**BÁO CÁO TUẦN 5**

*Nguyễn Ngọc Minh Trí*

**MỤC LỤC**

[**MỤC LỤC** 2](#_Toc192969449)

[1. Tìm hiểu cấu hình yêu cầu (requirement) của Zimbra Open Source Server bản 8.8.15 (bắt buộc) 3](#_Toc192969450)

[2. Request IP WAN và yêu cầu leader mở port SMTP (đã mở) 3](#_Toc192969451)

[3. Cài đặt Ubuntu 22.04 và cài đặt Zimbra 8.8.15 3](#_Toc192969452)

[4. Cấu hình Zimbra Server và DNS đáp ứng các tiêu chí 17](#_Toc192969453)

[5. Gửi test email tới gmail và đảm bảo vào inbox 21](#_Toc192969454)

[6. Email gmail gửi ngược lại và nhận được 25](#_Toc192969455)

[7. Cấu hình Zimbra đảm bảo hỗ trợ tự động config 26](#_Toc192969456)

[8. Tích hợp SMTP cho website của tuần 4 26](#_Toc192969457)

## **Tìm hiểu cấu hình yêu cầu (requirement) của Zimbra Open Source Server bản 8.8.15 (bắt buộc)**

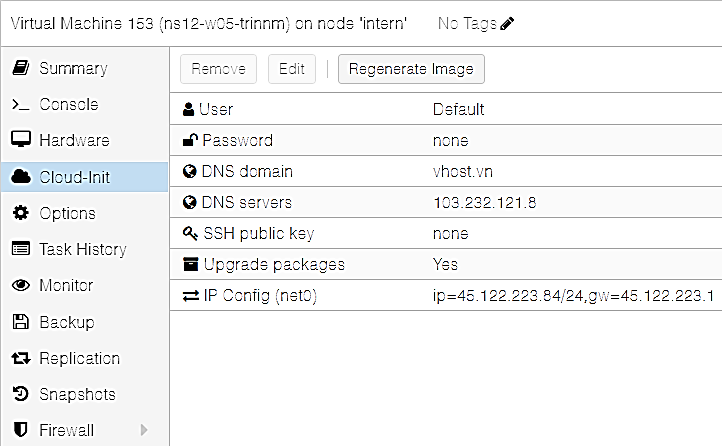
Để Zimbra hoạt động ổn định vHost khuyến cáo cấu hình server tối thiểu:

* CPU: 8 core CPU
* Memory: 16GB tối thiểu
* Storage: tối thiểu 20GB cho hệ thống và dung lượng ổ cứng tùy thuộc theo nhu cầu lưu trữ mail của khách hàng.

## **Request IP WAN và yêu cầu leader mở port SMTP (đã mở)**

Add card mạng ở phần Cloud-Init như đề bài

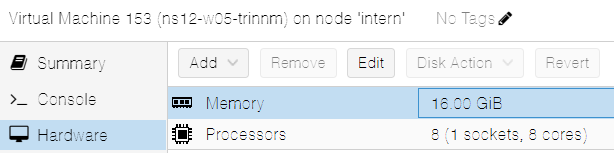
* Trí: 45.122.223.84
* Subnet: /24
* Gateway: 45.122.223.1



## **Cài đặt Ubuntu 22.04 và cài đặt Zimbra 8.8.15**

**Bước 1:** chỉnh lại Memory và Processors cho đúng với Requirement để cài Zimbra

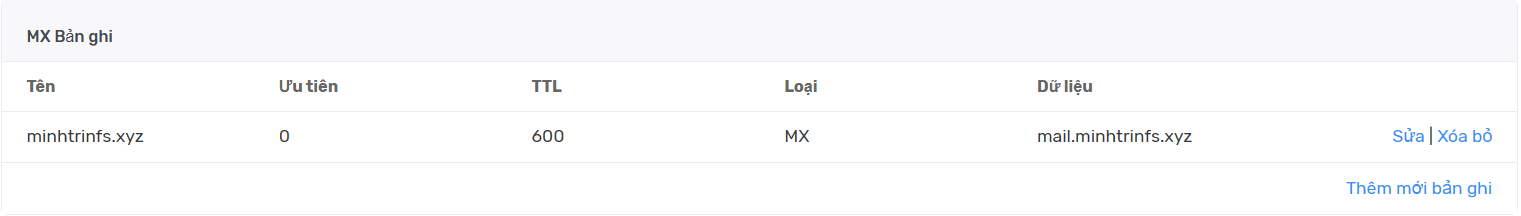
* CPU: 8 core CPU
* Memory: 16GB tối thiểu
* Storage: tối thiểu 20GB cho hệ thống và dung lượng ổ cứng tùy thuộc theo nhu cầu lưu trữ mail của khách hàng

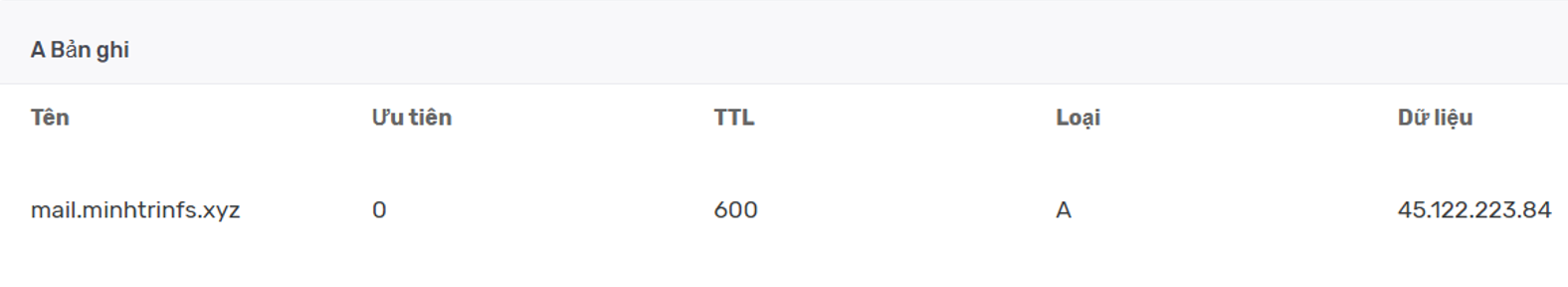


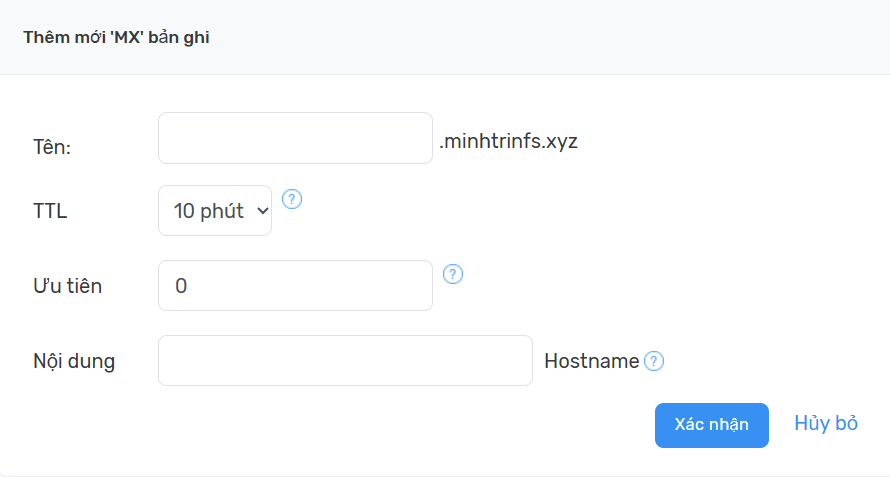
**Bước 2:** Thiết lập bản ghi DNS

Tạo sẵn bản ghi MX và bản ghi A như sau (bảng này được ghi theo cài đặt bên vHost):

|  |  |  |
| --- | --- | --- |
| **Type** | **Name** | **Value** |
| A | mail.minhtrinfs.xyz | 45.122.223.84 |
| MX | minhtrinfs.xyz | mail.minhtrinfs.xyz |







MX Record (Mail Exchange Record) là bản ghi DNS xác định máy chủ xử lý email cho tên miền. Nó giúp chuyển hướng email đến đúng máy chủ nhận, đảm bảo rằng email được gửi đến địa chỉ chính xác.

Kiểm tra bằng lệnh:

**dig MX minhtrinfs.xyz**

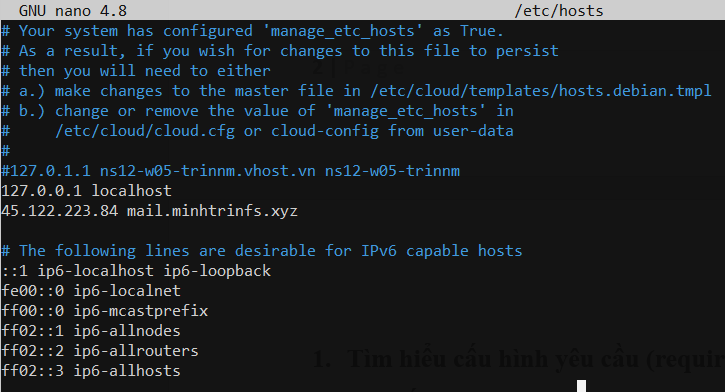
**dig A mail.minhtrinfs.xyz**

**dig -x 45.122.223.84**

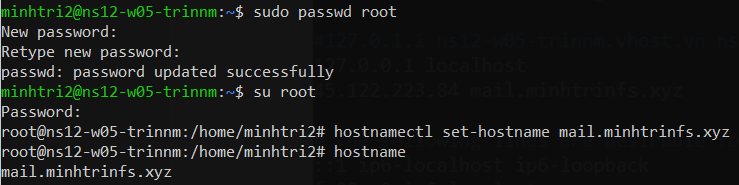
**Bước 3:** Thiết lập file hosts:

Mở file sudo nano /etc/hosts sau đó thêm vào các giá trị sau.

Thêm 45.122.223.84 mail.minhtrinfs.xyz



**Bước 4:** Thiết lập hostname:



**(QUAN TRỌNG): Cài đặt Zimbra bằng user root**

**Bước 5:** Cài đặt gói phụ thuộc

**sudo apt update && sudo apt upgrade -y**

**sudo apt install -y net-tools dnsutils unzip perl**

**Bước 6:** Cài đặt Dnsmasq

Tiếp theo, chúng ta cần cài đặt Dnsmasq để tạo và quản lý một số bản ghi DNS mà Zimbra yêu cầu. Chúng ta cũng cần disable systemd-resolve để tránh xung đột giữa dnsmasq và systemd-resolve.

**systemctl disable systemd-resolved**

**systemctl stop systemd-resolved**

Chỉnh file resolv.conf

**sudo nano /etc/resolv.conf**

Đảm bảo có nội dung:

**nameserver 8.8.8.8**

**nameserver 8.8.4.4**

**nameserver 1.1.1.1**

**search minhtrinfs.xyz**

File /etc/resolv.conf trên Ubuntu thường được tự động ghi đè bởi systemd-resolved hoặc Netplan. Do đó, nếu bạn chỉ sửa đổi trực tiếp bằng nano, nội dung của nó sẽ bị mất khi hệ thống khởi động lại hoặc khi dịch vụ này tự động cập nhật.

