

MECANISMOS DE ACCESO REMOTO

Eduardo Blanco Bielsa – U0285176

Aarón Orozco Fernández – U0281997

Jonathan Arias Busto – U0283586

Juan Gómez Tejeda – U0281835



ÍNDICE

ÍNDICE	2
Introducción.....	3
¿Para qué sirve el acceso remoto?.....	3
¿Cómo funciona el acceso remoto?	3
SSH	4
Arquitectura de SSH	4
Capa de transporte	4
Capa de autenticación y métodos de autenticación SSH	4
Capa de conexión	5
¿Cómo usar SSH?	6
RDP.....	7
Riesgos del RDP	7
¿Cómo usar RDP?	8
Windows RDP	8
VPN.....	11
¿Cómo se usa una VPN?.....	12
TELNET	14
¿Cómo funciona Telnet?.....	14
Problemas de seguridad con Telnet y SSH como sustituto	15
¿Cómo usar Telnet?	15

INTRODUCCIÓN

El **acceso remoto** se refiere a la capacidad de acceder a un ordenador, ya sea doméstico o de oficina, desde una ubicación remota. Esto permite a las personas trabajar desde cualquier ubicación sin dejar de tener acceso a un ordenador o red distante, como podría ser una red de trabajo.

El acceso remoto se puede configurar mediante una Red de Área Local (LAN), una Red de Área Amplia (WAN) o incluso una Red Privada Virtual (VPN) para que se pueda acceder a sus recursos de forma remota. Para establecer una conexión remota, tanto la máquina local como el ordenador/servidor remoto deben tener un Software de Acceso Remoto. Alternativamente, hay proveedores de servicios que ofrecen acceso remoto a través de Internet.

En los últimos años, el acceso remoto ha ganado una gran importancia en el ámbito empresarial debido a la flexibilidad de los horarios laborales y la incorporación del teletrabajo. Es por ello que muchas de las empresas más reconocidas han implementado múltiples mecanismos de acceso remoto como **Secure Shell (SSH)**, **Protocolo de Escritorio Remoto (RDP)**, **Red de Área Privada (VPN)** y **Telnet**, los cuales detallaremos más adelante.

¿Para qué sirve el acceso remoto?

- Acceder a los archivos desde cualquier lugar.
- Supervisión de empleados
- Asistencia técnica remota
- Comunicación interna

¿Cómo funciona el acceso remoto?

El acceso remoto funciona desde una **red virtual** que permite la conexión y comunicación entre dispositivos como ordenadores, tabletas y teléfonos inteligentes a un servidor.

La **condición** para que ocurra este suceso es que tanto el servidor como el dispositivo electrónico estén habilitados para admitir esta conexión.

Para que esta comunicación suceda y se eviten problemas de seguridad (como invasiones y pérdidas de datos) la **autenticación** entre dispositivos debe ser obligatoria.

MECANISMOS DE ACCESO REMOTO. SSH, RDP, VPN Y TELNET

SSH

SSH significa protocolo Secure Shell y es el nombre del protocolo cuya principal función es el acceso remoto a un servidor por medio un canal seguro en el que toda la información está cifrada.

Alguno de los usos de SSH son:

- Conexiones seguras con servidores, ya que con conexiones SSH podemos asegurar que las conexiones son seguras.
- Aprovechando la seguridad de las comunicaciones, el protocolo SSH también se utiliza para otros objetivos como la transferencia de datos entre máquinas. Por ejemplo, tenemos el comando SCP, el cual basa sus comunicaciones en SSH.

Una cosa a tener en cuenta es que está implementado por defecto en servidores Unix, Linux, Windows y MAC.

Arquitectura de SSH

SSH sigue una arquitectura en capas, siendo 3 las capas principales:

- Capa de transporte
- Capa de autenticación
- Capa de conexión

Capa de transporte

Normalmente la capa de transporte usa el paquete de protocolos TCP/IP siendo el número de puerto SSH predeterminado el 22. Esta capa es la que se encarga del intercambio de claves inicial y la autenticación.

Una cosa para tener en cuenta es que el puerto SSH se puede desviar del 22 para tener una mayor seguridad.

