

I have two fedora servers; my router's port 80 is pointed to my primary server, but I would also use server 2 to offer wordpress pages. How can I set it up for that?

ChatGPT said:

You can use **reverse proxying** with Apache (since you're using Let's Encrypt with Apache) to forward requests to your second Fedora server when necessary. Here's how:

## Steps to Set Up Reverse Proxy on Your Primary Server

### 1. Enable Necessary Modules

On your **primary Fedora server**, make sure the required Apache modules are enabled:

```
bash
CopyEdit
sudo dnf install -y httpd mod_proxy mod_proxy_http mod_ssl
```

### 2. Configure Virtual Host for Reverse Proxy

Modify your Apache virtual host configuration on the primary server. If you already have a virtual host for your main site, you can add a new block for WordPress.

Edit (or create) a new configuration file for the WordPress site:

```
bash
CopyEdit
sudo nano /etc/httpd/conf.d/wordpress-proxy.conf
```

Add the following content:

```
csharp
CopyEdit
<VirtualHost *:80>
    ServerName wordpress.example.com
    ProxyPreserveHost On
    ProxyPass / http://server2.lan/
    ProxyPassReverse / http://server2.lan/

    # Allow WebSockets if needed
    RewriteEngine on
    RewriteCond %{HTTP:Upgrade} ^WebSocket$ [NC]
    RewriteRule .* ws://server2.lan%{REQUEST_URI} [P]

    # Optional: Redirect non-HTTPS traffic
    # RewriteCond %{HTTPS} !=on
    # RewriteRule ^ https://%{SERVER_NAME}%{REQUEST_URI} [L,R=301]
</VirtualHost>
```

- Replace `wordpress.example.com` with your actual domain.
- Replace `server2.lan` with the internal IP or hostname of your second Fedora server.

### 3. Enable & Restart Apache

Run the following to apply changes:

```
bash
CopyEdit
sudo systemctl restart httpd
```

### 4. Set Up Let's Encrypt for SSL

If your WordPress site should be served over HTTPS, get a certificate with:

```
bash
CopyEdit
sudo certbot --apache -d wordpress.example.com
```

### 5. Ensure Server 2 is Configured Correctly

- On the second Fedora server, make sure Apache or Nginx is set up to serve WordPress properly.
- Ensure httpd or nginx is listening on server2.lan or the internal IP.

### 6. Adjust Firewall Settings (if needed)

If your Fedora firewall is enabled, allow HTTP and HTTPS:

```
bash
CopyEdit
sudo firewall-cmd --permanent --add-service=http
sudo firewall-cmd --permanent --add-service=https
sudo firewall-cmd --reload
```

---

### Optional: Use Subdirectory Instead of a Subdomain

If you want WordPress to be accessible at `example.com/blog` instead of `wordpress.example.com`, modify the ProxyPass and ProxyPassReverse directives:

```
bash
CopyEdit
ProxyPass /blog http://server2.lan/
ProxyPassReverse /blog http://server2.lan/
```

Let me know if you need adjustments! ?

4o

**You said:**

Yes, how does that adjustment work?

**ChatGPT said:**

If you want your WordPress site to be accessible at **example.com/blog** instead of a separate

subdomain like `wordpress.example.com`, you need to modify the **reverse proxy configuration** on your primary Fedora server. Here's how it works:

---

## 1. Update Apache Configuration on Primary Server

Edit (or create) your Apache config file:

```
bash
CopyEdit
sudo nano /etc/httpd/conf.d/wordpress-proxy.conf
```

Replace its contents with:

```
bash
CopyEdit
<VirtualHost *:80>
  ServerName example.com

  ProxyPreserveHost On

  # Reverse proxy WordPress site under /blog
  ProxyPass /blog http://server2.lan/
  ProxyPassReverse /blog http://server2.lan/

  # Allow WebSockets if needed
  RewriteEngine on
  RewriteCond %{HTTP:Upgrade} ^WebSocket$ [NC]
  RewriteRule .* ws://server2.lan%{REQUEST_URI} [P]

  # Redirect non-HTTPS traffic (optional)
  # RewriteCond %{HTTPS} !=on
  # RewriteRule ^ https://%{SERVER_NAME}%{REQUEST_URI} [L,R=301]
</VirtualHost>
```

- Replace **server2.lan** with your **WordPress server's internal IP or hostname**.
  - This routes all traffic under **example.com/blog** to your second server.
- 

## 2. Configure WordPress on Server 2

Since WordPress expects to run from `/`, you need to update its **site URL** to match the proxy path `/blog`:

### A. Update WordPress URL

Go to **WordPress Admin Dashboard** → **Settings** → **General**, then update:

- **WordPress Address (URL):** `http://example.com/blog`
- **Site Address (URL):** `http://example.com/blog`

If you can't access the admin panel, manually update these in the database:

```
bash
CopyEdit
mysql -u root -p
```

Then, run:

```
sql
CopyEdit
USE wordpress;
UPDATE wp_options SET option_value='http://example.com/blog' WHERE option_name IN ('siteurl', 'home');
```

---

## B. Modify .htaccess on WordPress Server

Edit the .htaccess file on your **second server** (server2.lan):

```
bash
CopyEdit
sudo nano /var/www/html/.htaccess
```

Replace its contents with:

```
perl
CopyEdit
<IfModule mod_rewrite.c>
RewriteEngine On
RewriteBase /blog/
RewriteRule ^index\.php$ - [L]
RewriteCond %{REQUEST_FILENAME} !-f
RewriteCond %{REQUEST_FILENAME} !-d
RewriteRule . /blog/index.php [L]
</IfModule>
```

---

## 3. Restart Apache on Both Servers

After making these changes, restart Apache on both servers:

```
bash
CopyEdit
sudo systemctl restart httpd
```

---

## 4. Apply SSL (if using HTTPS)

If your main site is HTTPS, make sure WordPress also works over HTTPS. Run:

```
bash
CopyEdit
sudo certbot --apache -d example.com
```

---

**Now, WordPress is available at [example.com/blog](http://example.com/blog).**

Let me know if you need any tweaks! ?

4o

**You said:**

is certbot generic linux or a LetsEncrypt product?

ChatGPT said:

Certbot is an **open-source tool** developed by the **Electronic Frontier Foundation (EFF)**, but it is designed specifically to work with **Let's Encrypt**, which is a **free Certificate Authority (CA)**.

So, while Certbot itself is not a Let's Encrypt product, it is **one of the most widely used clients for obtaining and renewing Let's Encrypt SSL certificates** on Linux and other operating systems. It can also work with other ACME-compatible certificate authorities, but by default, it is designed to interact with Let's Encrypt.

Would you like to explore alternative ACME clients, or are you good with Certbot?