1. Kiểm tra xem ai đang quản lý resolv.conf

**ls -l /etc/resolv.conf**

*lrwxrwxrwx 1 root root 29 Mar 12 02:56 /etc/resolv.conf -> ../run/resolvconf/resolv.conf*

1. Chỉnh sửa file cấu hình /etc/resolvconf/resolv.conf.d/head

**sudo nano /etc/resolvconf/resolv.conf.d/head**

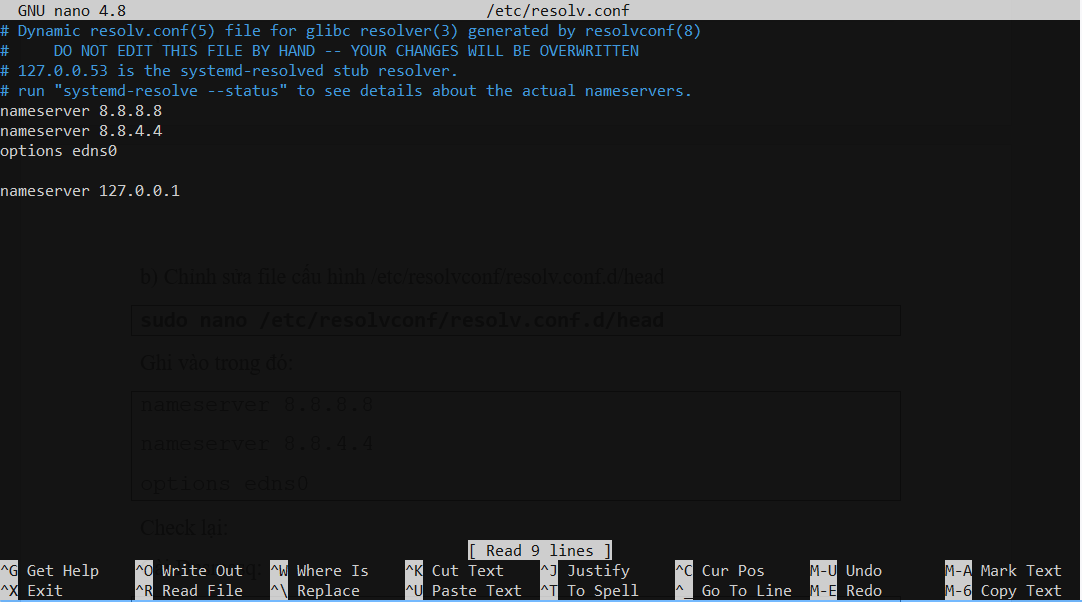
Ghi vào trong đó:

nameserver 8.8.8.8

nameserver 8.8.4.4

options edns0

Check lại:



Cài Dnsmasq:

**sudo apt install dnsmasq -y**

Cấu hình Dnsmasq:

**cp /etc/dnsmasq.conf /etc/dnsmasq.conf.bak**

**sudo nano /etc/dnsmasq.conf**

Chèn nội dung:

server= 45.122.223.84

domain=minhtrinfs.xyz

mx-host= minhtrinfs.xyz, mail.minhtrinfs.xyz, 5

mx-host= mail.minhtrinfs.xyz, mail.minhtrinfs.xyz, 5

listen-address=127.0.0.1

Chạy **/run/dnsmasq/resolv.conf** và thêm

nameserver 8.8.8.8

nameserver 8.8.4.4

nameserver 1.1.1.1

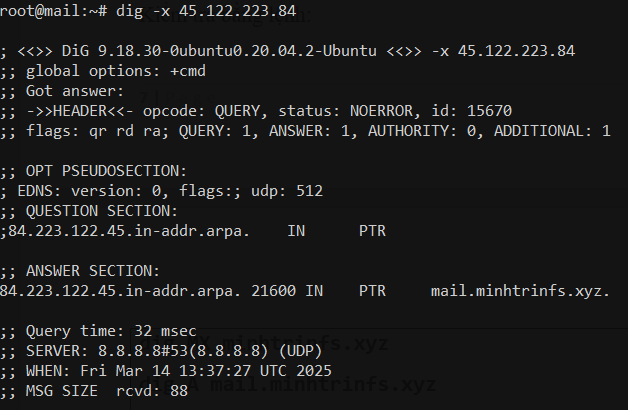
search minhtrinfs.xyz

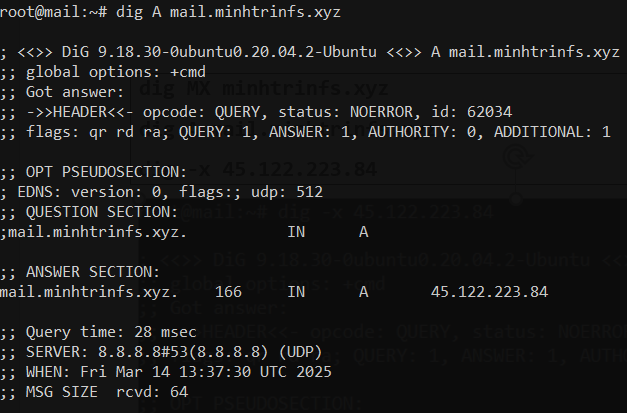
Kiểm tra bằng lệnh:

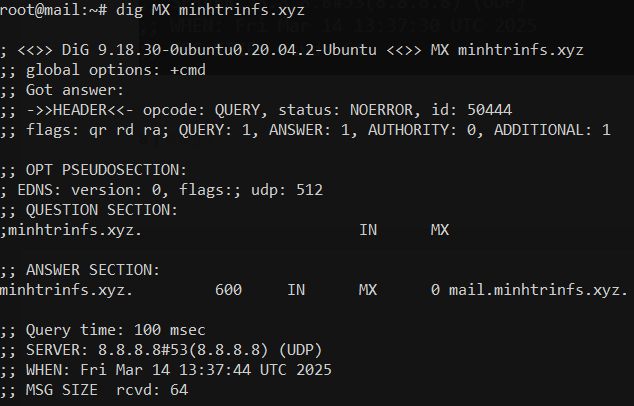
**dig MX minhtrinfs.xyz**

**dig A mail.minhtrinfs.xyz**

**dig -x 45.122.223.84**







**Bước 7:** Tải và cài đặt Zimbra 8.8.15

Tải bộ cài đặt Zimbra:

**wget https://files.zimbra.com/downloads/8.8.15\_GA/zcs-8.8.15\_GA\_4179.UBUNTU20\_64.20211118033954.tgz**

Giải nén:

**tar xvzf zcs-8.8.15\_GA\_4179.UBUNTU20\_64.20211118033954.tgz**

**cd zcs-8.8.15\_GA\_4179.UBUNTU20\_64.20211118033954**

Chạy cài đặt:

**sudo ./install.sh**

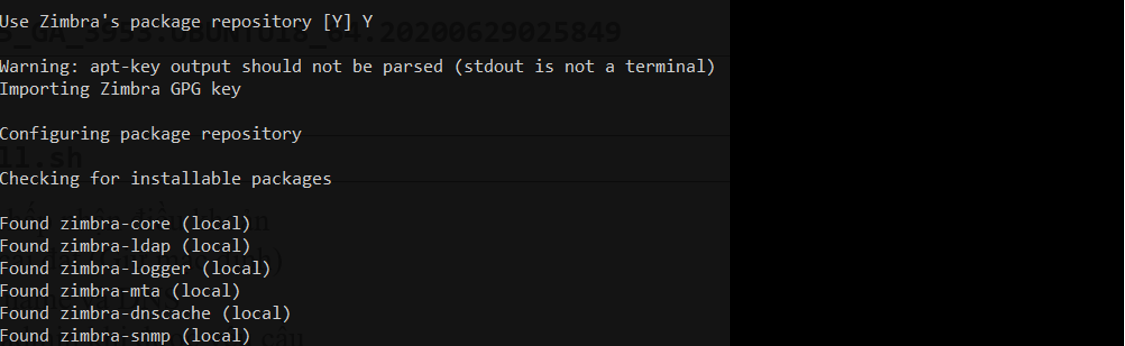
* Chọn "Y" để chấp nhận điều khoản
* Chọn các gói cài đặt (Giữ mặc định)
* Xác nhận hostname và DNS
* Đặt mật khẩu admin khi được yêu cầu

**NOTE:** Không cài các package sau:

**zimbra-dnscache = N**

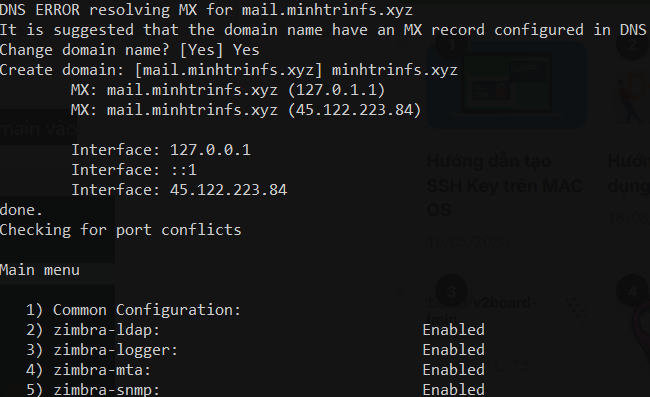
**zimbra-imapd (BETA – for evaluation only) = N**

**zimbra-drive = N**

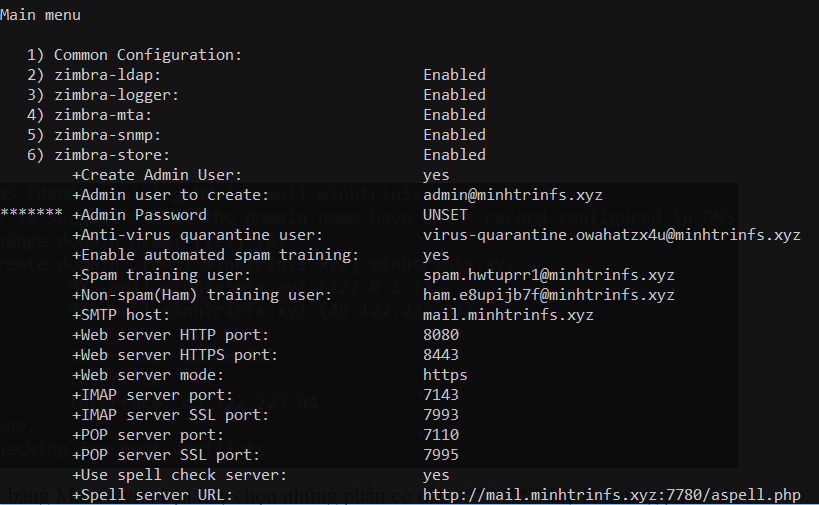


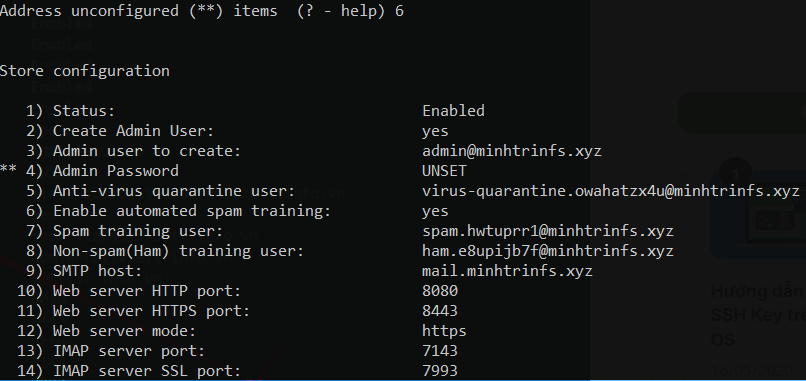
Đến bước Change domain name? [Yes] bạn hãy chọn Yes. Sau đó nhập domain vào

