

SERVIDOR FILEZILLA FTP EN WINDOWS 7

Requisitos previos: Tener instalado un sistema de virtualización en este caso VirtualBox y tener a disposición los siguientes sistemas Windows 7 y Server 2008R2, pfSense y Debian

Descripción de la práctica: Configurar un servidor de transferencia de ficheros con filezilla server, permitir conexiones desde la red local y red WAN, hacer que el servidor funcione con certificado (FTPS)

Descripción de Hardware: Equipo real, Intel Core i7 con 16GB de RAM y 199GB de disco duro

Esquema de la Red

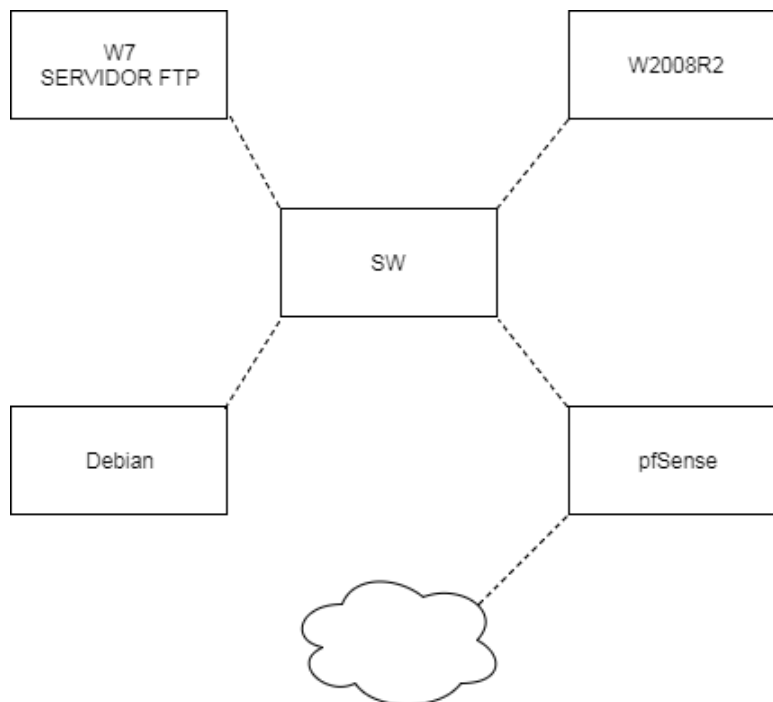
Rangos de direcciones:

192.168.99.1- pfSense

192.168.99.2- W2008

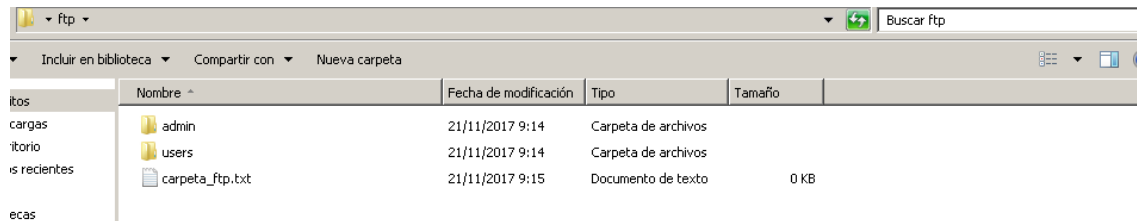
192.168.99.3- Debian

192.168.99.12- Windows7

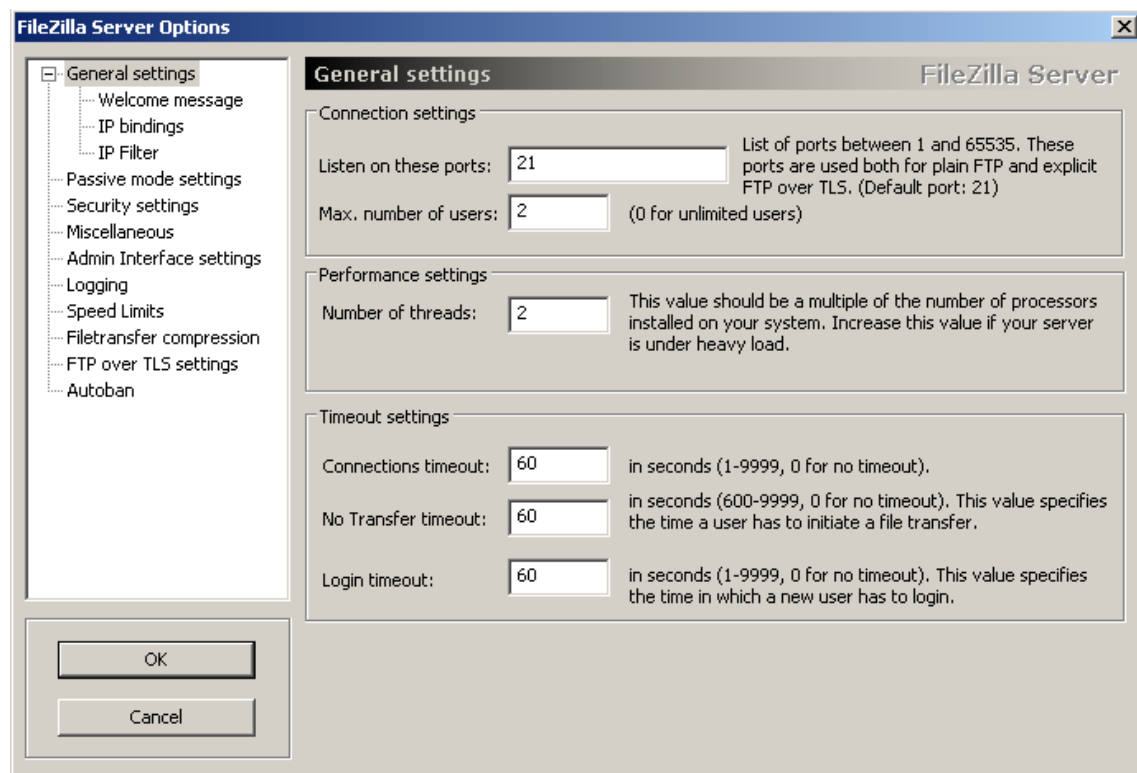


SERVIDOR FILEZILLA FTP EN WINDOWS 7

Como primer paso, dentro de la carpeta que queramos crearemos la estructura de carpetas, primero una carpeta llamada ftp, después admin y users.