Capa de autenticación y métodos de autenticación SSH

Cuando la capa de transporte finaliza la configuración del cifrado, se solicita que el usuario se autentique usando uno de los siguientes métodos de autenticación:

- Autenticación basada en contraseña
- Autenticación basada en clave pública (PKI)

En el primer caso la forma de conectarse a través de SSH se realiza mediante un nombre de usuario y una contraseña como en los métodos clásicos de autenticación. Esto puede ser poco seguro, debido a que los ataques de fuerza bruta pueden llegar a encontrar la contraseña para los usuarios, en caso de que no se establezcan contraseñas seguras y estas se cambien regularmente.

Por otro lado, en el caso de la autenticación con clave pública, este mecanismo es el preferido y recomendable para evitar dichos ataques de fuerza bruta. La autenticación PKI utiliza claves criptográficas para establecer una conexión de confianza entre servidor y cliente.

Para usar la autenticación PKI habrá que generar un par de claves SSH, que consisten en una clave pública, que se almacenará en el servidor, y una clave privada que se mantiene en la máquina del usuario que quiere conectarse al servidor a través de SSH.

Una vez autenticado el usuario se creará una clave de sesión entre el cliente SSH y el servidor que se usa para cifrar y poder compartir datos de forma segura entre dos puntos sin que una tercera persona pueda interceptar los datos en tránsito para así poder evitar ataques del tipo: Man in the Middle – MitM.

Capa de conexión

Cuando el proceso de autenticación se completa con éxito se inicia una conexión con el servidor. La comunicación se realiza a través de unos canales, siendo uno de estos el Secure File Transfer Protocol (SFTP) que te permite acceder y transferir archivos de forma segura a través de dicha conexión SSH.



¿Cómo usar SSH?

Introducimos la dirección de conexión con el servidor, en este caso un servidor de prueba de un compañero que tenía un puerto abierto. Una vez introducido dicho comando y le damos a Enter nos aparecerá una pregunta de si queremos que se guarde el fingerprint, le decimos que sí:

```
ssh server@[REDACTED] -p 1001
The authenticity of host '[REDACTED]:1001 ([REDACTED]:1001)' can't be established.
ED25519 key fingerprint is SHA256:eHki8jBojYbFqcqUDz+LVqqVSwYGrIGz03z31IxXvMs.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
```

Ahora introducimos la contraseña del servidor y podemos ver cómo nos conectamos con el servidor y podemos ejecutar comandos en el servidor en remoto:

```
[ariass@ariass-macbook-air ~] ssh server@[REDACTED] -p 1001
[server@[REDACTED] password:
Web console: https://poweredge:9090/ or https://192.168.0.88:9090/

Last login: Mon May  8 18:11:16 2023 from [REDACTED]
[server@poweredge ~] ks
fish: Unknown command: ks
[server@poweredge ~ [127]] ls
server/
[server@poweredge ~] cd server/
[server@poweredge ~/server] ls
ac/  mc/  [REDACTED]  mc_new/  mc_new2/  mc_old/  mcmc/  mctest/  [REDACTED]
[server@poweredge ~/server]
```

RDP

RDP, o Protocolo de Escritorio Remoto, puede resultar de gran ayuda a la hora de recibir u ofrecer asistencia remota.

Pero ¿qué es RDP?

RDP responde a (Remote Desktop Protocol). El protocolo RDP, da la posibilidad de que un equipo informático sea controlado a distancia por otro usuario remotamente.

Para que el protocolo RDP pueda funcionar, se deberá habilitar un puerto RDP en el equipo que vaya a ser controlado remotamente. De esta forma, el usuario que se encuentre controlando remotamente el equipo podrá utilizar el ratón y teclado como si estuviese delante de él. Así, el equipo anfitrión, permitirá al equipo remoto utilizar su sistema operativo y software.

Riesgos del RDP

Hay diferentes riesgos que podríamos considerar.