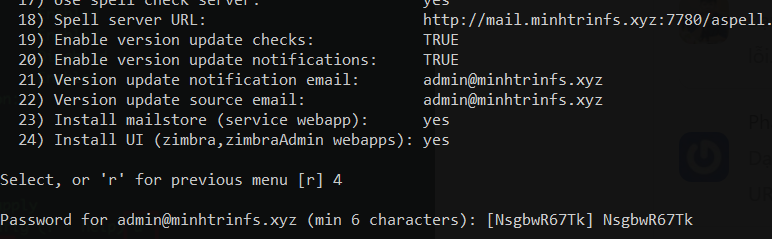
**mail.minhtrinfs.xyz → minhtrinfs.xyz**



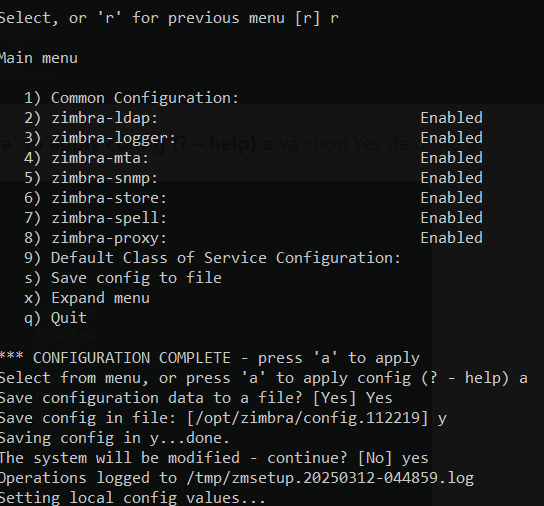
Ở bảng Main menu bạn hãy chọn những phần có dấu “\*\*\*\*\*\*” đây là những phần bắt buộc. Cụ thể là phẩn 6) zimbra-store



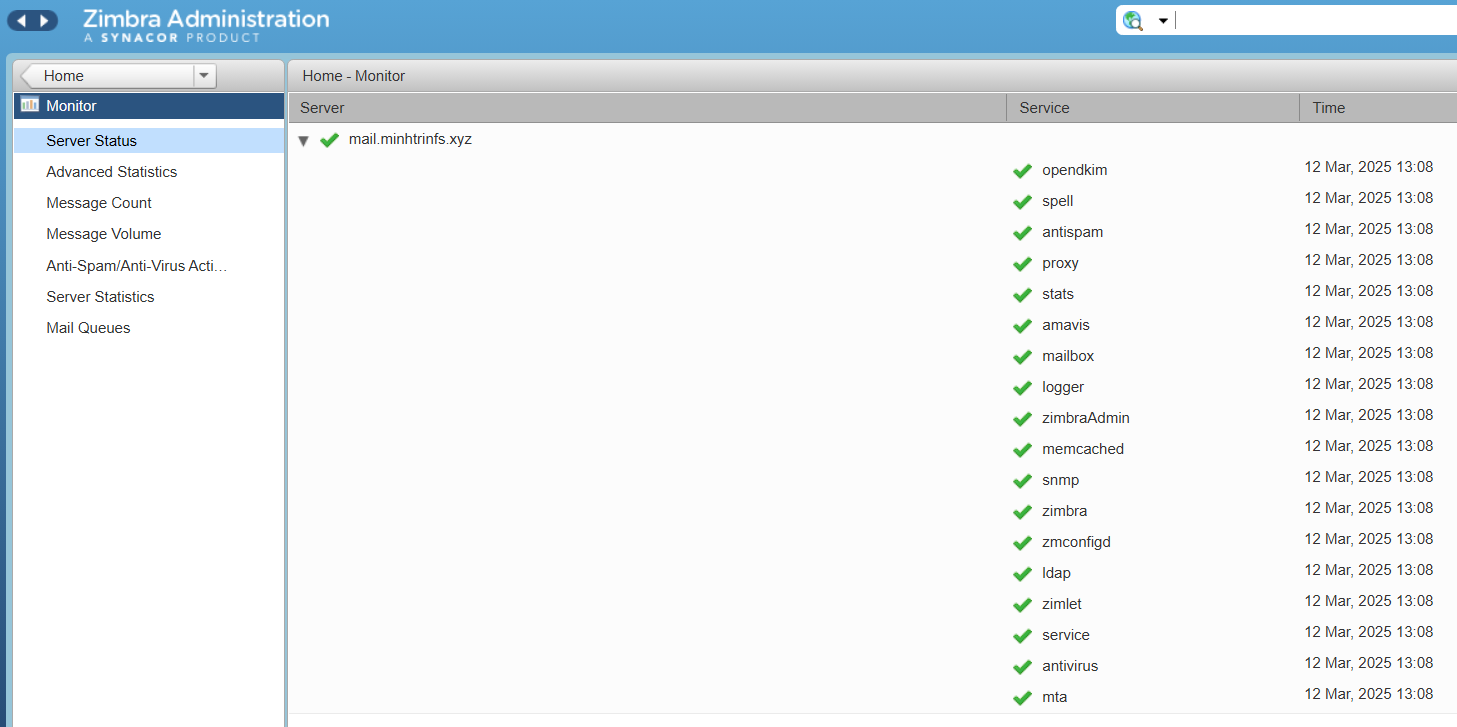




Đặt password: NsgbwR67Tk



**Bước 8:** Kiểm tra dịch vụ



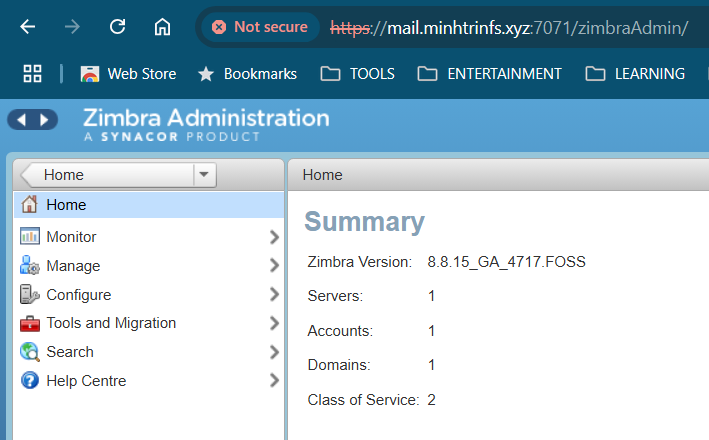
Kiểm tra dịch vụ Zimbra bằng lệnh:

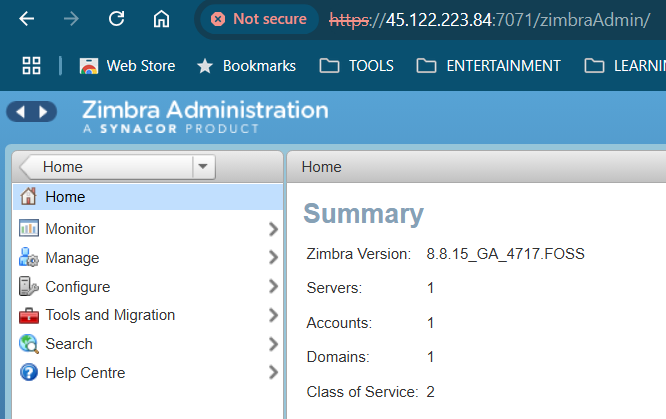
**sudo su - zimbra -c "zmcontrol status"**

**sudo su - zimbra -c "zmcontrol start"**

Trên trình duyệt:

* Gõ 45.122.223.84:7071
* Hoặc gõ mail.minhtrinfs.xyz:7071/zimbraAdmin/





**Bước 9:** Cấu hình SSL

Cài đặt Certbot:

**sudo apt update**

**sudo apt install certbot -y**

Tạo chứng chỉ SSL với Let’s Encrypt:

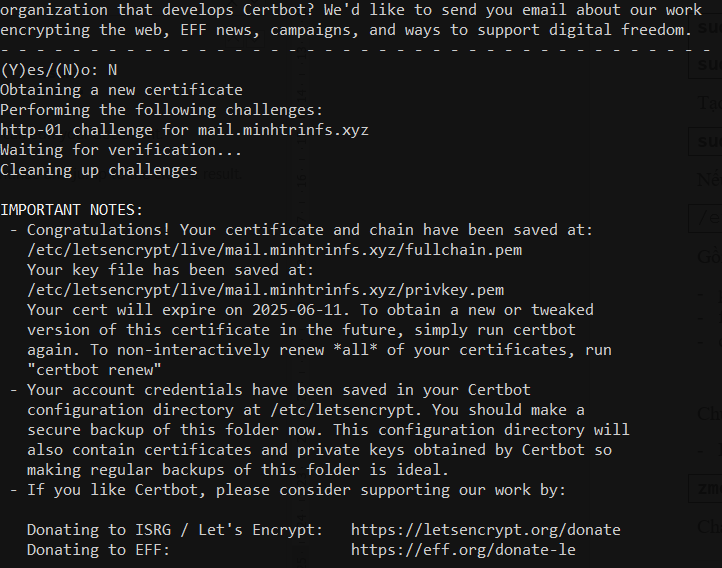
**sudo certbot certonly --standalone -d mail.minhtrinfs.xyz**

Nếu thành công, chứng chỉ được lưu tại

/etc/letsencrypt/live/mail.minhtrinfs.xyz/

Gồm các file:

|  |  |
| --- | --- |
| **TÊN FILE** | **MÔ TẢ** |
| privkey.pem | Private key (khóa bí mật) |
| fullchain.pem | Chứng chỉ đầy đủ (gồm cả cert và CA chain) |
| cert.pem | Chứng chỉ chính (không bao gồm chain) |
| chain.pem | Intermediate Certificate - Chứng chỉ trung gian (CA chain) |



Chuyển chứng chỉ sang định dạng Zimbra:

* Dừng dịch vụ Zimbra trước:

**sudo su - zimbra -c "zmcontrol stop"**

Chạy các lệnh sau để copy chứng chỉ vào thư mục Zimbra:

**sudo cp /etc/letsencrypt/live/mail.minhtrinfs.xyz/privkey.pem /opt/zimbra/ssl/letsencrypt/privkey.pem**

**sudo cp /etc/letsencrypt/live/mail.minhtrinfs.xyz/fullchain.pem /opt/zimbra/ssl/letsencrypt/fullchain.pem**

**sudo cp /etc/letsencrypt/live/mail.minhtrinfs.xyz/chain.pem /opt/zimbra/ssl/letsencrypt/chain.pem**

Chuyển quyền sở hữu file cho Zimbra:

**sudo chown zimbra:zimbra /opt/zimbra/ssl/letsencrypt/\***

**sudo chmod 640 /opt/zimbra/ssl/letsencrypt/\***

Cài đặt SSL vào Zimbra:

Chạy lệnh sau với user zimbra:

**sudo su zimbra**

Vì hiện tại user zimbra chưa có quyền nên mình cần cấp quyền cho nó:

