



TECNOLÓGICO NACIONAL DE MÉXICO

INSTITUTO TECNOLÓGICO DE TLAXIACO

SEGURIDAD Y VIRTUALIZACIÓN

Nombre de los Integrantes de equipo:

Edwin López Santiago

Yanet González García

No. Control

21620123

21620273

Tema:

Seguridad y Bloqueo de Páginas con Servidor Proxy

Docente:

Ing. Osorio Salinas Edward

Carrera:

Ingeniería en Sistemas Computacionales

Grupo: 7US

Tlaxiaco, Oaxaca. A 11 de Diciembre de 2024.



Índice

Introducción.....	4
Objetivos	4
Materiales.....	4
Preparación.....	5
Desarrollo.....	6
“Seguridad y Bloqueo de Páginas con Servidor Proxy”	6
Herramienta a trabajar con el servidor proxy.	6
Páginas de acceso restringido para los usuarios.....	8
Resultados	9
Configuración del servidor FTP	11
Recomendaciones Adicionales.....	18
Conclusión.....	19
Bibliografías:	20

TABLA DE ILUSTRACIONES

Ilustración 1: Herramienta de CCProxy.	6
Ilustración 2: Interfaz de Administrador de cuentas.....	6
Ilustración 3: Administrar cuentas de usuario.....	7
Ilustración 4: Configuración del Servidor proxy.	7
Ilustración 5: restricción de páginas de acceso para los usuarios.....	8
Ilustración 6: Tráfico de la red.	8
Ilustración 7: Acceso al dominio desde una computadora.	9
Ilustración 8: Acceso al dominio desde el celular.	9
Ilustración 9: Acceso denegado al dominio.	10
Ilustración 10: Acceso denegado al dominio de Facebook desde el celular.	10
Ilustración 11: Acceso denegado al dominio de Instagram desde la computadora.	11



Ilustración 12: Configuración del servidor FTP.....	11
Ilustración 13: Agregando el Servidor FTP.....	12
Ilustración 14: Visualización de la Página principal del servidor FTP.....	12
Ilustración 15: Rellenando sitio FTP.....	13
Ilustración 16: Configuración de enlaces.....	14
Ilustración 17: Permisos.	15
Ilustración 18: Acceso al servidor FTP con usuario.....	15
Ilustración 19: Acceso al servidor FTP desde la computadora.....	16
Ilustración 20: Acceso desde el dispositivo móvil.....	16
Ilustración 21: Acceso al servidor FTP con otro usuario.	17



Introducción

La configuración de un servidor proxy utilizando CCProxy y un servidor FTP es fundamental para gestionar y controlar el acceso a Internet de manera segura dentro de una red. Estos servicios permiten a las organizaciones asegurar su entorno digital, limitando el acceso a sitios no deseados y proporcionando una infraestructura confiable para la transferencia de archivos. En este contexto, la práctica de seguridad y bloqueo de páginas con servidor proxy nos ayuda a comprender mejor cómo funciona la gestión del acceso a Internet y la protección de datos en un entorno de red. A continuación, se presenta cada proceso.

Objetivos

- El objetivo de esta práctica es implementar y configurar un servidor proxy utilizando CCProxy para gestionar el acceso a Internet en la red.
- Instalar y configurar un servidor FTP.

Materiales

- Internet
- Software Ccproxy
- Computadora personal con el sistema operativo Windows Server 2016.
- Computadora personal con el sistema operativo Windows 11.



Preparación

- Por equipos de trabajo instalar y configurar el servidor FreeProxy en un equipo de cómputo.
- Se configura un equipo para que salga a Internet a través del equipo que actúa como servidor.
- Se configura el servidor para que filtre determinadas páginas.

HARDWARE – SOFTWARE:

- Se alternarán los equipos de trabajo para su revisión (administrador-cliente).

SERVIDOR:

1. Dirección IP del equipo que vas a configurar como servidor proxy.
2. Instala el servidor Proxy en el equipo que va a funcionar como servidor.
3. Desactiva el cortafuegos del antivirus para que pueda funcionar el servidor Proxy.

CLIENTE:

1. En la configuración TCP/IP del equipo cliente:
 - a) Dirección IP
 - b) Mascara de red
1. Configura los dos navegadores (Internet Explorer y Mozilla) del equipo cliente para que puedan acceder a Internet a través del servidor proxy.
2. Accede a varias páginas desde ese equipo y comprueba que navega.
3. Envío de paquetes a través del servidor.
4. Realizar alguna otra conectividad inalámbrica vista en las diapositivas.

Desarrollo

“Seguridad y Bloqueo de Páginas con Servidor Proxy”

Herramienta a trabajar con el servidor proxy.

1.- CCProxy fue la herramienta elegida para configurar el servidor proxy. Este software, especializado en la gestión de tráfico de red, es compatible con múltiples protocolos y tipos de conexión. Su funcionalidad abarca desde el correo electrónico hasta los protocolos más utilizados en la web, como HTTP y HTTPS. Gracias a CCProxy, se pudo establecer un servidor proxy que permite compartir la conexión a internet dentro de una red local de manera eficiente y segura.