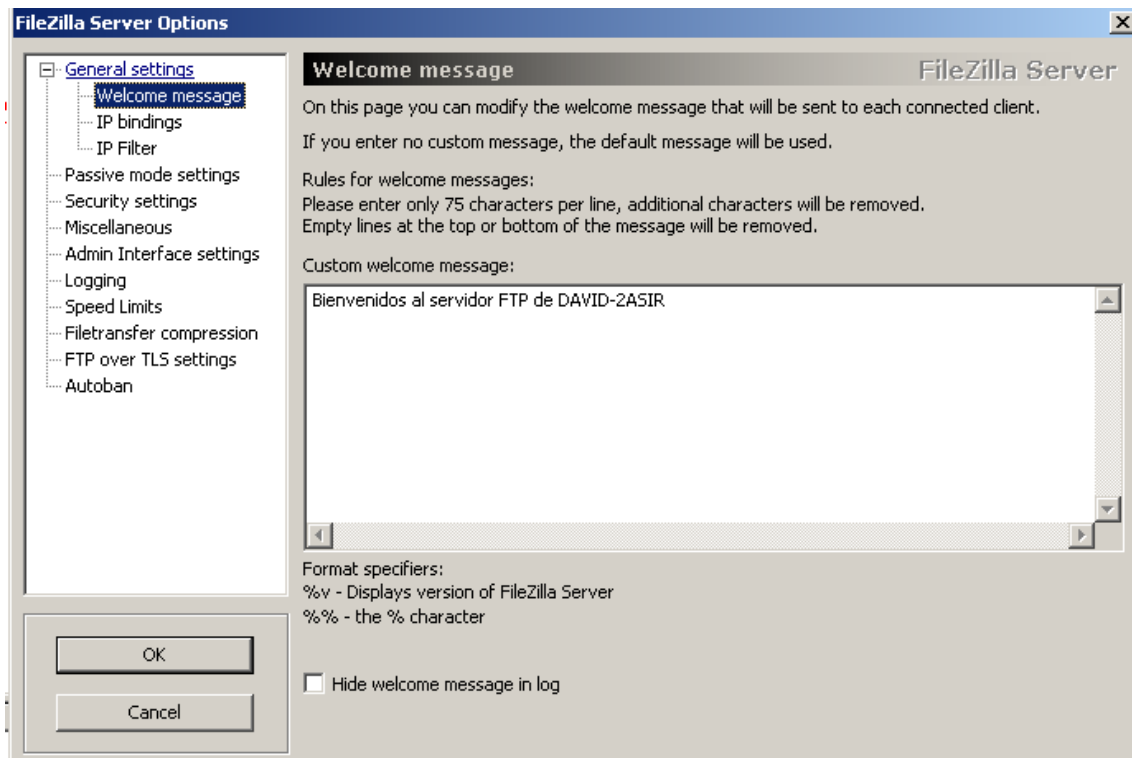


Ahora configuramos las opciones del servidor, el puerto de escucha y los tiempos de cierre de sesión.

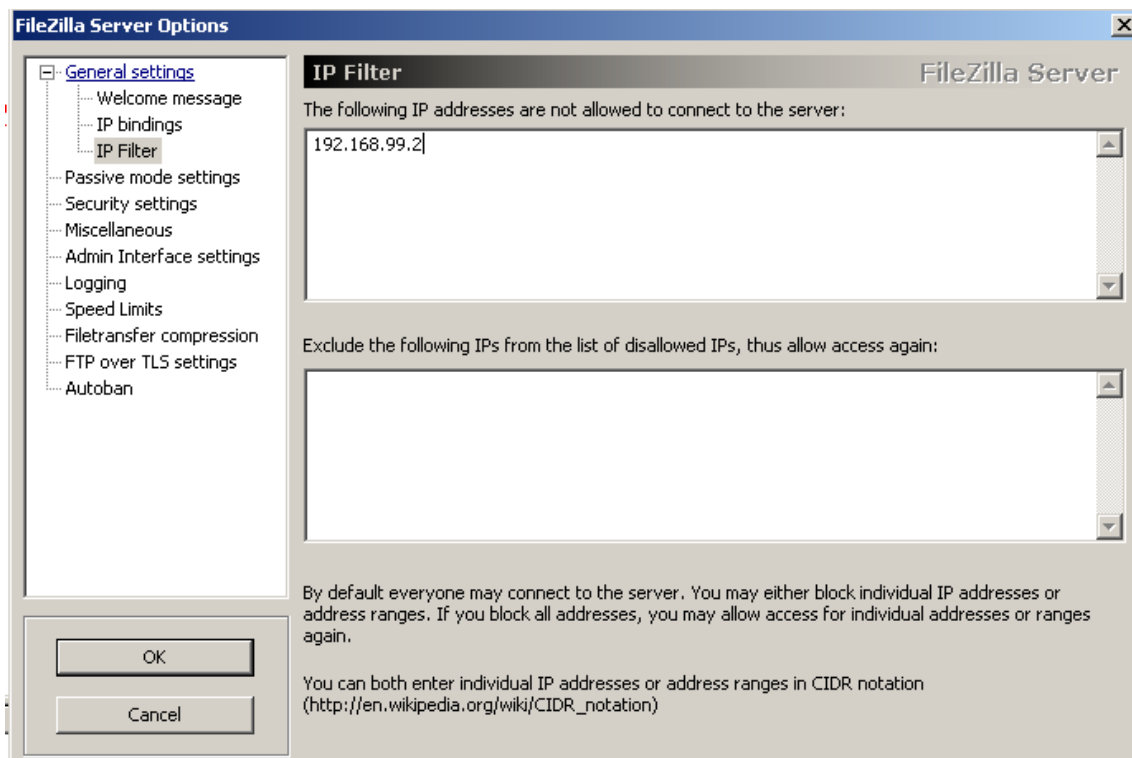


SERVIDOR FILEZILLA FTP EN WINDOWS 7

Añadimos también un mensaje de bienvenida al servidor.