**cd /opt/zimbra/ssl/letsencrypt**

**zmcertmgr verifycrt comm privkey.pem fullchain.pem chain.pem**

**zmcertmgr deploycrt comm fullchain.pem chain.pem**

**TROUBLESHOOTING**

**a) Lỗi: Connect: Unable to determine enabled services from ldap. Unable to determine enabled services. Cache is out of date or doesn't exist**

Lỗi này thường xuất hiện khi Zimbra không thể lấy thông tin dịch vụ từ LDAP. Nguyên nhân có thể do:

* LDAP không chạy

Kiểm tra trạng thái LDAP bằng lệnh:

**sudo su - zimbra -c "zmlocalconfig -s ldap\_url"**

Nếu kết quả rỗng hoặc không có địa chỉ LDAP hợp lệ, bạn cần khởi động lại LDAP:

**sudo su - zimbra -c "zmcontrol stop"**

**sudo su - zimbra -c "zmcontrol start"**

* Cache LDAP bị lỗi

Xóa cache LDAP cũ:

**sudo su - zimbra -c "rm -rf /opt/zimbra/data/ldap/mdb/db/\*"**

**sudo su - zimbra -c "zmcontrol restart"**

**b) Nếu bị lỗi và muốn cài lại Zimbra từ đầu:**

**Bước 1:** Dừng toàn bộ dịch vụ Zimbra

**sudo su - zimbra -c "zmcontrol stop"**

**Bước 2:** Xóa thư mục cài đặt Zimbra

**sudo rm -rf /opt/zimbra**

**Bước 3:** Xóa người dùng và nhóm Zimbra

**sudo userdel -r zimbra**

**sudo groupdel zimbra**

**Bước 4:** Xóa các gói Zimbra đã cài đặt

**sudo dpkg --purge $(dpkg -l | grep zimbra | awk '{print $2}')**

**Bước 5:** Xóa các thư mục cấu hình liên quan

**sudo rm -rf /etc/zimbra**

**sudo rm -rf /var/log/zimbra\***

**sudo rm -rf /var/spool/zimbra**

**sudo rm -rf /var/tmp/zimbra\***

**Bước 6:** Làm sạch lại hệ thống

**sudo apt autoremove -y**

**sudo apt clean**

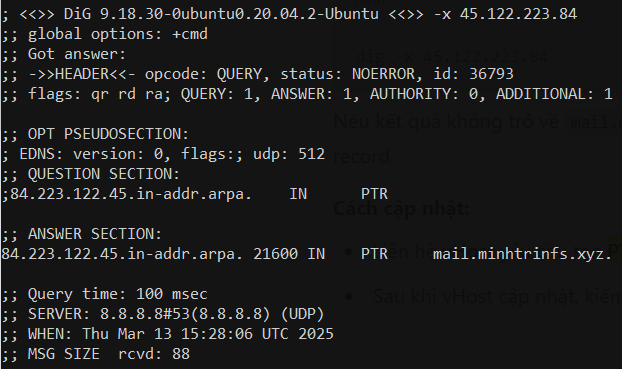
## **Cấu hình Zimbra Server và DNS đáp ứng các tiêu chí**

1. Cấu hình PTR Record (Reverse DNS) cho IP:

*PTR (Pointer Record) giúp ánh xạ IP ngược lại thành tên miền.*

Dùng lệnh **dig -x 45.122.223.84**

Nếu kết quả không trỏ về mail.minhtrinfs.xyz, bạn cần yêu cầu nhà cung cấp (vHost) cập nhật lại PTR record, yêu cầu tạo PTR Record cho IP 45.122.223.84 trỏ về mail.minhtrinfs.xyz



1. Cấu hình SPF Record:

*SPF giúp email từ server của bạn không bị đánh dấu spam.*

**Thêm bản ghi TXT cho SPF**

Tên: minhtrinfs.xyz

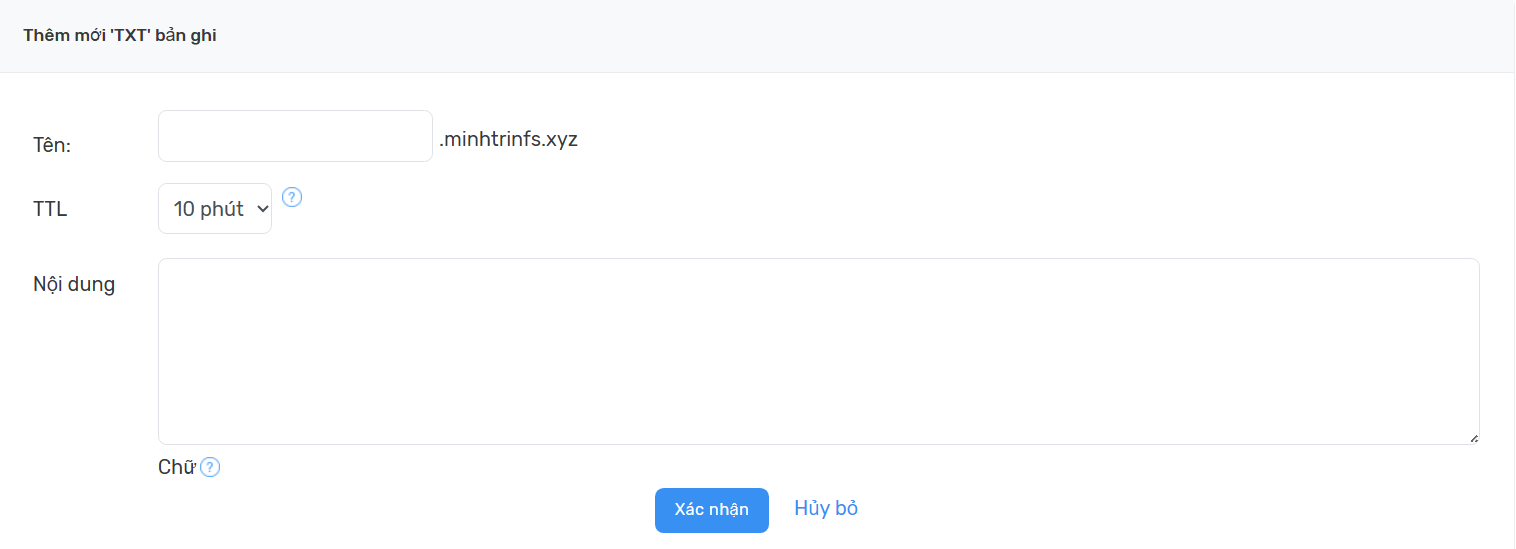
Loại: TXT

Giá trị: v=spf1 mx ip4:45.122.223.84 -all

TTL: 600

Giải thích:

* mx: Cho phép gửi mail từ máy chủ có bản ghi MX của domain.
* ip4:45.122.223.84: Cho phép IP này gửi mail.
* -all: Chỉ cho phép các server được liệt kê, chặn tất cả các server khác



Tại ô "Tên":

* Nếu bạn muốn bản ghi SPF áp dụng cho toàn bộ miền minhtrinfs.xyz, hãy để trống ô này.
* Nếu bạn chỉ muốn áp dụng cho một subdomain cụ thể (ví dụ: mail.minhtrinfs.xyz), thì nhập mail vào ô này.

Tại ô "TTL":

* Đặt giá trị là 10 phút hoặc theo yêu cầu của bạn.

Tại ô "Nội dung":

* Dán dòng này vào ô nội dung:

**v=spf1 mx ip4:45.122.223.84 -all**

Bấm nút "Xác nhận" để lưu lại bản ghi.

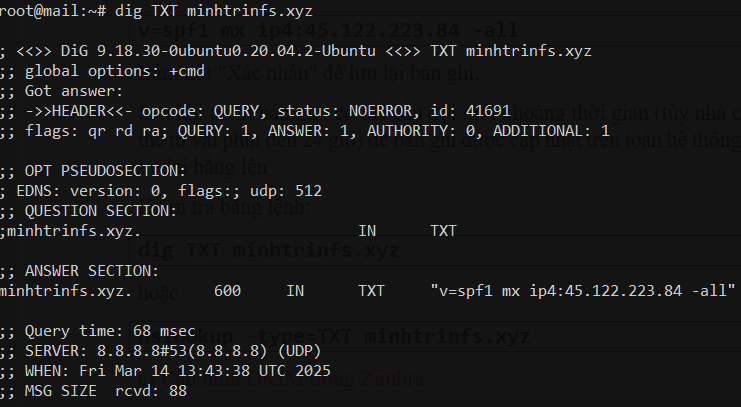
Sau khi thêm bản ghi, có thể cần đợi một khoảng thời gian (tùy nhà cung cấp DNS, có thể từ vài phút đến 24 giờ) để bản ghi được cập nhật trên toàn hệ thống. Bạn có thể kiểm tra lại bằng lện

Kiểm tra bằng lệnh:

**dig TXT minhtrinfs.xyz**

hoặc

**nslookup -type=TXT minhtrinfs.xyz**

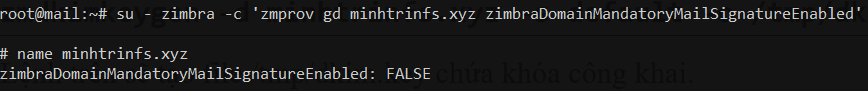


1. Cấu hình DKIM trong Zimbra:

*DKIM giúp xác thực email bằng chữ ký số. Việc thiết lập DKIM giúp giảm nguy cơ email bị đánh dấu là spam và tăng tỷ lệ email được gửi đến hộp thư đến của người nhận thay vì bị vào thư mục spam*

