1. Install vsftpd (Very Secure FTP Daemon)

- Update package lists:

  Bash

  ```
  sudo apt update
  ```

- Install vsftpd:

  Bash

  ```
  sudo apt install vsftpd
  ```

2. Configure vsftpd

- Edit the vsftpd configuration file:

  Bash

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

- Uncomment and modify the following lines:
  - `anonymous_enable=NO`
  - `local_enable=YES`
  - `write_enable=YES`
  - `local_umask=022`
  - `chroot_local_user=YES`
  - `allow_writeable_chroot=YES`
  - `listen_address=0.0.0.0`[1] (If you want to allow connections from any IP address)
- Save and close the `vsftpd.conf` file.

  1. forums.centos.org

3. Create a user account (if not already created)

- Create a new user:

  forums.centos.org

  Bash

  ```
  sudo adduser <username>
  ```

- Set a password for the user:

Bash

```
sudo passwd <username>
```

4. Restart vsftpd

- Restart the vsftpd service:

Bash

```
sudo systemctl restart vsftpd
```

5. Install and Test an FTP Client (e.g., FileZilla)

- Install FileZilla (on a separate machine):
  - Download the FileZilla client installer from the official website.
  - Run the installer and follow the on-screen instructions.
- Connect to the FTP server:
  - Open FileZilla.
  - In the "Host" field, enter the IP address or hostname of the Linux server.
  - In the "Username" and "Password" fields, enter the credentials of the user you created on the Linux server.
  - Click "Quickconnect".
- Test file transfers:
  - Try uploading and downloading files between your local machine and the FTP server.

6. (Optional) Configure Passive Mode

- Edit the vsftpd configuration file again:

Bash

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

- Uncomment the following line:
  - `pasv_enable=YES`
- Save and close the file.
- Restart vsftpd:

Bash

```
sudo systemctl restart vsftpd
```

- Passive mode allows the server to initiate connections to the client on a random port. This is often required for connections from behind firewalls or NAT devices.

Important Notes:

- Security:
  - Use strong passwords for your FTP accounts.
  - Consider using SSH File Transfer Protocol (SFTP) for more secure file transfers.
  - Regularly update vsftpd to the latest version for security patches.
- Permissions:
  - Ensure proper file and directory permissions are set on the server to control user access.
- Firewall:
  - If you have a firewall enabled, make sure it allows FTP traffic (ports 21 for control connections and 20 for data connections, or a range of ports for passive mode).

This guide provides a basic setup. You can further customize vsftpd by configuring advanced options like:

- Virtual users
- Directory restrictions
- File size limits
- Logging options

Refer to the official vsftpd documentation for detailed information and advanced configuration options.

Disclaimer: This information is for educational purposes only. I am not responsible for any issues that may arise from implementing these instructions. Always exercise caution and follow security best practices.