- **Falta de encriptación.** Las conexiones no cuentan con una encriptación robusta, de manera que la información que manejen los usuarios (tanto enviada como recibida) podría llegar a ser interceptada por terceros.
- **Apertura de puertos.** Esto puede llegar a ser una gran vulnerabilidad en tu sistema. La apertura de puertos RDP para habilitar la conexión remota puede permitir que personas con objetivos maliciosos puedan acceder a nuestro equipo a través del mismo puerto que hemos habilitado para el RDP, dando lugar a posibles robos de datos, o ataques en general.
- **Vulneración de cuentas.** Si un usuario ajeno a nuestro sistema consigue tener acceso a una cuenta de administrador de RDP, este usuario podría entrar en los equipos que conformen por ejemplo una empresa. Pudiendo usar cuentas de correo, descarga o eliminar archivos, etc.
- **Son fáciles de localizar.** Como ya se mencionó en puntos anteriores, usuarios que estén interesados en robar o atacar un sistema. Podrían utilizar herramientas como Shodan para localizar redes RDP abiertas.

Bien ya sabemos que riesgos tiene RDP, pero debemos encontrar formas para hacerlo seguro. Para proteger tu conexión algunas medidas de seguridad que podemos utilizar son las siguientes:

- **Cambiar el puerto RDP.** Una opción es cambiar el puerto por uno no estándar, esto puede resultar útil ya que dificultará la tarea de un hacker que esté tratando de localizar un punto de acceso RDP a nuestros equipos.
- **Restringir IPs.** Es posible restringir el acceso RDP para que solo las IPs de nuestra elección tenga acceso.

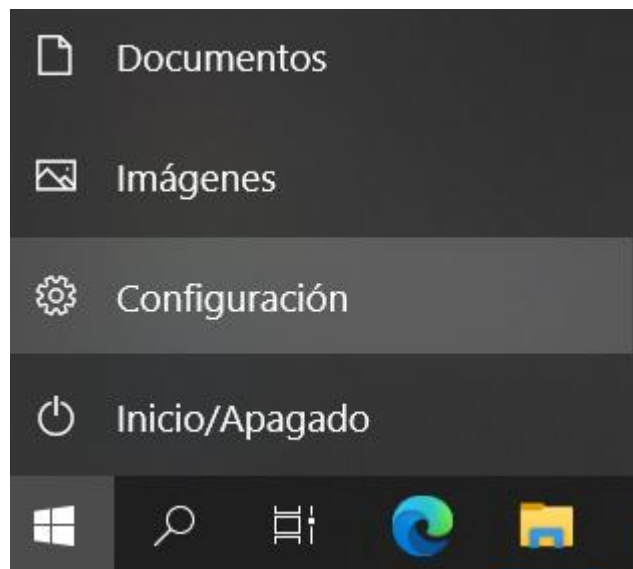
- **Utilizar valores por defecto.** Uno de los mayores errores que se pueden cometer en la informática es mantener los valores por defecto de contraseñas o usuarios. De esta forma los atacantes con simples búsquedas pueden tener acceso.
- **Mantener el software actualizado.** Como con cualquier otro software, mantener actualizado es la única manera de garantizar que cuente con los parches de seguridad más recientes y esté libre de vulnerabilidades conocidas.
- **Utilizar VPNs.** Utilizar una VPN permite encriptar el tráfico que se envía a través de los RDPs y mantener la información transmitida a salvo. De esta forma se cuenta con la posibilidad de proporcionar asistencia remota y, al mismo tiempo, con la protección de la encriptación de una VPN.

¿Cómo usar RDP?

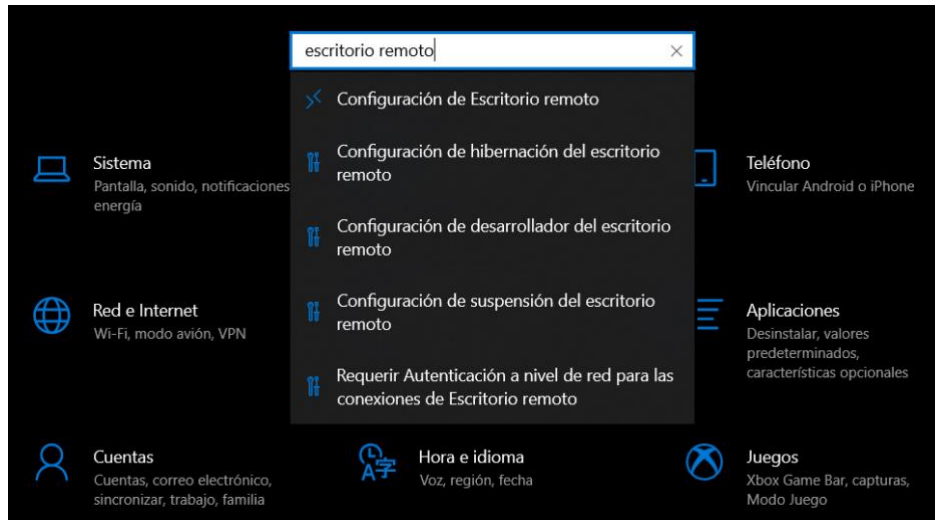
Tenemos varias formas de utilizar RDP dependiendo del software.

