**BÁO CÁO TUẦN 6   
(& UPDATE TUẦN 5)**

*Nguyễn Ngọc Minh Trí*

**MỤC LỤC**

[**MỤC LỤC** 2](#_Toc193832053)

[1. Cài đặt Proxmox Mail Gateway (PMG) 3](#_Toc193832054)

[2. Cấu hình SSL 11](#_Toc193832055)

[3. Cấu hình toàn bộ hệ thống email từ server Email Server của tuần 5 gửi và nhận email qua hệ thống PMG này 13](#_Toc193832056)

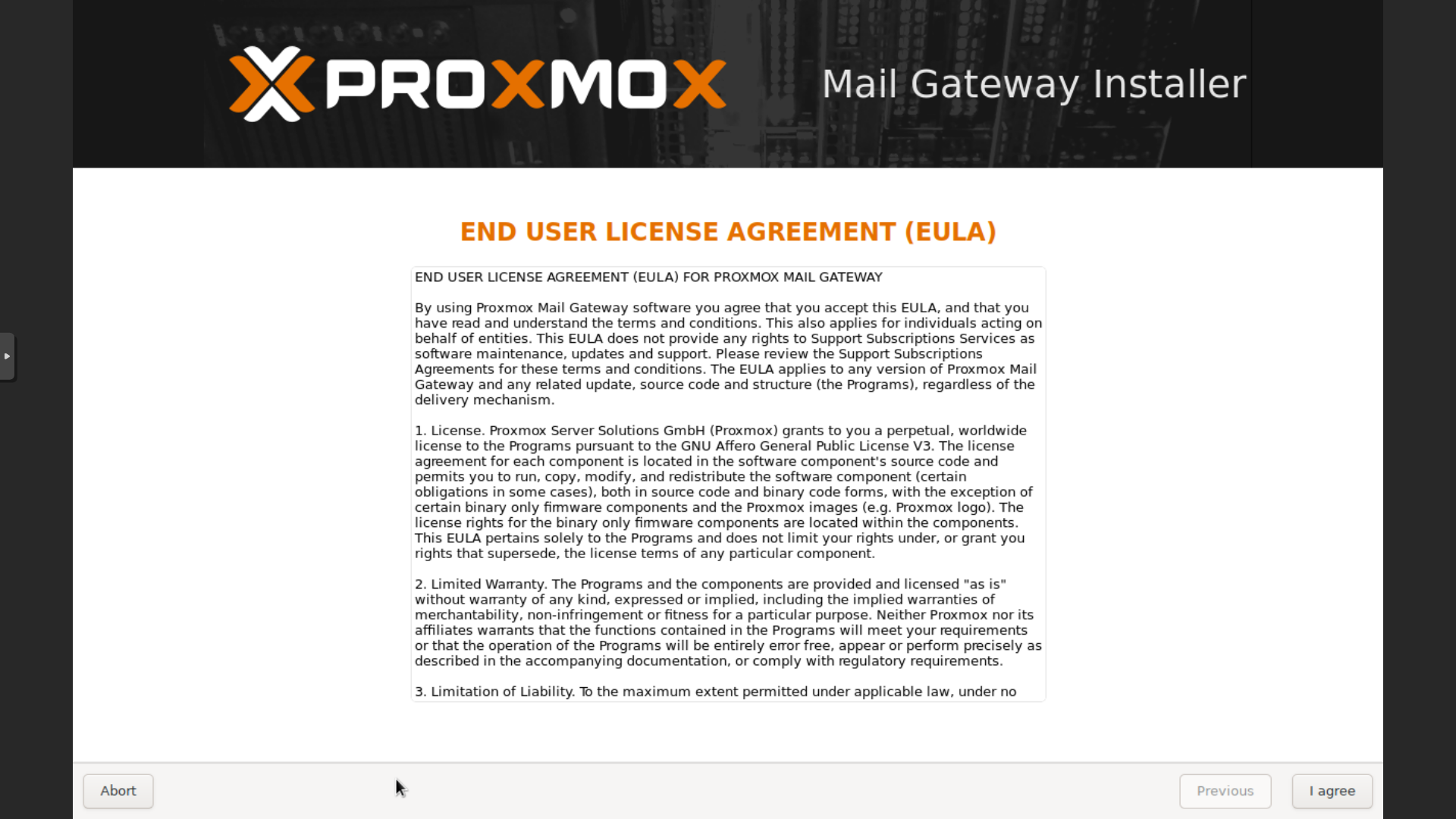
[4. Tìm hiểu về các chức năng có trên PMG 19](#_Toc193832057)

## **Cài đặt Proxmox Mail Gateway (PMG)**



Em cài Graphical cho dễ dùng

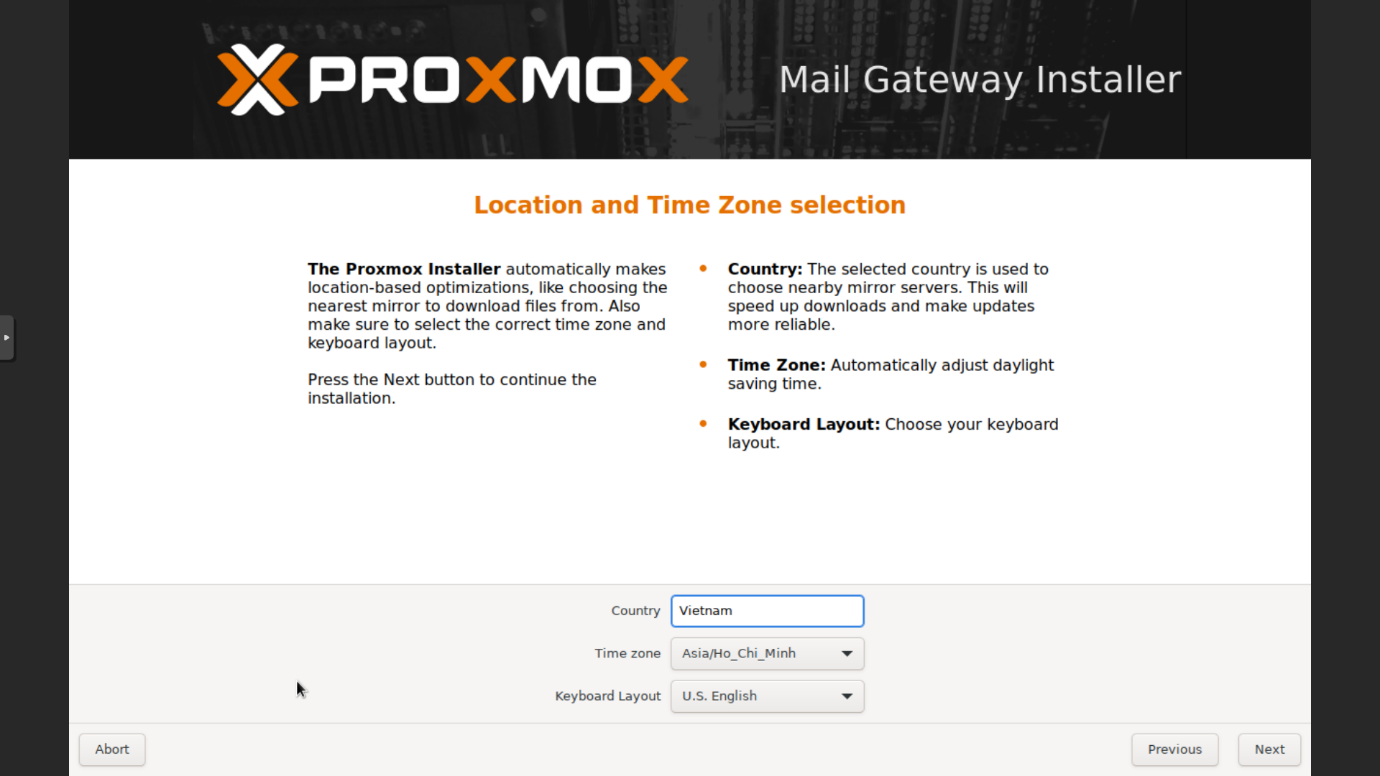




Bấm Agree.



Bước này chọn ổ đĩa để cài, vì hiện tại cũng chỉ có 1 ổ đó nên cứ bấm Next.





Password: Asphalt9\_sucks (user là root, ghi nhớ để tí nữa đăng nhập)

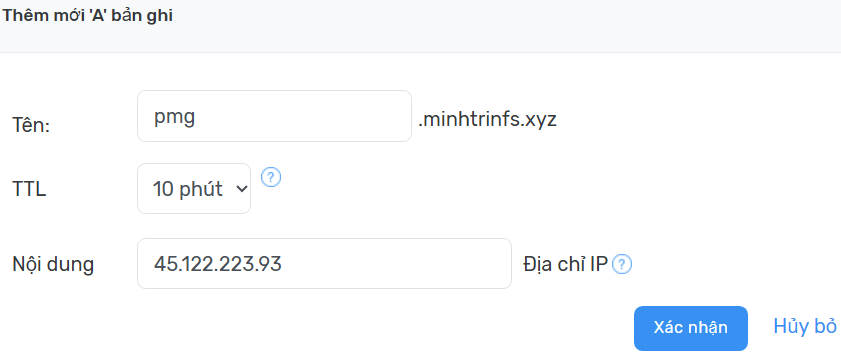
Email: (lấy email của tuần 5) [admin@minhtrinfs.xyz](mailto:admin@minhtrinfs.xyz)

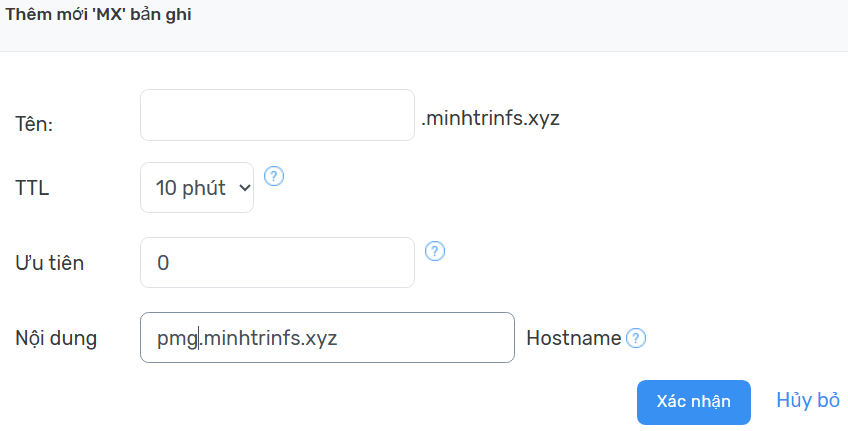
(Test thử xem coi gửi email bên máy tuần 6 qua bên máy tuần 5 xem như thế nào)

