



By: Justin Ellingwood

Subscribe

How To Configure vsftpd to Use SSL/TLS on an Ubuntu VPS

Posted October 25, 2013 176k

SECURITY

SYSTEM TOOLS

UBUNTU

21

Introduction

Warning: FTP is inherently insecure! Consider using SFTP instead of FTP.

FTP, or file transfer protocol, was a popular way to transfer files between local and remote computers in the past. The protocol is inherently insecure, so its usage has fallen out of favor.

If you still want to use FTP instead of a more secure alternative like SFTP, which uses the SSH protocol to implement file transfers, you can secure it somewhat by configuring FTP to use SSL.

In this guide, we will configure vsftpd to use SSL certificates on an Ubuntu 12.04 VPS.

Install vsftpd

The vsftpd server is available in Ubuntu's default repositories. You can install it by typing:

```
sudo apt-get install vsftpd
```

We now have vsftpd on our server, but we still must configure it.

Configure Basic vsftpd Functionality

The default configuration file is at `/etc/vsftpd.conf`. Open it with root privileges:

```
sudo nano /etc/vsftpd.conf
```

Disable the ability for users to log in anonymously by finding the `anonymous_enable` parameter and changing it to read "NO":

```
anonymous_enable=NO
```

Next, we need to enable user logins that use the local authentication files, since we disabled anonymous access. Uncomment this line:

```
local_enable=YES
```

To enable users to make modifications to the filesystem, we will uncomment the `write_enable` parameter as well:

```
write_enable=YES
```

Additionally, uncomment the `chroot_local_user` option to restrict users to their own home directories:

```
chroot_local_user=YES
```

Save and close the file.

Create an FTP User

Because of the way vsftpd secures its chroot jails, the chroot must not be owned by the user and must not be writeable. Because of this, it is best to implement a user specifically for use with FTP.

Create the user like this:

```
sudo adduser ftpuser
```

Assign a password and feel free to press "ENTER" through the other prompts. Now, give root ownership of the ftpuser's home directory:

```
sudo chown root:root /home/ftpuser
```

We need to create a separate directory within this home directory where files can be uploaded. Then, we need to give this directory over to our FTP user:

```
sudo mkdir /home/ftpuser/files  
sudo chown ftpuser:ftpuser /home/ftpuser/files
```

Now, we should be able to log in (insecurely) as the `ftpuser` and upload files to the `files` directory.

Configure SSL with vsftpd

We need to create some SSL certificates to use with vsftpd. We can do this with the following command:

```
sudo openssl req -x509 -nodes -days 365 -newkey rsa:1024 -keyout /etc/ssl/private/vsftpd.pem
```

This will create a certificate that will last a year. It will be placed in the `/etc/ssl/private/` directory, which we can reference in our configuration file.

Add the SSL Details to the vsftpd Configuration

Open the vsftpd configuration file again with root privileges:

```
sudo nano /etc/vsftpd.conf
```

Towards the bottom of the file, you should find a line that matches the SSL certificate we just created:

```
rsa_cert_file=/etc/ssl/private/vsftpd.pem
```

We will add the additional SSL info below this.

When we created the certificate, we included both the key file and the certificate in one file, so we can also point our private key line to that:

```
rsa_private_key_file=/etc/ssl/private/vsftpd.pem
```

After that, we will add the following lines to force SSL. This will restrict clients that can't deal with TLS, but that is what we want.

```
ssl_enable=YES  
allow_anon_ssl=NO  
force_local_data_ssl=YES  
force_local_logins_ssl=YES
```

After this we configure the server to use TLS, which is actually a successor to SSL, and preferred:

```
ssl_tlsv1=YES  
ssl_sslv2=NO  
ssl_sslv3=NO
```

Finally, we will require add some additional options to flesh out our configuration file:

```
require_ssl_reuse=NO  
ssl_ciphers=HIGH
```

Save and close the file.

Now, we need to restart our server for our changes to take effect:

```
sudo service vsftpd restart
```

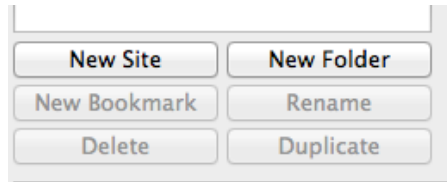
How To Connect to the Server with FileZilla

Most modern FTP clients can be configured to use SSL and TLS encryption. We will be demonstrating how to connect using FileZilla due to its cross platform support.

