

Conexiones remotas

Alexys Gomez Elizalde

Investigación

Para esta tarea decidí preguntarle a copilot y chatgpt por empresas que usan vpn para sus actividades con el prompt: "dame ejemplos de empresas que usen vpn", ambas coincidieron en Google, Microsoft, Apple y Amazon. No me gustaron sus resultados así que decidí preguntar con más dando este prompt "puedes ayudarme con otras empresas y que tipo de vpns ocupan(acceso remoto, punto a punto o interna)" para especificar más el tema y dar más contexto de mi búsqueda. Estos fueron los resultados:

- **Copilot:**

¡Claro! Las empresas utilizan diferentes tipos de VPNs según sus necesidades específicas. Aquí te doy ejemplos de los tipos de VPN que podrían usar las empresas mencionadas:

- Google: Acceso remoto: Para permitir que sus empleados accedan de manera segura a los recursos internos desde cualquier lugar del mundo.
- Microsoft: Acceso remoto: Para proteger las comunicaciones y los datos de sus empleados que trabajan de forma remota. VPN interna: Para asegurar la comunicación dentro de sus oficinas y centros de datos.
- Apple: Acceso remoto: Para que los empleados puedan acceder a la red interna de la empresa de manera segura desde ubicaciones remotas.
- JPMorgan Chase: Acceso remoto: Para proteger las transacciones y la información sensible de sus clientes. Punto a punto: Para conectar de manera segura sus diferentes sucursales y oficinas.
- Deloitte: Acceso remoto: Para garantizar que los datos de sus clientes se mantengan seguros durante el acceso remoto y las transferencias de información.
- AT&T: VPN interna: Para gestionar y proteger sus redes internas y las comunicaciones de sus empleados. Punto a punto: Para conectar sus diversas instalaciones y centros de datos de manera segura.

Cada tipo de VPN tiene sus propias ventajas y se elige en función de las necesidades específicas de la empresa, como la seguridad, la accesibilidad y la gestión de datos.

¿Te gustaría más información sobre cómo implementar alguno de estos tipos de VPN en tu empresa?

- **Chatgpt:**

Muchas empresas utilizan diferentes tipos de VPN dependiendo de sus necesidades específicas. Aquí te dejo algunos ejemplos de empresas reconocidas y los tipos de VPN que utilizan:

1. Google

Tipo de VPN: Acceso remoto y Zero Trust

Detalles: Google utiliza un enfoque llamado BeyondCorp, que elimina el uso de VPN tradicionales para empleados remotos y adopta un modelo Zero Trust. En lugar de una VPN punto a punto, BeyondCorp permite a los empleados acceder a los recursos de la empresa de manera segura desde cualquier ubicación sin necesidad de pasar por una VPN tradicional. Utilizan una combinación de herramientas de acceso seguro, autenticación fuerte, y políticas basadas en el contexto del usuario.

2. Microsoft

Tipo de VPN: Acceso remoto y SASE

Detalles: Microsoft ofrece su propia solución de VPN con Azure VPN Gateway, que permite conectividad segura desde ubicaciones remotas a la infraestructura en la nube de Azure. Esto

se combina con la plataforma Microsoft Defender for Identity para implementar un enfoque de Zero Trust, verificando la identidad de los usuarios y asegurando el acceso a los recursos solo a través de autenticación multifactor y políticas de control de acceso basadas en roles.

3. Amazon (AWS)

Tipo de VPN: Punto a punto (site-to-site) y Acceso remoto

Detalles: Amazon Web Services (AWS) ofrece AWS Client VPN, una solución de acceso remoto que permite a los empleados conectarse de forma segura a la infraestructura de la empresa en la nube. Además, AWS utiliza AWS Site-to-Site VPN para conectividad entre centros de datos locales y sus servicios en la nube, lo que permite un acceso seguro y cifrado entre redes distribuidas geográficamente.

4. Netflix

Tipo de VPN: Acceso remoto y SASE

Detalles: Netflix adoptó un enfoque de Zero Trust con soluciones de acceso remoto para sus empleados y contratistas, especialmente para aquellos que trabajan en producción y postproducción. Utilizan VPN basadas en la nube para garantizar que el acceso a su infraestructura de TI sea seguro, especialmente dado que gran parte de su equipo trabaja en proyectos desde diferentes ubicaciones geográficas.

5. IBM

Tipo de VPN: Acceso remoto y Punto a punto (site-to-site)

Detalles: IBM ofrece soluciones de VPN empresarial para sus empleados y clientes. Utilizan IBM Cloud VPN para acceso remoto, lo que permite a los empleados acceder a las aplicaciones y datos de la empresa de manera segura. También ofrecen soluciones de site-to-site VPN para interconectar redes locales con la nube de IBM.

6. Facebook (Meta)

Tipo de VPN: Acceso remoto

Detalles: Facebook utiliza una combinación de herramientas de seguridad, incluyendo VPN de acceso remoto para proteger los datos de los empleados que trabajan desde casa o en ubicaciones remotas. Implementan soluciones avanzadas de Zero Trust y autenticación multifactor para garantizar que las conexiones sean seguras.

7. Tesla

Tipo de VPN: Acceso remoto

Detalles: Tesla utiliza una combinación de acceso remoto y soluciones VPN para permitir que sus empleados accedan de forma segura a los sistemas de producción y datos sensibles desde cualquier lugar. Tesla es conocida por su adopción de soluciones de seguridad robustas, incluyendo VPN con autenticación de múltiples factores.

Estas empresas demuestran cómo las grandes organizaciones usan una combinación de tecnologías de VPN y enfoques avanzados de seguridad como Zero Trust para proteger sus redes y recursos en diferentes escenarios de trabajo remoto o acceso desde múltiples ubicaciones. Cada organización adapta sus herramientas de seguridad según sus necesidades y arquitectura de red.

Conclusiones

Aunque muchas compañías implementan soluciones similares, como el acceso remoto o VPN punto a punto, también existe una tendencia hacia el uso de tecnologías más nuevas como Zero Trust. Esto sugiere que la seguridad y la flexibilidad son factores cruciales en la elección de VPN, permitiendo a las organizaciones proteger sus datos. Esta diversidad en las estrategias adoptadas por grandes empresas como Google, Microsoft, Amazon, y otras, muestra cómo cada organización adapta su infraestructura de seguridad según sus necesidades específicas, lo que remarca la importancia de una planificación cuidadosa al implementar estas soluciones en cualquier entorno empresarial.