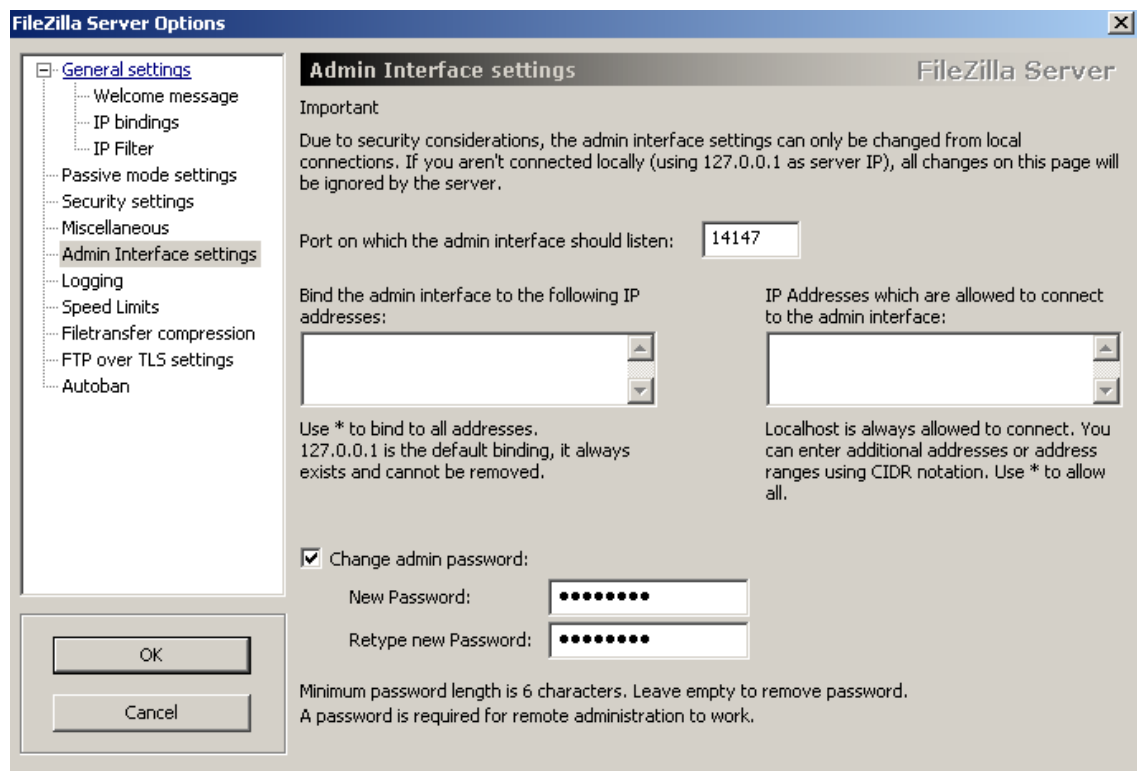


También prohibiremos al equipo 192.168.99.2 acceder al servidor.

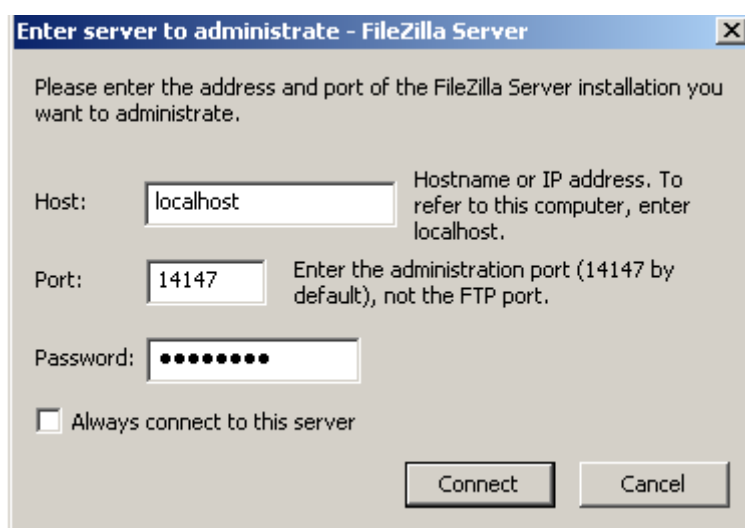


SERVIDOR FILEZILLA FTP EN WINDOWS 7

Modificaremos la contraseña de administrador ya que no queremos que nadie con acceso al equipo tenga acceso al servidor.

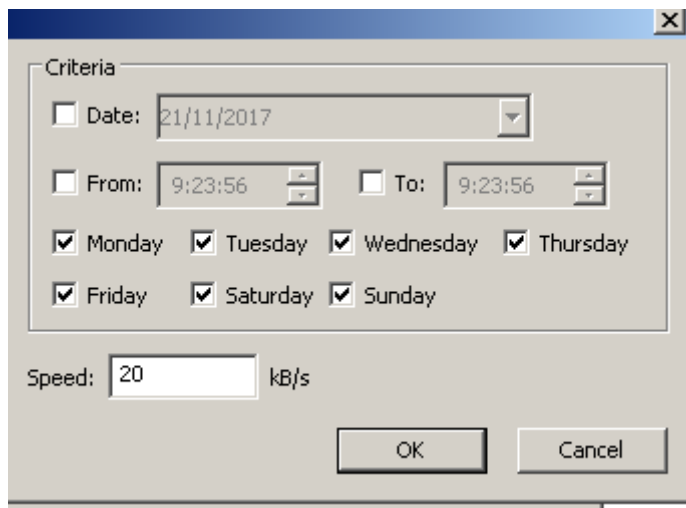


Probamos a salir y volver a entrar al servidor con contraseña.