In the configuration panel, you should see a button on the far left to open "Site Manager". Click this:

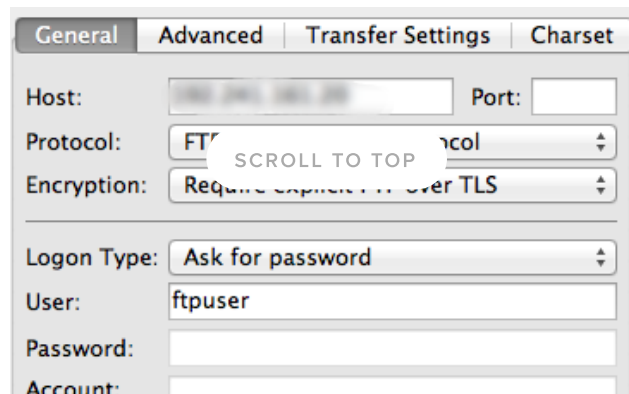


Click on "New Site" in the bottom right corner of the window interface that appears:

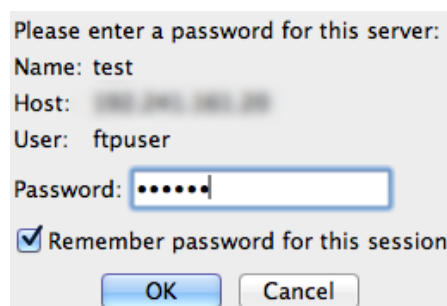


Name the new configuration. Fill out the IP address. Under the "Encryption" drop down menu, select "Require explicit FTP over TLS".

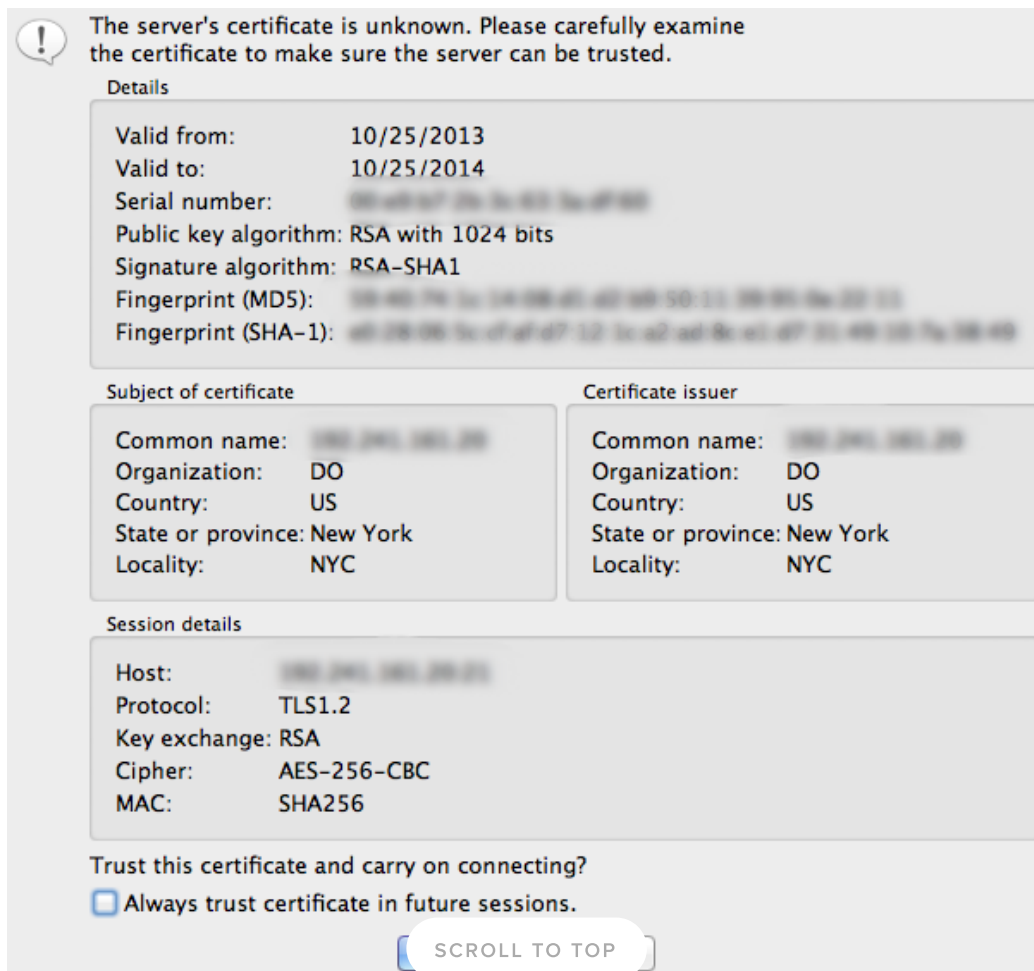
For "Logon Type", select "Ask for password". Fill in the ftp user you created in the "User" field:



Click "Connect" at the bottom of the interface. You will be asked for your user's password:



You will then be asked to accept the TLS certificate:



You should now be connected with your server with TLS/SSL encryption.