Windows RDP

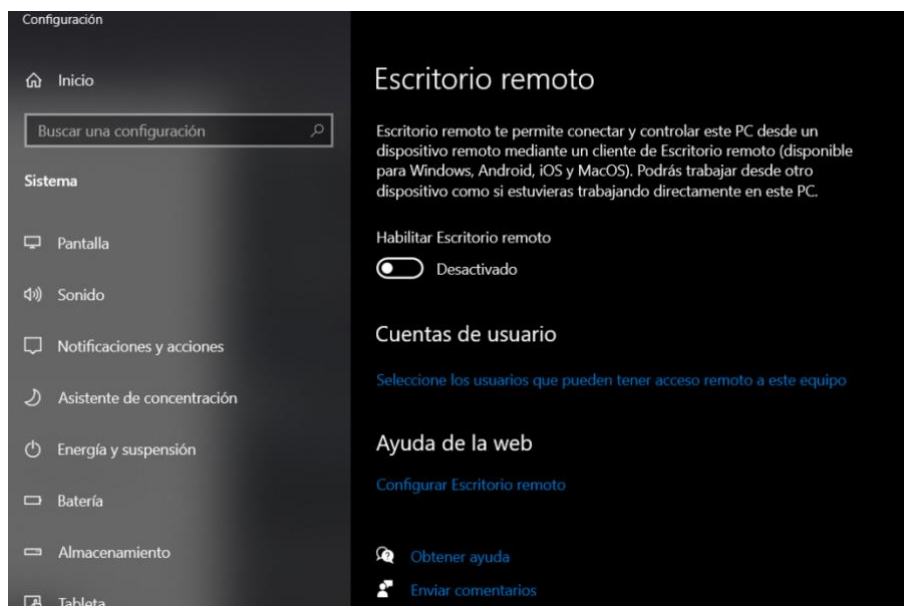
1. Nos dirigimos al menú de inicio de Windows y pulsamos en la opción de configuración.



2. Buscamos el menú de Escritorio remoto en la barra superior.



3. Finalmente, habilitamos las pestañas de Escritorio remoto, seleccionando con quién queramos compartir nuestro escritorio.



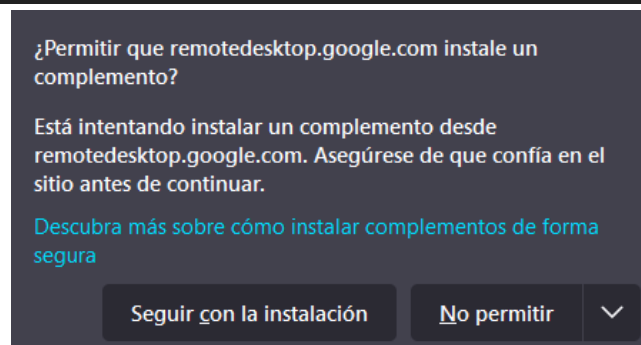
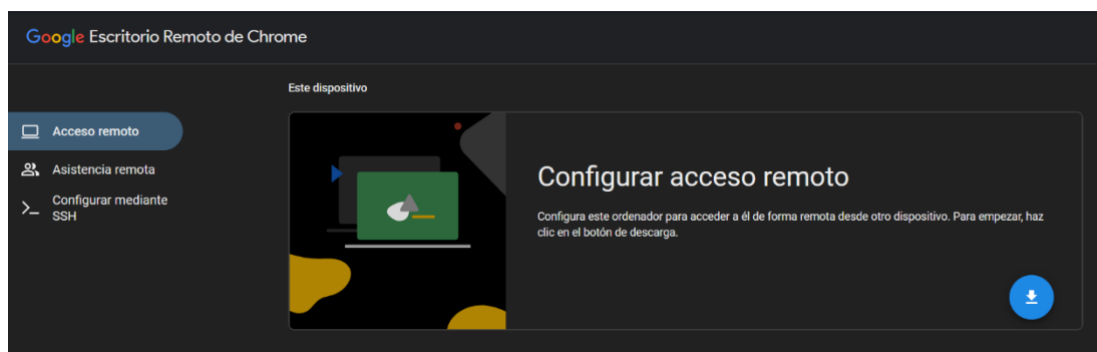
Otra opción que se puede utilizar es Google Chrome. Google Chrome tiene otra función que permite utilizar el escritorio remoto de forma online. Los pasos para realizarlo son los siguientes:

1. Abrimos la web del escritorio remoto de Chrome
<https://remotedesktop.google.com/>

2. Seleccionamos la conexión que queramos hacer. En mi caso le daré a “Acceder a mi ordenador”



3. Descargamos y permitimos que se instalen complementos



4. Y por último concedemos los permisos necesarios para la instalación del escritorio remoto.

VPN

VPN, siglas inglesas de **Virtual Private Network**, en español, Red Virtual Privada, es un mecanismo de acceso remoto consistente en la creación de una Red de Área Amplia (WAN) privada entre dos dispositivos, obteniendo así un túnel privado entre ambas máquinas.

Este tipo de mecanismos tiene las siguientes características:

- **Autenticación:** Garantiza que ambas máquinas sean quien dicen ser.
- **Integridad:** Garantiza que los mensajes no han sido alterados de ninguna forma. Esto se logra al usar una función hash sobre el mensaje y comprobar que corresponde a la Hash correcta.
- **Confidencialidad:** Al estar los mensajes cifrados de forma asimétrica, solo el otro miembro de la comunicación puede descifrar lo que ha enviado el primero, impidiendo así que miembros externos accedan a esa información.
- **No repudio:** Todos los mensajes enviados deben ir firmados, y la persona no puede negar que envió un mensaje firmado.
- **Control de acceso:** Garantiza que solo acceden los dispositivos que tengan permiso.

Todas las VPN deben cumplir con los siguientes requisitos básicos:

- **Identificación de usuario:** Debe verificar la identidad de los usuarios y evitar el acceso a aquellos que no estén autorizados.
- **Cifrado de datos:** Todos los mensajes deben ser cifrados mediante cifrado simétrico, al ser este mucho más rápido que el asimétrico.
- **Administración de claves:** Las claves del cifrado asimétrico deben ser previamente cifradas mediante cifrado asimétrico, cuyas dos claves deben ser actualizadas periódicamente.
- Deben seguir el algoritmo de seguridad **SEAL**.

Hay cuatro diferentes tipos de arquitectura de conexión VPN:

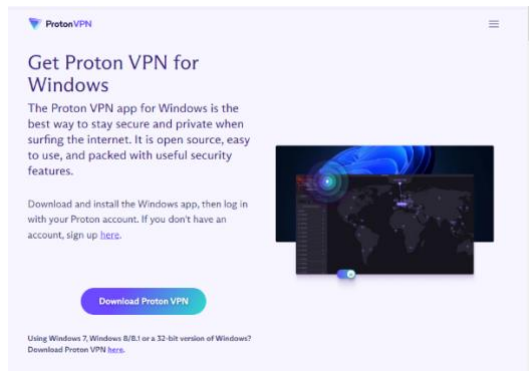
- **VPN de acceso remoto:**
 - Consiste en que los usuarios se conecten a un dispositivo desde cualquier sitio externo usando Internet como vínculo de acceso.
 - Este tipo da un nivel de acceso similar a estar conectado directamente dentro de la red local del dispositivo.
- **VPN punto a punto:**
 - Consiste en conectar a dispositivos externos con otros dispositivos externos mediante un servidor que acepta las conexiones externas y establece un túnel entre ambos dispositivos.
- **Tunelado:**
 - Consiste en encapsular un protocolo de red sobre otro, creando de esta forma un túnel directo entre dos dispositivos de una red concreta.

