|  |  |
| --- | --- |
| **Instrumento** | **Práctica de ejercicios** |

|  |  |  |
| --- | --- | --- |
| **Alumno**: Peña Ortiz Jose Alberto | | **Fecha:** 20 de enero de 2023 |
| **Carrera:** TI Area Desarrollo de software Multiplataforma | | **Grupo:** TIDSM51 |
| **Asignatura:** Aplicaciones Web para I4.0 | **Unidad temática:** Unidad 1: I. Comunicación segura. | |
| **Profesor:** MGTICésar Geovanni Machuca Pereida | | |

Contenido

[I.- Ejercicios a resolver: 1](#_Toc125145591)

[II.-Procedimientos y resultados: 2](#_Toc125145592)

[SCP 2](#_Toc125145593)

[SFTP 2](#_Toc125145594)

[HTTPS 3](#_Toc125145595)

[SMTPS 4](#_Toc125145596)

[IMAPS 5](#_Toc125145597)

[SSH 6](#_Toc125145598)

[SET 6](#_Toc125145599)

[SSL 7](#_Toc125145600)

[Certificados de seguridad 8](#_Toc125145601)

# I.- Ejercicios a resolver:

En esta actividad, el alumno explicará el proceso de implementación de protocolos y servicios de seguridad en internet. Desarrolle la explicación de forma gráfica para cada uno de los protocolos con una descripción detallada. Utilice un formato de práctica de ejercicios para realizar la actividad.

# II.-Procedimientos y resultados:

# SCP



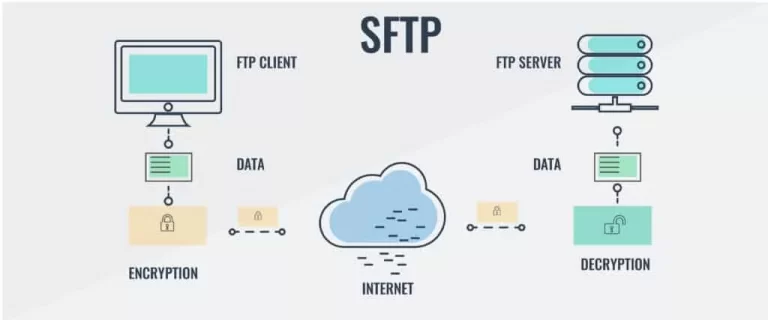
Secure Copy requiere una autenticación de los dos equipos involucrados. Para que se pueda realizar la transmisión a través del protocolo, habrá que establecer, en primer lugar, una conexión SSH desde el equipo local al equipo de destino remoto. Para ello se necesitan, o bien los datos de acceso SSH o una clave autorizada para la autenticación con clave pública.

Una vez que se establece la conexión SSH entre los dos equipos, el cliente SCP inicia un proceso de copia segura en la que están disponibles dos modos diferentes:

Modo fuente: una solicitud SCP en modo fuente lee archivos en el sistema de destino y los envía de vuelta al cliente.

Modo sink: se utiliza en las solicitudes a través del SCP protocol en páginas de clientes del modo sink, le indica al sistema remoto que se trata de datos entrantes y que deben escribirse en el sistema.

# SFTP



Antes de establecer una conexión, el servidor SFTP envía una huella digital encriptada de sus claves públicas de host para asegurarse que la conexión SFTP intercambie datos con el servidor correcto.

La primera vez que se establece la conexión, el programa cliente aún no conoce esta clave y, por lo tanto, el usuario debe confirmar antes del intercambio de datos.

Después de establecer una conexión con el servidor FTP y asegurarse que realmente sea el servidor correcto, el protocolo SFTP guarda la información de la huella digital localmente.

Esto te permite comparar la información de la huella digital con los datos guardados cada vez que estableces una nueva conexión, para asegurarte de que no haya nadie entre tú y el servidor.

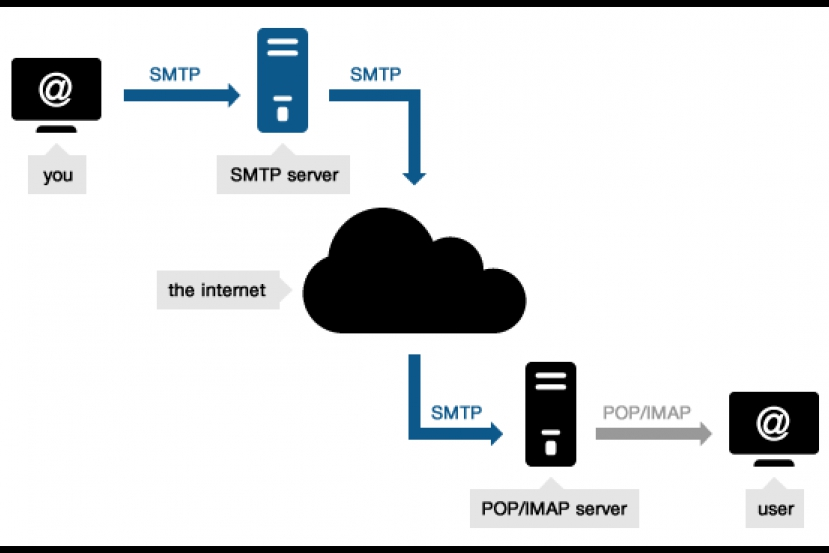
Los diferentes servidores emiten huellas digitales solo una vez. Son generados por la clave privada de un servidor.