Conclusion

This setup improves the security of FTP, but it still suffers from insecurity when establishing a connection. If at all possible, it is better to switch to SFTP for these kinds of operations. However, if you do decide to go with FTP, you should make sure to use TLS/SSL whenever possible.

By Justin Ellingwood

By: Justin Ellingwood

♡ Upvote (21)

✚ Subscribe

Spin up an SSD cloud server in under a minute.

Simple setup. Full root access.
Straightforward pricing.

DEPLOY SERVER

Related Tutorials

[How To Protect Your Linux Server Against the GHOST Vulnerability](#)

[How to Protect Your Server Against the Shellshock Bash Vulnerability](#)

[How to Protect Your Server Against the Heartbleed OpenSSL Vulnerability](#)

[How to Install TrueCrypt \(CLI\) on Linux](#)

[How To Use WPScan to Test for Vulnerable Plugins and Themes in Wordpress](#)


[SCROLL TO TOP](#)

27 Comments

Leave a comment...

[Log In to Comment](#)

 [plaporta](#) *December 12, 2013*

0  This worked great with the ftpuser however I try to create an additional user and it won't connect. I get a "Cant read from control socket. Socket error = #0". ftpuser connect fine, is there anything else that needs to be added besides the additional user with he's own home folder?

 [kamaln7](#) MOD *December 12, 2013*

0 @plaporta: Check vsftpd's error logs, do you see anything?

^ [plaporta](#) December 12, 2013

0 vsftpd.log entries.

Thu Dec 12 16:30:34 2013 [pid 2] CONNECT: Client "174.250.xxx.xxx"

Thu Dec 12 16:30:38 2013 [pid 1] [raff] OK LOGIN: Client "174.220.xxx.xxx"

This was in the log, raff is the user I am trying to add. I did notice that when I created the user, it also created a user folder /home/raff containing .profile .bashrc and .bash_logout. The /home/ftpuser folder does not have those files.

^ [plaporta](#) December 12, 2013

0 I just created ftpuser2 and it worked fine (raff still . Is it mandatory that the user name has ftp in it?

^ [plaporta](#) December 12, 2013

0 *raff still doesn't work.

^ [plaporta](#) December 12, 2013

SCROLL TO TOP

0 Nevermind, got it working. I just deleted the use account and recreated (several times) and finally got it working when I used a shorter password. The original password i was trying to use was 15 characters (numbers and letters). Changed it to less than 8 and it worked.

^ [jjwdesign](#) December 23, 2013

0 Problem: I'm able get it to auth/login. It accepts the login, but when Filezilla tries to LiST my /var/www/vhosts/ directory, it fails. I can configure it to work with the regular FTP passive mode, but not with FTP over TLS.

Response: 227 Entering Passive Mode (.....)

Command: LIST

Error: Connection timed out

Error: Failed to retrieve directory listing

Using

Limit to user www-ftp

the list of users to give access

userlist_file=/etc/vsftpd.userlist

this list is on

userlist_enable=YES

It is not a list of users to deny ftp access

userlist_deny=NO

Could the user limiting be an issue? I'm also using iptables, but that works fine with regular FTP.

^ [SamiF](#) January 25, 2014

0 Followed instructions, failed to allow logins with TLS/SSL enabled. Once the encryption-related lines at the bottom of the vsftpd.conf file were commented out, everything worked fine without encryption.

Any suggestions on safely/properly undo-ing what I did with this tutorial so I can restart from the beginning?

^ [ximo_cid](#) April 2, 2014

0 Great tutorial, but If I need to connect by console rather than Filezilla ?

Thanks

^ [a.starr.b](#) April 3, 2014

0 @ximo_cid

If you need to connect to the ftp server on the command line, consider using curlftpfs. It allows you to mount the ftp host as a fuse filesystem. See:

<http://manpages.ubuntu.com/manpages/precise/man1/curlftpfs.1.html>

SCROLL TO TOP

^ [luzanta.abdullah](#) July 31, 2014

0 Hi Guys, I kind of stuck here. I manage to connect via ftp client. but Im still in 'files' folder. I cant even see my other folder when I try to click the '!!'.

Hope someone will help me on this

^ [kamaln7](#) MOD August 1, 2014

0 @luzanta.abdullah: This tutorial chroots you to the files directory so you can browse outside of it. If you want to access other files, you should use SFTP instead: [How To Use Filezilla to Transfer and Manage Files Securely on your VPS](#).



How To Use Filezilla to Transfer and Manage Files Securely on your VPS

by Pablo Carranza

This article will teach you how to use Filezilla to transfer and manage files securely on your VPS.

SCROLL TO TOP

^ [swlicensing](#) August 8, 2014

0

I was able to log in with the ftpuser before setting up SSL. Once I set up the SSL section I was not prompted by Filezilla to accept the certificate and was not able to connect. In my vsftpd.conf I had ssl-cert-snakeoil.pem instead of vsftpd.pem and same for the .key files. I tried it both ways with restarting the service and had the same result. I'm on Ubuntu 14.04 64 bit. Filezilla's log says:

Status: Connecting to xxx.xxx.xxx.xxx:21...