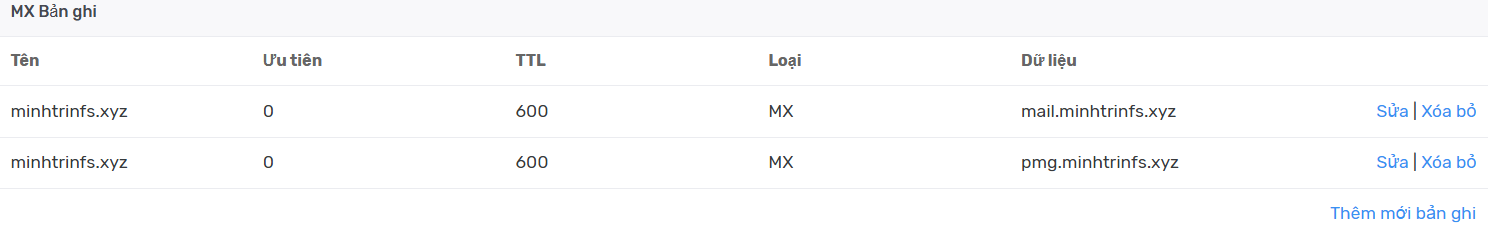
Tới bước điền Management Network Configuration:

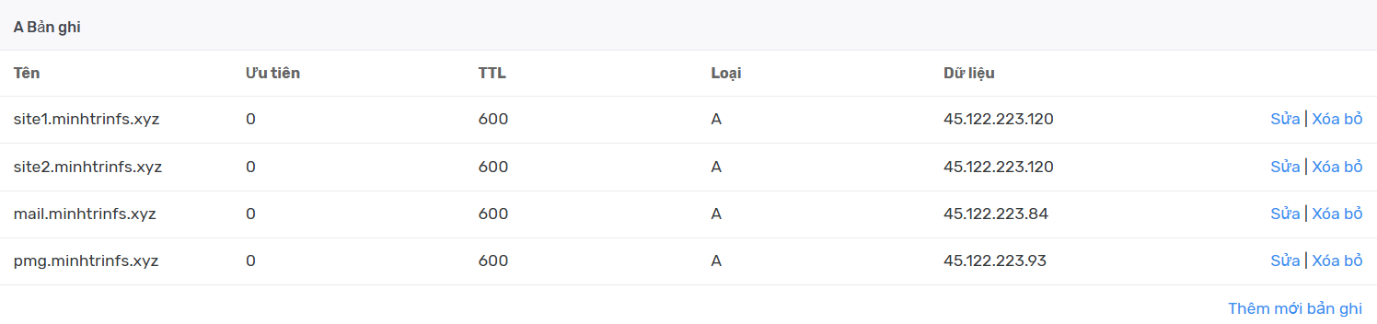


Mình cần thêm một bản ghi A và MX ở cấu hình DNS:

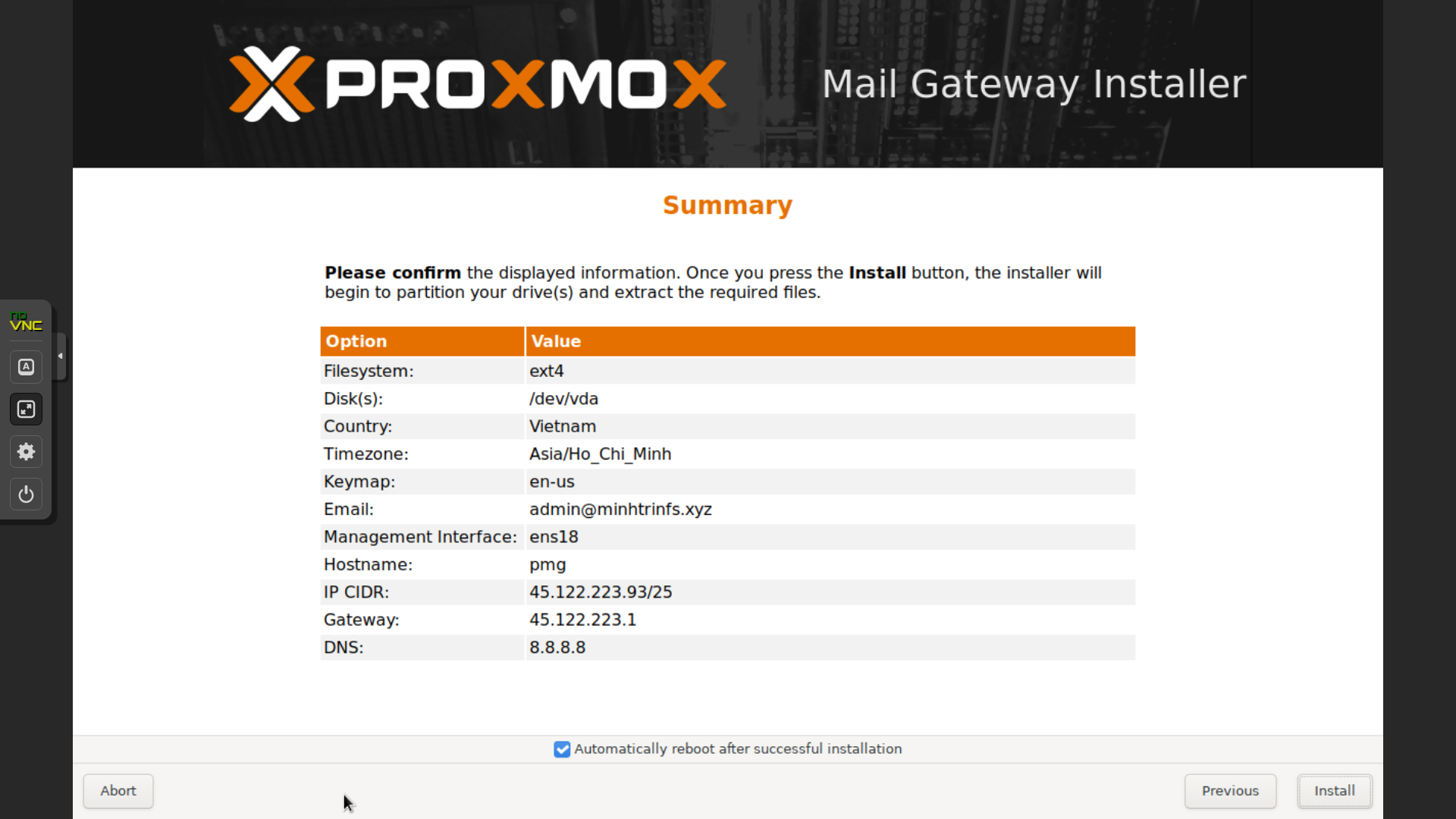






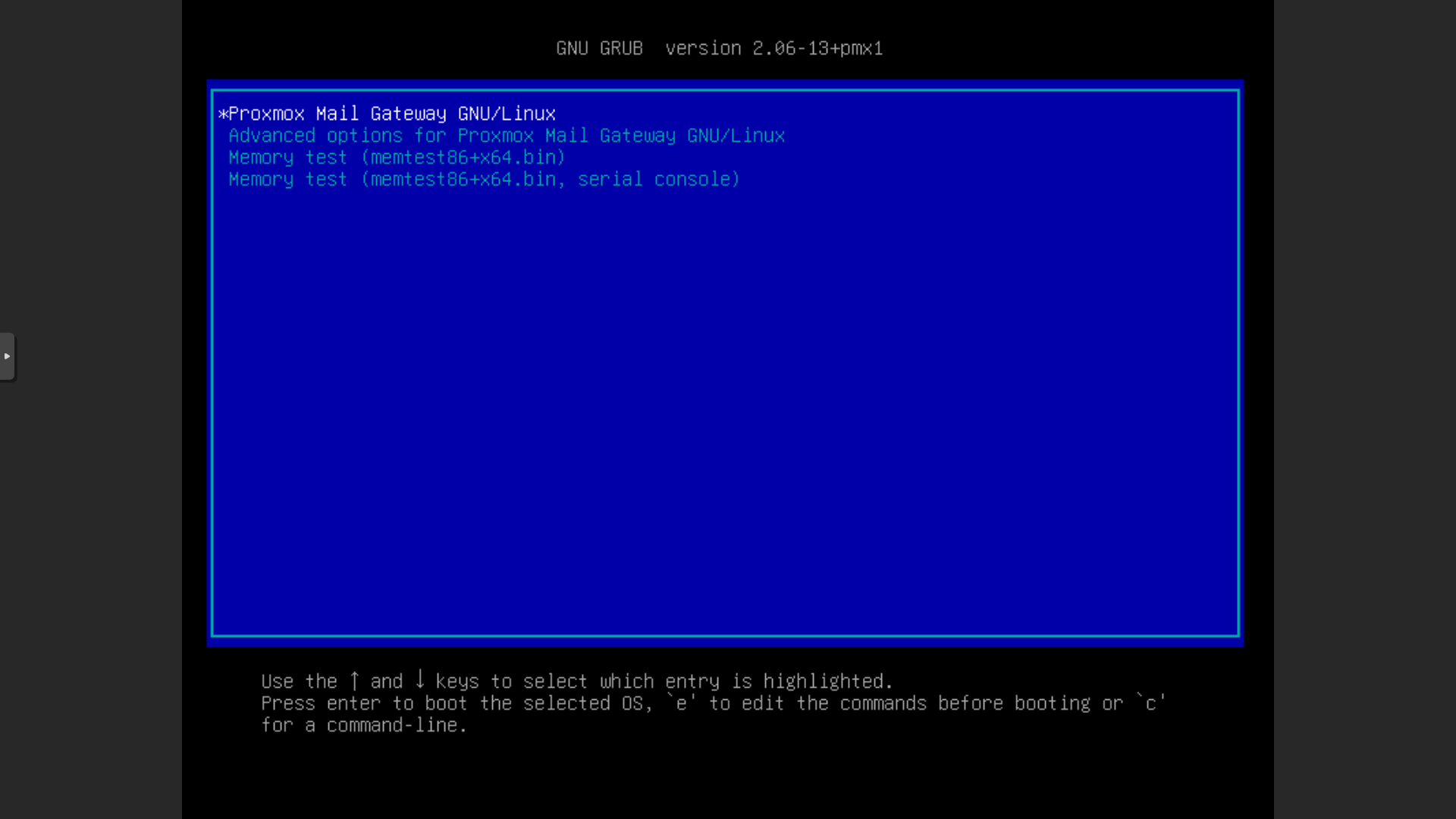


Sau khi xong hết, hãy xác nhận lại rồi cài đặt:

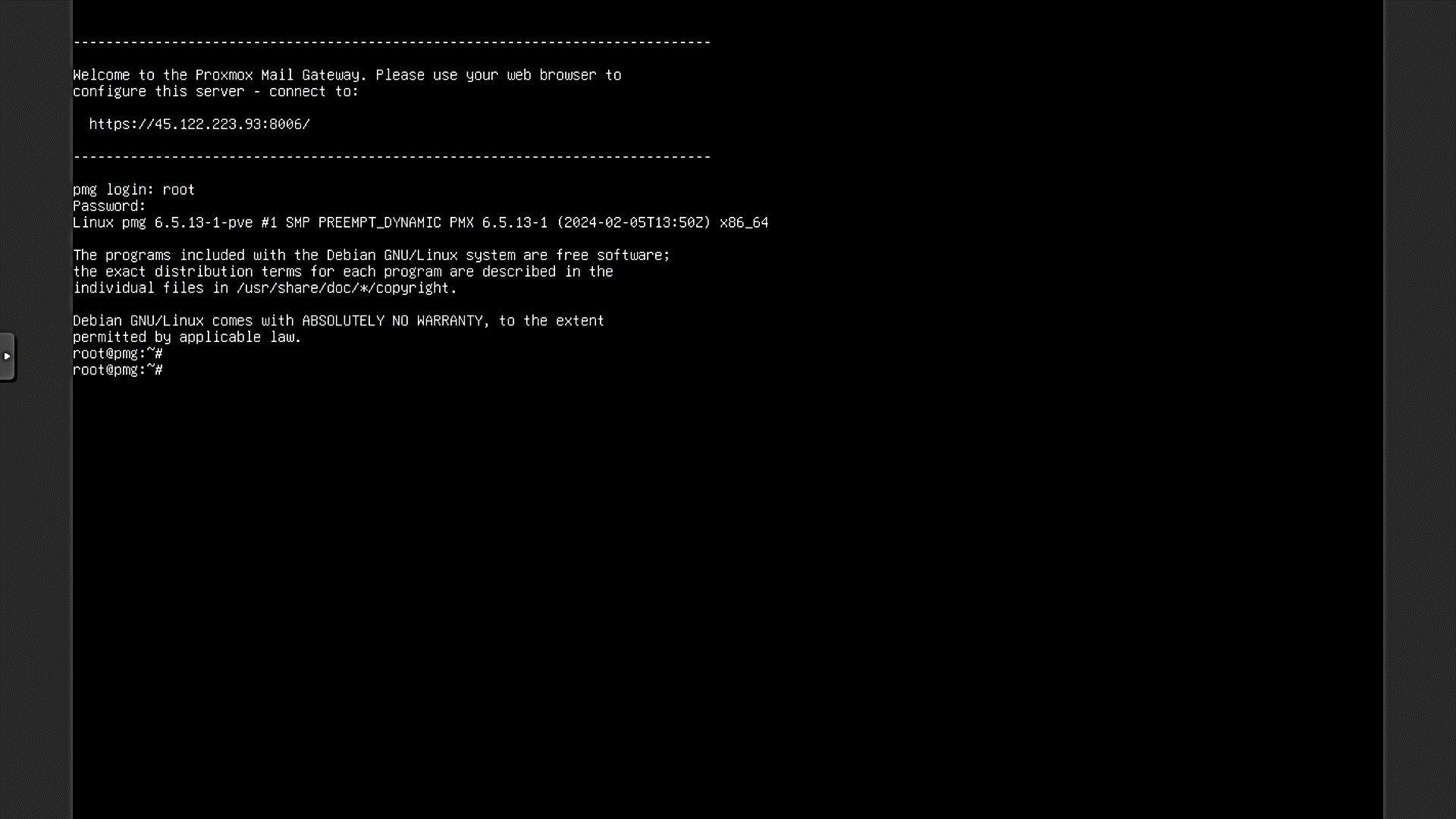




Sau khi cài xong:



Đăng nhập bằng tài khoản root, password là Asphalt9\_sucks



Lên trình duyệt gõ <địa chỉ WAN>:8006 – của em là 45.122.223.93:8006

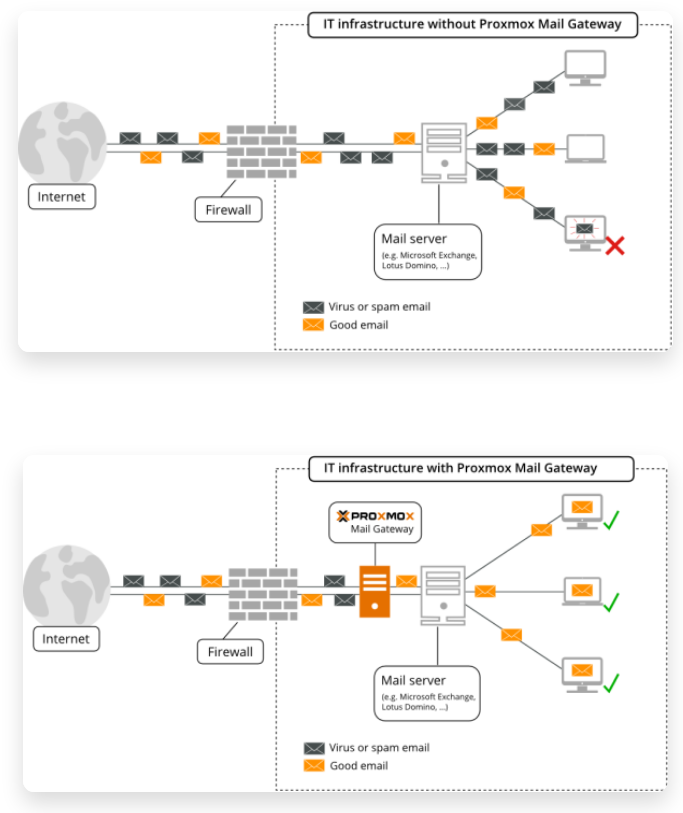


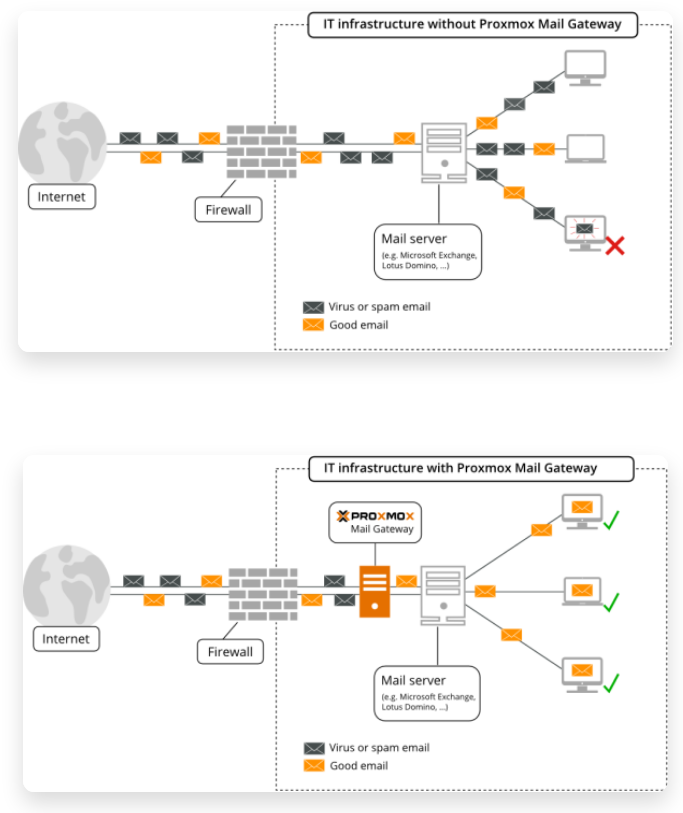


Mục đích của việc dùng Proxmox Mail Gateway:

* Lọc thư rác với độ chính xác cao.
* Ngăn chặn virus và các phần mềm độc hại.
* Đảm bảo an toàn email với công nghệ SPF, DKIM và TLS.
* Giao diện quản lý thân thiện, dễ sử dụng và triển khai nhanh chóng.

Phần mềm này không chỉ miễn phí mà còn giúp doanh nghiệp tiết kiệm chi phí mà vẫn đạt hiệu quả tối ưu trong quản lý và bảo mật email.





## **Cấu hình SSL**

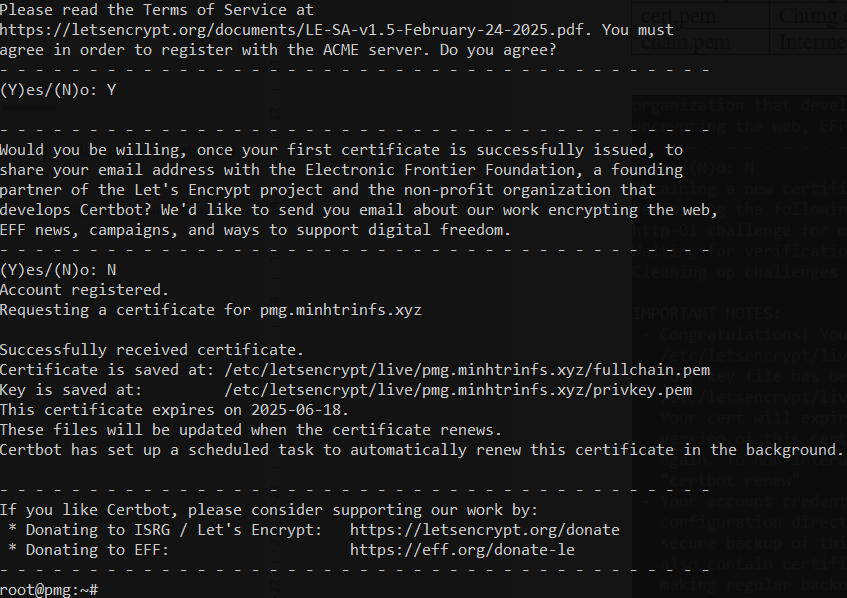
Cài đặt Certbot:

**sudo apt update**

**sudo apt install certbot -y**

Tạo chứng chỉ SSL với Let’s Encrypt:

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



Nếu thành công, chứng chỉ được lưu tại

/etc/letsencrypt/live/pmg.minhtrinfs.xyz/

Tiếp theo, sao lưu chứng chỉ cũ của PMG:

**sudo cp /etc/pmg/pmg-api.pem /etc/pmg/pmg-api.pem.bak**

Phòng trường hợp cần khôi phục lại chứng chỉ mặc định (lỗi tệp /etc/pmg/pmg-api.pem không tồn tại trên hệ thống của bạn):

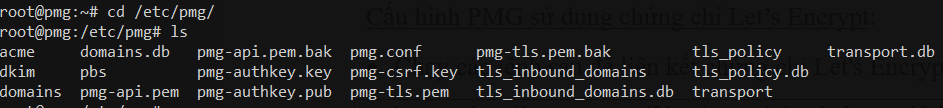
Kiểm tra xem PMG đang dùng chứng chỉ nào:

**sudo ls -l /etc/pmg/**

Nếu không có tệp pmg-api.pem và pmg-tls.pem thì có thể tạo chứng chỉ tự ký tạm thời sử dụng lệnh:

**sudo pmgconfig cert generate**

Lệnh này sẽ tạo lại chứng chỉ



**NOTE:** Sẽ có nhầm lẫn giữa 2 file là pmg-api.pem và pmg-tls.pem

1. **pmg-api.pem – Chứng chỉ API của giao diện web PMG**

Đây là chứng chỉ SSL chính mà PMG sử dụng để bảo mật giao diện quản trị web trên cổng 8006 (<https://pmg.minhtrinfs.xyz:8006>). Nó thường cần được thay thế bằng chứng chỉ Let's Encrypt để tránh cảnh báo bảo mật khi truy cập giao diện quản trị.