**Kiểm tra Zimbra đã bật DKIM hay chưa?**





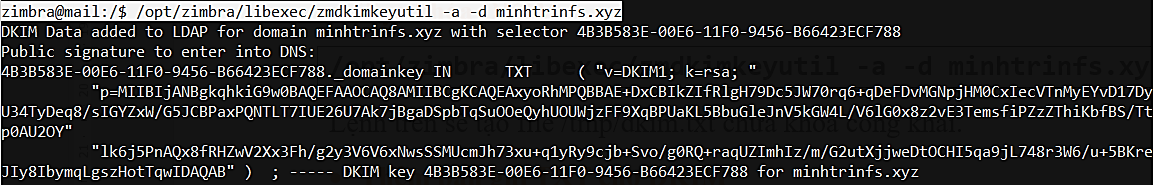
**Bật DKIM trong Zimbra:**

* **Truy cập user Zimbra**

**su zimbra**

* **Tạo khóa DKIM**

**/opt/zimbra/libexec/zmdkimkeyutil -a -d minhtrinfs.xyz**



* **Thêm bản ghi TXT cho DKIM**

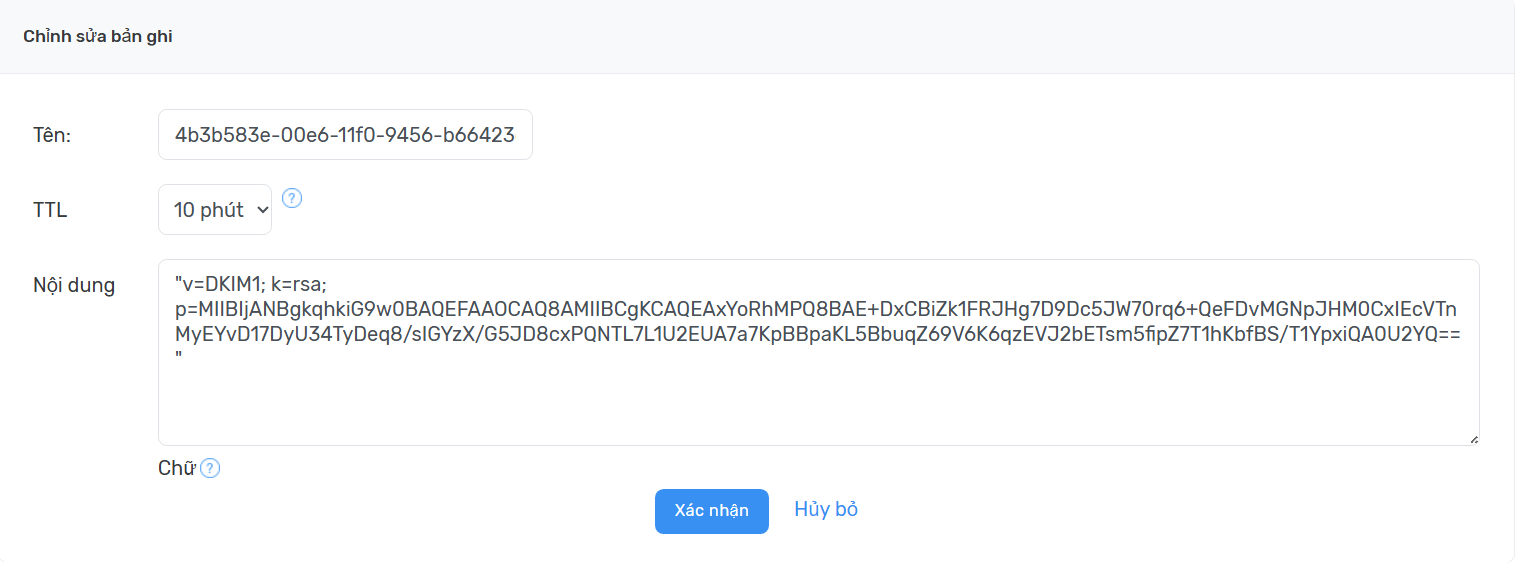
Mở file và copy giá trị khóa công khai, sau đó vào trang DNS thêm bản ghi:

**Tên:** 4B3B583E-00E6-11F0-9456-B66423ECF788.\_domainkey.minhtrinfs.xyz

**Loại:** TXT

**Giá trị:** (Copy nội dung từ file key trên hình)  
v=DKIM1; k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxyoRhMPQBBAE+DxCBIkZIfRlgH79Dc5JW70rq6+qDeFDvMGNpjHM0CxIecVTnMyEYvD17DyU34TyDeq8/sIGYZxW/G5JCBPaxPQNTLT7IUE26U7Ak7jBgaDSpbTqSuOOeQyhUOUWjzFF9XqBPUaKL5BbuGleJnV5kGW4L/V6lG0x8z2vE3TemsfiPZzZThiKbfBS/Ttp0AU2OYlk6j5PnAQx8fRHZwV2Xx3Fh/g2y3V6V6xNwsSSMUcmJh73xu+q1yRy9cjb+Svo/g0RQ+raqUZImhIz/m/G2utXjjweDtOCHI5qa9jL748r3W6/u+5BKreJIy8IbymqLgszHotTqwIDAQAB

**TTL:** 600



* Ở ô Tên, nhập: 4B3B583E-00E6-11F0-9456-B66423ECF788.\_domainkey
* Ở ô Nội dung, nhập đoạn TXT trên vào.
* Nhấn Xác nhận để lưu bản ghi.
* Chờ một khoảng thời gian để DNS cập nhật.
* Xác minh bằng lệnh:

**dig TXT 4B3B583E-00E6-11F0-9456-B66423ECF788.\_domainkey.minhtrinfs.xyz +short**



1. Cấu hình DMARC Record

*DMARC giúp kiểm soát cách xử lý email không vượt qua SPF/DKIM.*

**Thêm bản ghi TXT cho DMARC**

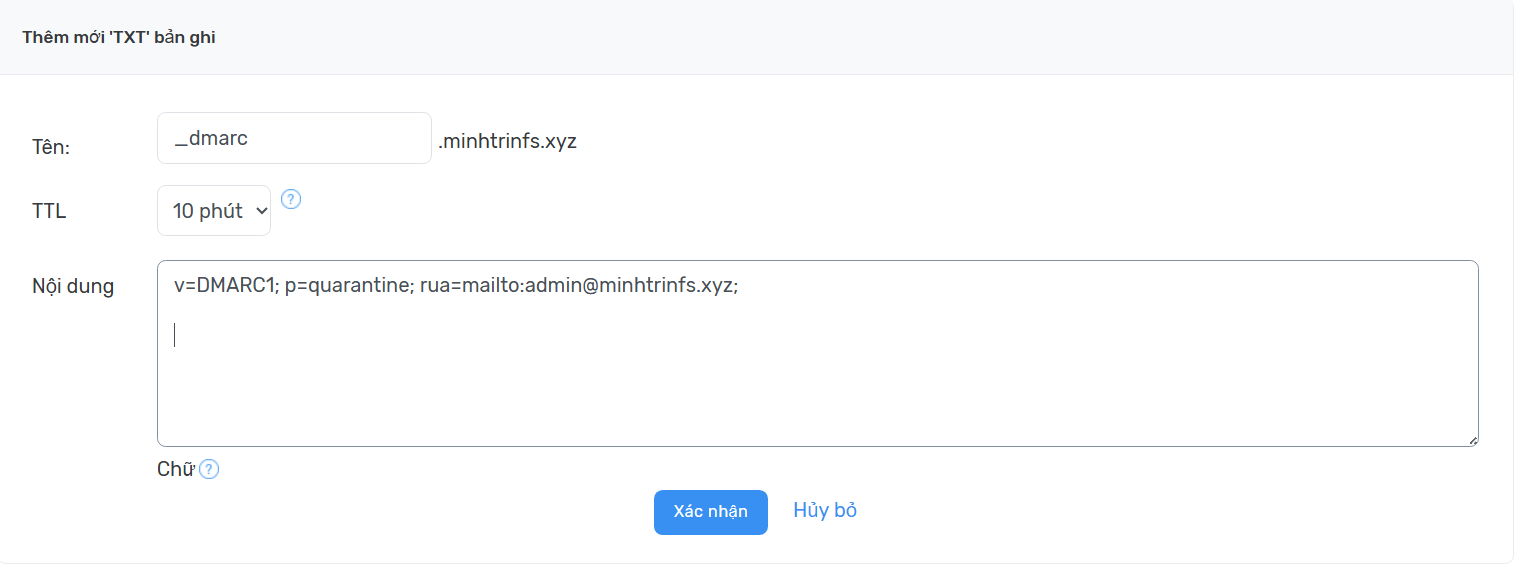
* **Điền vào trường "Tên"**: Nhập \_dmarc.minhtrinfs.xyz
* **Chọn TTL**: Chọn giá trị 10 phút (600 giây)
* **Điền vào trường "Nội dung"**

Tên: \_dmarc.minhtrinfs.xyz

Loại: TXT

Giá trị: v=DMARC1; p=quarantine; rua=mailto:admin@minhtrinfs.xyz;

TTL: 600



Giải thích:

* p=quarantine: Email không đạt SPF/DKIM sẽ bị đưa vào spam.
* rua=mailto:admin@minhtrinfs.xyz: Nhận báo cáo về các email bị chặn

Kiểm tra bằng lệnh

**dig TXT \_dmarc.minhtrinfs.xyz +short**

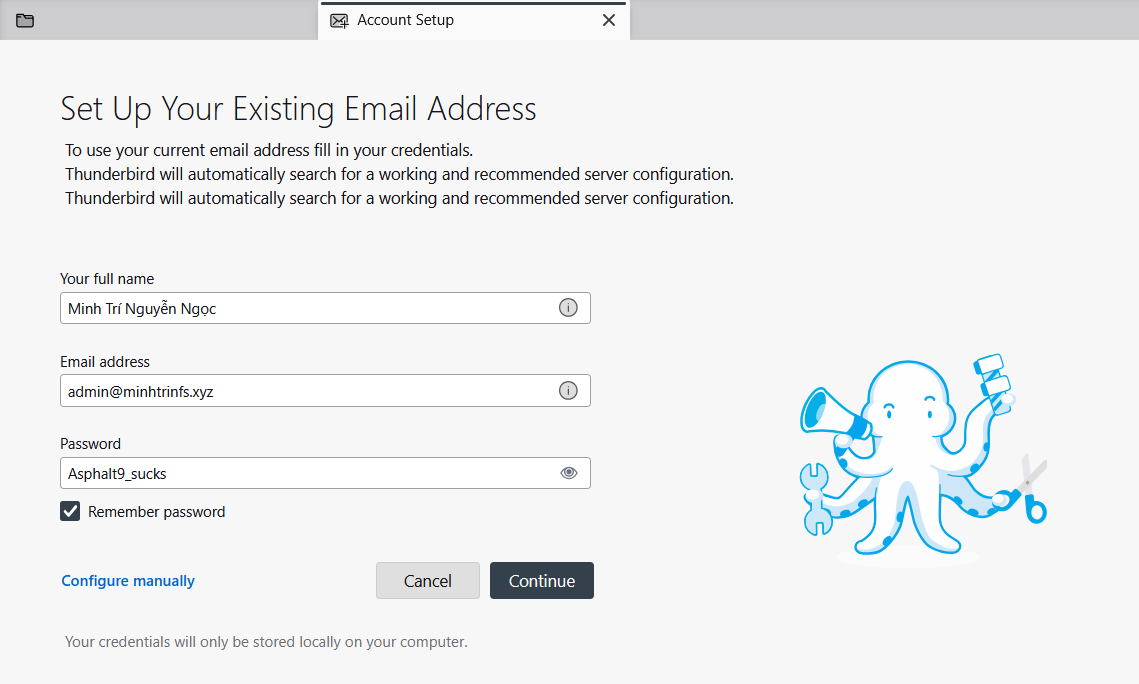
## **Gửi test email tới gmail và đảm bảo vào inbox**

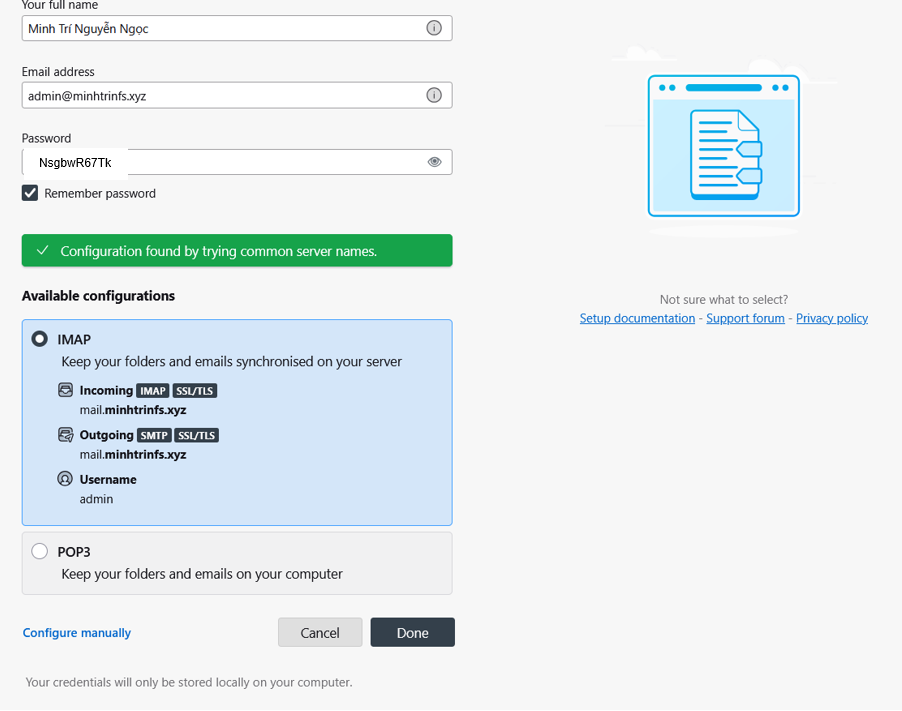
**Cách 1:** Gửi email test bằng SMTP

Cấu hình SMTP trong Thunderbird hoặc Outlook:

* SMTP Server: smtp.gmail.com
* Port: 587 (STARTTLS) hoặc 465 (SSL)
* Username: admin@minhtrinfs.xyz
* Password: NsgbwR67Tk
* Authentication: Yes

Sau đó, gửi email test đến một tài khoản Gmail cá nhân của bạn.