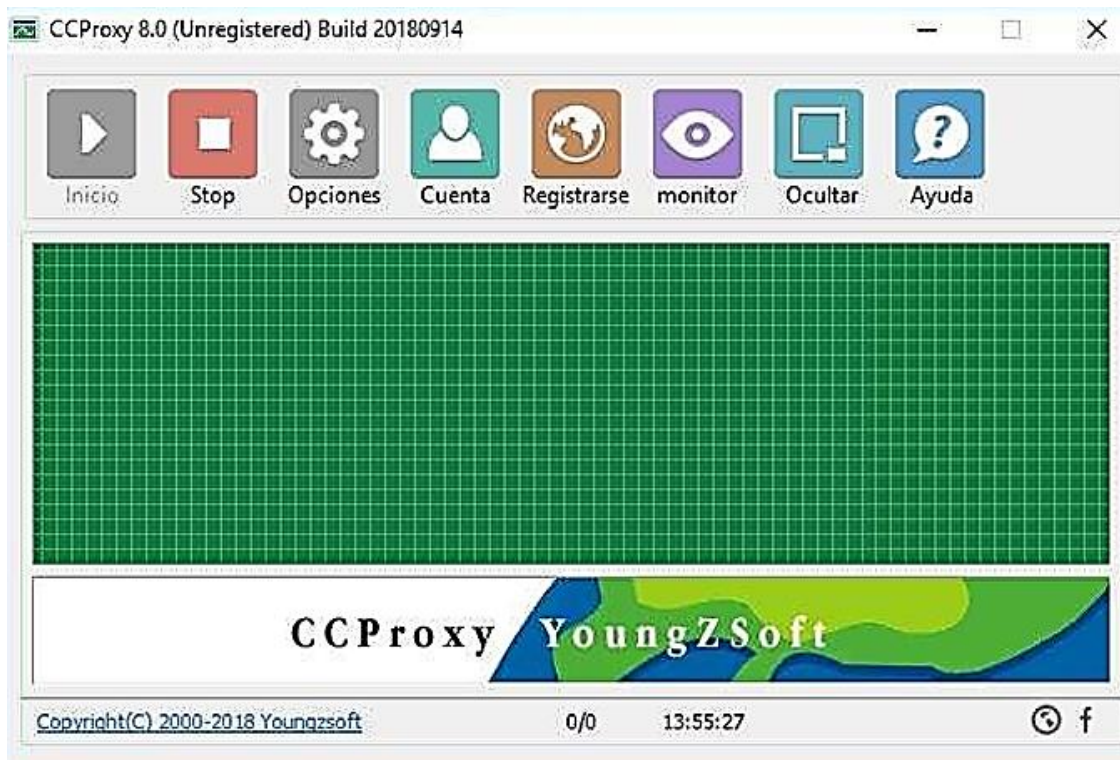


Ilustración 1: Herramienta de CCProxy.

2.- A continuación, se muestra una interfaz de usuario intuitiva y fácil de usar para gestionar las cuentas de usuarios en un servidor proxy.

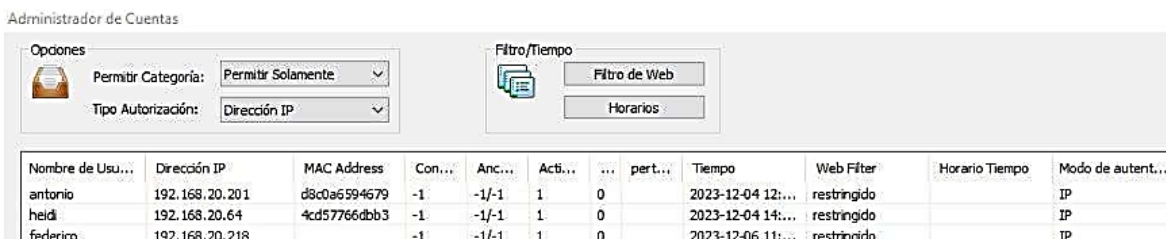


Ilustración 2: Interfaz de Administrador de cuentas.

3.- Esta interfaz proporciona un conjunto completo de herramientas para administrar cuentas de usuario en un servidor proxy, lo que permite a los administradores controlar el acceso, el uso del ancho de banda y la configuración de seguridad.

Usuario/Grupo: antonio

Enable: ☒ Dirección IP/Rango IP: 192.168.20.1

Dirección MAC / nombre d: d8:Da:a5:59:46:79

As Grupo: ☐ Pertenece al grupo: [dropdown]

Outgoing IP: 0.0.0.0

Máximo Número de Conexiones: -1

Descarga de ancho de banda (KB/h): -1

Sube Ancho de banda (KB/h): -1

WWW: ☒ Correo: ☒ Telnet: ☒ Marcado Automático: ☒

FTP: ☒ SOCKS: ☒ Otros: ☒

Filtro de Web: restringido

Horarios: [dropdown]

Auto desactivar at: 04/12/2023 12:21:40 p.m.

Cuota de ancho de b: 0 MB 1 días

Tiempo restante: 0:00:00 00:00:00

Ilustración 3: Administrar cuentas de usuario.

4.- En este apartado ambas capturas muestran diferentes aspectos de la configuración de un servidor proxy. La captura de la izquierda ofrece una vista general de la configuración de red, mientras que la captura de la derecha se enfoca específicamente en la configuración del proxy.

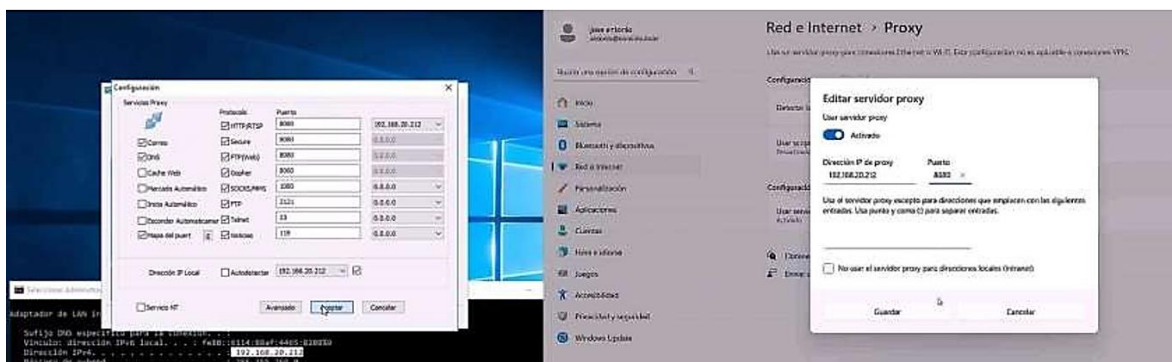


Ilustración 4: Configuración del Servidor proxy.

Páginas de acceso restringido para los usuarios.

5.- Las direcciones web de Facebook e Instagram en el bloque de notas sugieren que el usuario está interesado en estas plataformas.

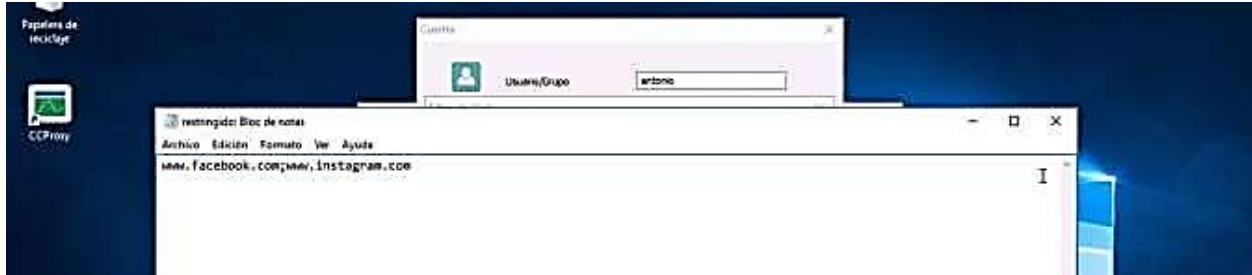


Ilustración 5: restricción de páginas de acceso para los usuarios.

6.- Información en tiempo real sobre el tráfico de la red.