Status: Connection attempt failed with "ECONNREFUSED - Connection refused by server".

Error: Could not connect to server

Can anyone tell what I'm missing?

Also, I want to have another user - one with write privileges and one with read-only privileges to the same directory tree. How can I accomplish this?

^ [sepehrmmm](#) February 22, 2015

1

I think you missed the point that both 'rsacertfile' and 'rsaprivatekey_file' should refer to the same file.

^ [iam766252](#) August 13, 2014

0

Thanks. Working great.

^ [chromyhomy](#) September 1, 2014

0

I followed the instructions above to setup vsftpd on my ubuntu 14.04 home server. My plan is to connect from an internal client (192.168.x.x) via. Filezilla and transfer/upload files. I was able to accept the TLS certificate but get the below error? something i missed? any help to troubleshoot is greatly appreciated..

Status: Verifying certificate...
Command: USER ftpuser2
Status: TLS/SSL connection established.
Response: 331 Please specify the password.
Command: PASS *****
Error: GnuTLS error -15: An unexpected TLS packet was received.
Error: Could not connect to server

^ [xxx31fr](#) October 3, 2014

0 Hi,

I've a problem to connect when I use lftp on debian 7:

`ls' at 0 [Making data connection...]

did you already get this error, and how did you fixed it?
thanks.

^ [Ali3n0id](#) October 15, 2014

0 I'm using WinSCP set to TLS explicit encryption and get:

Using TLSv1.2, cipher TLSv1/SSLv3: AES256-GCM-SHA384, 1024 bit RSA
SSL3 alert write: fatal: protocol version
Disconnected from server
Connection failed.

[SCROLL TO TOP](#)

Any ideas?

^ [Ali3n0id](#) October 15, 2014

0 In Filezilla:

Status: Connection established, waiting for welcome message...
Response: 220 (vsFTPd 2.3.5)
Command: AUTH TLS
Response: 234 Proceed with negotiation.
Status: Initializing TLS...
Status: Verifying certificate...
Command: USER ftpuser
Status: TLS/SSL connection established.
Response: 331 Please specify the password.
Command: PASS *****
Error: GnuTLS error -15: An unexpected TLS packet was received.
Error: Could not connect to server

^ [imcaps](#) November 5, 2014

1 GnuTLS error -15: An unexpected TLS packet was received.

what it means?

 [jellingwood](#) MOD November 5, 2014

4 Can you try adding a line to your configuration file? Open the config here:

```
sudo nano /etc/vsftpd.conf
```

And put this line at the bottom:

```
allow_writeable_chroot=YES
```

Afterwards, restart the service:

```
sudo service vsftpd restart
```

Does that fix anything for you?

 [imcaps](#) November 24, 2014

1 yes, thank you very much

 [guillermogfer](#) January 22, 2016

SCROLL TO TOP

0 I was experimenting this error too and only was solved when I finally added following lines (enable passive mode) to the `/etc/vsftpd.conf` file

```
pasvenable=YES
pasvmaxport=10100
pasvmin_port=10090
```

 [babyjungle](#) April 15, 2015

0 I can't connect to the ftp:

Error: Authentication failed.

Error: Critical error: Could not connect to server

Actually I think that I did something wrong. I don't know what to do in the step "Add the SSL Details to the vsftpd Configuration". This tutorial says:

Towards the bottom of the file, you should find a line that matches the SSL certificate we just created:

```
rsa_cert_file=/etc/ssl/private/vsftpd.pem
```

But I can't find that line, instead I found this at the bottom:


```
# This option specifies the location of the RSA certificate to use for SSL
# encrypted connections.
rsa_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
# This option specifies the location of the RSA key to use for SSL
# encrypted connections.
rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
```

So I just added this at the bottom of the file:

```
ssl_enable=YES
allow_anon_ssl=NO
force_local_data_ssl=YES
force_local_logins_ssl=YES
ssl_tlsv1=YES
ssl_sslv2=NO
ssl_sslv3=NO
require_ssl_reuse=NO
ssl_ciphers=HIGH
```

Is there something that I'm missing?

 [smahi.a](#) May 17, 2015

 Thank you very much.

[\[SCROLL TO TOP \]](#)



This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.



Copyright © 2016 DigitalOcean™ Inc.

[Community](#) [Tutorials](#) [Questions](#) [Projects](#) [Tags](#) [Newsletter](#) [RSS](#) 

[Distros & One-Click Apps](#) [Terms, Privacy, & Copyright](#) [Security](#) [Report a Bug](#) [Get Paid to Write](#) [Shop](#)