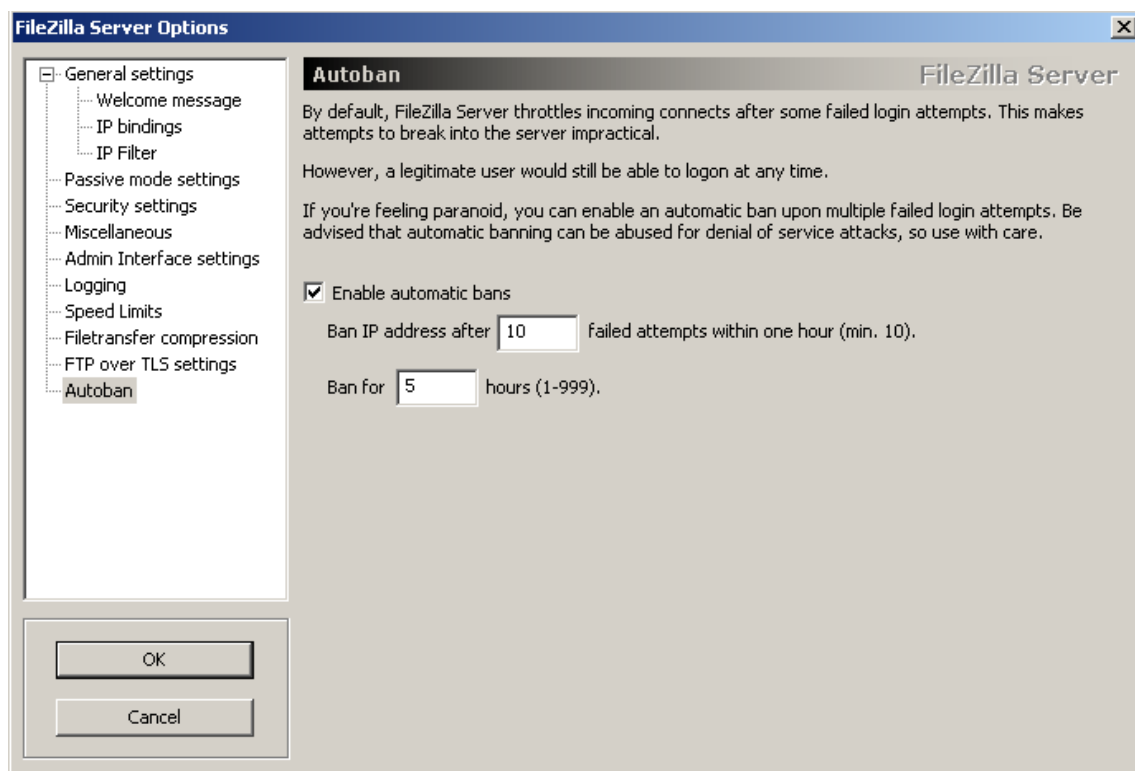


SERVIDOR FILEZILLA FTP EN WINDOWS 7

Ahora limitaremos la velocidad de transferencia a 20kB/S

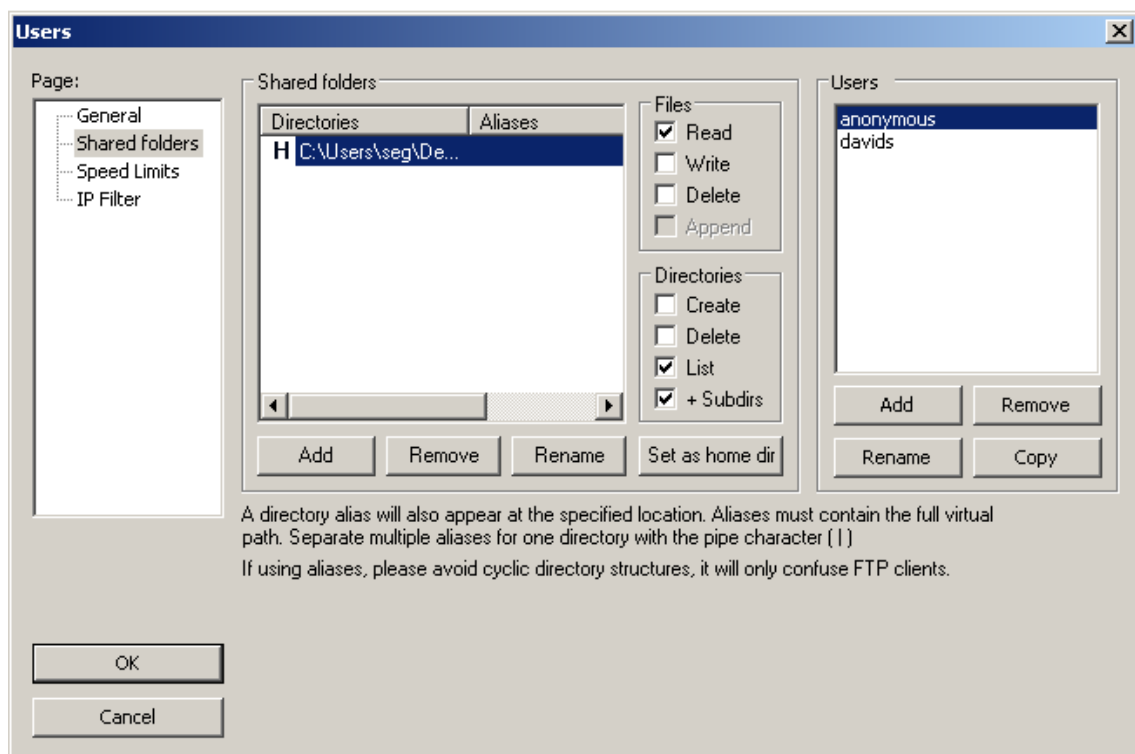


Activamos el autoban que su función consiste en bloquear una dirección IP después de 10 fallos de conexión y será bloqueado por 5 horas.



SERVIDOR FILEZILLA FTP EN WINDOWS 7

Ahora añadiremos los usuarios y les asignaremos las carpetas a las que tendrán acceso. En este caso davids y anonymous, a anonymous le asignaremos permisos de lectura en la carpeta users



SERVIDOR FILEZILLA FTP EN WINDOWS 7

Probamos la conexión de anonymous.

The screenshot shows the FileZilla Server interface and a Windows command prompt. The FileZilla Server window displays the status of the server, including the version (0.9.60 beta) and the current connection status. The command prompt shows the execution of the 'ftp localhost' command, which results in a connection to the local FTP server. The user 'anonymous' is logged in, and the server responds with '220 Bienvenidos al servidor FTP de DAVID-2ASIR'. The user then enters the command 'ls', and the server responds with '150 Opening data channel for directory listing of "/"'. The command prompt also shows the output of the 'ls' command, which lists the contents of the current directory.

FileZilla Server (127.0.0.1)

File Server Edit ?

FileZilla Server 0.9.60 beta
Copyright 2001-2016 by Tim Kosse (tim.kosse@filezilla-project.org)
https://filezilla-project.org/
Connecting to server localhost:14147...
Connected, waiting for authentication
Logged on
You appear to be behind a NAT router. Please configure the passive mode settings and forward a range of ports in your router.
Warning: FTP over TLS is not enabled, users cannot securely log in.
Retrieving account settings, please wait...
Done retrieving account settings:
Sending account settings, please wait...
Done sending account settings:
(000011/21/11/2017 9:29:20 - [not logged in] [-1]) Connected on port 21, sending welcome message...
(000011/21/11/2017 9:30:20 - [not logged in] [-1]) 220 Bienvenidos al servidor FTP de DAVID-2ASIR
(000011/21/11/2017 9:30:21 - [not logged in] [-1]) 421 Connection timed out.
(000011/21/11/2017 9:30:21 - [not logged in] [-1]) disconnected.
(000011/21/11/2017 9:30:52 - [not logged in] [-1]) Connected on port 21, sending welcome message...
(000011/21/11/2017 9:30:52 - [not logged in] [-1]) 220 Bienvenidos al servidor FTP de DAVID-2ASIR
(000011/21/11/2017 9:30:55 - [not logged in] [-1]) USER anonymous
(000011/21/11/2017 9:30:55 - [not logged in] [-1]) 331 Password required for anonymous
(000011/21/11/2017 9:30:55 - [not logged in] [-1]) PASS
(000011/21/11/2017 9:30:59 - anonymous [-1]) 230 Logged on
(000011/21/11/2017 9:31:01 - anonymous [-1]) EPRT [2:1H9441]
(000011/21/11/2017 9:31:01 - anonymous [-1]) 200 Port command successful
(000011/21/11/2017 9:31:01 - anonymous [-1]) NLST
(000011/21/11/2017 9:31:01 - anonymous [-1]) 150 Opening data channel for directory listing of "/"
(000011/21/11/2017 9:31:01 - anonymous [-1]) 226 Successfully transferred "/"

ID	Account	IP	Transfer	Progress	Speed
000012	anonymous	:::1			

Ready 49 bytes received 0 B/s 312 bytes sent 0 B/s

The screenshot shows the FileZilla Server interface and a Windows command prompt. The FileZilla Server window displays the status of the server, including the version (0.9.60 beta) and the current connection status. The command prompt shows the execution of the 'ftp localhost' command, which results in a connection to the local FTP server. The user 'anonymous' is logged in, and the server responds with '220 Bienvenidos al servidor FTP de DAVID-2ASIR'. The user then enters the command 'ls', and the server responds with '150 Opening data channel for directory listing of "/"'. The command prompt also shows the output of the 'ls' command, which lists the contents of the current directory.

FileZilla Server (127.0.0.1)

File Server Edit ?