1. **pmg-tls.pem – Chứng chỉ TLS cho máy chủ SMTP của PMG**

Đây là chứng chỉ được sử dụng cho SMTP TLS (STARTTLS) khi gửi/nhận email qua PMG. Nó bảo vệ kết nối SMTP trên các cổng như 25, 465, hoặc 587. Nếu nó không có sẵn trên hệ thống của bạn, có thể vì PMG không tạo tự động hoặc bạn chưa bật cấu hình TLS cho SMTP.

Cấu hình PMG sử dụng chứng chỉ Let’s Encrypt:

* Chạy các lệnh sau để liên kết chứng chỉ Let's Encrypt với PMG.

**sudo cat /etc/letsencrypt/live/pmg.minhtrinfs.xyz/fullchain.pem /etc/letsencrypt/live/pmg.minhtrinfs.xyz/privkey.pem > /etc/pmg/pmg-tls.pem**

* Thiết lập quyền cho file chứng chỉ.

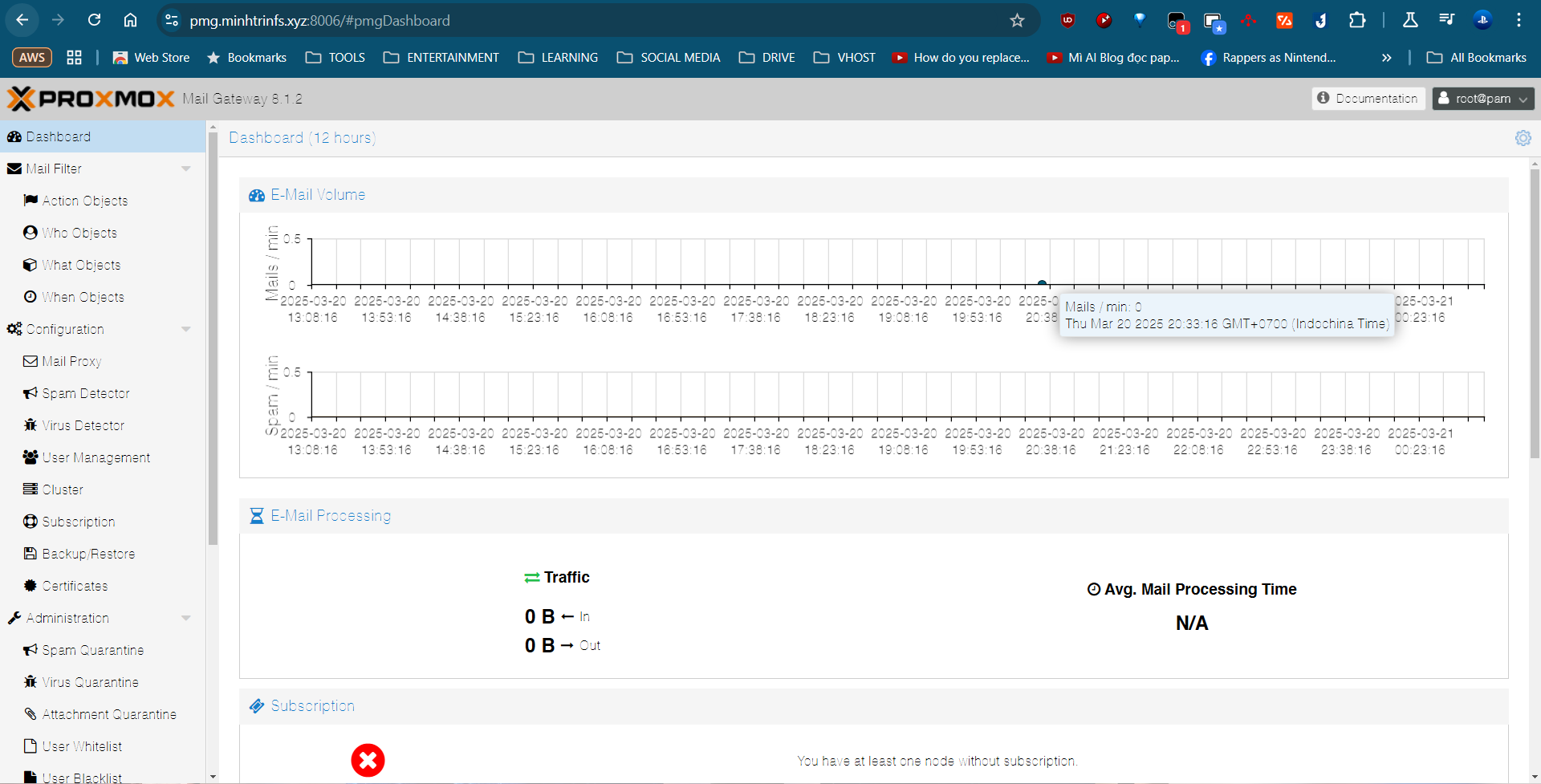
**sudo chmod 640 /etc/pmg/pmg-tls.pem**

**sudo chown root:root /etc/pmg/pmg-tls.pem**

Khởi động lại dịch vụ PMG:

**sudo systemctl restart pmgproxy**

Giờ bạn có thể truy cập giao diện web của PMG bằng HTTPS qua: <https://pmg.minhtrinfs.xyz:8006>



## **Cấu hình toàn bộ hệ thống email từ server Email Server của tuần 5 gửi và nhận email qua hệ thống PMG này**

**Bước 1:** Cấu hình Zimbra gửi email qua PMG

Trên Zimbra (mail.minhtrinfs.xyz), bạn cần đặt PMG làm Mail Relay để mọi email gửi đi qua PMG trước khi ra Internet.

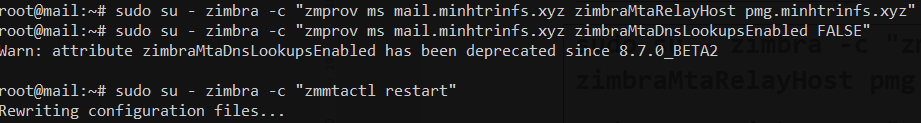
1. Cấu hình Mail Relay trên Zimbra

SSH vào Zimbra và chạy:

**sudo su - zimbra -c "zmprov ms mail.minhtrinfs.xyz zimbraMtaRelayHost pmg.minhtrinfs.xyz"**

**sudo su - zimbra -c "zmprov ms mail.minhtrinfs.xyz zimbraMtaDnsLookupsEnabled FALSE"**

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



1. Cấu hình PMG để nhận email trước khi chuyển đến Zimbra

Bạn cần đảm bảo PMG biết Zimbra là mail server chính để chuyển email đến đúng máy chủ sau khi kiểm tra spam:

SSH vào PMG (pmg.minhtrinfs.xyz) và sửa file:

**sudo nano /etc/pmg/transport**

Thêm dòng:

minhtrinfs.xyz smtp:[mail.minhtrinfs.xyz]:25

Lưu lại. Sau đó áp dụng thay đổi:

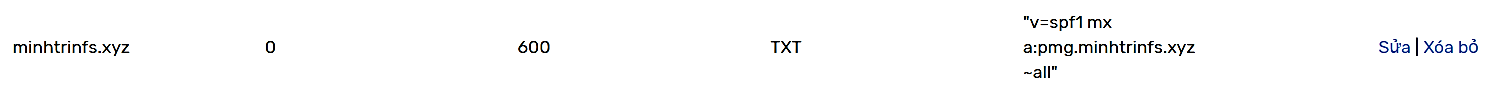
**sudo pmgconfig sync**

**sudo systemctl restart postfix**

1. Cập nhật SPF, DKIM, DMARC

SPF Record (TXT) (thêm pmg.minhtrinfs.xyz vào SPF):

**minhtrinfs.xyz TXT "v=spf1 mx a:pmg.minhtrinfs.xyz ~all"**

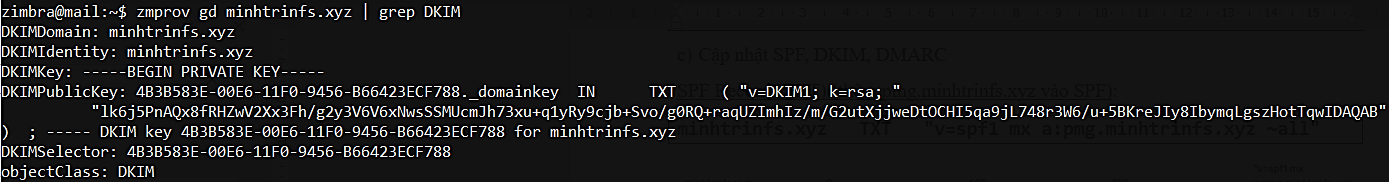


DKIM & DMARC:

* Kiểm tra DKIM:

**su - zimbra**

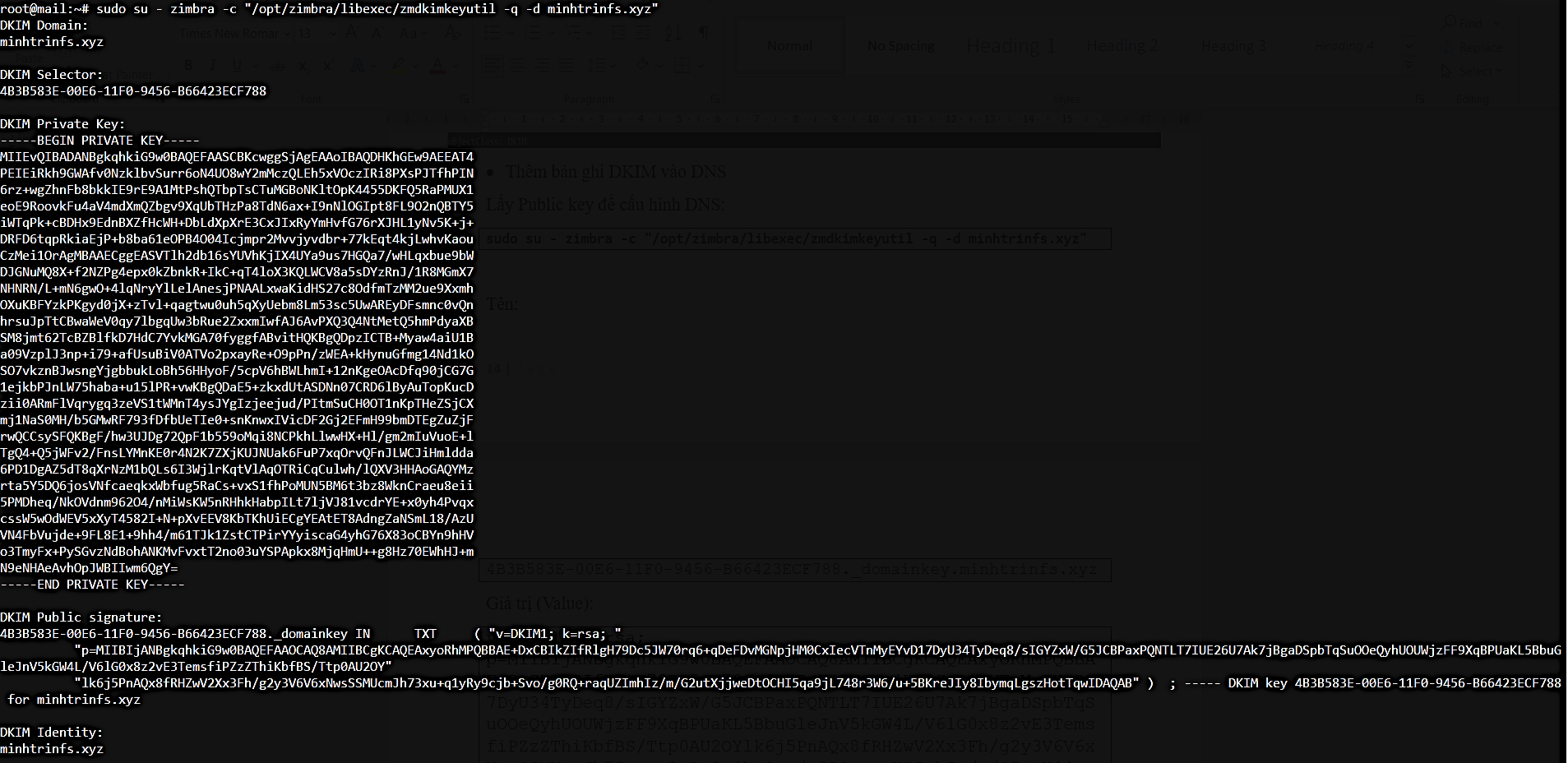
**zmprov gd minhtrinfs.xyz | grep DKIM**

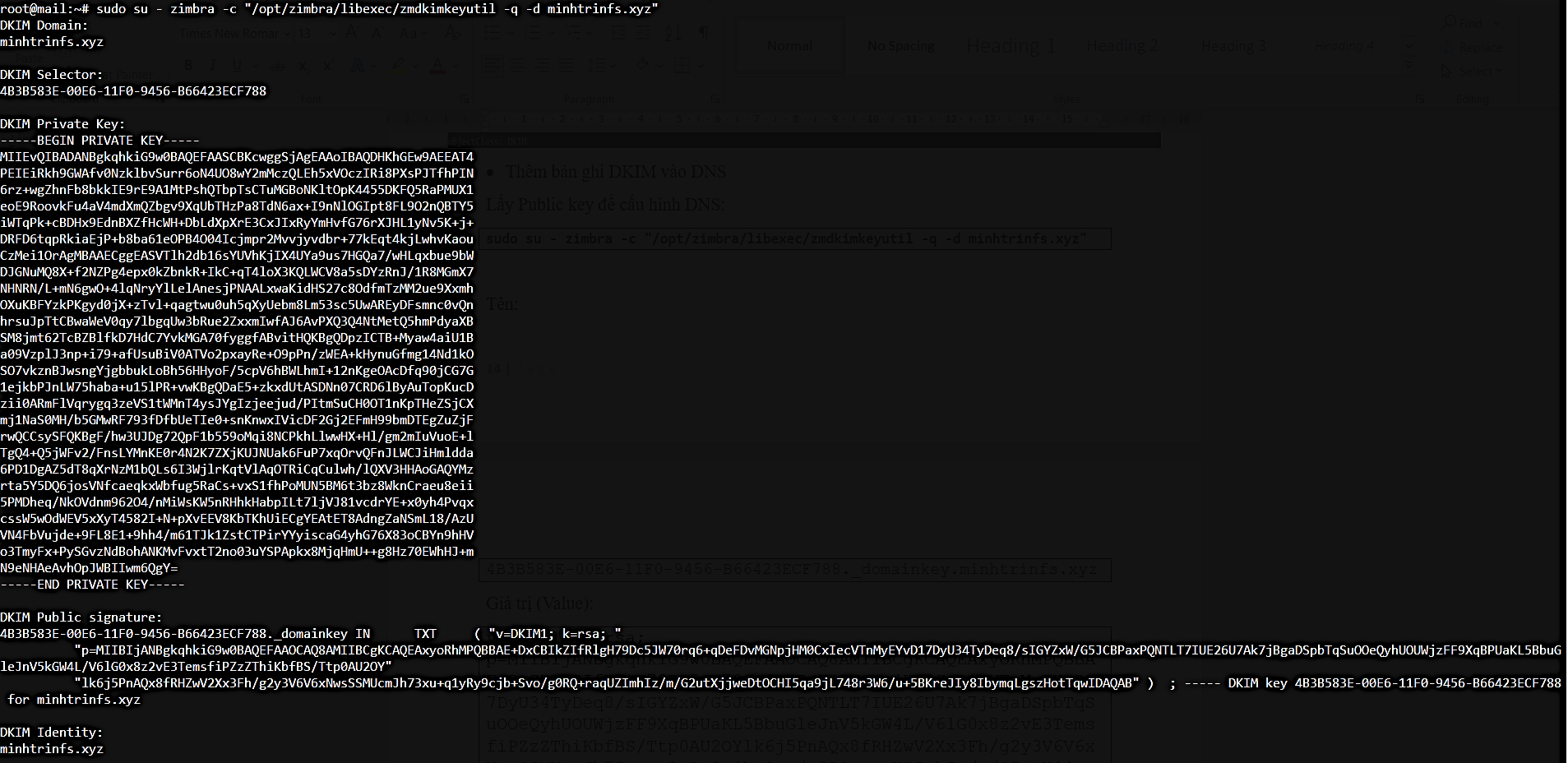


* Check thêm bản ghi DKIM vào DNS

Lấy Public key để cấu hình DNS:

**sudo su - zimbra -c "/opt/zimbra/libexec/zmdkimkeyutil -q -d minhtrinfs.xyz"**





Tên:

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

Giá trị (Value):

v=DKIM1; k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxyoRhMPQBBAE+DxCBIkZIfRlgH79Dc5JW70rq6+qDeFDvMGNpjHM0CxIecVTnMyEYvD17DyU34TyDeq8/sIGYZxW/G5JCBPaxPQNTLT7IUE26U7Ak7jBgaDSpbTqSuOOeQyhUOUWjzFF9XqBPUaKL5BbuGleJnV5kGW4L/V6lG0x8z2vE3TemsfiPZzZThiKbfBS/Ttp0AU2OYlk6j5PnAQx8fRHZwV2Xx3Fh/g2y3V6V6xNwsSSMUcmJh73xu+q1yRy9cjb+Svo/g0RQ+raqUZImhIz/m/G2utXjjweDtOCHI5qa9jL748r3W6/u+5BKreJIy8IbymqLgszHotTqwIDAQAB

* Nếu cần thêm DMARC, thêm bản ghi TXT (**NOTE:** nếu có thêm 1 cái mailto thì hãy để nó chung 1 dòng, tạo dòng mới mà chung tên là sẽ bị lỗi):

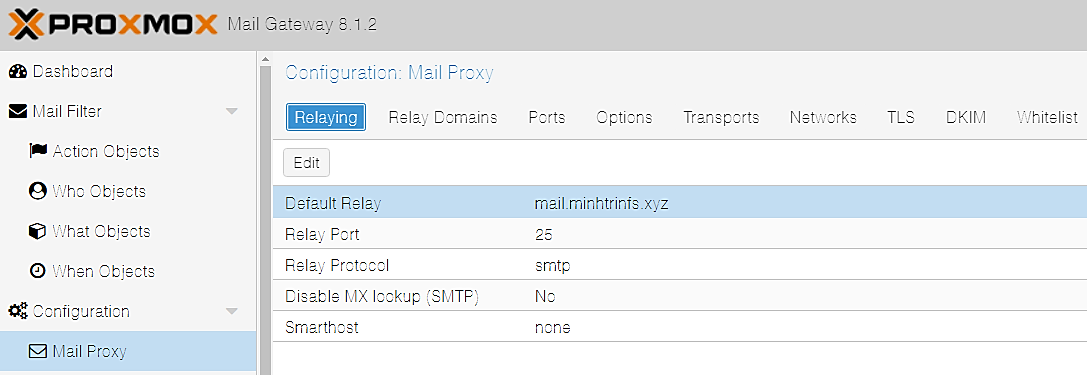
**\_dmarc.minhtrinfs.xyz TXT "** **v=DMARC1; p=quarantine; pct=100; rua=mailto:dmarc@minhtrinfs.xyz,mailto:admin@minhtrinfs.xyz"**