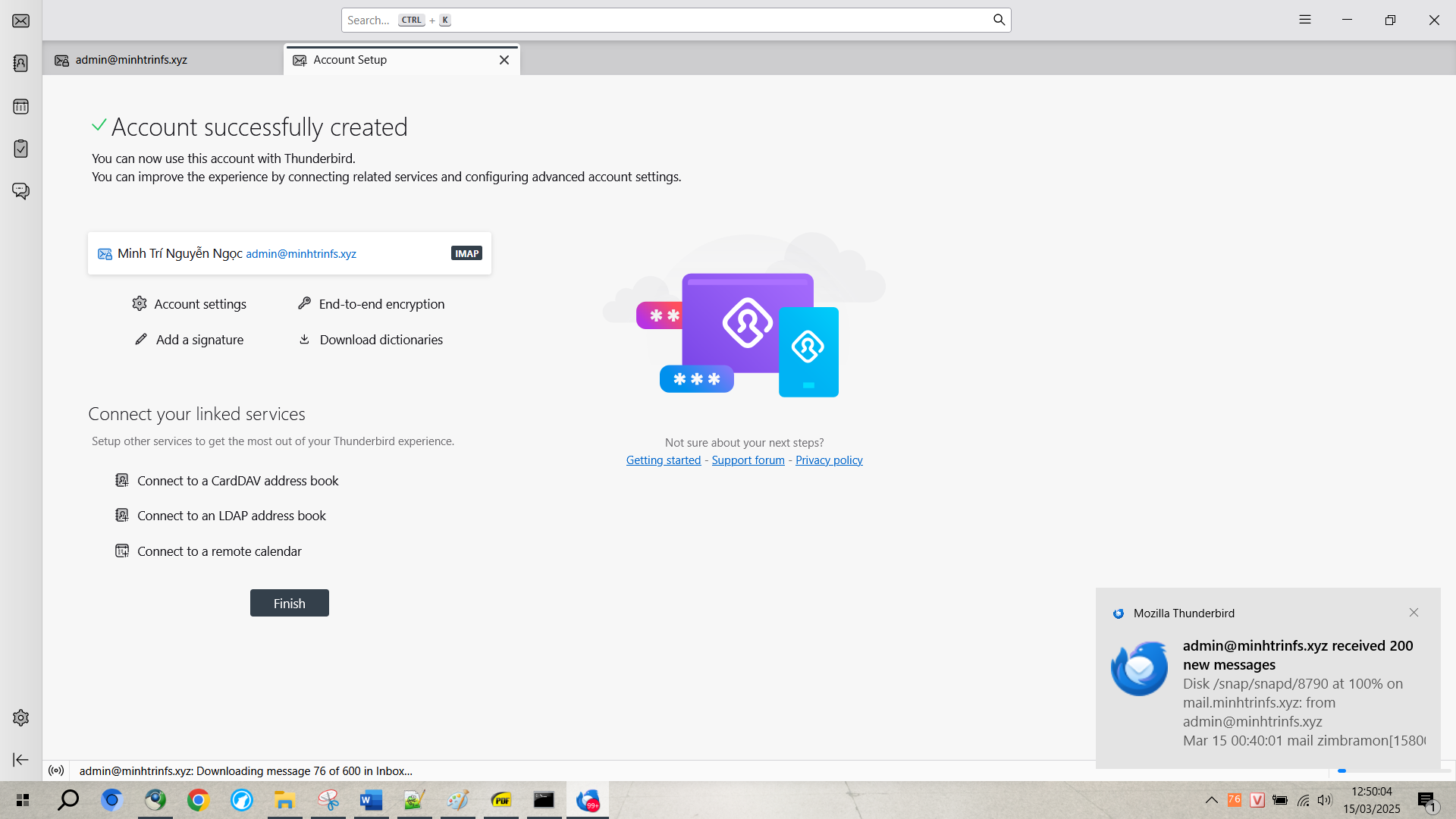
Trường hợp chỉnh cấu hình thủ công (nếu Thunderbird không tự động nhận diện - Manual config):

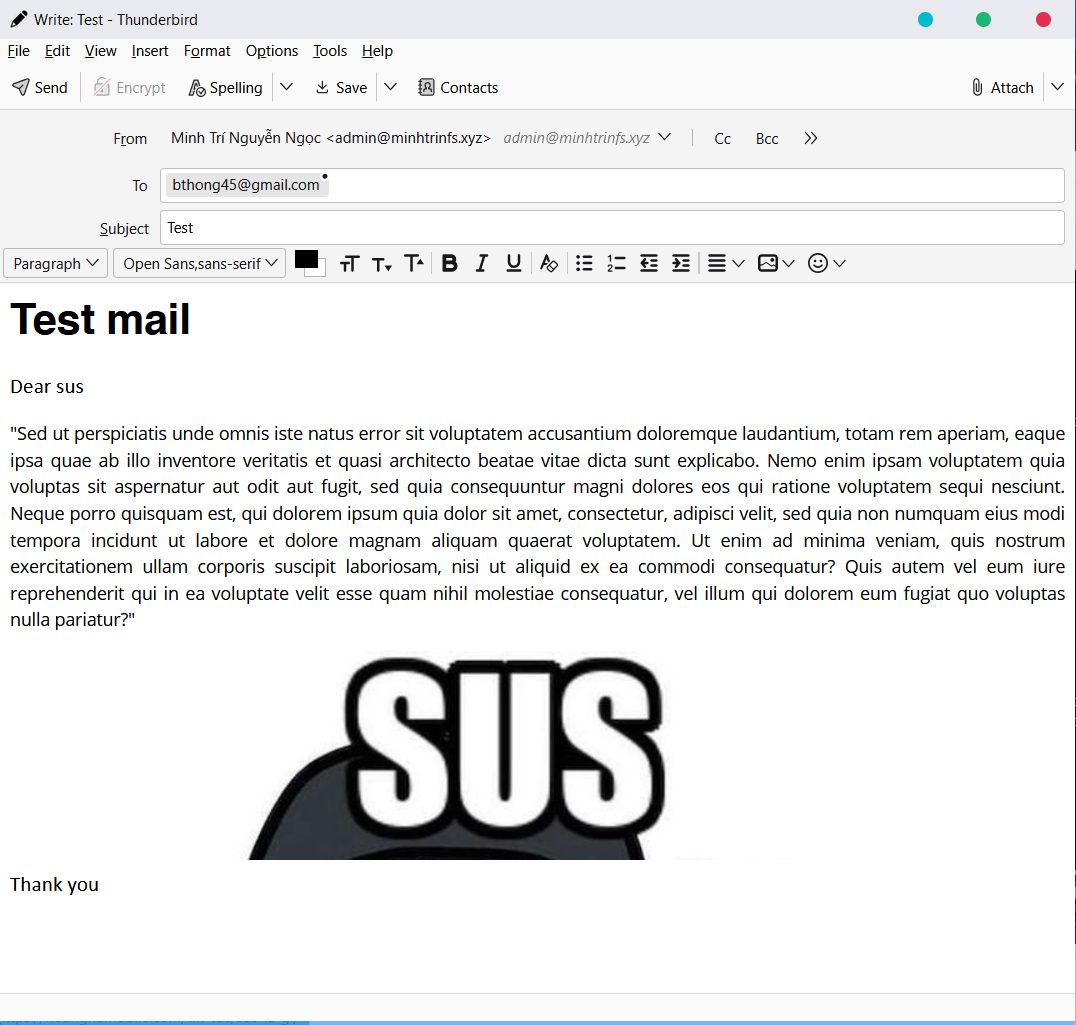
📩 Incoming Mail (IMAP hoặc POP3)

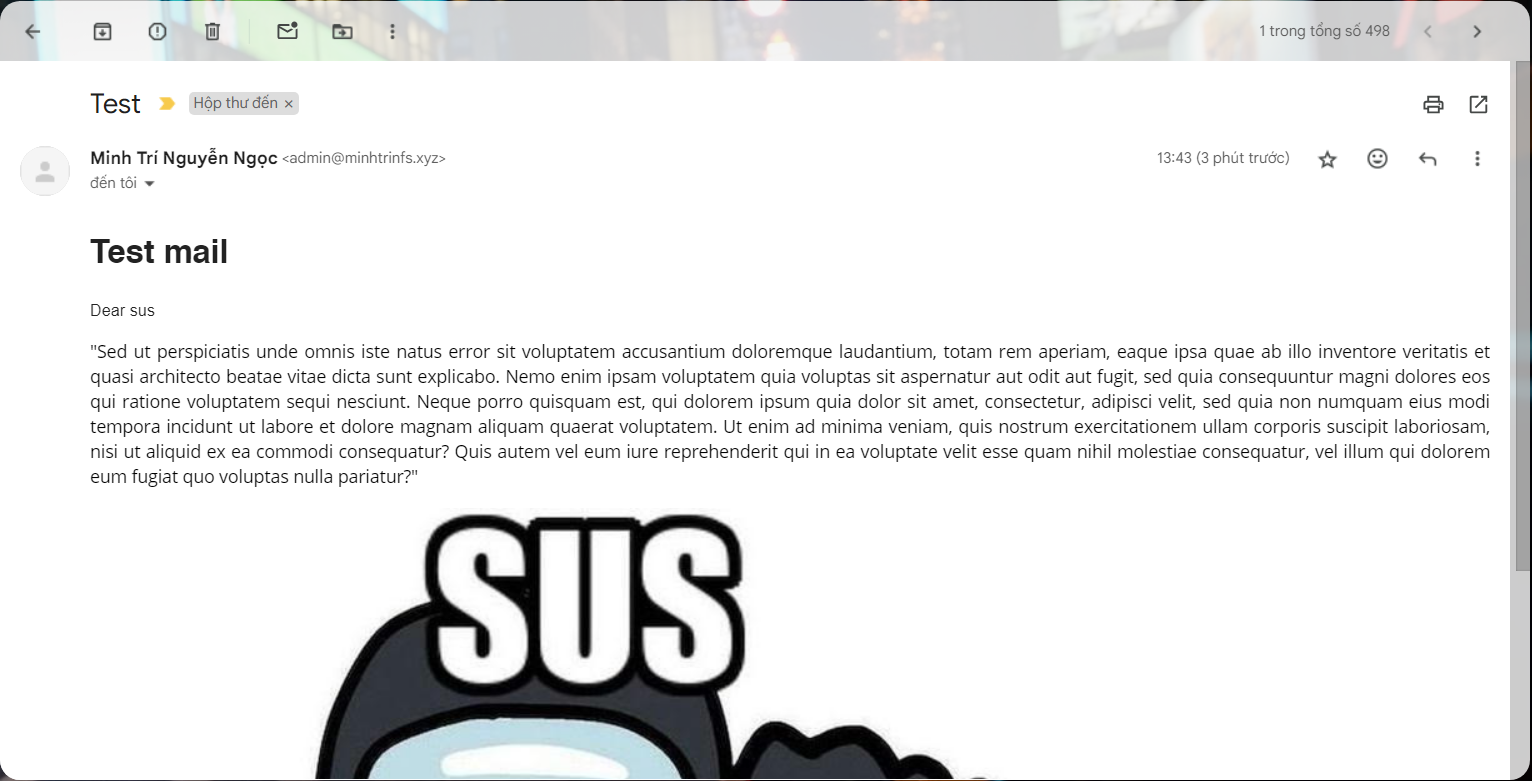
* Protocol: Chọn IMAP hoặc POP3
* Server hostname: mail.minhtrinfs.xyz (hoặc IP 45.122.223.84)
* Port: 993 (IMAP) hoặc 995 (POP3)
* SSL: SSL/TLS
* Authentication: Normal password