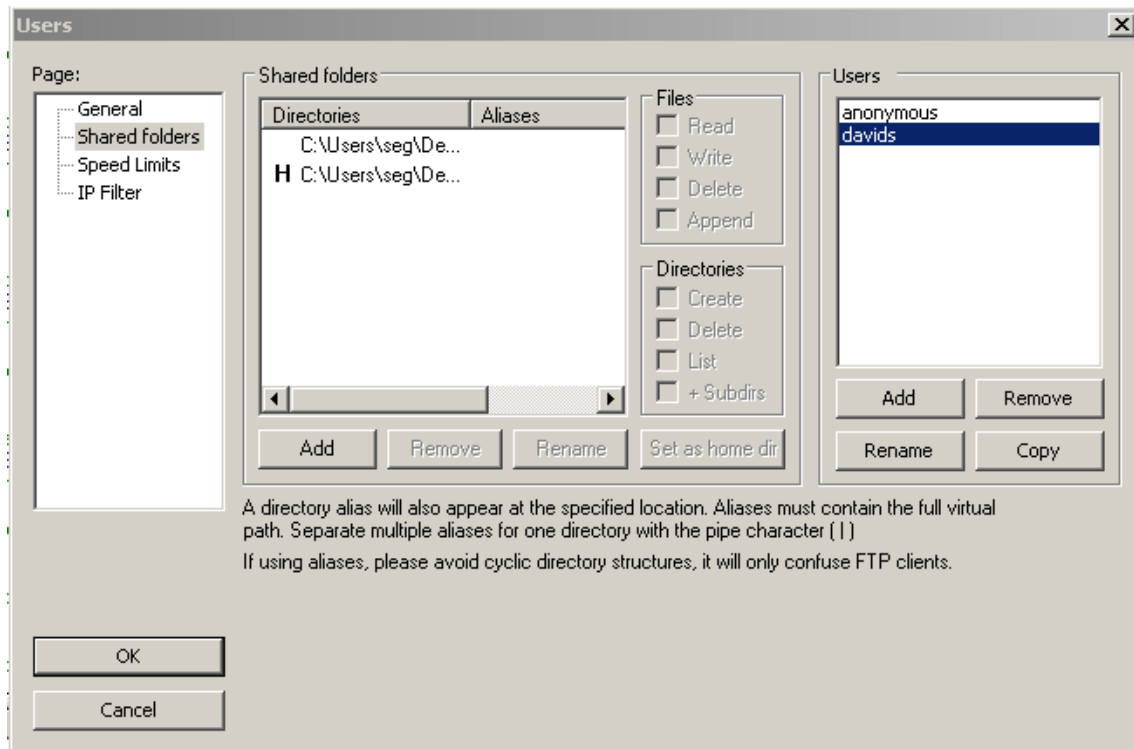
FileZilla Server 0.9.60 beta
Copyright 2001-2016 by Tim Kosse (tim.kosse@filezilla-project.org)
https://filezilla-project.org/
Connecting to server localhost:14147...
Connected, waiting for authentication
Logged on
You appear to be behind a NAT router. Please configure the passive mode settings and forward a range of ports in your router.
Warning: FTP over TLS is not enabled, users cannot securely log in.
Retrieving account settings, please wait...
Done retrieving account settings:
Sending account settings, please wait...
Done sending account settings:
(000011/21/11/2017 9:29:20 - [not logged in] [-1]) Connected on port 21, sending welcome message...
(000011/21/11/2017 9:30:20 - [not logged in] [-1]) 220 Bienvenidos al servidor FTP de DAVID-2ASIR
(000011/21/11/2017 9:30:21 - [not logged in] [-1]) 421 Connection timed out.
(000011/21/11/2017 9:30:21 - [not logged in] [-1]) disconnected.
(000011/21/11/2017 9:30:52 - [not logged in] [-1]) Connected on port 21, sending welcome message...
(000011/21/11/2017 9:30:52 - [not logged in] [-1]) 220 Bienvenidos al servidor FTP de DAVID-2ASIR
(000011/21/11/2017 9:30:55 - [not logged in] [-1]) USER anonymous
(000011/21/11/2017 9:30:55 - [not logged in] [-1]) 331 Password required for anonymous
(000011/21/11/2017 9:30:55 - [not logged in] [-1]) PASS
(000011/21/11/2017 9:30:59 - anonymous [-1]) 230 Logged on
(000011/21/11/2017 9:31:01 - anonymous [-1]) EPRT [2:1H9441]
(000011/21/11/2017 9:31:01 - anonymous [-1]) 200 Port command successful
(000011/21/11/2017 9:31:01 - anonymous [-1]) NLST
(000011/21/11/2017 9:31:01 - anonymous [-1]) 150 Opening data channel for directory listing of "/"
(000011/21/11/2017 9:31:01 - anonymous [-1]) 226 Successfully transferred "/"

ID	Account	IP	Transfer	Progress	Speed
000012	anonymous	:::1			

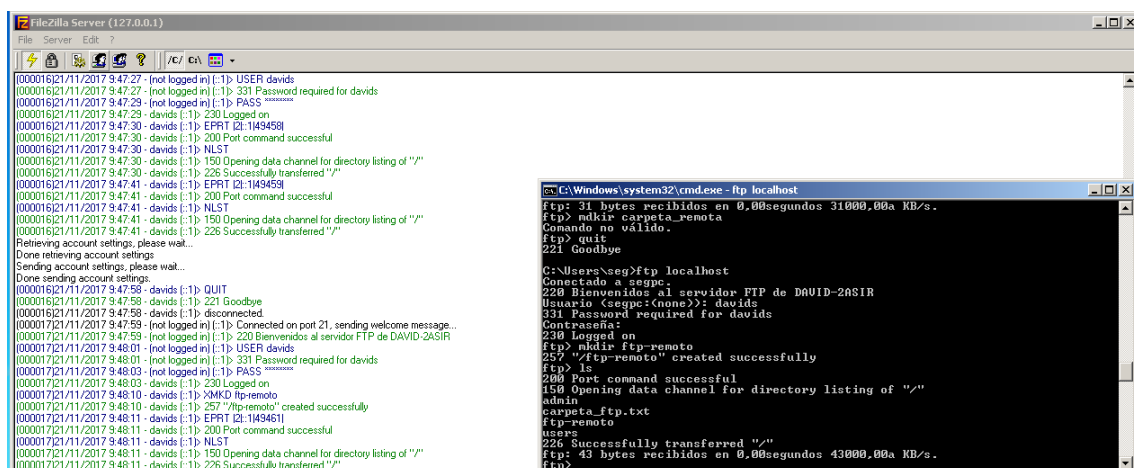
Ready 49 bytes received 0 B/s 339 bytes sent 0 B/s

SERVIDOR FILEZILLA FTP EN WINDOWS 7

Ahora añadimos la carpeta davids como home del usuario davids con permisos de escritura y lectura.



Probamos la conexión de davids.