- Este túnel se implementa incluyendo una Unidad de Datos de Protocolo dentro de otra para así transmitirla entre desde un extremo al otro del túnel sin necesidad de ser interpretada entre uno y otro.
- El túnel se define al final por los dos puntos de los extremos y un protocolo de comunicación, por ejemplo, SSH.
- **VPN sobre LAN**
 - Es el tipo menos utilizado, pese a ser uno de los más seguros dentro de las redes de empresa.
 - Esto se debe a que se trata de una variante del primer tipo, solo que esta vez emplea directamente la red LAN de destino.

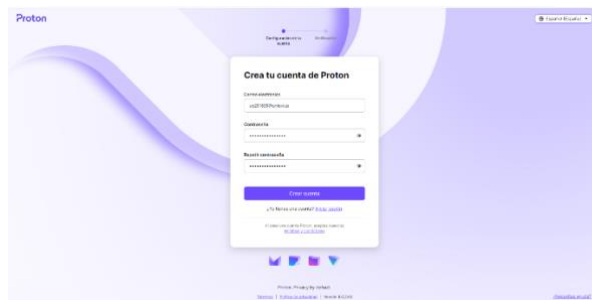
¿Cómo se usa una VPN?

En este caso, se enseñará como usar la VPN **ProtonVPN**

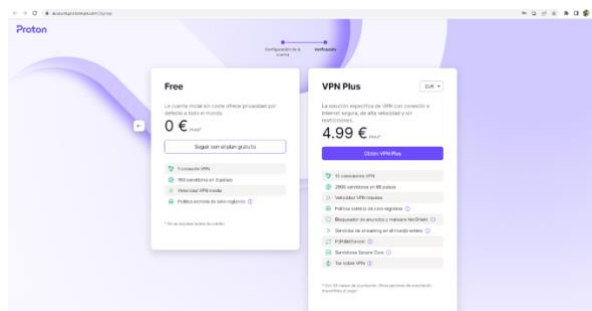
1. Instalación:



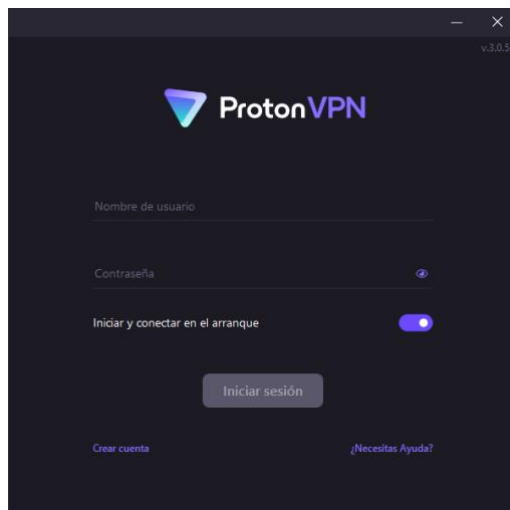
2. Creación de cuenta



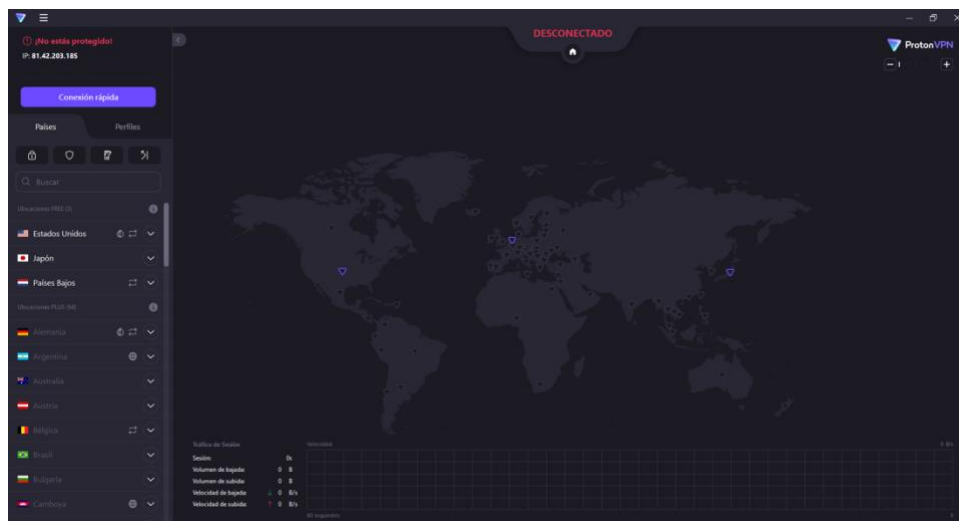
3. Elegimos la versión gratuita.



