

**Centro de Enseñanza Técnica Industrial**

**Desarrollo de Software**

**Instalación del servidor FTP + SSL**

**Jesús Alberto Aréchiga Carrillo**

**22310439 5N**

**Profesor**

**José Francisco Pérez Reyes**

**Diciembre 2024**

**Guadalajara, Jalisco**

## Introducción

El protocolo FTPes una herramienta estándar utilizada para la transferencia de archivos entre sistemas cliente y servidor. Sin embargo, en su forma básica, FTP transmite datos sin cifrar, lo que puede ser un riesgo de seguridad en redes públicas o no confiables.

Para mitigar este problema, se puede utilizar FTPS (FTP Secure), una versión de FTP que agrega una capa de seguridad mediante el protocolo SSL/TLS. El servidor vsftpd, conocido por su seguridad y eficiencia, soporta el uso de certificados SSL/TLS para habilitar conexiones FTPS, asegurando que las comunicaciones entre el cliente y el servidor estén cifradas.

## Desarrollo

El objetivo principal de este proyecto es habilitar conexiones FTPS en un servidor vsftpd mediante la instalación y configuración de un certificado SSL/TLS. Esto garantizará que todas las transferencias de archivos y credenciales sean seguras, protegiendo la integridad y confidencialidad de los datos. Se va a utilizar una VM con el servidor ya instalado previamente, en este caso la VM tiene una IP 10.0.0.8.

Para instalar el certificado se utiliza el comando “openssl req -x509 -nodes -days 1825 -newkey rsa:2048 -keyout /etc/ssl/private/vsftpd.key -out /etc/ssl/certs/vsftpd.crt”

La consola va a mostrar los campos del certificado que hay que ingresar para poder generarlo:

Country Name (2 letter code) [GB]: MX

State or Province Name (full name) [Berkshire]: Jalisco

Locality Name (eg, city) [Newbury]: Guadalajara

Organization Name (eg, company) [My Company Ltd]: Empresa, S.A. de C.V.

Organizational Unit Name (eg, section) []: Departamento de TI

Common Name (eg your name or your server's hostname) []: \*.dominio.org

Email Address []: webmaster@dominio.org

Se le dan los permisos al certificado y a la clave privada con “chmod 400 /etc/ssl/certs/vsftpd.crt /etc/ssl/private/vsftpd.key”

Ahora se agregan las configuraciones al archivo vsftpd.cfg

# Habilita el soporte de TLS/SSL

ssl\_enable=YES

# Deshabilita o habilita utilizar TLS/SSL con usuarios anónimos

allow\_anon\_ssl=NO

# Obliga a utilizar TLS/SSL para todas las operaciones,

# es decir, transferencia de datos y

# autenticación de usuarios locales. Establecer el valor NO,

# hace que sea opcional utilizar TLS/SSL.

force\_local\_data\_ssl=YES

force\_local\_logins\_ssl=YES

# Se prefiere TLSv1 sobre SSLv2 y SSLv3

ssl\_tlsv1=YES

ssl\_sslv2=NO

ssl\_sslv3=NO

# Rutas del certificado y firma digital

rsa\_cert\_file=/etc/ssl/certs/vsftpd.crt

rsa\_private\_key\_file=/etc/ssl/private/vsftpd.key

# Los desarrolladores de FileZilla decidieron con la versión 3.5.3 que eliminarían el soporte para

# el algoritmo de cifrado 3DES-CBC-SHA, con el argumento de que este algoritmo es una de los más

# lentos. Sin embargo con ésto rompieron compatibilidad con miles de servidores FTP que utilizan

# FTPES. La solución temporal, mientras los desarrolladores de FileZilla razonan lo absurdo de su

# decisión, es utilizar la siguiente opción:

ssl\_ciphers=HIGH

# Filezilla además requiere desactivar la siguiente opción que puede romper compatibilidad con otros

# clientes. Cabe señalar que Filezilla se ha convertido en un desarrollo políticamente incorrecto

# por dejar de respetar los estándares.

require\_ssl\_reuse=NO

Se reinicia el servicio y se prueba.

## Evidencias

Consola mostrando la dirección IP de la máquina virtual con la que está trabajando en ese momento

A computer screen with white text

Description automatically generated

Consola mostrando los procesos que se están ejecutando en la máquina virtual y visualizando correctamente el proceso vsftpd

A screen shot of a computer

Description automatically generated

Consola del Dom0 mostrando la información de la ejecución de tu máquina virtual que está ejecutando el servidor de FTP

A computer screen with white text

Description automatically generated

Ventana del cliente FTP para establecer la conexión (antes de establecer conexión) con toda la información y configuración requerida

A screenshot of a computer

Description automatically generated

Ventana del cliente FTP mostrando la conexión realizada y mostrando las carpetas que tienes en tu servidor FTP.

A screen shot of a computer error

Description automatically generated A screenshot of a computer

Description automatically generated

Consola de la máquina virtual mostrando el detalle de la carpeta y archivo (comando: ls -la) que subiste desde el cliente FTP

A screenshot of a computer

Description automatically generated A computer screen with a green circle

Description automatically generated A screenshot of a computer

Description automatically generated A computer screen with white text

Description automatically generated

## Conclusiones

La implementación de un certificado SSL en el servidor vsftpd para habilitar conexiones FTPS constituye un avance significativo hacia la protección de la información en entornos de transferencia de archivos.

La transición de FTP a FTPS responde a la creciente necesidad de mitigar riesgos asociados con la interceptación de datos sensibles, particularmente en redes públicas. Al incorporar un certificado SSL, se garantiza una comunicación segura y verificable, protegiendo tanto las credenciales como los archivos intercambiados.