SERVIDOR FILEZILLA FTP EN WINDOWS 7

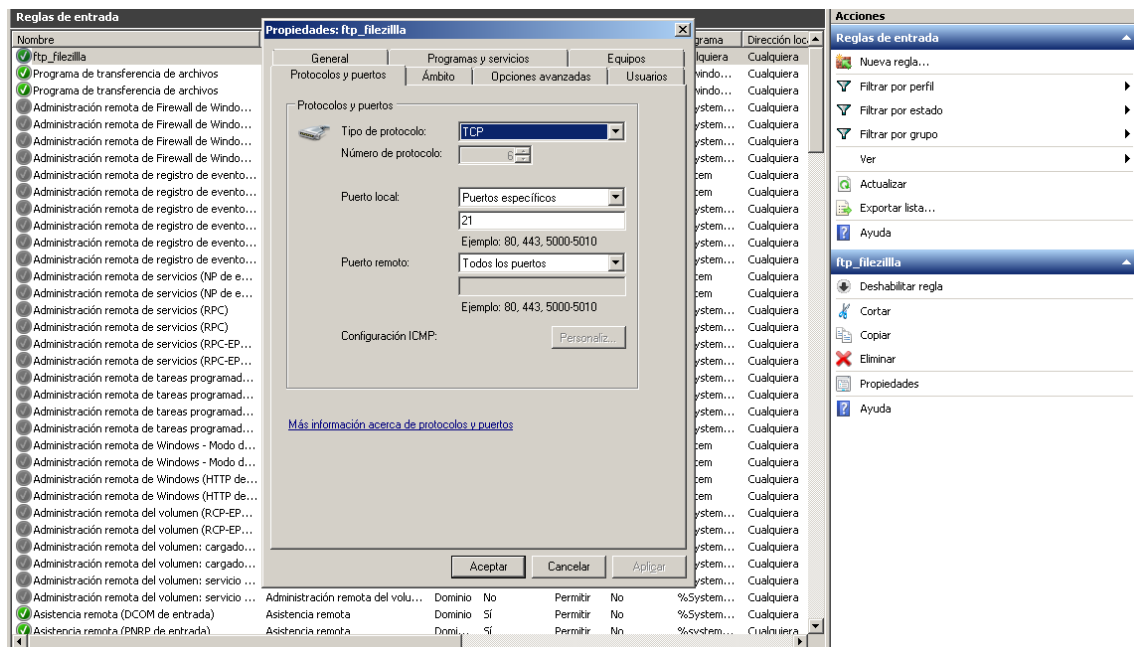
Vamos a probar a subir ficheros a la carpeta de davids

```

C:\Windows\system32\cmd.exe - ftp localhost
200 Port command successful
150 Opening data channel for file upload to server of "/prueba_subida.txt"
226 Successfully transferred "/prueba_subida.txt"
ftp> ls
200 Port command successful
150 Opening data channel for directory listing of "/"
admin
carpeta_ftp.txt
ftp-remoto
prueba_subida.txt
users
226 Successfully transferred "/"
ftp: 62 bytes recibidos en 0,00segundos 62000,00a KB/s.
ftp> cd ftp-remoto
250 CWD successful. "/ftp-remoto" is current directory.
ftp> ls
200 Port command successful
150 Opening data channel for directory listing of "/ftp-remoto"
226 Successfully transferred "/ftp-remoto"
ftp> put prueba_subida.txt
200 Port command successful
150 Opening data channel for file upload to server of "/ftp-remoto/prueba_subida
.txt"
226 Successfully transferred "/ftp-remoto/prueba_subida.txt"
ftp>
  
```

Vamos a hacer el servidor accesible a través de la red real, es decir autorizar a pfSense para que redirija las conexiones ftp hacia nuestro servidor filezilla.

Primero, añadimos una regla de entrada en el firewall de Windows como en la captura.



SERVIDOR FILEZILLA FTP EN WINDOWS 7

Y en pfsense > NAT > añadimos una regla que permita desde la red WAN(red real) acceder a la red interna de las máquinas virtuales por el puerto 21 y como destino la IP de nuestro servidor.

Disabled

☐ **Disable this rule**
Set this option to disable this rule without removing it from the list.

☐ **No RDR (NOT)**
Enabling this option will disable redirection for traffic matching this rule.
Hint: this option is rarely needed, don't use this unless you know what you're doing.

Interface
WAN
Choose which interface this rule applies to.
Hint: in most cases, you'll want to use WAN here.

Protocol
TCP
Choose which IP protocol this rule should match.
Hint: in most cases, you should specify TCP here.

Source
Advanced - Show source address and port range

Destination
☐ **not**
Use this option to invert the sense of the match.
Type: WAN address
Address: /

Destination port range
from: (other) 21
to: (other) 21
Specify the port or port range for the destination of the packet for this mapping.
Hint: you can leave the to field empty if you only want to map a single port.

Redirect target IP
192.168.99.12
Enter the internal IP address of the server on which you want to map the ports.
e.g. 192.168.1.12

Redirect target port
FTP 21
Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically).
Hint: this is usually identical to the 'from' port above.

Description
You may enter a description here for your reference (not parsed).

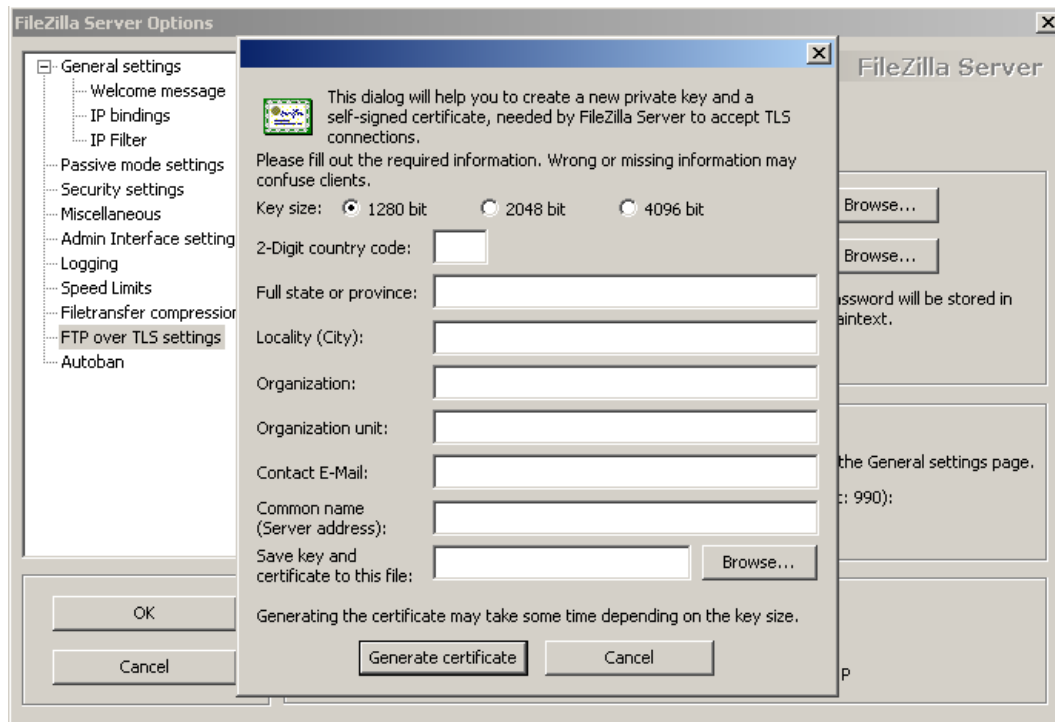
☐ **No XMLRPC Sync**
Hint: This prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent other Master-to-Slave or Slave-to-Slave syncs with other CARP members.

