Trey Research Corporation

Redes privadas virtuales: información general técnica para Fabrikam, Inc.

15 de diciembre de 2023

Las redes privadas virtuales (VPN) son una solución de seguridad de red popular que puede ayudar a cifrar el tráfico de red. Las VPN funcionan como un túnel seguro y cifran el tráfico de Internet, lo que dificulta que terceros supervisen las actividades y roben datos.[1].

Ventajas de implementar VPN:

- Las VPN ofrecen una capa de privacidad y seguridad al cifrar el tráfico de Internet. Esto dificulta que terceros supervisen las actividades y roben datos.
- Las VPN pueden ayudar a evitar pirateos al utilizar la Wi-Fi pública en un aeropuerto o en la biblioteca. Esto se debe a que las VPN funcionan como un túnel seguro y cifran el tráfico de Internet.
- Las VPN pueden evitar que su proveedor de servicios de Internet sepa qué sitios ha visitado, ya que el tráfico que entra y sale de su equipo viaja por los servidores de la VPN o los servidores que las VPN pagan por utilizar[1].
- Las VPN pueden evitar las restricciones geográficas al contenido [2] al enmascarar su dirección IP y cifrar su conexión a Internet. Al conectarse a un servidor VPN, su tráfico de Internet se enruta mediante el servidor VPN, que le asigna una nueva dirección IP. Esto hace que parezca que accede a Internet desde una ubicación diferente, lo que le permite evitar las restricciones geográficas al contenido

Inconvenientes de implementar VPN:

- La velocidad de la conexión puede ser más lenta que la de su ISP. Esto se debe a que las VPN agregan una capa adicional de cifrado y enrutamiento a su tráfico de Internet [2].
- El uso de VPN está prohibido en algunos países autoritarios. En algunos países, las VPN están prohibidas o muy reguladas [2].
- Utilizar VPN gratis genera el riesgo de exposición a anuncios, malware y filtraciones. Puede que las VPN gratis vendan los datos del usuario a anunciantes de terceros o inserten anuncios en páginas web [2].

Detalles específicos de la instalación:

- Una VPN establece un túnel cifrado entre el sistema que ejecuta el cliente VPN y un servidor VPN que, posteriormente, autoriza el tráfico mediante el túnel al resto de la red empresarial [4]. Se incluyen los siguientes pasos:

    1. Se instala un cliente VPN en el dispositivo del usuario, que cifra todo el tráfico entre el dispositivo y el servidor VPN.
    2. El servidor VPN descifra el tráfico y lo reenvía al destino previsto.
    3. El servidor de destino responde a la solicitud al enviar el tráfico de vuelta al servidor VPN.
    4. El servidor VPN cifra el tráfico y lo envía de vuelta al cliente VPN.
    5. El cliente VPN descifra el tráfico y lo envía al dispositivo del usuario [1].

- Para instalar y configurar un servidor VPN, siga estos pasos:
    1. Crear un perfil VPN en su equipo.
    2. Hacer clic en iniciar y luego en Configuración para abrir el menú de configuración.
    3. En el menú de configuración, hacer clic en Red e Internet y luego en VPN.
    4. Seleccionar Agregar una conexión VPN.
    5. En la ventana Agregar una conexión VPN, debe realizar algunas tareas.
    6. Guardar los cambios realizados [5].

Riesgos y mitigaciones:

- Los atacantes saben que el trabajo remoto es un vector de amenaza desde hace tiempo. El entorno de trabajo remoto es especialmente atractivo para los atacantes por diversos motivos. En primer lugar, el entorno de la red doméstica no se administra de forma profesional. Esto significa que muchos más sistemas

en redes domésticas no reciben revisiones con regularidad y muchos de ellos están anticuados respecto a la mitigación de vulnerabilidades. Para persistir en una red empresarial, el atacante que ha vulnerado el sistema debe evitar la detección y resistir la corrección. Aquí también, la red doméstica ayuda al atacante. La detección de amenazas está casi ausente y la corrección es fortuita, como cuando se reinstala o retira un equipo porque funciona lento. Para proteger el entorno de trabajo remoto, es fundamental ampliar todavía más las hipótesis de confianza cero. No solo se debe asumir que la red es hostil, sino todo lo que no está bajo el control de la empresa [4].
- Actualizar las VPN, los dispositivos de infraestructura de red y los dispositivos que se utilizan en los entornos de trabajo remoto con las últimas revisiones de software y configuraciones de seguridad [6].

Procedimientos recomendados para la implementación:

Los procedimientos recomendados para implementar VPN en una red corporativa incluyen los siguientes:

- Seleccionar una VPN basada en estándares que utilice estándares aceptados, como intercambio de claves por red/protocolo de seguridad de Internet (IKE/IPSec), que suelen ser menos peligrosos y más seguros que las VPN de capas de sockets seguros/seguridad de la capa de transporte (SSL/TLS), que utilizan código personalizado para enviar tráfico mediante TLS [12].
- Utilizar una VPN con criptografía sólida. Validar que los algoritmos de cifrado, algoritmos de autenticación y los protocolos que utiliza una VPN sean sólidos y validados para FIP. Configurar todas las VPN para que utilicen la autenticación multifactor (MFA) y reemplazar la autenticación basada en contraseñas con la autenticación de cliente mediante certificados digitales (almacenados en tarjetas inteligentes) cuando sea posible[12].
- Administrar las vulnerabilidades de software. La explotación de las vulnerabilidades de VPN es un vector de ataque común para los ciberdelincuentes. Seleccionar un proveedor de VPN con un historial sólido de revisiones de vulnerabilidades y solicitar una lista de materiales de software (SBOM) para validar que el código de terceros esté actualizado y sea seguro. Además, buscar un producto que pueda realizar la validación de su código al ejecutarse para detectar posibles intrusiones. Tras implementar una VPN, compruebe con regularidad y aplique sin demora las actualizaciones de software [12].
- Prepararse para las sobrecargas de uso. El personal de seguridad de TI debe probar las limitaciones de las VPN para prepararse para un uso masivo [2].

- Evitar las VPN gratis. Utilizar VPN gratis genera el riesgo de exposición a anuncios, malware y filtraciones [3].