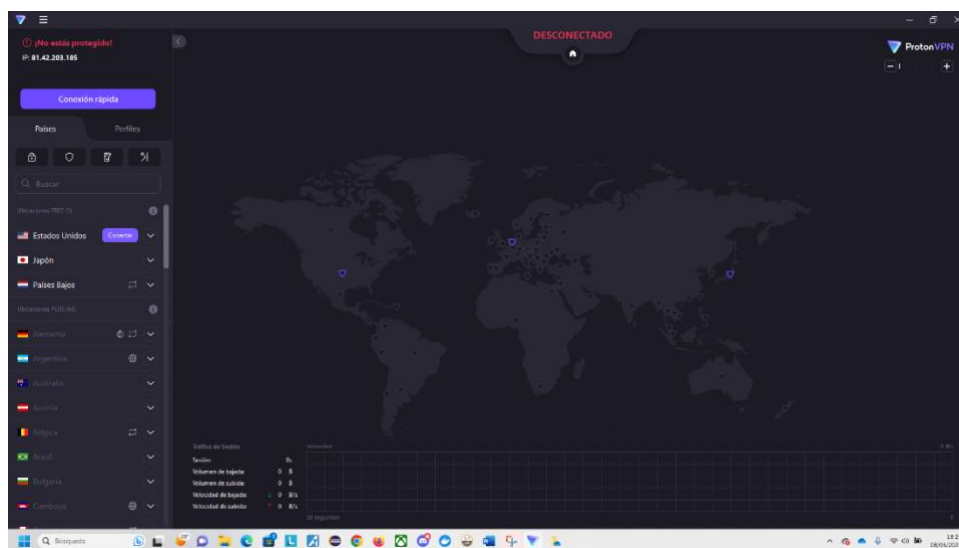
4. Iniciamos sesión



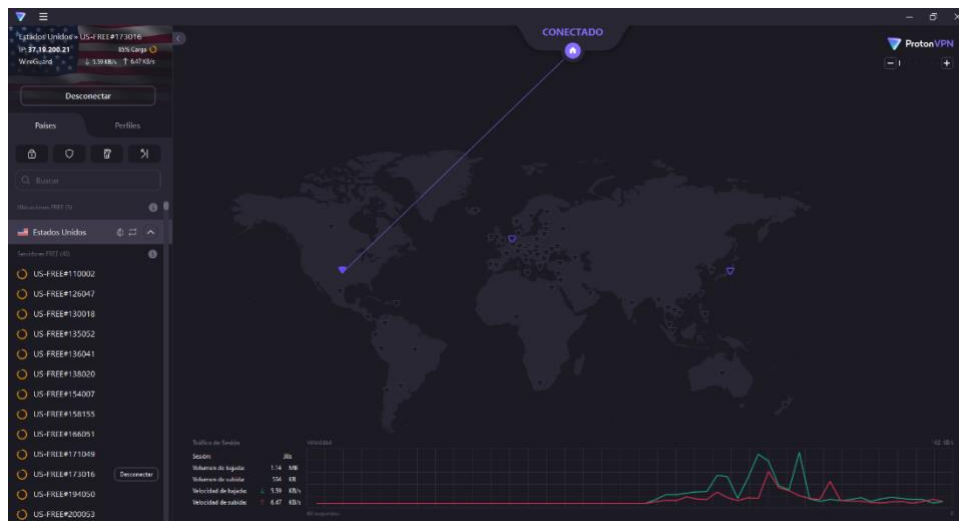
5. Accedemos a la pestaña principal.