A nuestro servidor lo vamos a hacer funcionar con TLS, observamos con Wireshark antes de configurar el acceso seguro que FTP envía las contraseñas en texto plano.

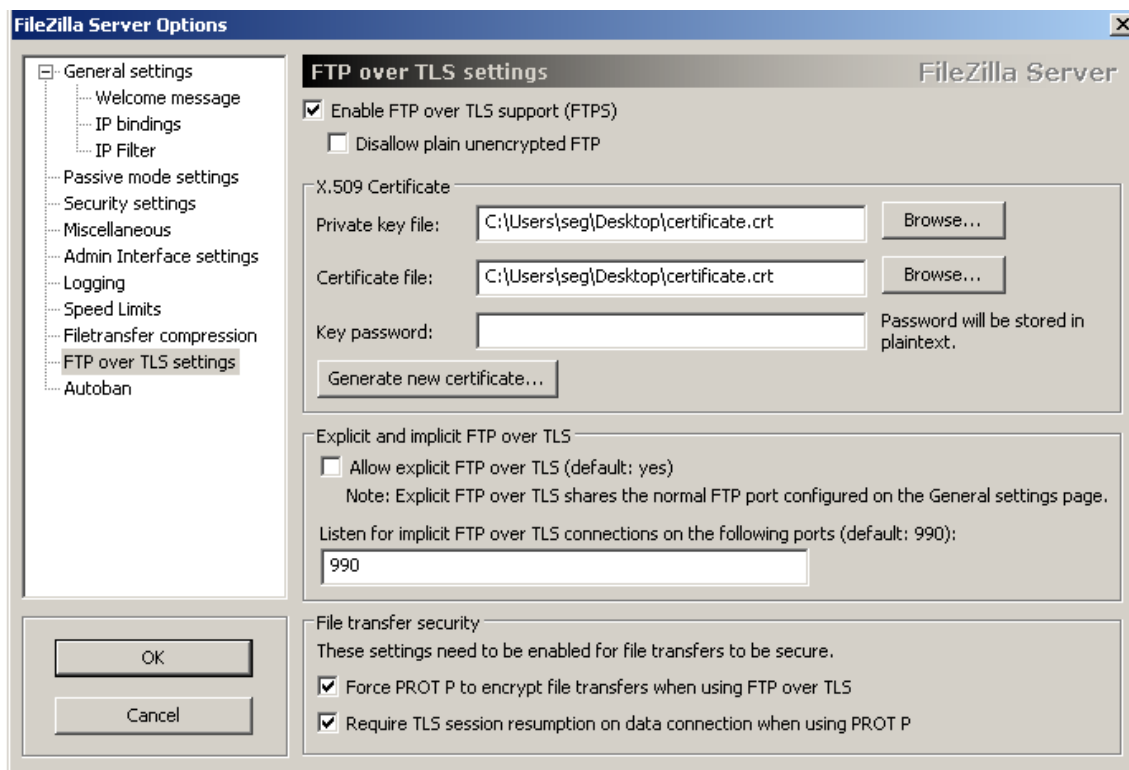
20.3.935183000	192.168.99.12	192.168.99.2	TCP	66.49929-21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=1 SACK_PERM=1
21.3.935332000	192.168.99.2	192.168.99.12	TCP	66.21-49929 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
22.3.935577000	192.168.99.12	192.168.99.2	TCP	54.49929-21 [ACK] Seq=1 Ack=1 Win=8192 Len=0
23.3.935667000	192.168.99.2	192.168.99.12	FTP	81 responses: 220 Microsoft FTP service
24.4.140317000	192.168.99.12	192.168.99.2	TCP	54.49929-21 [ACK] Seq=1 Ack=28 Win=8165 Len=0
25.6.008249000	192.168.99.12	192.168.99.2	FTP	67 Request: USER davids
26.6.008469000	192.168.99.2	192.168.99.12	FTP	89 Responses: 331 Password required for davids.
27.6.218266000	192.168.99.12	192.168.99.2	TCP	54.49929-21 [ACK] Seq=14 Ack=63 Win=8130 Len=0
28.8.888216000	192.168.99.12	192.168.99.2	FTP	71 Request: PASS 123456789
29.8.888666000	192.168.99.2	192.168.99.12	FTP	73 responses: 230 user logged in.
30.9.108650000	192.168.99.12	192.168.99.2	TCP	54.49929-21 [ACK] Seq=31 Ack=84 Win=8109 Len=0
31.14.794319000	216.58.201.142	192.168.99.12	TLSv1.2	117 Application Data
32.14.794321000	216.58.201.142	192.168.99.12	TCP	60.443-49913 [FIN, ACK] Seq=64 Ack=2 Win=176 Len=0

SERVIDOR FILEZILLA FTP EN WINDOWS 7

Vamos a las opciones de filezilla y en la pestaña FTP over TLS settings generamos un nuevo certificado.

