**ANEXO II**

**Práctica 2: Configuración de una VPN con OpenVPN.**

**Trabajo preparatorio**

* **Consultar que es una VPN, su funcionalidad y los protocolos VPN más comunes.**

Una VPN es una tecnología que establece una conexión segura y cifrada a través de una red pública como Internet, asegurando la privacidad y la protección de los datos transmitidos. Permite a los usuarios navegar de forma anónima y acceder a recursos de manera remota, garantizando tanto la seguridad como la funcionalidad. [41]

**Funcionalidades Principales de una VPN:**

* Cifrado de Datos: Protege la información transmitida mediante el uso de cifrado, evitando que terceros puedan interceptar los datos.
* Ocultación de la Dirección IP: Reemplaza la dirección IP del usuario con la del servidor VPN, garantizando anonimato en línea.
* Acceso a Contenido Restringido: Permite superar bloqueos geográficos y restricciones regionales, facilitando el acceso a contenido censurado o limitado.
* Conexión Remota Segura: Facilita el acceso seguro a redes privadas, especialmente útiles para el teletrabajo y la colaboración remota.

**Protocolos VPN Más Utilizados:**

* OpenVPN: Protocolo de código abierto conocido por su flexibilidad y alta seguridad. Utiliza cifrado avanzado y es compatible con diversas plataformas.
* WireGuard: Protocolo moderno enfocado en la velocidad y simplicidad. Ofrece rendimiento superior y utiliza criptografía avanzada, aunque aún se encuentra en desarrollo en algunos entornos. [42]
* IKEv2/IPSec: Destaca por su capacidad de reconectar rápidamente en caso de interrupciones, ideal para dispositivos móviles que alternan entre redes Wi-Fi y datos móviles.[42]
* L2TP/IPSec: Combina el protocolo L2TP con IPsec para ofrecer una conexión segura, aunque puede ser más lento debido al doble encapsulamiento de datos. [42]
* PPTP (Protocolo de Túnel Punto a Punto): Uno de los protocolos más antiguos. Aunque es rápido, presenta vulnerabilidades importantes y un cifrado débil, por lo que no se recomienda para aplicaciones de alta seguridad. [42]
* SSTP (Protocolo de Túnel de Socket Seguro): Desarrollado por Microsoft, ofrece buena seguridad y está integrado en sistemas Windows. Sin embargo, al ser de código cerrado, limita la transparencia y la posibilidad de auditorías externas. [42]

**Escribir un breve resumen sobre OpenVPN y las ventajas que posee ante otros protocolos.**

OpenVPN es un protocolo de código abierto ampliamente reconocido para configurar redes privadas virtuales (VPN). Su arquitectura flexible y segura facilita la creación de conexiones cifradas entre dispositivos, incluso cuando se utiliza una red pública como Internet. [43]

Las ventajas que tiene ante otros protocolos son las siguientes:

* Seguridad Avanzada: OpenVPN emplea cifrados de alta robustez, como AES de 256 bits, y soporta certificados SSL/TLS, proporcionando un nivel de protección excepcional para los datos transmitidos.
* Flexibilidad en Puertos: Puede configurarse para operar en cualquier puerto, incluido el puerto TCP 443 (usado por HTTPS), facilitando la evasión de firewalls y sistemas de filtrado que bloquean otros protocolos VPN.
* Compatibilidad Multiplataforma: Es compatible con numerosos sistemas operativos y dispositivos, como Windows, macOS, Linux, Android y iOS, permitiendo su uso en entornos diversos y heterogéneos.
* Estabilidad y Rendimiento: Ofrece conexiones confiables y estables, permitiendo el uso de TCP o UDP para ajustar el equilibrio entre velocidad y estabilidad según las necesidades específicas.
* Comunidad Activa y Soporte: Al ser un proyecto de código abierto, cuenta con una comunidad activa que contribuye a su desarrollo continuo, brindando soporte técnico y actualizaciones frecuentes.
* **Revisar y comprender acerca de la configuración de redes en Ubuntu.**

Configurar redes en Ubuntu es un aspecto clave para asegurar una conectividad efectiva y segura, tanto en configuraciones domésticas como en entornos empresariales.

**Asignación de Direcciones IP en Ubuntu:**

* IP Dinámica: Con esta opción, Ubuntu utiliza el Protocolo de Configuración Dinámica de Host (DHCP) para obtener automáticamente una dirección IP del servidor DHCP. Es una configuración común en redes donde las direcciones IP pueden variar con el tiempo.
* IP Estática: En este caso, se asigna manualmente una dirección IP fija al dispositivo, asegurando que la dirección permanezca constante. Esta configuración es ideal para servidores y dispositivos que requieren una IP invariable para su correcto funcionamiento.

**Configuración de Red mediante la Interfaz Gráfica (GUI) en Ubuntu**

Ubuntu ofrece una interfaz gráfica sencilla e intuitiva para gestionar conexiones de red, para ello se realiza lo siguiente:

* Acceder a la Configuración de Red: Se hace clic en el ícono de red ubicado en la esquina superior derecha del escritorio y se selecciona "Configuración de red".
* Seleccionar la Interfaz de Red: En la pestaña "Red", se identifica la interfaz a configurar (por ejemplo, Ethernet o Wi-Fi) y luego clic en el ícono de engranaje para acceder a las propiedades de la conexión.
* Configurar la Dirección IP: En la sección "IPv4", se selecciona la opción "Manual" y se ingresan los datos necesarios: dirección IP, máscara de subred, puerta de enlace y servidores DNS.
* Guardar y Aplicar los Cambios: Una vez completada la configuración, se guardan los ajustes. La nueva configuración se aplicará automáticamente.
* **Consultar el uso de ufw para gestionar reglas de firewall.**

UFW es una herramienta de configuración de cortafuegos diseñada para facilitar la administración de reglas de firewall en sistemas Linux, especialmente en distribuciones basadas en Debian, como Ubuntu. Ofrece una interfaz de línea de comandos sencilla e intuitiva, que simplifica la creación y gestión de reglas de seguridad. Funciona como una capa sobre iptables, proporcionando una experiencia más amigable y accesible para los usuarios [45].

Es fundamental considerar que caundo se habilita UFW, todas las conexiones entrantes se bloquean de manera predeterminada, a menos que se configuren reglas específicas para permitirlas. Lo comandos básicos de UFW son los siguientes:

**Tabla 5.3.** Comandos básicos de UFW

|  |  |
| --- | --- |
| Comando | Uso |
| sudo ufw status | Verificar el estado del firewall |
| sudo ufw status verbose | Verificar el estado del firewall más detallada |
| sudo ufw deny puerto | Denegar conexiones entrantes en un puerto específico |
| sudo ufw allow from ipaddress | Permitir conexiones desde una dirección IP específica |
| sudo ufw status numbered | Obtener una lista numerada de las reglas |
| sudo ufw delete number | Para eliminar una regla |
| sudo ufw reset | Para regresar a la configuración predeterminada |