📤 Outgoing Mail (SMTP)

* Server hostname: mail.minhtrinfs.xyz
* Port: 587
* SSL: STARTTLS
* Authentication: Normal password







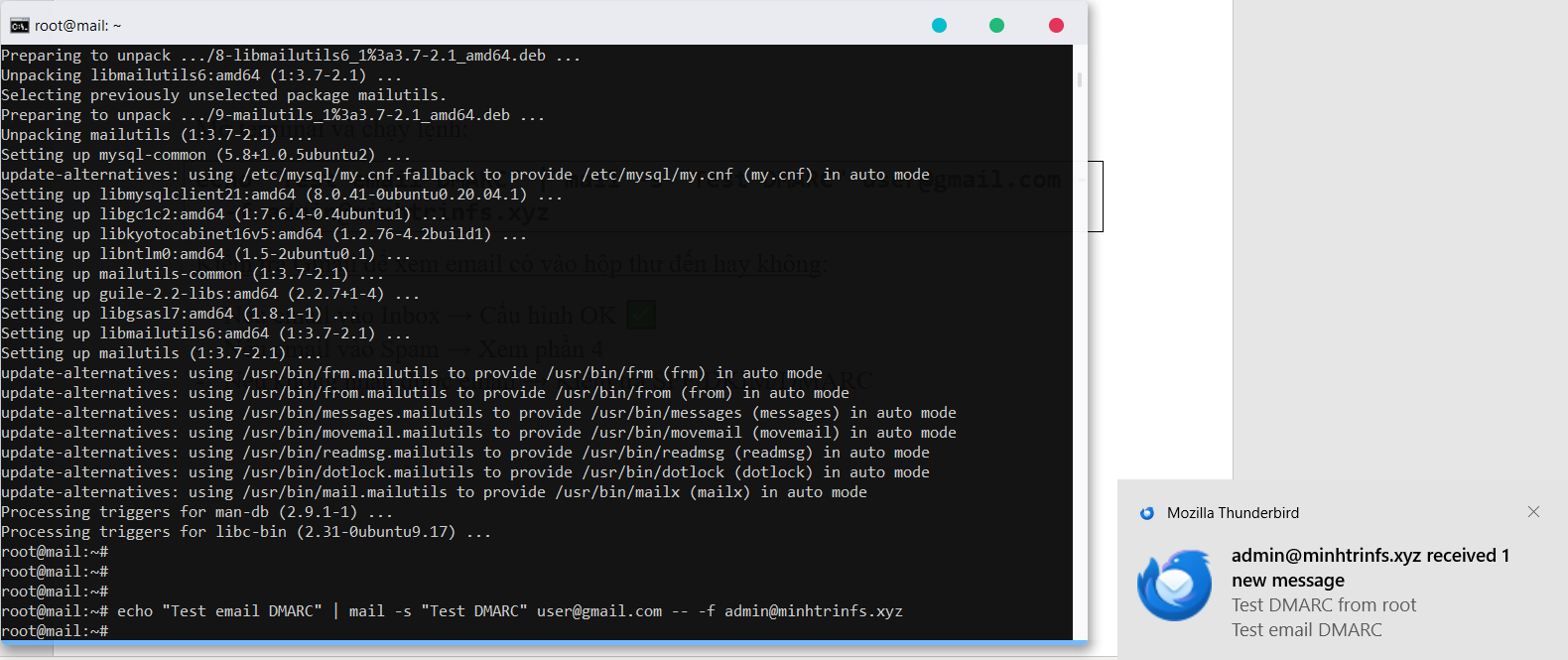
**Cách 2:** Gửi email test bằng lệnh sendmail hoặc mail trong Linux

Mở terminal và chạy lệnh:

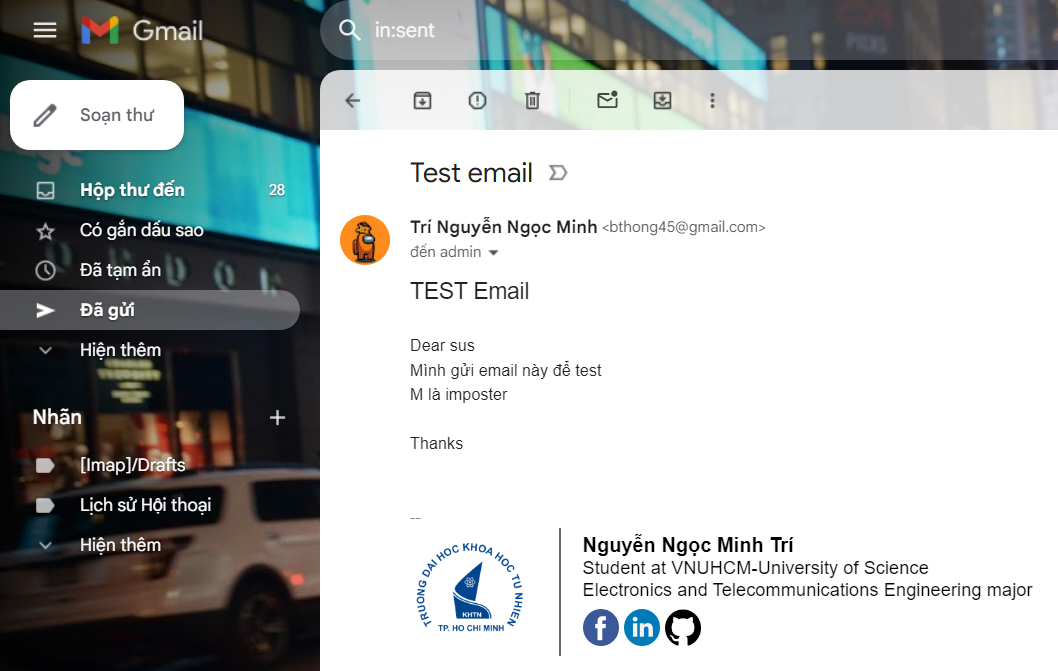
**echo "Test email DMARC" | mail -s "Test DMARC" user@gmail.com -- -f admin@minhtrinfs.xyz**

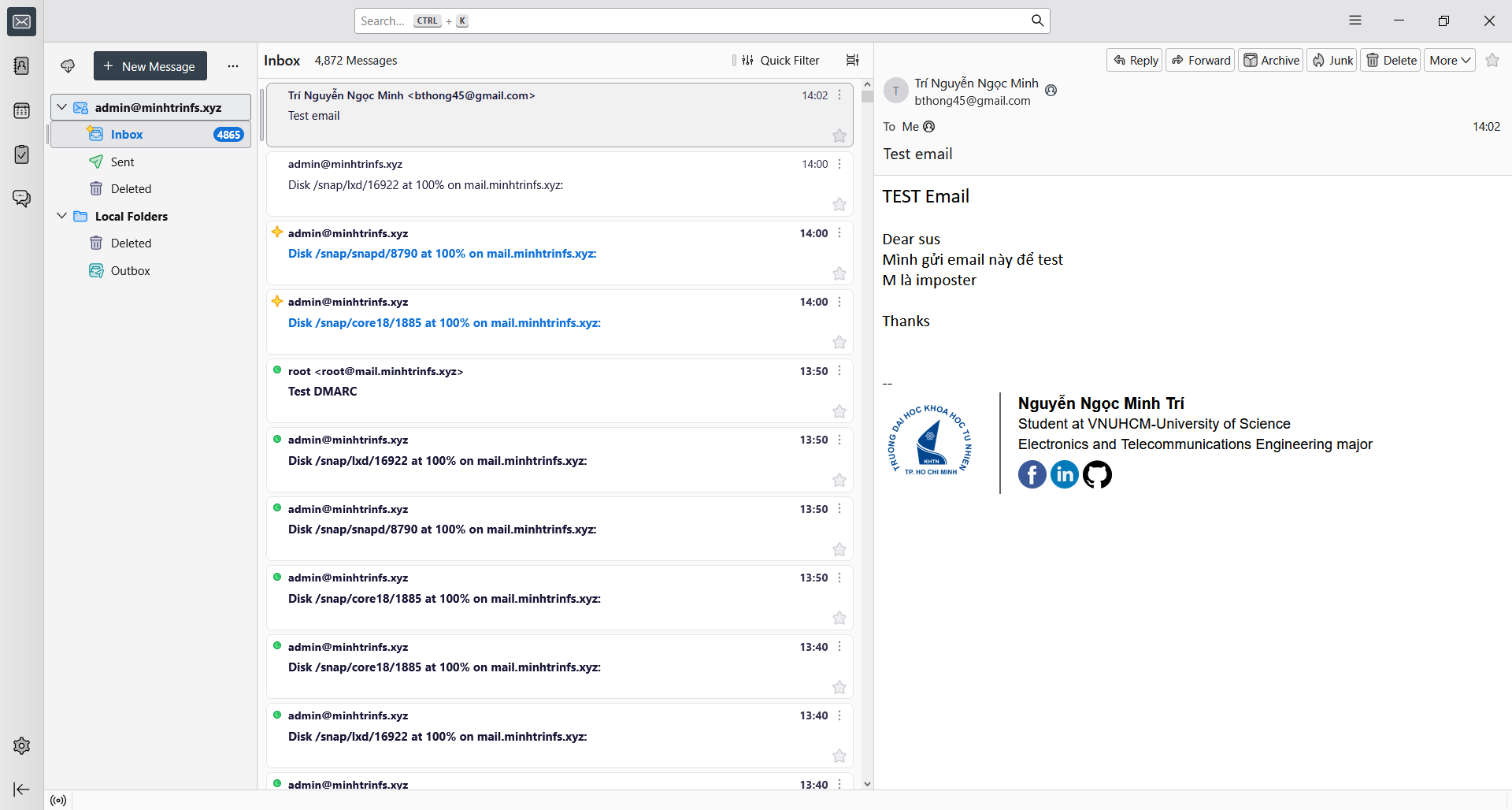
Kiểm tra Gmail để xem email có vào hộp thư đến hay không:

* Nếu email vào Inbox → Cấu hình OK ✅
* Nếu email vào Spam → Xem phần 4
* Nếu không nhận được email → Kiểm tra SPF/DKIM/DMARC