En este apartado se muestra la información del uso de los recursos de red en tiempo real para identificar patrones de tráfico, las de actividad y otros eventos que pueden afectar el rendimiento de la red.



Ilustración 6: Tráfico de la red.

Resultados

7.- A continuación, se muestra en donde el usuario Yanet ha establecido una conexión exitosa a través del servidor proxy con el sitio web www.wikipedia.org

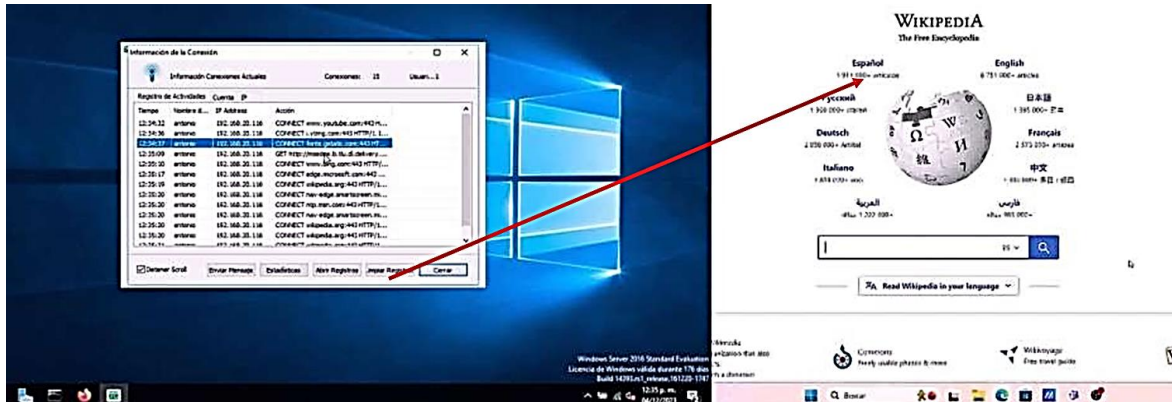


Ilustración 7: Acceso al dominio desde una computadora.

8.- Cuando el usuario Yanet establece una conexión exitosa a través de un servidor proxy con el sitio web www.google.com, implica que todas las solicitudes que ella realiza a Google, así como las respuestas que recibe, están siendo gestionadas y canalizadas por este servidor proxy.



Ilustración 8: Acceso al dominio desde el celular.

9.- En el siguiente apartado se muestra un ejemplo donde se ha denegado el acceso a ciertos dominios.

Se ha denegado acceso a ciertos dominios al cliente Yanet para mantener un entorno de red seguro, cumplir con políticas internas y externas, y promover un uso productivo y apropiado de Internet en diferentes contextos.

Esta medida forma parte de una estrategia de administración de la red que tiene como objetivo garantizar la seguridad, el cumplimiento normativo y la eficiencia en el uso de los recursos tecnológicos disponibles.

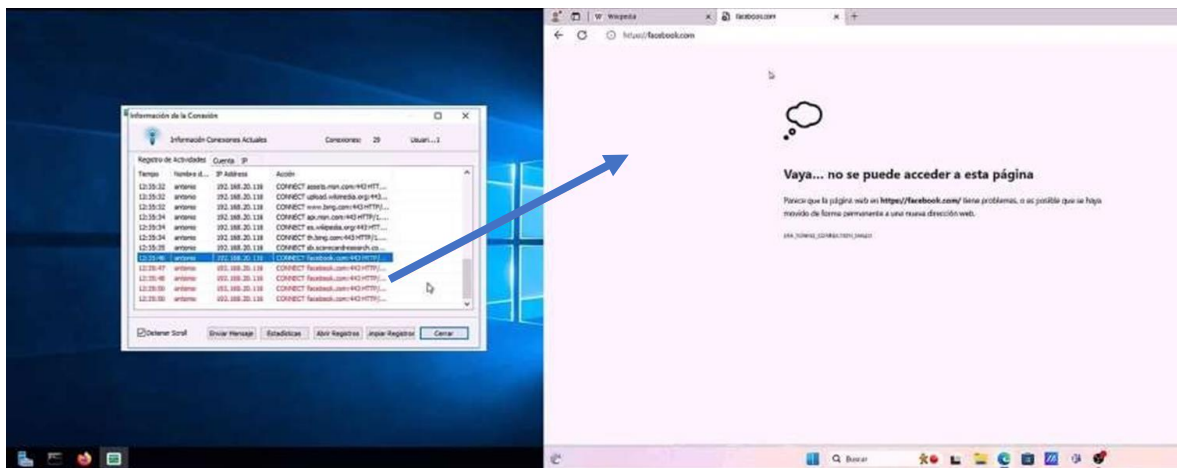


Ilustración 9: Acceso denegado al dominio.

10.- "Se le denegó el acceso al sitio web www.instagram.com al usuario Yanet en su dispositivo móvil". Este evento es un ejemplo claro de cómo las políticas de administración de red pueden configurarse para limitar el acceso a determinados sitios web, en este caso, Instagram. Este tipo de medidas se implementan con diversos fines, como garantizar un entorno seguro, optimizar el uso de los recursos de red y fomentar la productividad de los usuarios.

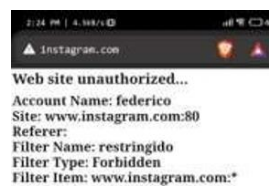


Ilustración 10: Acceso denegado al dominio de Facebook desde el celular.

11.- Esta siguiente acción es la denegación al acceso de Instagram. "Se le denegó el acceso al sitio web www.instagram.com al usuario Yanet en su computadora".

Este evento refleja la implementación de controles de acceso en una red administrada, donde se establecen políticas para restringir el uso de ciertos sitios web, como Instagram, en dispositivos conectados a la red, en este caso, una computadora.

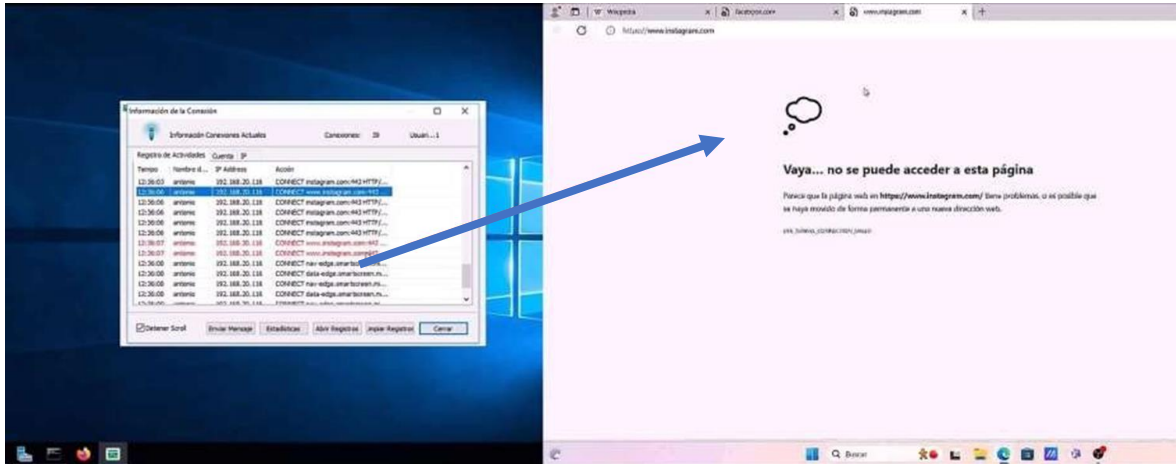


Ilustración 11: Acceso denegado al dominio de Instagram desde la computadora.