# HTTPS



* Abrimos una página de Internet y el navegador intentará conectarse a un sitio que ha sido protegido con SSL.
* El navegador requerirá que el servidor web se identifique.
* Será así como el servidor mandará una copia de su certificado SSL a nuestro navegador.
* El navegador, una vez ha recibido la copia, comprobará si el sitio web es de confianza. Si es así, manda un mensaje que lo acredita.
* El servidor mandará un acuse de recibo con firma digital que permitirá que se inicie la conexión cifrada.
* Así es como empezarán a transferirse datos cifrados entre el servidor y el navegador.

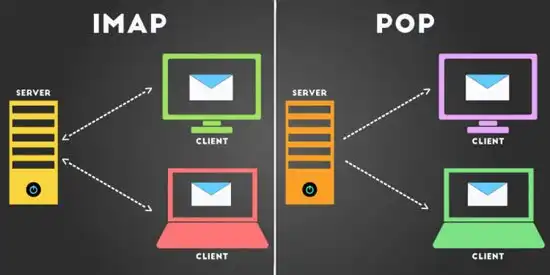
# SMTPS



Durante este proceso, las máquinas “dialogan” utilizando SMTPS: el protocolo provee un estándar, y establece la guía para que los servidores se identifiquen y comuniquen, comprendiendo quién es el remitente, quién es el destinatario, hacia donde deben dirigir el contenido, etc.

En pocas palabras, cómo entregar en forma adecuada el email (y también resolver cualquier problema). Cualquier proveedor de email normal (tal como Gmail o Hotmail) posee un servidor SMTPS asociado para el proceso de entrega.

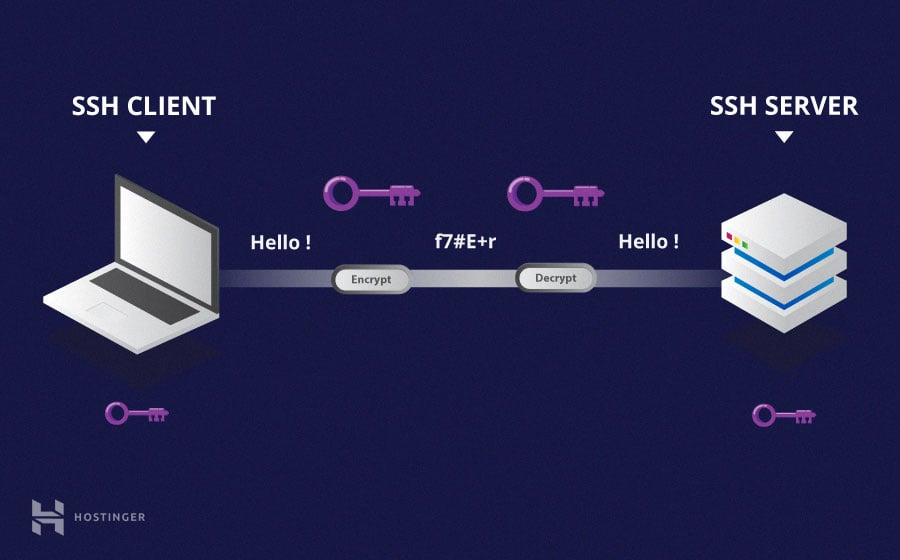
# IMAPS

\

S

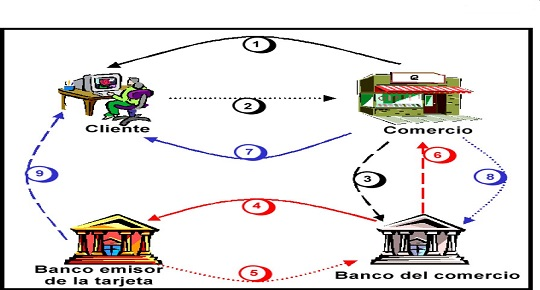
Permite acceder a los mensajes que hay almacenados en un determinado servidor. Simplemente es necesario contar con un equipo que tenga acceso a Internet y poder entrar a ese servidor. Este protocolo no permite enviar correos. Lo que hace realmente es dar acceso a los mensajes que hay almacenados en ese servidor. Tiene una ventaja frente a otros protocolos similares y es que IMAP permite visualizar el contenido en ese servidor sin necesidad de descargarlo. De esta forma, un usuario puede acceder desde un ordenador a un servidor, ver los mensajes y no tener que bajarlos a su propio equipo.

