

# Very Secure FTP Daemon (vsftpd)

## Conexiones seguras SSL

Como el protocolo ftp no encripta la información que fluye entre la aplicación cliente y el servidor, los datos privados pueden ser obtenidos con mucha facilidad mediante el escaneado de paquetes. Para aumentar la seguridad se puede activar la encriptación de paquetes utilizando SSL para tener un servicio FTP menos vulnerable (FTPS).

1. El primer paso consiste en generar un Certificado SSL, para ello necesitamos tener instalados los paquetes openssl y openssl-certs. Nos dirigimos al directorio /etc/ssl/certs y ahí ejecutamos el siguiente comando:

```
openssl req -x509 -nodes -days 7300 -newkey rsa:2048 -keyout  
/etc/ssl/certs/vsftpd.pem -out /etc/ssl/certs/vsftpd.pem
```

Para preparar el certificado, el comando openssl nos solicitará que ingresemos varios datos. Cuando finalice tendremos el certificado concluido con el nombre vsftpd.pem.

2. Para el siguiente paso editamos el archivo de configuración vsftpd.conf, nos dirigimos hasta el final donde agregaremos las siguientes líneas:

```
# Secure FTP  
# Activamos el soporte SSL  
ssl_enable=YES  
  
# Obligamos el establecimiento de conexiones encriptadas mediante  
# SSL para usuarios locales.  
force_local_logins_ssl=YES  
  
# No se obliga a que las transferencias de datos locales sean  
# encriptados con SSL.  
force_local_data_ssl=NO  
  
# Se habilitan los soportes para las diversas versiones de SSL.  
ssl_tlsv1=YES  
ssl_sslv2=YES  
ssl_sslv3=YES  
  
# Soluciona el problema de incompatibilidad entre la suite cipher  
# implementada por FileZilla y la implementada por defecto en vsftpd  
# (DES-CBC3-SHA). Ref: http://trac.filezilla-project.org/ticket/7873  
ssl_ciphers=HIGH  
  
# Se especifica la ubicación del Certificado Generado.  
rsa_cert_file=/etc/ssl/certs/vsftpd.pem  
rsa_private_key_file=/etc/ssl/certs/vsftpd.pem
```

3. Por último, reiniciamos nuevamente el servicio vsftpd:

```
service vsftpd restart
```

Podemos probar de establecer conexiones seguras utilizando clientes que soportan esta funcionalidad (FilleZilla, gfTP). Para establecer una conexión segura desde la aplicación cliente **Filezilla** debemos agregar un sitio en el gestor de sitios con la opción **Tipo de Servidor = FTPES** (FTP sobre TLS/SSL explícito).