Configuración del servidor FTP

12.- "La configuración de roles y características para el servidor FTP". La configuración de un servidor FTP (Protocolo de Transferencia de Archivos) es un paso esencial para permitir el intercambio de archivos en una red de manera controlada, segura y eficiente. En esta sección, se aborda el proceso de configuración de los roles y características que permiten definir los permisos, accesos y funciones específicas, garantizando que el servidor cumpla con las necesidades del entorno donde será implementado.

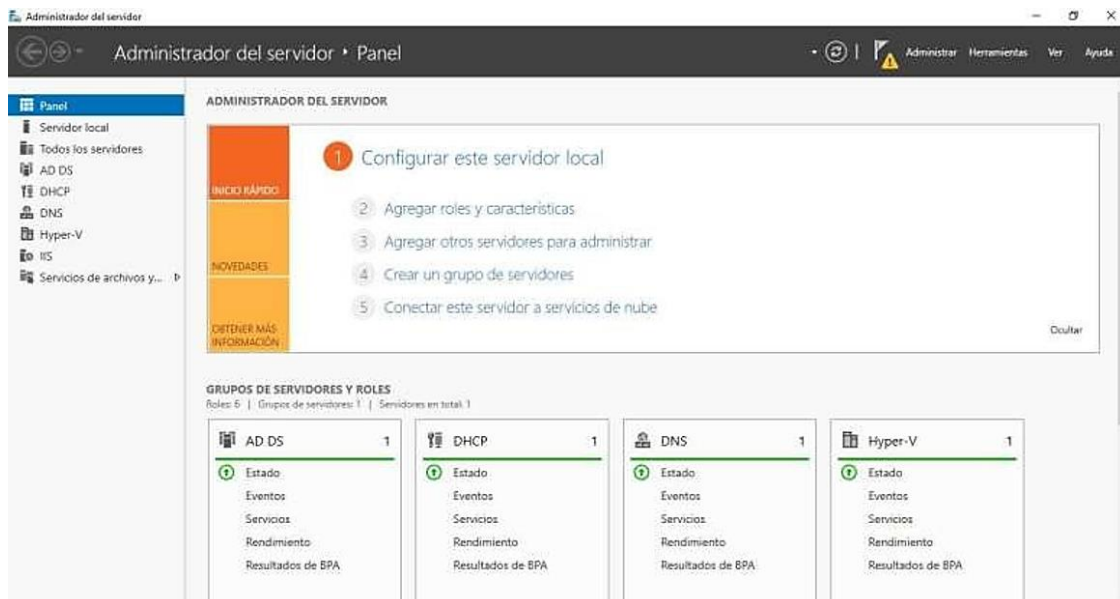


Ilustración 12: Configuración del servidor FTP.

13.- Se muestra del asistente para agregar roles y características en un servidor Windows. Este asistente es una herramienta clave utilizada para configurar y gestionar diferentes roles en el servidor, como servicios de red, gestión de archivos, servidores web, entre otros. En este caso, se enfoca específicamente en la instalación del Servidor FTP.

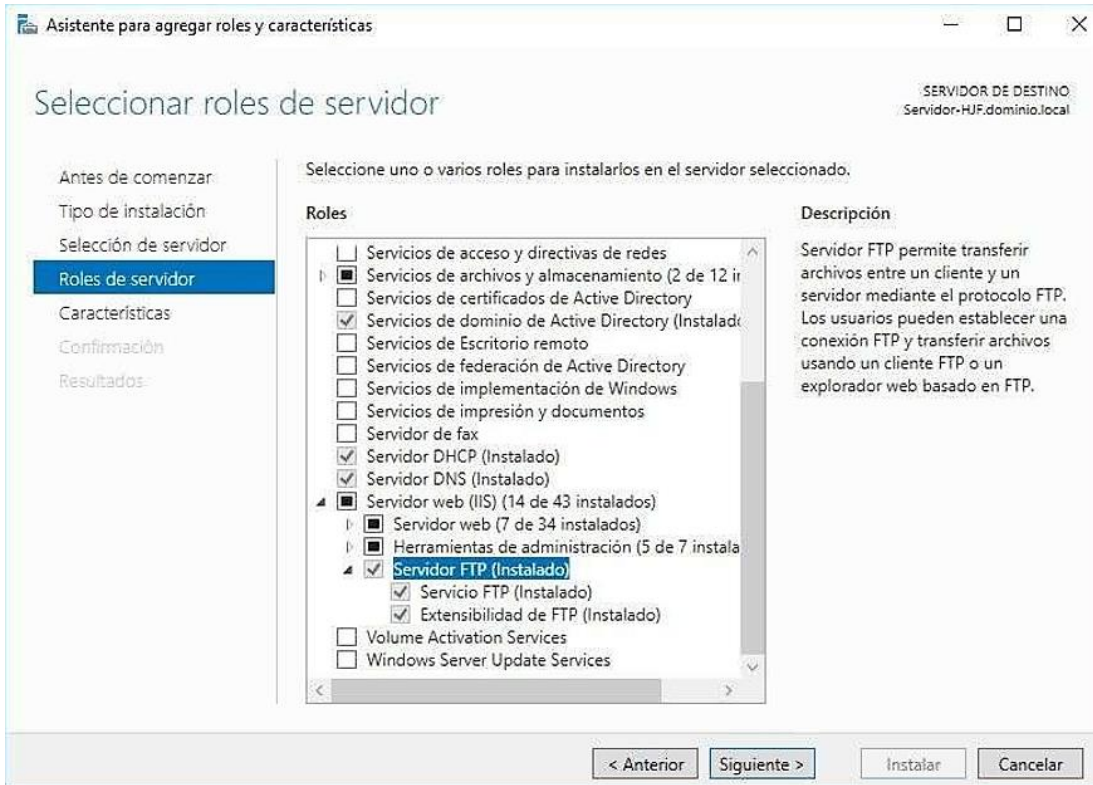


Ilustración 13: Agregando el Servidor FTP.