# SSH



el cliente SSH lleva a cabo el proceso de configuración de la conexión y usa el cifrado de clave pública para verificar la identidad del servidor SSH. Después de la fase de configuración, el protocolo SSH utiliza un cifrado métrico fuerte y algoritmos de hash para garantizar la privacidad e integridad de los datos intercambiados entre el cliente y el servidor.

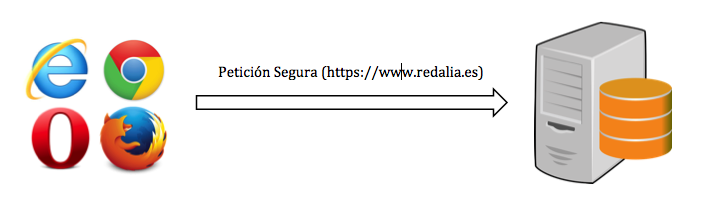
# SET



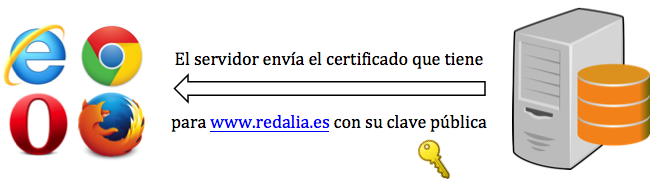
cuando se realiza una transacción segura por medio de SET, los datos del cliente son enviados al servidor del vendedor, pero dicho vendedor sólo recibe la orden. Los números de la tarjeta del banco se envían directamente al banco del vendedor, quien podrá leer los detalles de la cuenta bancaria del comprador y contactar con el banco para verificarlos en tiempo real.

# SSL

Un usuario realiza una petición HTTP segura a través de un navegador a un sitio web (<HTTPS://www.redalia.es/>)

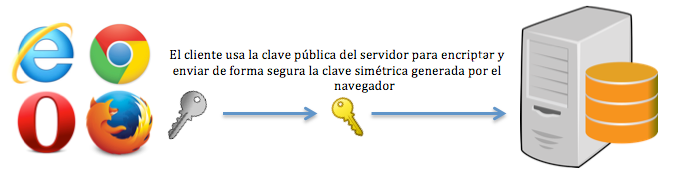


El servidor donde está alojado el sitio web, envía (si lo tiene) el certificado que incluye la clave pública del servidor. En caso de no tener certificado SSL, se producirá un error.

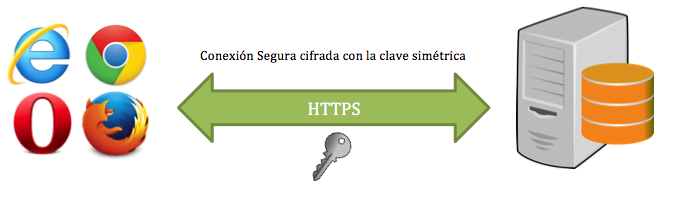


El navegador comprueba que la entidad emisora del certificado o CA sea de confianza. En caso contrario, pedirá al usuario que acepte el certificado bajo su responsabilidad.

Llegados a este punto, el navegador generará una clave simétrica, que será cifrada mediante la clave pública del servidor para ser enviada de manera segura al mismo.



De esta forma, la comunicación ya se ha establecido de manera segura, y será cifrada en ambos sentidos mediante la clave generada en el punto anterior.



# Certificados de seguridad



Los certificados SSL funcionan garantizando que los datos transferidos entre usuarios y sitios web, o entre dos sistemas, sean imposibles de leer. Utiliza algoritmos de cifrado para cifrar los datos en tránsito, lo que evita que los hackers la información que se envía a través de la conexión. Estos datos incluyen información potencialmente confidencial, como nombres, direcciones, números de tarjetas de crédito u otros detalles financieros.

El proceso funciona de la siguiente manera:

* Un navegador o servidor intenta conectarse a un sitio web (es decir, un servidor web) protegido mediante certificados SSL.
* El navegador o servidor solicita que el servidor web se identifique.
* En respuesta el servidor web envía al navegador o servidor una copia de su certificado SSL.
* El navegador o servidor evalúa si el certificado SSL es confiable. En caso afirmativo, envía una señal al servidor web.
* A continuación, el servidor web devuelve un reconocimiento firmado digitalmente para iniciar una sesión cifrada mediante SSL.
* Los datos cifrados se comparten entre el navegador o servidor y el servidor web.

Este proceso a veces se conoce como “enlace SSL”. Aunque parece ser un proceso largo, se lleva a cabo en milisegundos.