6. Nos conectamos remotamente a un dispositivo de Estados Unidos



Comprobamos la conexión



TELNET

El nombre de Telnet proviene del acrónimo Telecommunication Network y es básicamente un protocolo de TCP/IP usado desde la década de los 60 para establecer conexiones remotas con otros ordenadores, servidores y dispositivos con un sistema compatible para el acceso mediante este tipo de comunicación. De forma predeterminada, Telnet utiliza el puerto de conexión 23.

Además del propio protocolo, también recibe este nombre el programa que lo utiliza para establecer la propia conexión. Para acceder a la otra máquina debemos usar un terminal (por ejemplo, el de Linux). De esta forma, podemos interactuar en la máquina remota navegando por sus archivos, ejecutando comandos internos y monitorizando el estado de la máquina remota sin la necesidad de ir físicamente al lugar en el que se encuentra.

Además de ser compatible con sistemas MSDOS y Windows, también es compatible con sistemas basados en UNIX y FreeBSD.

Con este protocolo también se puede comprobar la conectividad de otras máquinas y comprobar si tienen determinados puertos abiertos al exterior.

¿Cómo funciona Telnet?

Este protocolo y programa sólo se puede usar mediante comandos. Para poder establecer una conexión entre dos ordenadores con Telnet, primero necesitaremos tener un cliente en nuestro terminal y un servidor en la máquina a la que pretendemos acceder. Si además lo hacemos fuera de una Intranet o red LAN, deberemos tener habilitado el puerto 23 en la máquina destino.

Lo siguiente que vamos a necesitar es abrir una sesión en la máquina destino en la que exista una o varias cuentas de usuario que tengan permitido el acceso. Nosotros

necesitaremos conocer el nombre y la contraseña del usuario para establecer la comunicación.

Problemas de seguridad con Telnet y SSH como sustituto


Actualmente el uso de Telnet está prácticamente limitado a redes internas en donde existe un escudo de seguridad que aísla la red del exterior. En los demás casos siempre se usa el protocolo SSH.

El gran problema de Telnet es que la información de un terminal a otro viaja sin ningún tipo de cifrado (en texto plano). Para un hacker, esta información es extremadamente fácil de conseguir, y si tenemos en cuenta que tanto el nombre de usuario como la contraseña también viajan en texto plano, nos damos cuenta de que la brecha de seguridad es brutal.

En respuesta a estos problemas, se popularizó el uso de otro protocolo de comunicación basado en el sistema de cifrado de UNIX, llamado SSH (Secure Shell), que utiliza el puerto de conexión 22.

¿Cómo usar Telnet?

En este ejemplo, se mostrará cómo usar Telnet en un Windows 10 Professional.

En primer lugar, deberemos activar el servicio en **Activar o desactivar las características de Windows**. ☒  **Cliente Telnet**

Una vez hecho esto, en un terminal escribimos el comando **\$ telnet**

Ahora podemos usar la aplicación y ver las distintas opciones de telnet si escribimos el comando **\$ help**

```
Cliente Telnet de Microsoft
El carácter de escape es "CTRL++"
Microsoft Telnet> help
Los comandos se pueden abreviar. Los comandos permitidos son:
c      - close                cerrar la conexión actual
d      - display              mostrar los parámetros de visualización
o      - open nombre_host [puerto] conectarse a nombre_host (el puerto
                                predeterminado es 23)
q      - quit                 salir de telnet
set    - set                  activar opciones (escriba 'set ?' para
                                mostrar una lista)
sen    - send                 enviar cadenas al servidor
st     - status               mostrar la información del estado
u      - unset                desactivar opciones (escriba 'unset ?'
                                para mostrar una lista)
?/h   - help                 mostrar información de ayuda
Microsoft Telnet>
```

En lugar de usar la aplicación, podemos realizar una conexión directa mediante el comando **\$ telnet <IP/dominio del host>**

Vamos a probar a realizar una conexión directa Telnet al dominio público www.uniovi.es:

```
Microsoft Windows [Versión 10.0.19044.2846]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\blanc>telnet www.uniovi.es
Conectándose a www.uniovi.es...No se puede abrir la conexión al host, en puerto 23: Error en la conexión
C:\Users\blanc>_
```

En este caso, el puerto 23 está cerrado, y vemos cómo Telnet nos avisa de ello.