14.- Esta configuración permite al administrador de sistema gestionar de manera efectiva el servidor FTP, asegurando que se cumplan las políticas de seguridad y se optimice el uso de la red para la transferencia de archivos. A continuación, agregamos un nuevo sitio FTP y la ruta de disco en la que se desea que se guarden los datos, al igual que esto se configurará la dirección IP y el puerto por el que se atenderán las peticiones de FTP.

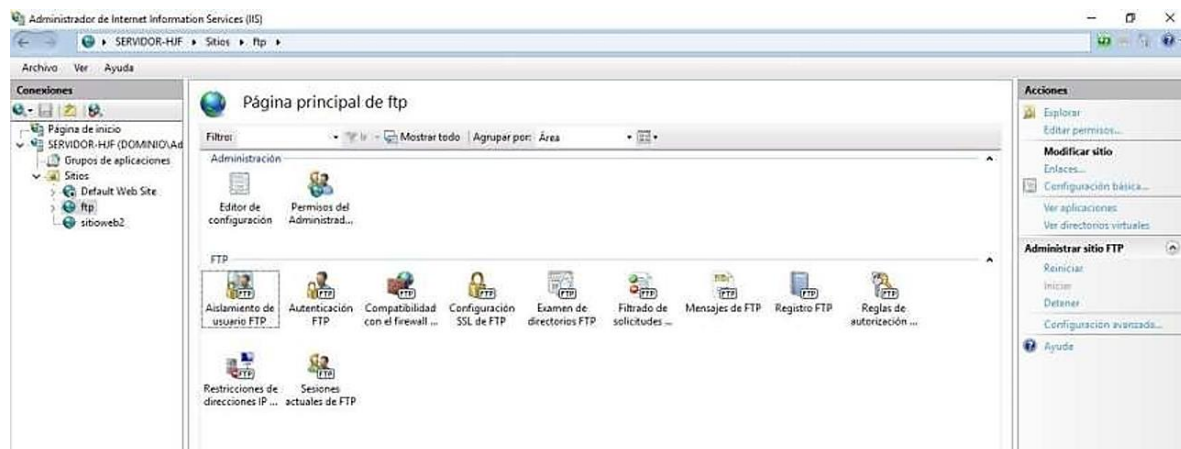
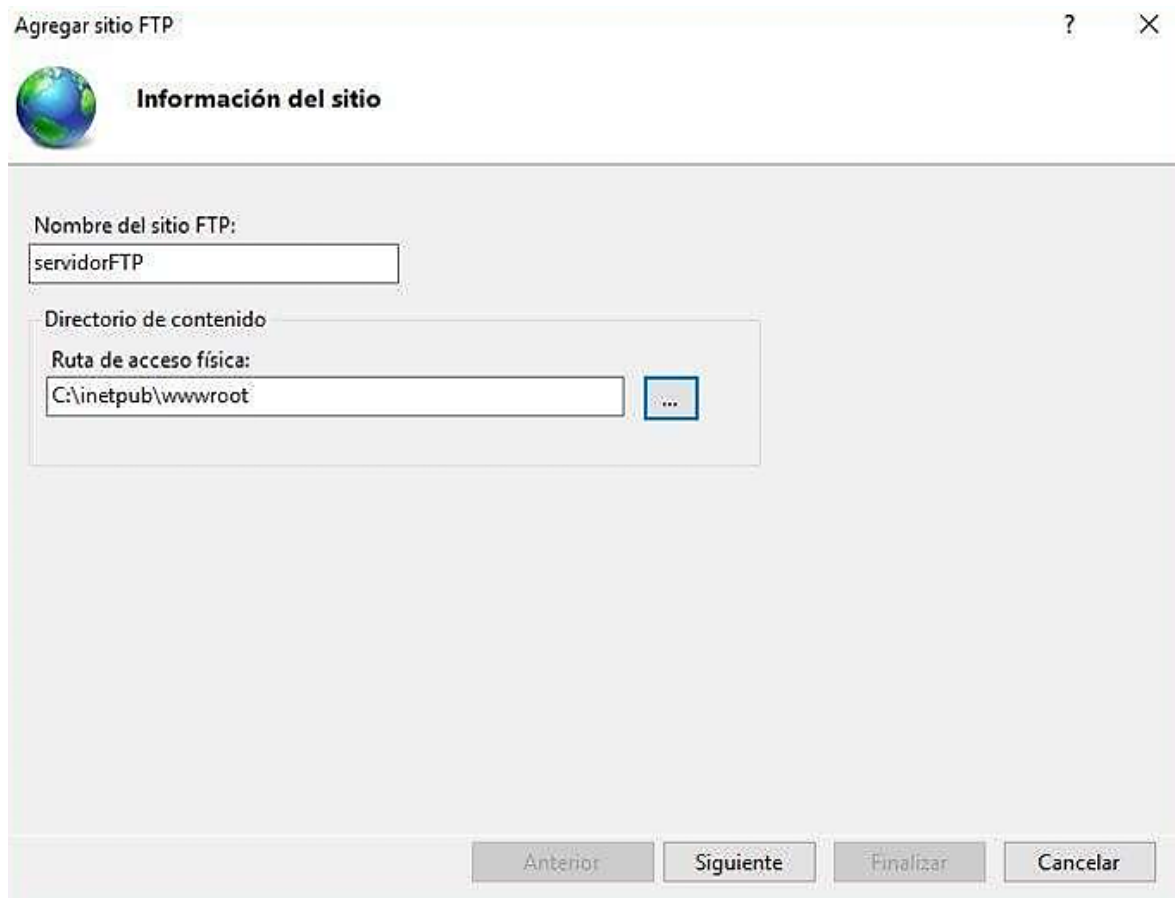


Ilustración 14: Visualización de la Página principal del servidor FTP.

15.- Se muestra el asistente para agregar un sitio FTP en un servidor Windows, específicamente en la configuración del servidor FTP.

Campo “Nombre del sitio FTP”: En este campo, el administrador de sistema debe introducir un nombre descriptivo para el sitio FTP que está creando. Este nombre será visible para los usuarios cuando se conecten al servidor.

Ruta: C:\inetpub\wwwroot es una ubicación común en los servidores Windows para almacenar archivos web accesibles por FTP. Esto facilita la integración con otros servicios web y mantiene la organización del servidor.