## **Email gmail gửi ngược lại và nhận được**





## **Cấu hình Zimbra đảm bảo hỗ trợ tự động config**

(em nghĩ nó ở phần trên luôn rồi nên em qua câu 8 vậy)

## **Tích hợp SMTP cho website của tuần 4**

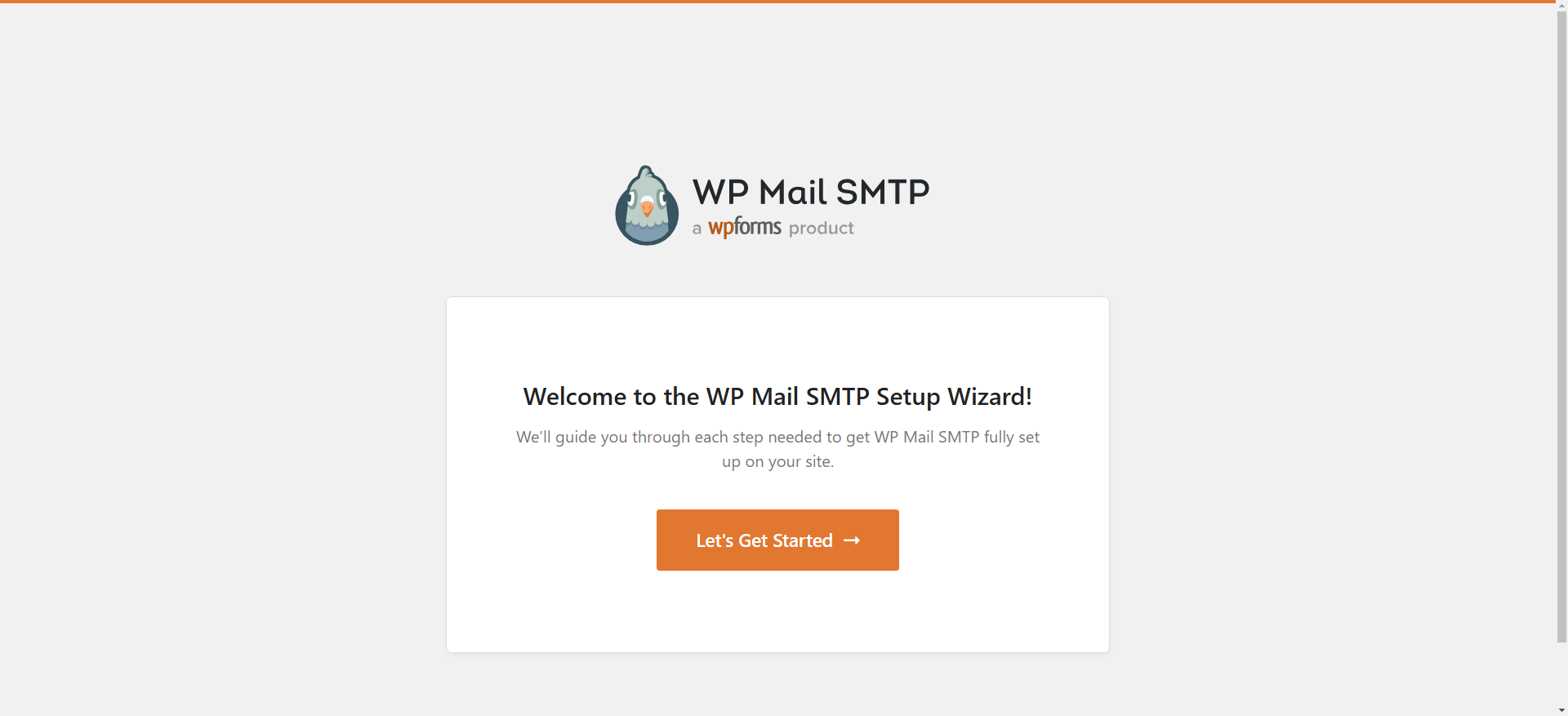
Em lấy site1 của WordPress ra để làm

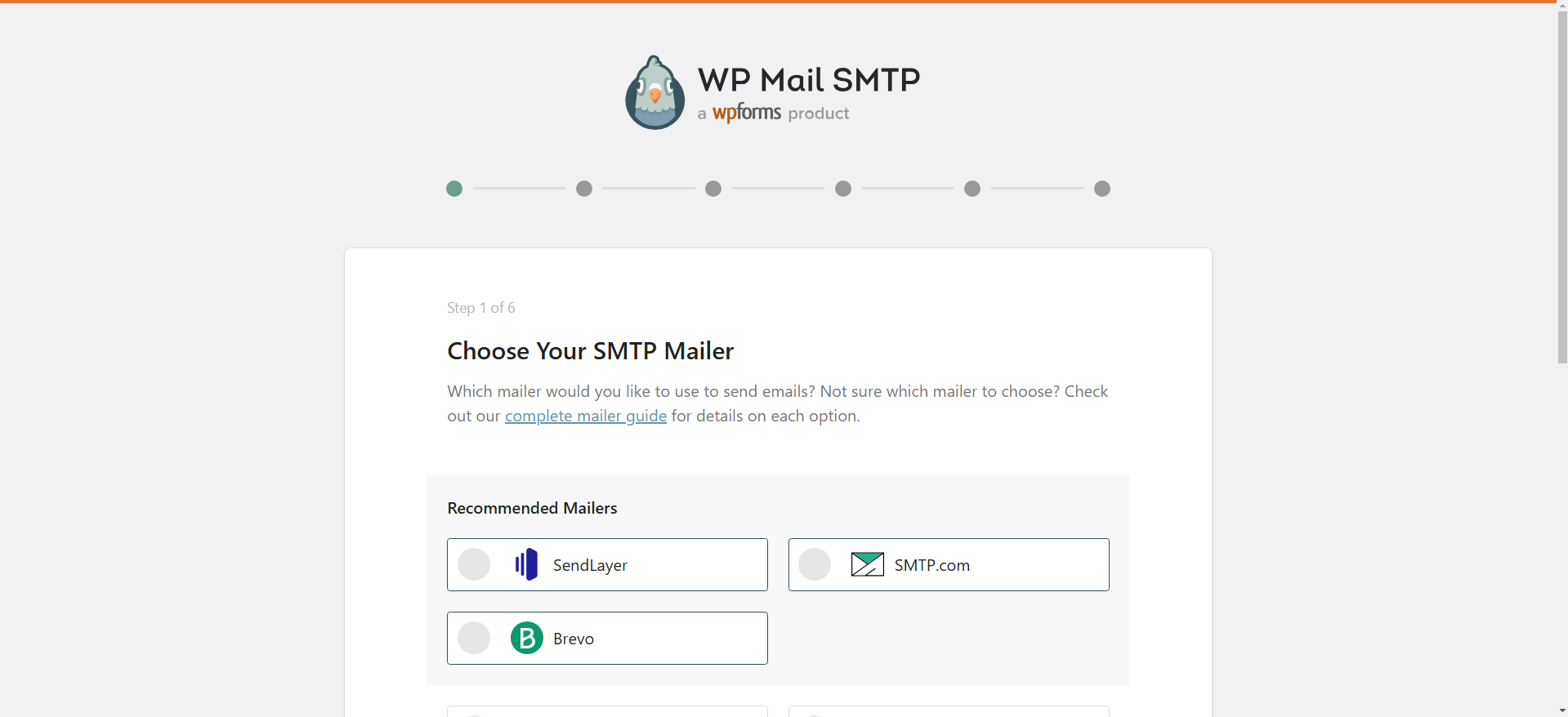
(trước đó đặt mật khẩu)

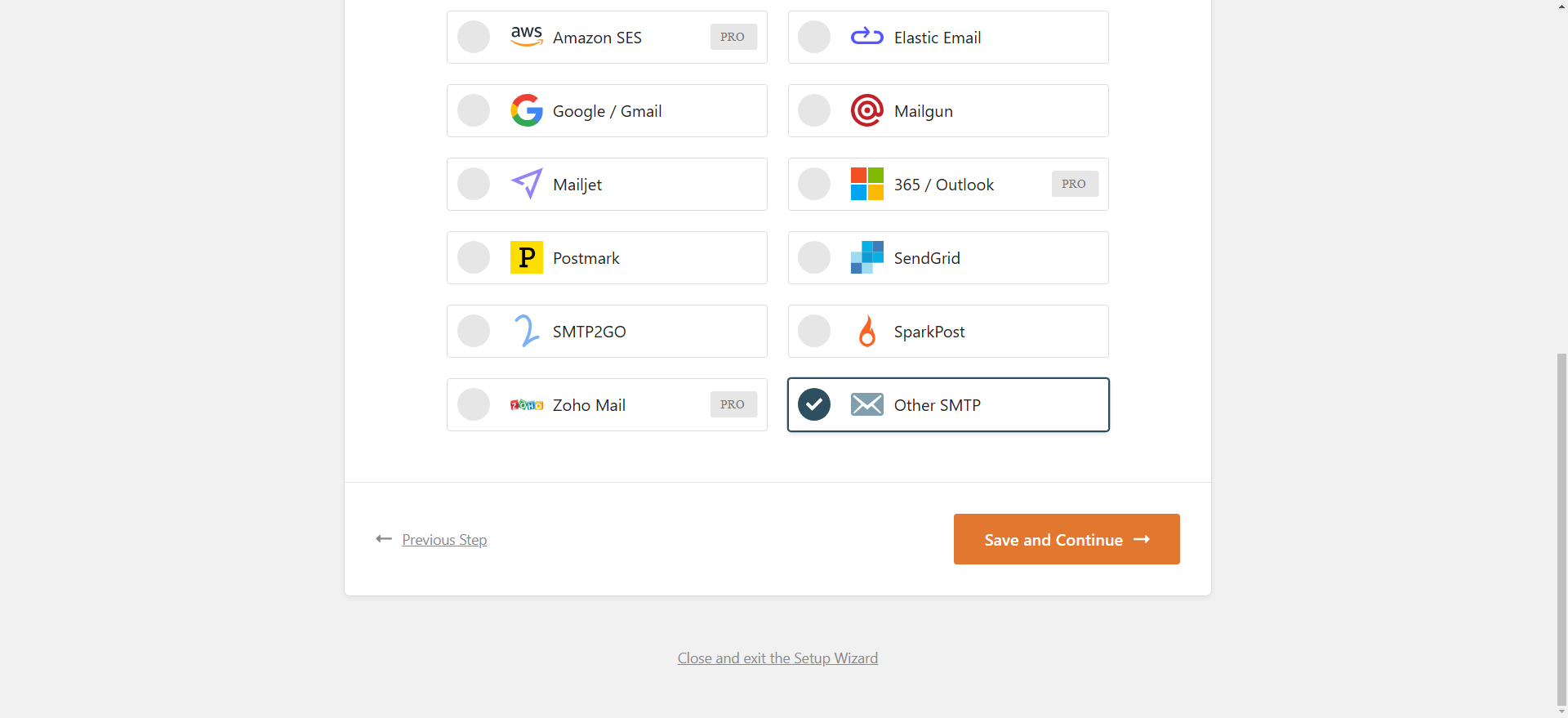
**sudo passwd site1**

**Asphalt9\_sucks**

Ngoài ra nhớ check coi vsftpd service đã chạy chưa. Rồi cài plugin WordPress thôi.









Username: admin@minhtrinfs.xyz

Password: NsgbwR67Tk