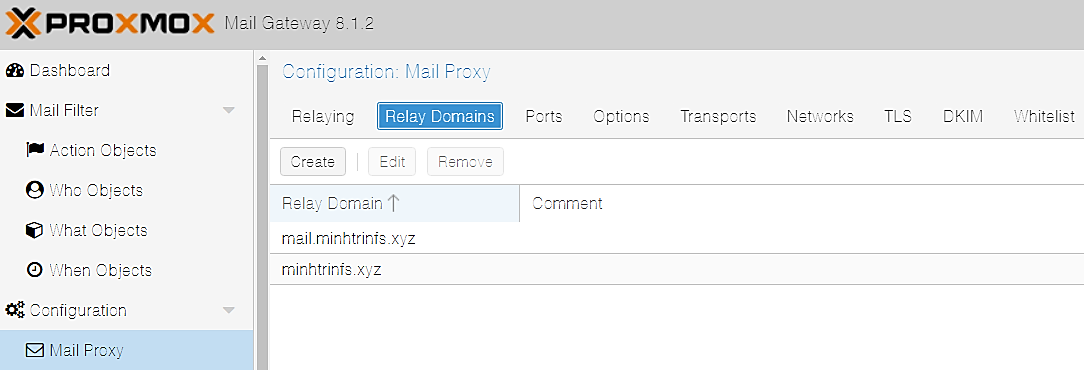


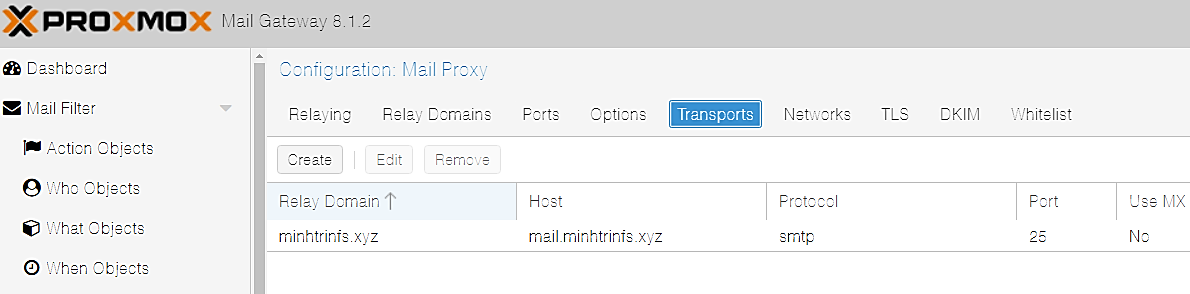


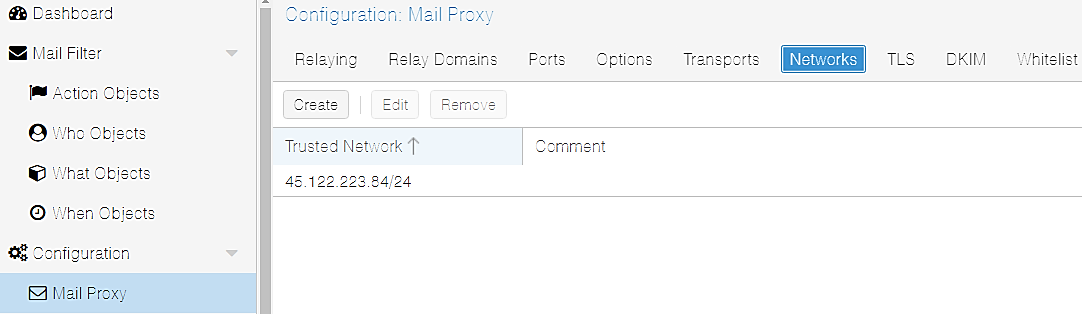
*(Theo tiêu chuẩn, một miền chỉ nên có một bản ghi DMARC duy nhất. 1 tên miền có 2 bản ghi DMARC, điều này có thể khiến hệ thống email không biết dùng bản ghi nào)*

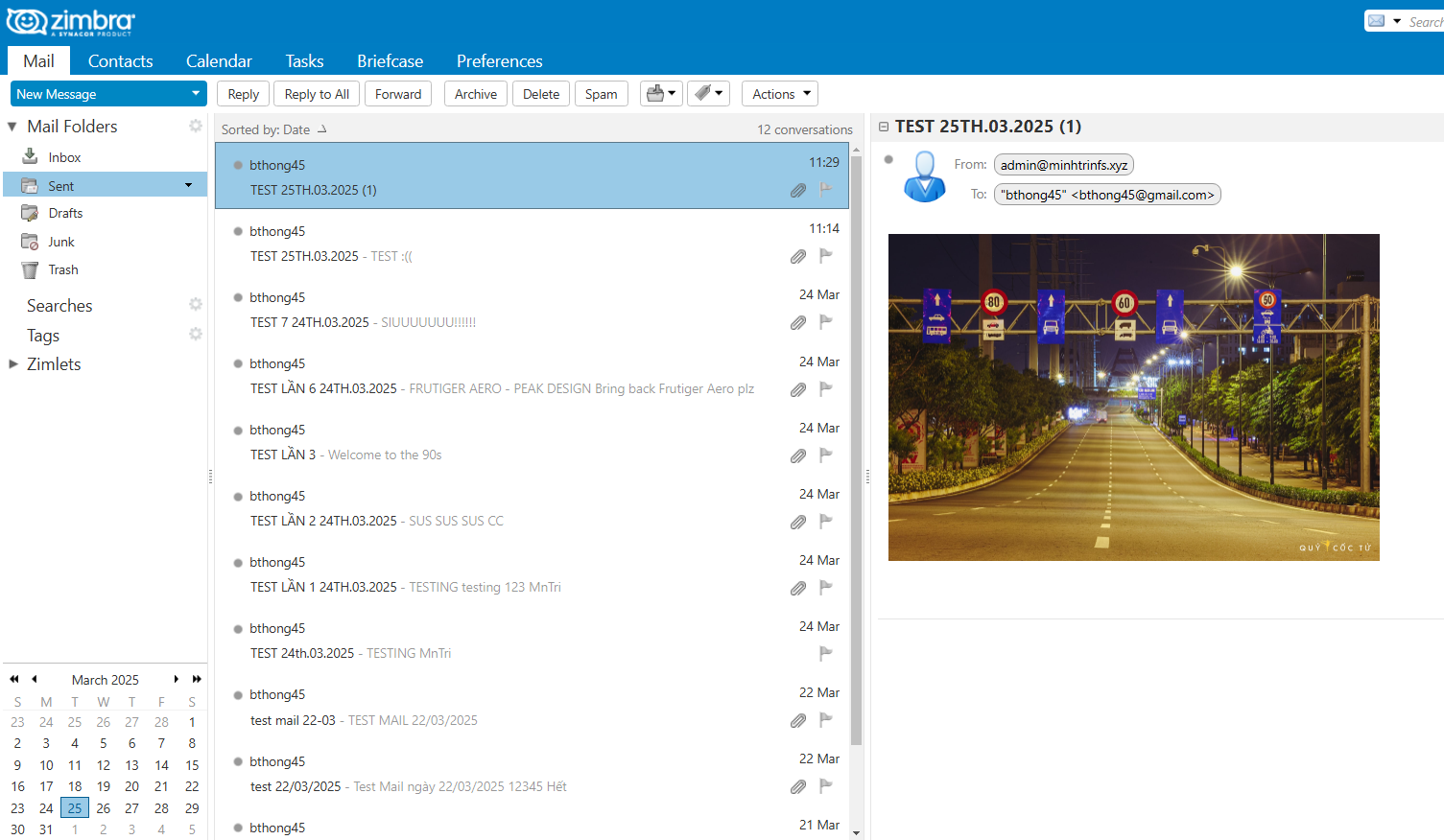
1. Vô trong dashboard PMG chỉnh một số thứ sau đây:

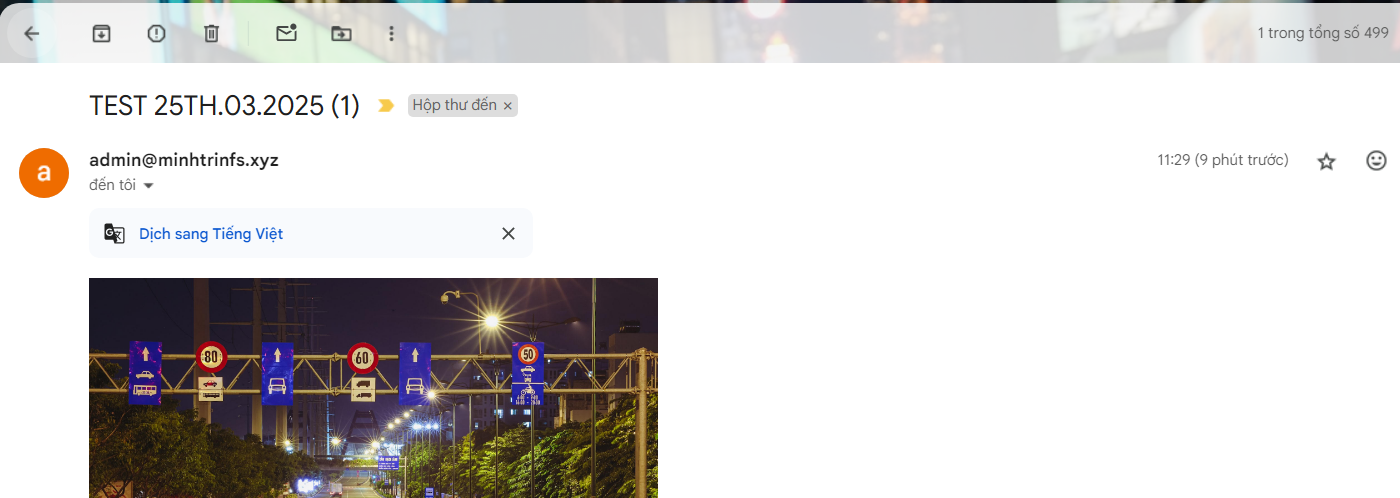


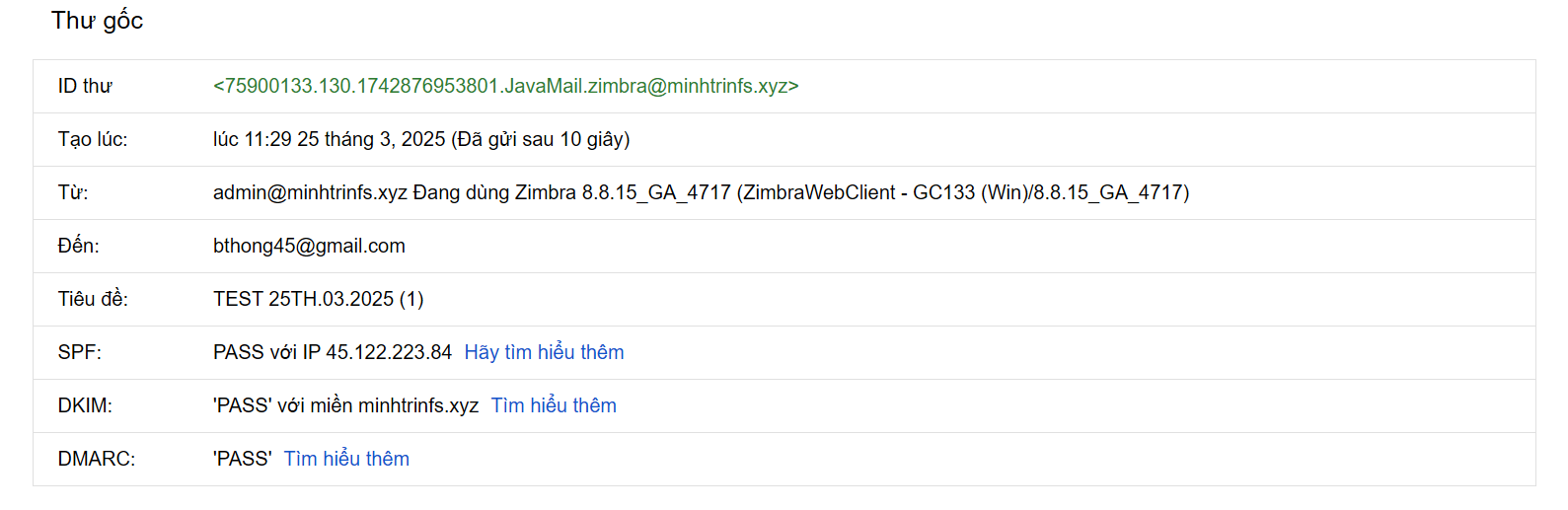




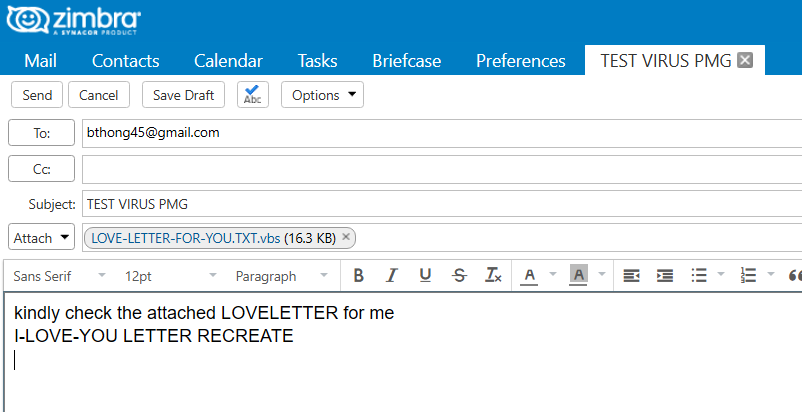




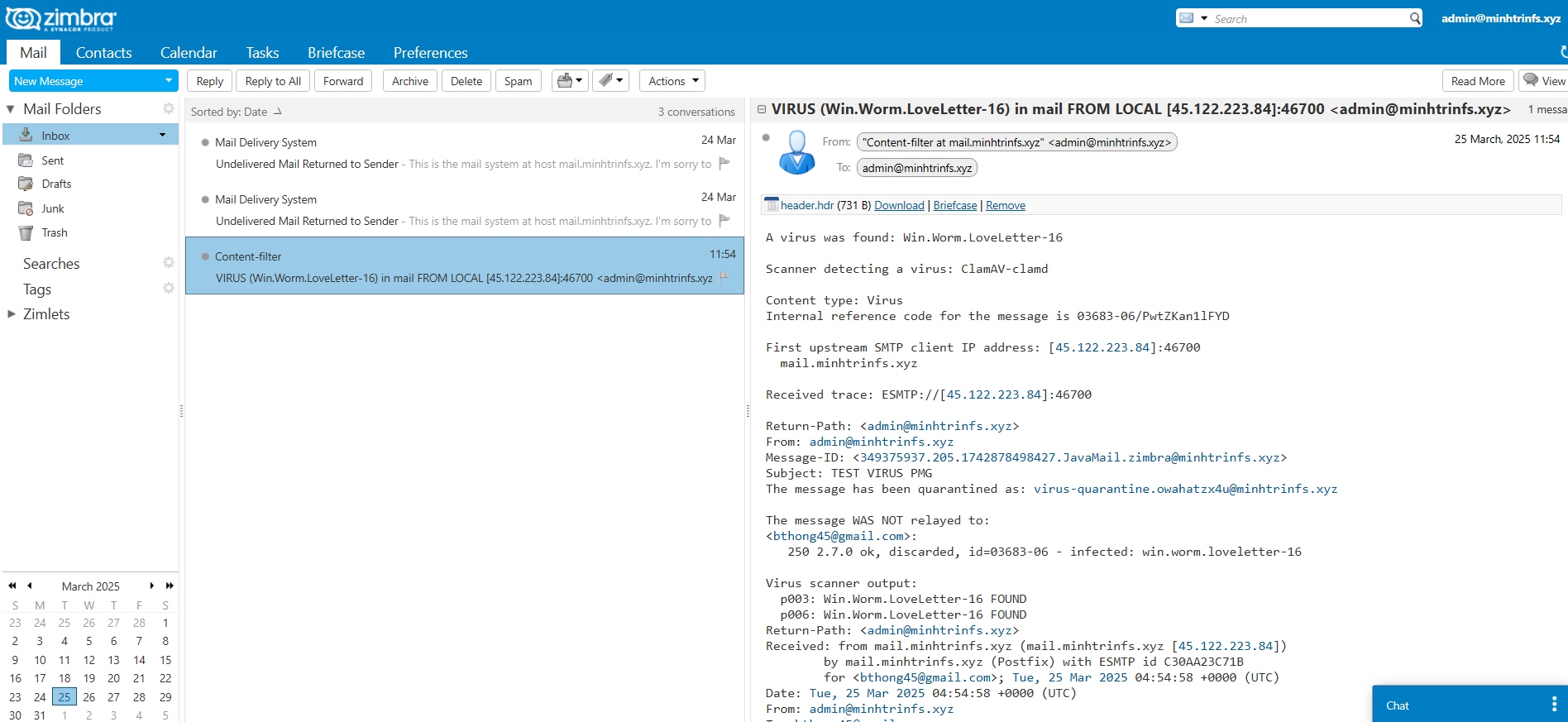




Test gửi virus xem PMG có chặn không? (Gửi thử worm I-LOVE-YOU huyền thoại năm 2000)

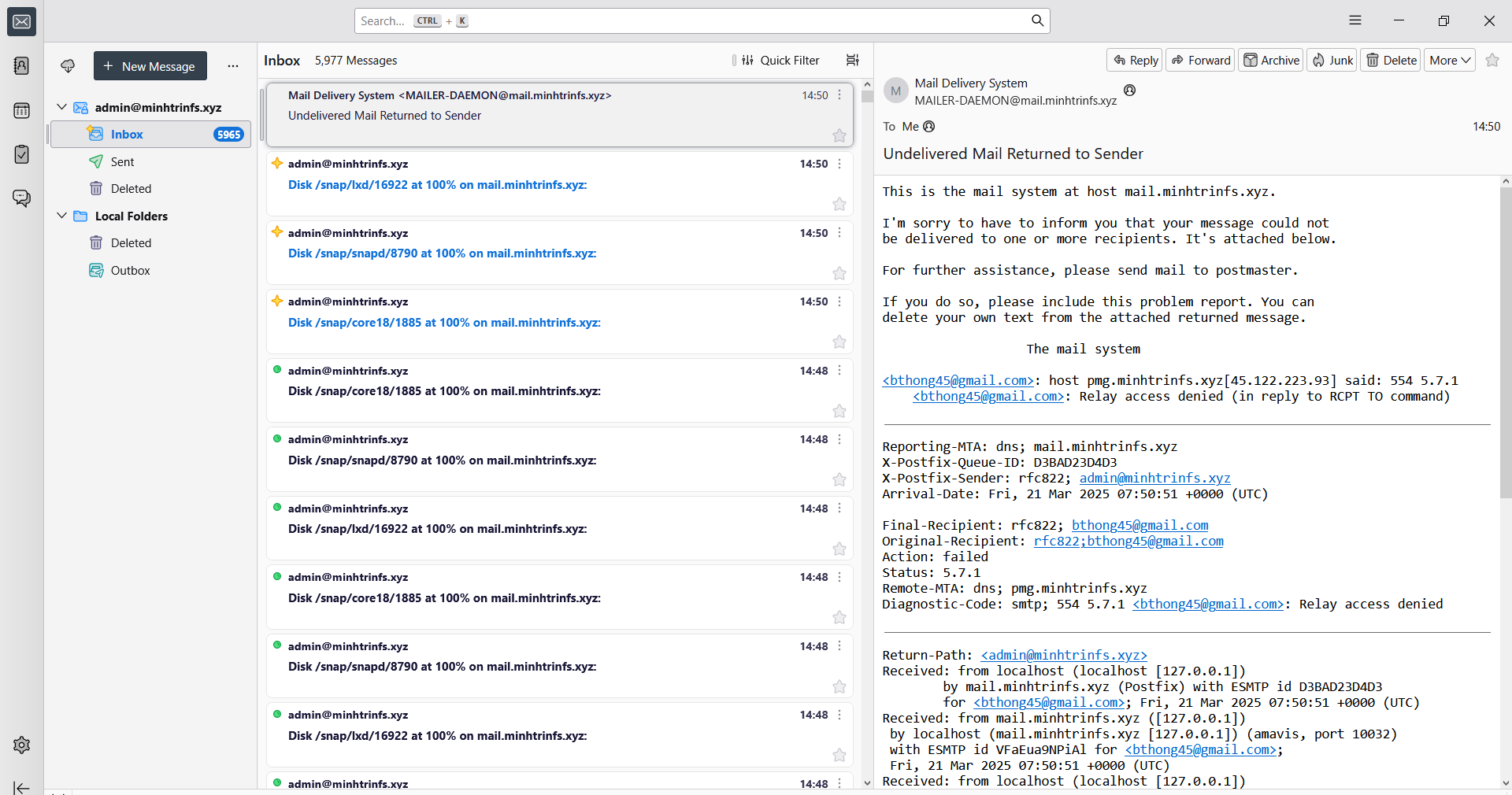


Đã chặn thành công virus.



**TROUBLESHOOTING:**

*Lúc làm có bị lỗi "554 5.7.1 Relay access denied" xuất hiện khi máy chủ Proxmox Mail Gateway (PMG) chặn việc gửi thư vì nó không nhận diện được mail.minhtrinfs.xyz là một máy chủ hợp lệ để gửi mail qua PMG:*



Nguyên nhân có thể xảy ra:

* PMG chưa được cấu hình để chấp nhận mail từ Zimbra.
* Zimbra chưa được thiết lập để relay mail qua PMG.
* PMG có chính sách chặn relay do xác thực chưa đúng.
* Không có bản ghi SPF/DKIM/DMARC hợp lệ cho miền minhtrinfs.xyz