Agregar sitio FTP

Información del sitio

Nombre del sitio FTP:
servidorFTP

Directorio de contenido
Ruta de acceso física:
C:\inetpub\wwwroot

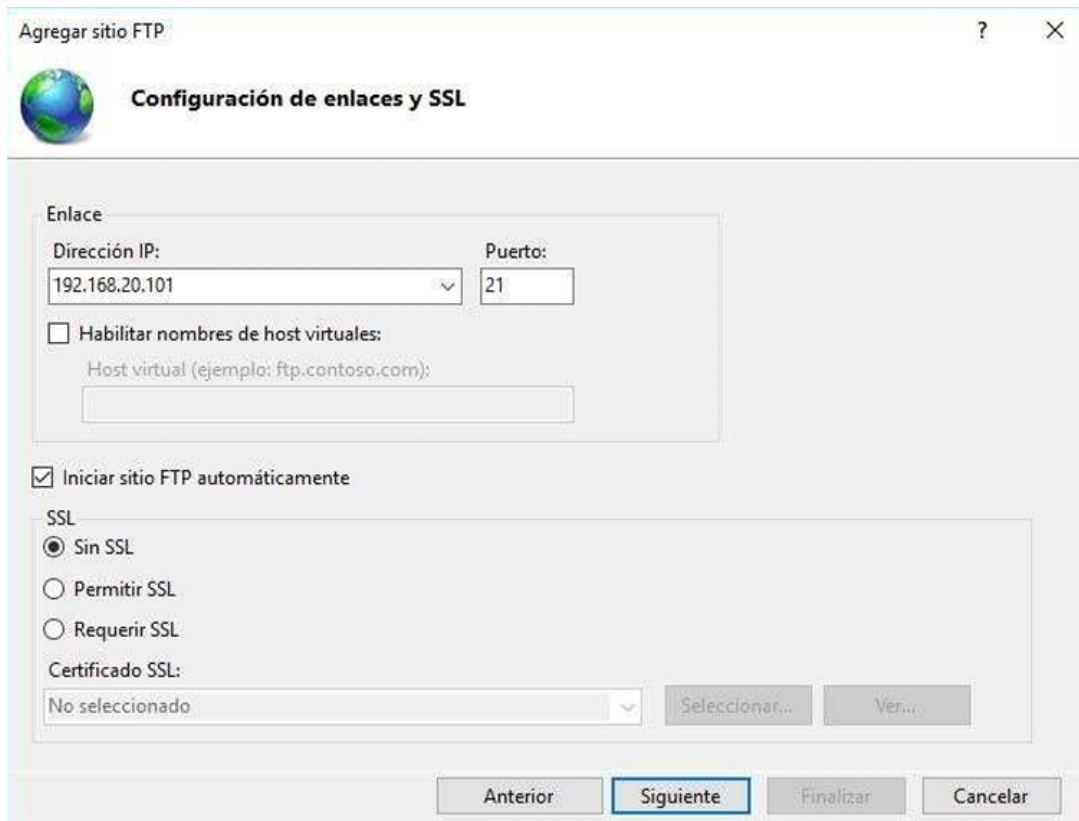
Anterior Siguiente Finalizar Cancelar

Ilustración 15: Rellenando sitio FTP.


16.- Estos son elementos esenciales para la correcta configuración y utilización del servidor FTP:

1. **Dirección IP del Servidor FTP:** Es la dirección IP local en la red interna del servidor. Permite a los usuarios identificar y conectarse al servidor dentro de una red privada.
2. **Número de Puerto:** El puerto por el cual el servidor FTP acepta conexiones. El puerto estándar para FTP es el 21. Este puerto se utiliza para establecer una conexión segura y habilitar la transferencia de archivos entre el cliente y el servidor.

Con estos elementos configurados correctamente, se facilita el acceso al servidor FTP y se asegura la correcta comunicación y transferencia de datos en un entorno seguro.



Agregar sitio FTP

 Configuración de enlaces y SSL

Enlace

Dirección IP: 192.168.20.101 Puerto: 21

☐ Habilitar nombres de host virtuales:
Host virtual (ejemplo: ftp.contoso.com):

☒ Iniciar sitio FTP automáticamente

SSL

☒ Sin SSL
☐ Permitir SSL
☐ Requerir SSL

Certificado SSL: No seleccionado Selecciones... Ver...

Anterior Siguiente Finalizar Cancelar

Ilustración 16: Configuración de enlaces.

17.- Estos permisos determinan quién tiene acceso y qué acciones pueden realizar los usuarios en la carpeta compartida:

La configuración de permisos para una carpeta compartida en un servidor FTP o similar se enfoca en garantizar que solo los usuarios autorizados puedan acceder a los archivos y realizar acciones específicas en ellos. Los permisos establecen un control detallado sobre quién puede leer, escribir, modificar o eliminar archivos en la carpeta.

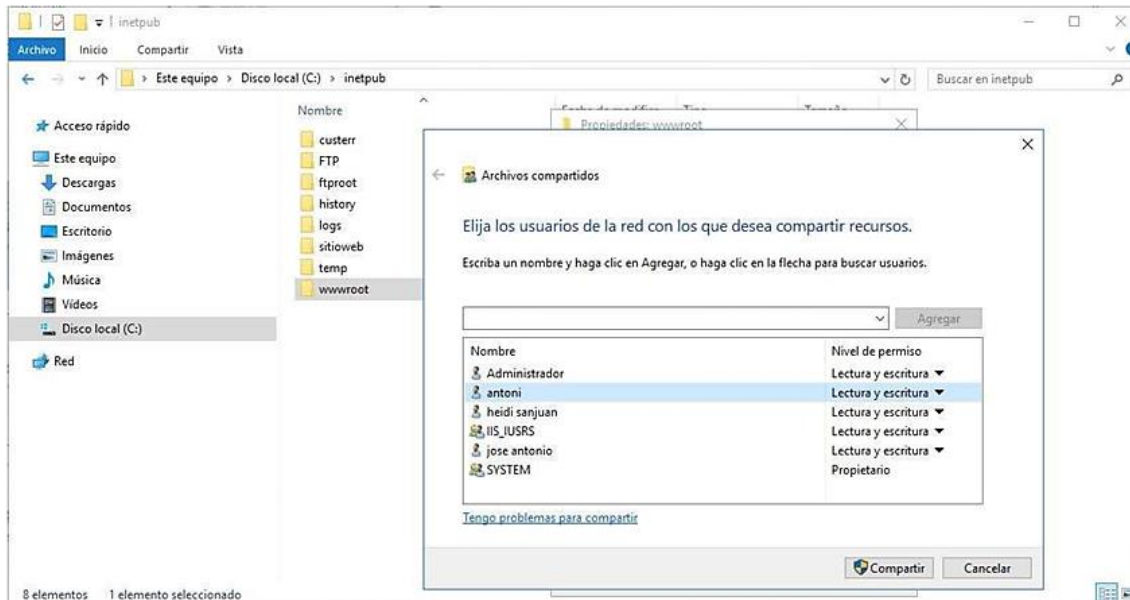


Ilustración 17: Permisos.

