. Debe configurar el dispositivo usted mismo.

Después de crear la conexión de VPN, descargue el archivo de configuración de la consola de Amazon VPC, que contiene información específica sobre la conexión de VPN. Utilice esta información para configurar el dispositivo de gateway de cliente. En algunos casos, hay archivos de configuración específicos del dispositivo disponibles para los dispositivos que hemos probado. De lo contrario, puede descargar el archivo de configuración genérico.

Bibliografía:

https://www.cisco.com/c/es_mx/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14106-how-vpn-works.html

https://docs.aws.amazon.com/es_es/vpn/latest/s2svpn/your-cgw.html