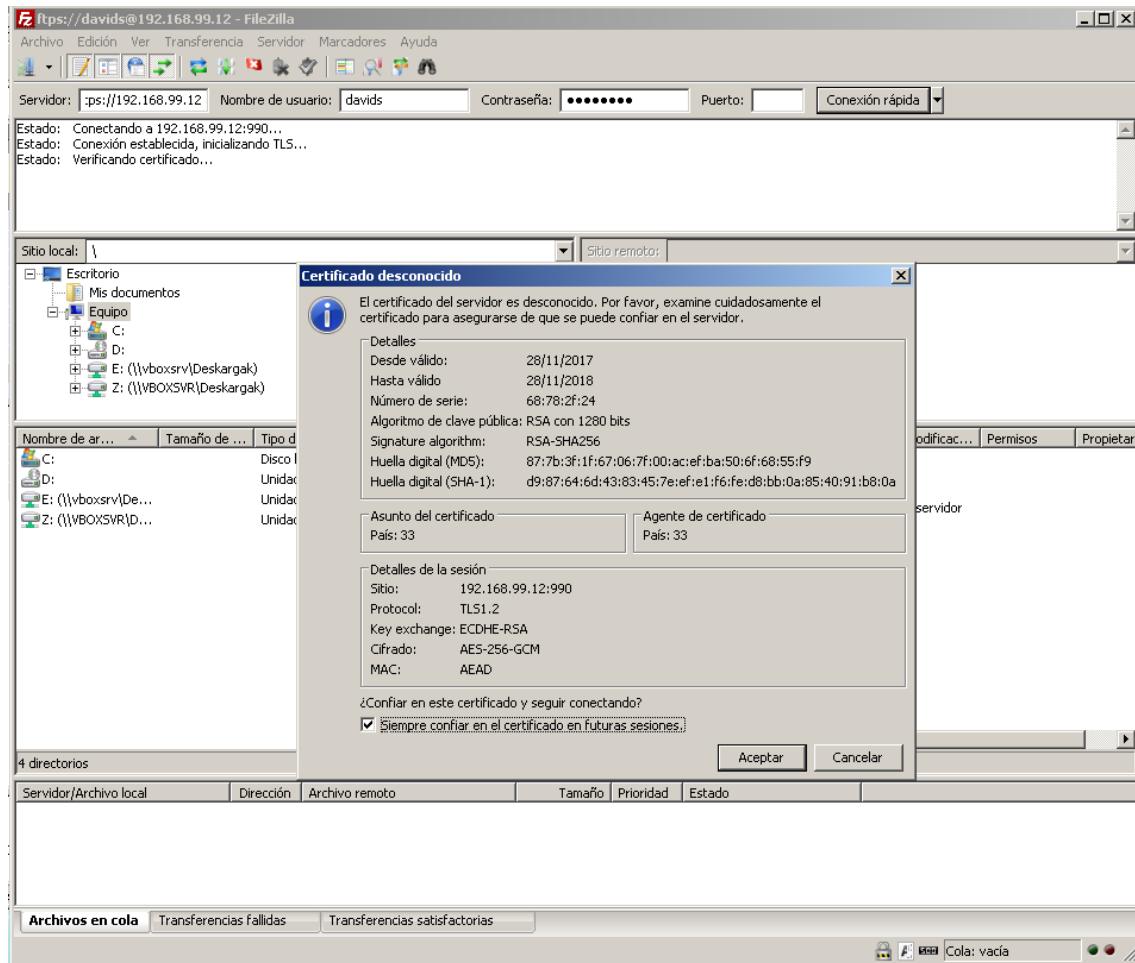


Ahora buscamos y añadimos el certificado y pulsamos ok.



SERVIDOR FILEZILLA FTP EN WINDOWS 7

Probamos a conectarnos desde el cliente Filezilla, con `ftps://192.168.99.12` y nuestras credenciales y aceptamos el certificado del servidor.



De nuevo abrimos Wireshark y vemos que bajo TLS las conexiones pasan a estar cifradas por lo que tenemos un servidor seguro.

2	0.000000000	192.168.99.2	192.168.99.2	TCP	54	990-49222	[ACK] Seq=1 Ack=2 win=254 Len=0
3	0.000000000	192.168.99.2	192.168.99.2	TCP	54	990-49222	[FIN, ACK] Seq=1 Ack=2 win=256 Len=0
4	0.000468000	192.168.99.2	192.168.99.12	TCP	60	49222-990	[ACK] Seq=2 Ack=2 win=256 Len=0
5	0.002137000	192.168.99.2	192.168.99.12	TCP	66	49224-990	[SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
6	0.002198000	192.168.99.12	192.168.99.2	TCP	66	990-49224	[SYN, ACK] Seq=0 Ack=1 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
7	0.002730000	192.168.99.2	192.168.99.12	TCP	60	49224-990	[ACK] Seq=1 Ack=1 win=65536 Len=0
8	0.004218000	192.168.99.2	192.168.99.12	TCP	280	49224-990	[PSH, ACK] Seq=1 Ack=1 win=65536 Len=226
9	0.007806000	192.168.99.2	192.168.99.12	TCP	855	990-49224	[PSH, ACK] Seq=1 Ack=227 win=65536 Len=801
10	0.008655000	192.168.99.2	192.168.99.12	TCP	129	49224-990	[PSH, ACK] Seq=227 Ack=802 win=64768 Len=75
11	0.008715000	192.168.99.2	192.168.99.12	TCP	60	49224-990	[PSH, ACK] Seq=302 Ack=802 win=64768 Len=6
12	0.008716000	192.168.99.2	192.168.99.12	TCP	99	49224-990	[PSH, ACK] Seq=308 Ack=802 win=64768 Len=45
13	0.008726000	192.168.99.12	192.168.99.2	TCP	54	990-49224	[ACK] Seq=802 Ack=353 win=65536 Len=0
14	0.009642000	192.168.99.2	192.168.99.12	TCP	280	990-49224	[PSH, ACK] Seq=802 Ack=353 win=65536 Len=226
15	0.009824000	192.168.99.2	192.168.99.12	TCP	131	990-49224	[PSH, ACK] Seq=1028 Ack=353 win=65536 Len=77
16	0.009951000	192.168.99.2	192.168.99.12	TCP	60	49224-990	[ACK] Seq=353 Ack=1105 win=64512 Len=0
17	0.012317000	192.168.99.2	192.168.99.12	TCP	96	49224-990	[PSH, ACK] Seq=353 Ack=1105 win=64512 Len=42
18	0.012456000	192.168.99.12	192.168.99.2	TCP	117	990-49224	[PSH, ACK] Seq=1105 Ack=395 win=65280 Len=63
19	0.012602000	192.168.99.2	192.168.99.12	TCP	98	49224-990	[PSH, ACK] Seq=395 Ack=1168 win=64512 Len=44
20	0.012881000	192.168.99.12	192.168.99.2	TCP	98	990-49224	[PSH, ACK] Seq=1168 Ack=439 win=65280 Len=44
21	0.013041000	192.168.99.2	192.168.99.12	TCP	91	49224-990	[PSH, ACK] Seq=439 Ack=1212 win=64256 Len=37
22	0.013200000	192.168.99.12	192.168.99.2	TCP	95	990-49224	[PSH, ACK] Seq=1212 Ack=476 win=65280 Len=41
23	0.013415000	192.168.99.2	192.168.99.12	TCP	91	49224-990	[PSH, ACK] Seq=476 Ack=1253 win=64256 Len=37
24	0.013529000	192.168.99.12	192.168.99.2	TCP	114	990-49224	[PSH, ACK] Seq=1253 Ack=513 win=65280 Len=60
25	0.014012000	192.168.99.2	192.168.99.12	TCP	88	49224-990	[PSH, ACK] Seq=513 Ack=1313 win=64256 Len=34
26	0.014835000	192.168.99.12	192.168.99.2	TCP	114	990-49224	[PSH, ACK] Seq=1313 Ack=547 win=65280 Len=60
27	0.015077000	192.168.99.2	192.168.99.12	TCP	91	49224-990	[PSH, ACK] Seq=547 Ack=1373 win=64256 Len=37
28	0.015186000	192.168.99.12	192.168.99.2	TCP	102	990-49224	[PSH, ACK] Seq=1373 Ack=584 win=65280 Len=48
29	0.015374000	192.168.99.2	192.168.99.12	TCP	89	49224-990	[PSH, ACK] Seq=584 Ack=1421 win=64256 Len=35