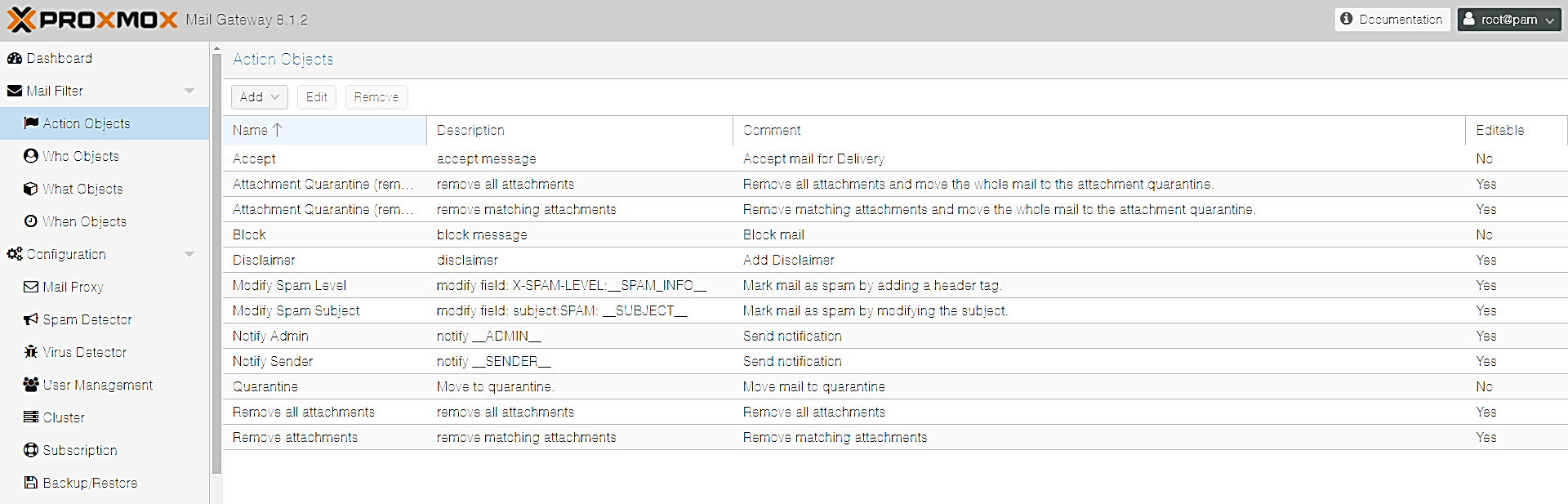
## **Tìm hiểu về các chức năng có trên PMG**

**CÁC MỤC CHÍNH TRONG MAIL FILTER:**

A. Action Objects:

Là các hành động áp dụng lên email khi khớp với điều kiện của bộ lọc. Một số hành động phổ biến:

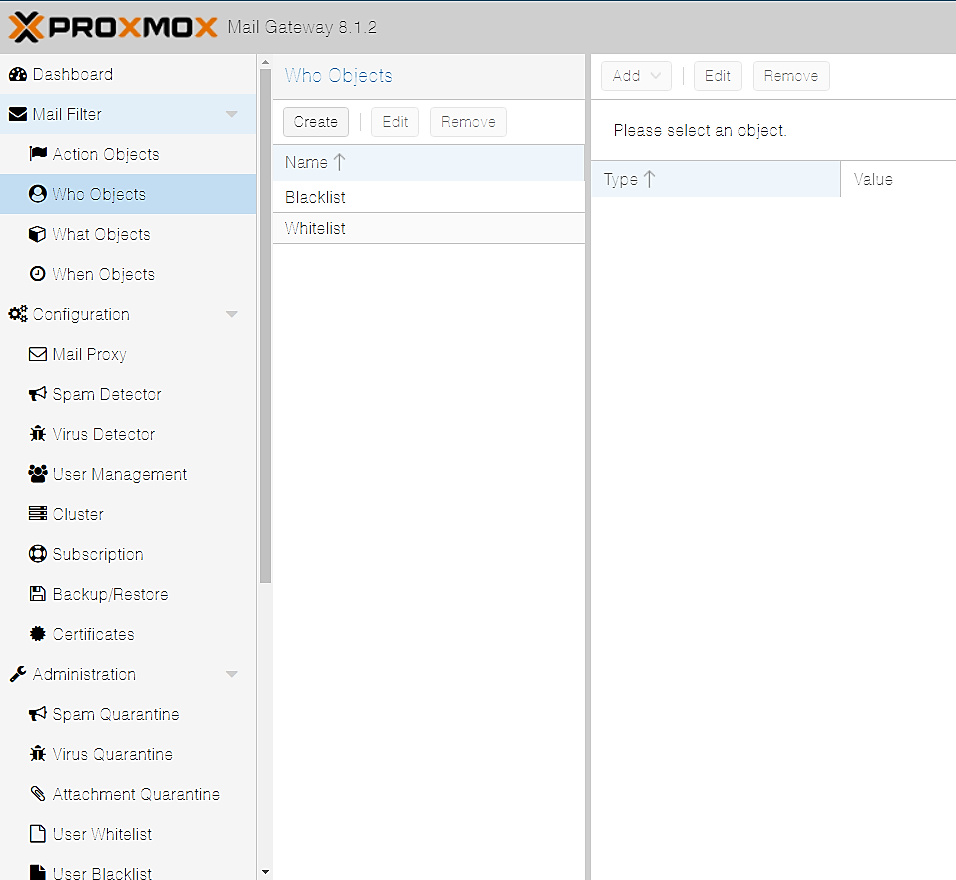
* Accept: Chấp nhận email mà không thay đổi gì.
* Quarantine: Cách ly email vào vùng kiểm dịch.
* Discard: Xóa email mà không gửi thông báo.
* Modify Subject: Thay đổi tiêu đề email (ví dụ: thêm "[SPAM]" vào tiêu đề).
* Notify: Gửi thông báo cho admin hoặc người nhận



B. Who Objects:

Xác định người gửi hoặc người nhận mà quy tắc sẽ áp dụng:

* Blacklist: Danh sách các địa chỉ email hoặc domain bị chặn.
* Whitelist: Danh sách các địa chỉ email hoặc domain được phép gửi.



C. What Objects

Xác định nội dung email cần lọc, có thể bao gồm:

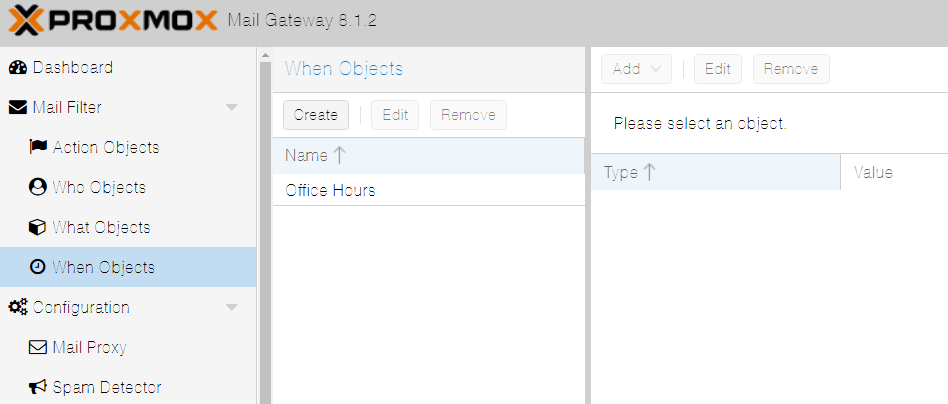
* Kích thước email
* File đính kèm
* Nội dung chứa từ khóa (ví dụ: quảng cáo, nội dung nhạy cảm)



D. When Objects

Xác định thời điểm áp dụng quy tắc lọc email, có thể dựa vào:

* Ngày trong tuần
* Giờ cụ thể



Vọc Mail Filter trong Proxmox Mail Gateway

**Bước 1: Tạo một quy tắc lọc email mới**

* Truy cập Mail Filter → Chọn Create để tạo quy tắc mới.
* Đặt tên quy tắc (ví dụ: "Block Spam Emails").
* Chọn điều kiện lọc email bằng cách thêm Who Objects, What Objects.
* Chọn hành động cần thực hiện trong Action Objects (ví dụ: "Quarantine" hoặc "Discard").
* Lưu lại và kích hoạt quy tắc.

**Bước 2: Thêm một địa chỉ email vào danh sách Blacklist**

* Vào Mail Filter → Who Objects.
* Chọn Blacklist → Add.
* Nhập địa chỉ email hoặc domain cần chặn (ví dụ: spam@example.com hoặc @spammer.com).
* Lưu lại.

**Bước 3: Định cấu hình kiểm dịch thư rác (Spam Quarantine)**

* Vào Administration → Spam Quarantine.
* Kiểm tra danh sách email bị cách ly.
* Nếu có email hợp lệ bị lọc nhầm, bạn có thể chọn "Deliver" để gửi nó đến người nhận.

**PHẦN CONFIGURATION TRONG PROXMOX MAIL GATEWAY**

Phần **Configuration** trong PMG cho phép bạn thiết lập cài đặt tổng thể của hệ thống, bao gồm Mail Proxy, Spam Detector, Virus Detector và các thông số quản lý khác.

**A. Mail Proxy**

Đây là thành phần cốt lõi của PMG, hoạt động như một **SMTP Proxy** để lọc email trước khi gửi đến mail server nội bộ.

**Các thiết lập quan trọng:**

* **Relay Domains**: Xác định domain email mà PMG sẽ xử lý (ví dụ: minhtrinfs.xyz).
* **Transports**: Cấu hình đường đi của email đến mail server đích.
* **Default Relay**: Cấu hình máy chủ SMTP mà PMG sẽ sử dụng để gửi thư ra ngoài.
* **TLS Policy**: Bật/Tắt mã hóa TLS khi giao tiếp SMTP.

**Cách kiểm tra Mail Proxy hoạt động**

1. Vào **Configuration** → **Mail Proxy**.
2. Xem **Mail Log** để kiểm tra email đi/đến.
3. Dùng lệnh telnet kiểm tra SMTP Proxy:

**telnet mail.minhtrinfs.xyz 25**

1. Kiểm tra relay bằng cách gửi email từ một domain bên ngoài.

**B. Spam Detector**

Spam Detector trong PMG sử dụng **SpamAssassin** để quét email rác dựa trên điểm số spam.

**Các tùy chọn chính:**

* **Spam Score Levels**: Thiết lập ngưỡng spam:
  + Kill Level: Email bị xóa ngay.
  + Quarantine Level: Email bị cách ly.
  + Tag Level: Email được đánh dấu [SPAM] nhưng vẫn chuyển đến hộp thư.
* **Use Bayesian Filter**: Học thói quen spam từ dữ liệu.
* **Enable SPF Checking**: Kiểm tra SPF record để phát hiện email giả mạo.
* **Custom Rules**: Thêm bộ lọc spam tùy chỉnh.

**Cách vọc Spam Detector:**

1. Vào **Configuration** → **Spam Detector**.
2. Tăng giảm Spam Score Levels để thử nghiệm.
3. Bật SPF, DKIM, DMARC check để chặn email giả mạo.
4. Kiểm tra spam log bằng lệnh:

**journalctl -u pmg-smtp-filter --no-pager**

**C. Virus Detector**

Virus Detector trong PMG sử dụng **ClamAV** để quét virus trong email.

**Các tính năng chính:**

* **Enable ClamAV**: Bật/Tắt công cụ quét virus.
* **Archive Scan**: Quét cả file nén (.zip, .rar).
* **Block Encrypted Archives**: Chặn file nén có mật khẩu.
* **Update ClamAV Definitions**: Cập nhật cơ sở dữ liệu virus.

**Cách kiểm tra Virus Detector:**

1. Vào **Configuration** → **Virus Detector**.
2. Kiểm tra cập nhật ClamAV:

**freshclam**

1. Test bằng cách gửi email chứa file **EICAR test virus**.