18.- Después de configurar los permisos de acceso a una carpeta en un servidor FTP, se solicitará al usuario que introduzca su nombre de usuario y contraseña para autenticarse. Esta verificación es crucial ya que garantiza que solo las personas autorizadas puedan acceder al servidor y a las carpetas compartidas.

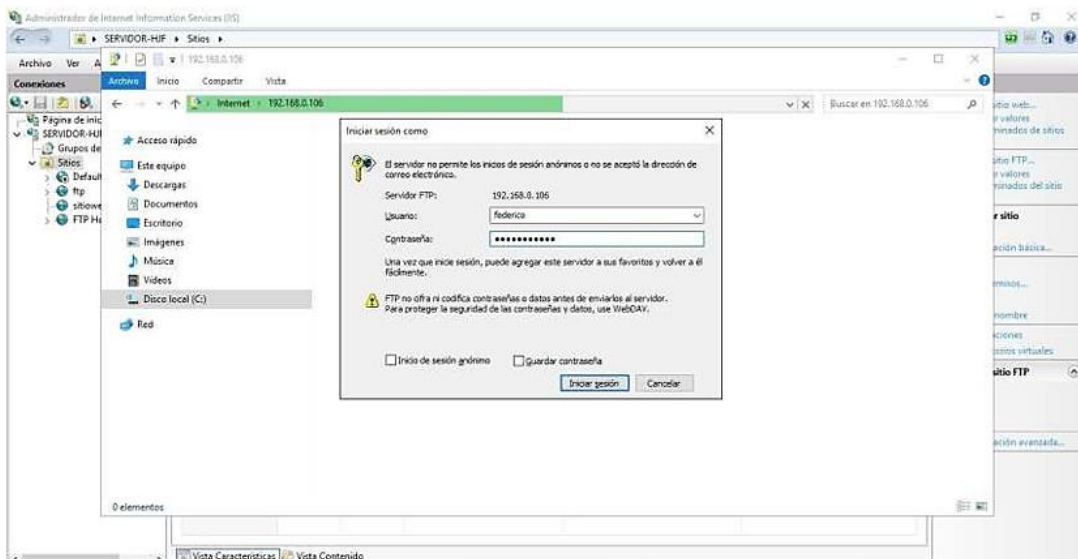


Ilustración 18: Acceso al servidor FTP con usuario.

19.- Podemos observar el acceso al servidor FTP desde una computadora, resaltando la capacidad de compartir archivos de manera efectiva mediante el servidor FTP.

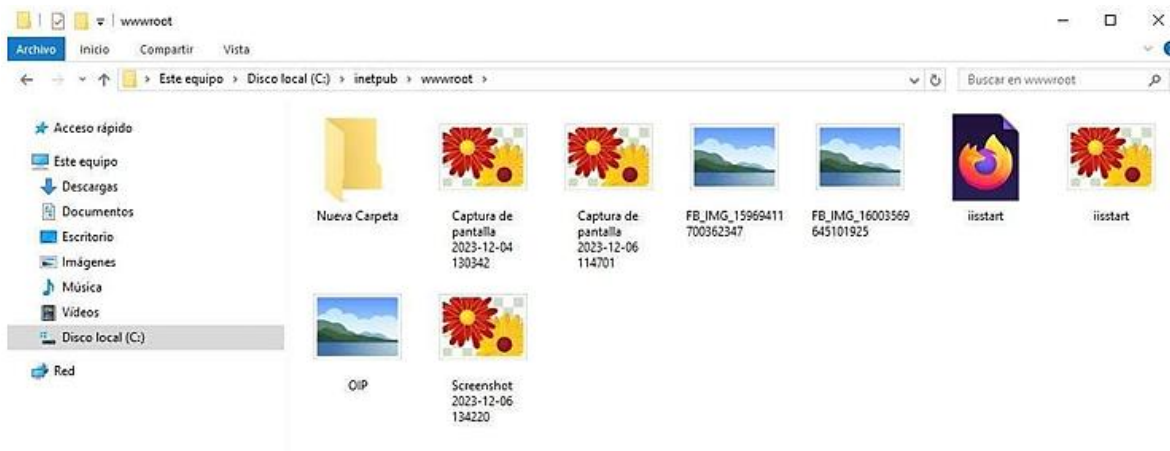


Ilustración 19: Acceso al servidor FTP desde la computadora.

20.- Al acceder desde un dispositivo móvil con el usuario Yanet:

En este contexto, el acceso al servidor FTP desde un dispositivo móvil implica utilizar una aplicación o un cliente FTP compatible en el dispositivo para conectarse al servidor. Esto permite a Yanet acceder a los archivos y carpetas compartidas en el servidor FTP directamente desde su dispositivo móvil.

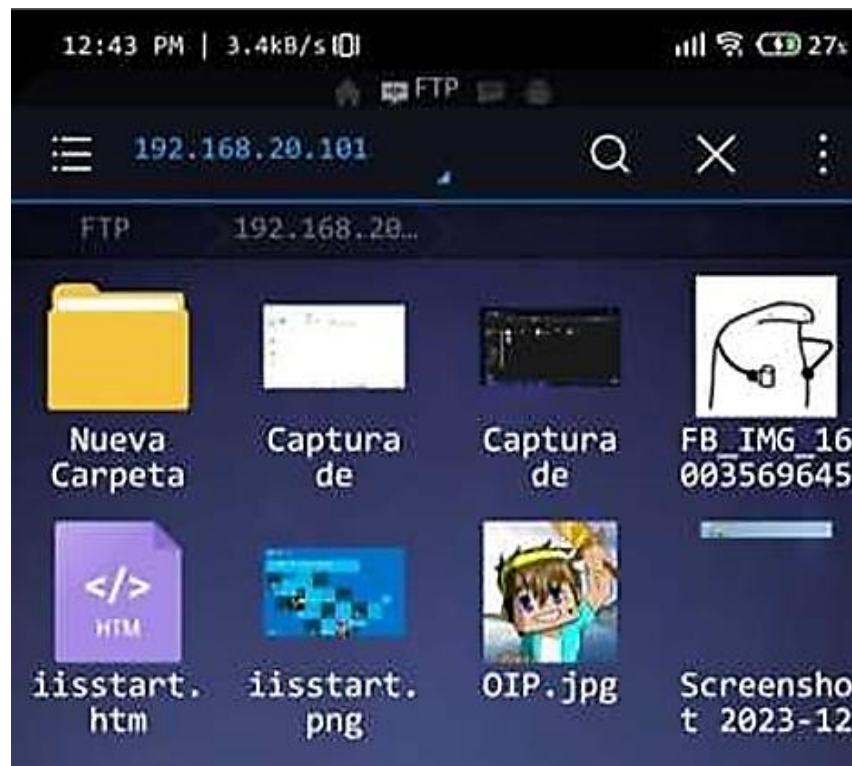


Ilustración 20: Acceso desde el dispositivo móvil.

