REDES PRIVADAS VIRTUALES

Una VPN permite extender una red privada a través de una red publica como internet. Permite que los usuarios puedan enviar y recibir datos en redes compartidas o publicas como si sus dispositivos estuvieran directamente conectados a la red privada. Esto asegura protección a los datos.

**Túneles.** Los VPN crean túneles entre el dispositivo del usuario y el servido de la red privada, toda la información que pasa, es a través de ese túnel que este encriptado.

**Cifrado.** Asegura que los datos no puedan ser leídos por terceros.

**Autenticación.** Como contraseñas, certificados digitales, tokens, etc. Para verificar que solo usuarios autorizados accedan a la VPN.

TIPOS DE VPNs

VPN de acceso remoto. Conectarse de manera remota a una red privada, es muy usada en entornos corporativos.

VPN de sitio a sitio. Conecta dos o mas redes físicas, permitiendo que distintos sitios de una organización se comuniquen como si estuviesen en la misma red (oficinas en diferentes ubicaciones geográficas).

Protocolos de VPNs.

Ipsec. Para proteger las VPN de sitio a sitio y en ocasiones también en las VPN de acceso remoto. Proporciona autenticación y cifrado de datos, se compone de protocolos AH y ESP.

SSL/TLS. Utilizando principalmente VPNs de acceso remoto, permite conexiones seguras a través de un navegador web.

L2TP y PPTP. Son mas antiguos y se usan en entornos específicos. L2TP se combina con Ipsec para mejorar la seguridad.

Topologías de VPN.

Topología Hub-and-Spoke (Estrella). Varias sucursales (spokes) están coenctadas a una sede central (hub). Las conexiones son centralizadas.

To;pologia Full-Mesh. Red telaraña que todos los sitios tienen conectividad con todos los sitios, aumenta su complejidad.

Hibrida: Combina hub-and-spoke y full-mesh. Se tiene una central conectada todos contra todos, la sucursal se conecta con la más cerca o dependiendo de la necesidad. Equilibra eficiencia y complejidad.

VENTAJAS DE USO Y ADMINISTRACION DE VPNs

Seguridad de Redes públicas. Las VPNs protegen la información transmitida a través de redes publicas como Internet, al encriptar los datos. Blindar a la información y asegura que va por un camino seguro.

Acceso remoto seguro. Permite que los empleados accedan de forma segura a la red corporativa desde cualquier lugar.

Reducción de costos. Eliminan la necesidad de enlaces privados dedicados como líneas arrendadas, se reducen los costos considerablemente.

Flexibilidad en la administración de redes. Se deben añadir routers (una estructura) que facilite la comunicación entre oficinas, mejorando la eficiencia.

REDES DE ALTA DISPONIBILIDAD.

Es la capacidad de una red para garantizar un tiempo de actividad continuo incluso en presencia de fallos o interrupciones.

Componentes de redes de alta disponibilidad.

Redundancia.

Implica tener dispositivos, enlaces y sistemas duplicados o alternativos que toman el control si uno falla.

Failover. Mecanismo para cambiar automáticamente a un sistema secundario cuando el principal falla.

Resiliencia. Capacidad de un sistema para recuperarse rápidamente después de un fallo.

Etherchannel. Permite agrupar varios enlaces físicos Erhernet dentro dos dispositivos en un único enlace lógico.

Diseñado para mejorar el ancho de banda reduciendo la escalabilidad.