21.- En este entorno, muestra como también accedemos a nuestro servidor FTP con otro usuario para compartir archivos y recursos desde Filezilla.

Utilizar FileZilla para acceder al servidor FTP con el usuario Heidi permite una gestión eficiente de archivos y recursos, garantizando una experiencia de usuario intuitiva y segura para compartir información entre computadoras y dispositivos.

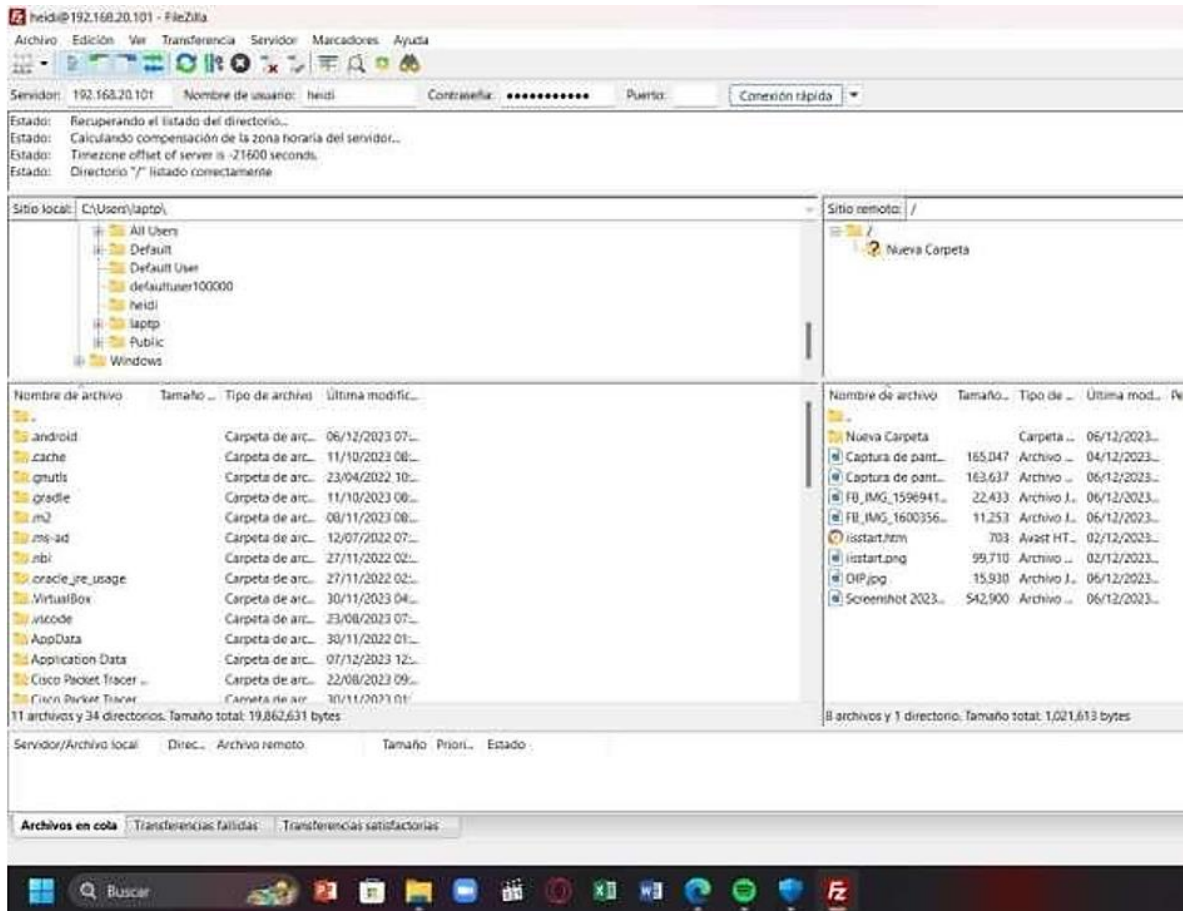


Ilustración 21: Acceso al servidor FTP con otro usuario.



Recomendaciones Adicionales

Para mantener la seguridad en el servidor, es crucial implementar conexiones seguras (SSL/TLS) para cifrar la comunicación entre el servidor y los clientes, así como configurar restricciones de acceso basadas en direcciones IP para limitar quién puede conectarse. Además, es recomendable usar un cortafuegos con reglas estrictas para controlar el tráfico y asegurar un entorno protegido contra amenazas.

En cuanto a la red, utilizar una red dedicada para los servidores ayuda a evitar congestiones y mejorar el rendimiento, mientras que un monitoreo continuo de la red permite detectar problemas a tiempo y mantener una red estable.



Conclusión

Configurar un servidor proxy con CCProxy nos permitió controlar y gestionar el acceso a Internet de manera eficaz dentro de la red. La creación de cuentas de usuario proporcionó una capa adicional de seguridad, asegurando que solo los usuarios autorizados puedan navegar en línea.

El servidor FTP también juega un papel crucial en la transferencia segura de archivos dentro de la red, creando una infraestructura de intercambio de datos eficiente y confiable. Realizar esta práctica de seguridad y bloqueo de páginas con servidor proxy fue valioso porque nos permitió ver que los procedimientos se llevaron a cabo correctamente, asegurando un entorno seguro para el acceso a Internet y la transferencia de archivos en la red. Fue una experiencia útil que subraya la importancia de proteger y gestionar el acceso a la red en un mundo cada vez más digital. Fue muy importante documentar este proceso ya que así cuando se requiera realizar otras funciones, recordar que se tiene este proceso ya configurado y así poder seguir implementando más.



Bibliografías:

- <https://www.avg.com/es/signal/proxy-server-definition#:~:text=Los%20servidores%20proxy%20pueden%20desbloquear.y%20se%20de%20sbloquea%20el%20contenido.>
- <https://www.fortinet.com/lat/resources/cyberglossary/proxy-server>
- <https://axessnet.com/servidor-proxy-para-proteger-la-privacidad-en-internet/>
- <https://www.ibm.com/docs/es/was-nd/8.5.5?topic=security-proxy-server>
- <https://www.netskope.com/es/security-defined/what-is-a-proxy-server>